Advanced Cryptography – Master SCCI

Vanessa Vitse

2015-2016

Contents

Part I

H-ECC

Motivations

The goal of these lectures is to give an overview of the properties of (hyper-)elliptic or more generally algebraic curves, that are useful for cryptographic applications. In particular, we will try to answer the following questions:

1. Why are finite fields no longer considered secure for discrete-log based cryptosystems? What is all this hype about index calculus methods?
2. In SAC lectures, a "magical" geometric addition of points on elliptic curves has been described. What are the reasons behind the existence of this group law? Is it possible to define similar laws on more general algebraic curves? One of our goal will be to explain Hyperelliptic Curves Cryptography (HECC) and to understand its pros and cons.
3. Very interesting features on ECC are given by the existence of pairings. How are they defined and computed? on which curves? what are the security implications?
4. Elliptic curves in cryptography must have near prime cardinalities. How can we find such curves? more generally, how can we determine the structure and the cardinality of the group of points?

In a second part, we will talk about polynomial systems and multivariate cryptography, which is one of the few areas that are not threatened by quantum computers. This will be presented as a motivation for the study of Gröbner bases computations, which are the main tool to deal with systems of polynomial equations.

1 The discrete logarithm problem

Let us recall the definition of the general *discrete logarithm problem* (DLP) on a group G:

Problem. *Let G be a group and $g \in G$ be an element of finite order n. The discrete logarithm of $h \in \langle g \rangle$ is the integer $x \in \mathbb{Z}/n\mathbb{Z}$ such that $h = g^x$.*
Given g and $h \in \langle g \rangle$, the discrete logarithm problem consists in computing the discrete logarithm of h in base g.

1.1 Reminders about generic attacks

Definition 1.1. *An algorithm is* generic *when the only authorized operations are*

- *addition of two elements,*
- *opposite of an element,*
- *equality test of two elements.*

In particular, generic attacks can be applied indifferently to any group, which is represented as a black box.

Example. *Brute force search: $\forall x \in \{0; \cdots : n-1\}$, test if $g^x = h$. This algorithm has an exponential complexity in the size of the group.*

1.2 Pohlig-Hellman reduction

Let $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ be the prime factorization of the cardinality $\#G$ of the cyclic group G. Thanks to the Chinese Remainder Theorem (CRT), G can be written as

$$G \simeq \prod_{i=1}^{N} G_i, \text{ where } G_i \simeq \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$

The basic outline of Pohlig-Hellman is:

1. Work with the subgroup G_i to find the discrete logarithms modulo $p_i^{\alpha_i}$ and use CRT to deduce the DL in G.
2. Further simplification: to obtain DL modulo $p_i^{\alpha_i}$, compute iteratively its expression in base p_i by solving α_i DLPs in the subgroup of order p_i of G_i.

We illustrate this algorithm on the following example:

Let $E : y^2 = x^3 + 77x + 28$ be an elliptic curve defined over $\mathbb{F}_{157}$. We want to solve the DLP of the point $Q = (2, 70)$ in base $P = (9; 115)$ which has order $162 = 2 \cdot 3^4$.

1. Solving DLP mod2: we want to find x such that $[x]([3^4]P) = [3^4]Q$; as $[3^4]P = [3^4]Q = (24, 0)$, we deduce that $x = 1 \bmod 2$.
2. Solving DLP mod3^4: we want to find x such that $[x]([2]P) = [2]Q$, i.e. $[x](135, 51) = (12, 47)$. We compute iteratively $x_0, \ldots, x_3$ such that $x = x_0 + x_1 3 + \cdots + x_3 3^3$. We first compute x_0 by multiplying both points by 3^3: $[x_0][3^3](135, 51) = [3^3](12, 47) \Rightarrow [x_0](57, 41) = (57, 41) \Rightarrow x_0 = 1$. Then x_1 satisfies $[1+x_1 2+x_2 3^2+x_3 3^3](135, 51) = (12, 47)$, so $[3x_1][3^2](135, 51) = [3^2]((12, 47) - (135, 51)) \Rightarrow [x_1](57, 41) = \mathcal{O} \Rightarrow x_1 = 0$. After similar iterative computations, we get $x_2 = 2$ and $x_3 = 2$, so that $x = 73 \bmod 3^4$ and $x = 73 \bmod 162$.

As illustrated on this example, we see that solving DLP in a group of size n is approximately as hard as solving DLP in a group of size the largest prime factor of n.

1.3 Baby-step Giant-step

The basic idea behind BSGS is to use birthday paradox and space time trade-off to speed up exhaustive search.

Let $d = \lfloor \sqrt{\#G} \rfloor$. The outline of the algorithm is composed of three steps:

1. Store the list $L = \{(g^j, j) : 0 \leq j \leq d\}$;
2. for $0 \leq k \leq \#G/d$, compute $h(g^{-d})^k$ and check if it appears in L;
3. search for a collision $h(g^{-d})^k = g^j$ and deduce that the DL of h is $j + dk$.

The complexity of this algorithm is clearly in $O(\sqrt{\#G})$ in memory and time (considering that the cost of membership test is in $O(1)$ using an hash table).

1.4 Pollard-Rho

This generic algorithm is an improvement of BSGS based on an iteration of pseudo-random functions, that has the same time complexity but a memory cost in $O(1)$. You can find more detail for example in the Handbook of Elliptic and Hyperelliptic Curves.

Theorem 1.2 (Shoup)**.** *The complexity of generic attacks on the DLP defined over G is in $\Omega(\sqrt{p})$, where p is the largest prime factor of $\#G$.*

In particular, to improve the complexity, one has to use additional information on the given group.

1.5 Index Calculus methods

1.5.1 Outline

These methods were originally developed for factorization of large integers and essentially based on Fermat's method about square congruences. The most popular algorithms among these index calculus methods are the *Number Field Sieve* and *Function Field Sieve* that gives the last records for integer factorization and finite field DLP.

The basic idea of these algorithms is to first find group relations between "small enough" number of generators (also called *factor base elements*), and then, once sufficiently many relations are collected, to deduce with sparse linear algebra techniques the group structure and DL of the factor base elements.

Wlog, we now describe the basic outline of index calculus on a cyclic group $G = \langle g \rangle$ of prime order r when searching for the DL of $h \in G$:

1. Choice of the factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$:
2. Relation search: decompose $[a_i]g + [b_i]h$ in $\mathcal{F}$ for many couples (a_i, b_i):
$$[a_i]g + [b_i]h = \sum_{j=1}^{\#\mathcal{F}} c_{ij} g_j.$$
3. Linear algebra: once $k \geq N$ independent relations are found, construct the matrices $M = (c_{ij})$ and $A = \begin{pmatrix} a_i & b_i \end{pmatrix}$. Then compute $v = \begin{pmatrix} v_1 & \ldots & v_k \end{pmatrix}$ such that $vA \neq \begin{pmatrix} 0 & 0 \end{pmatrix} \bmod r$ and $v \in \ker({}^tM)$.

Basically, in the linear algebra phase, we are trying to find a linear combination of the relations such that the right-hand side vanishes. Indeed, we can write the relations matricially as

$$A \begin{pmatrix} g \\ h \end{pmatrix} = M \begin{pmatrix} g_1 \\ \vdots \\ g_N \end{pmatrix}$$

Multiplying on the left by v, which amounts to taking the linear combination of the relations with coefficients given by v, we obtain

$$vA \begin{pmatrix} g \\ h \end{pmatrix} = [\sum_i a_i v_i]g + [\sum_i b_i v_i]h = vM \begin{pmatrix} g_1 \\ \vdots \\ g_N \end{pmatrix} = 0.$$

Another possible outline is the following.

1. Choice of the factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$:
2. Relation search: decompose $[a_i]g$ in $\mathcal{F}$ for many a_i:
$$[a_i]g = \sum_{j=1}^{\#\mathcal{F}} c_{ij} g_j.$$
3. Linear algebra: once $k \geq N$ independent relations are found, construct the matrix $M = (c_{ij})$ and the vector $A = \big(a_i\big)$. Then find $X = (x_j)$ solution of the equation $MX = A \bmod r$; it should be unique and contain the discrete logarithms in base g of the factor base elements.
4. Descent phase: find a relation involving h,
$$[a]g + [b]h = \sum_{j=1}^{N} c_j g_j, \text{ where } b \wedge r = 1$$
and deduce the solution of the DLP $\left(\sum_{j=1}^{N} c_j x_j - a\right) b^{-1} \bmod r$.

A last possibility is to consider "pure" relations, i.e. as in step 2 above but with $a_i = 0$ for all i. Once enough relations are collected, the set of solutions of $MX = 0$, i.e. the kernel of X, should form a 1-dimensional vector space containing the discrete log of the factor base elements up to multiplication by a constant (since the relations do not involve the base point g). Then the descent phase requires to obtain two independent relations involving g and h.

Some general remarks:

1. The relation search is of course the less obvious step, and is very specific to the group considered. It is the main obstacle to the existence of efficient index calculus algorithms in some groups, and in particular for elliptic curves.

2. On the other hand, the linear algebra step is almost the same for all groups.

3. There is a balance to find between the two phases:

   - if $\#\mathcal{F}$ is small, few relations are needed and the linear algebra is fast, but it is harder to find decompositions.

   - if $\#\mathcal{F}$ is large, it is easy to find relations but many of them are needed and it slows down the linear algebra.

1.5.2 Examples

Prime field case

We will follow the second outline. To compute discrete logarithms in the multiplicative group of a prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we use the fact that elements of $\mathbb{F}_p$ can be represented as integers, which in turn can be decomposed as products of prime numbers. More precisely, we make the following adaptations (g is the logarithm base and h is the challenge; here of course everything is written multiplicatively)

- The factor base is composed of (equivalence classes of) prime integers smaller than a smoothness bound B (usually together with -1)

- Relation search: the element $g^{a_i} \in \mathbb{F}_p^*$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth, i.e. if all its prime factors are smaller than B. The relation is then simply

$$g^{a_i} = \pm \prod_j p_j^{c_{ij}}.$$

Example: Let $p = 107$ and $g = 31 \in \mathbb{Z}/107\mathbb{Z}^*$ (it has order 106); we want to find the DL of $h = 19$.

We choose the smoothness bound $B = 7$, so that $\mathcal{F} = \{-1; 2; 3; 5; 7\}$.

$$\begin{aligned}
&g^1 = 31, \text{ not smooth} \\
&g^2 = -2 = -1 \times 2 \\
&g^3 = 45 = 3^2 \times 5 \\
&g^4 = 4 = 2^2 \\
&g^5 = 17, \text{ not smooth} \\
&\vdots \\
&g^{13} = -49 = -1 \times 7^2 \\
&g^{14} = -21 = -1 \times 3 \times 7 \\
&g^{15} = -9 = -1 \times 3^2 \\
&g^{16} = 42 = 2 \times 3 \times 7 \\
&g^{21} = -35 = -1 \times 5 \times 7
\end{aligned}$$

We stop the relation search here, having collected 8 relations, which is probably more than needed. In the linear algebra step, we get to solve the equation

$$\begin{pmatrix} 2 \\ 3 \\ 4 \\ 13 \\ 14 \\ 15 \\ 16 \\ 21 \end{pmatrix} = \begin{array}{c} \begin{array}{ccccc} -1 & 2 & 3 & 5 & 7 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array} X \mod 106 \quad \Rightarrow \quad X = \begin{pmatrix} 53 \\ 55 \\ 34 \\ 41 \\ 33 \end{pmatrix}$$

This means that $\log(-1) = 53$ (this can have been deduced before!), $\log(2) = 55$, $\log(3) = 34$, $\log(5) = 41$ and $\log(7) = 33$. For the descent phase, we try and factorize gh:

$$gh = 54 = 2 \times 3^3 = (g^{55})(g^{34})^3 = g^{51} \Rightarrow h = g^{50}$$

Small characteristic case

A similar approach can be used for the resolution of the DLP in $\mathbb{F}_{p^n}^*$ when p is small (e.g. $p = 2$). This time we use the construction of $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(f(X))$ where f is a degree n irreducible polynomial. In particular the elements of $\mathbb{F}_{p^n}$ are represented as polynomials in $\mathbb{F}_p[X]$, of degree smaller than n. To obtain relations, we rely on the decomposition of polynomials as product of irreducible factors; there exist efficient algorithms to compute such factorizations in $\mathbb{F}_p[X]$.

- The factor base is composed of (equivalence classes of) irreducible polynomials in $\mathbb{F}_p[X]$ of degree smaller than a smoothness bound B.

- Relation search: the element $g^{a_i} \in \mathbb{F}_{p^n}^*$ yields a relation if its representative in $\mathbb{F}_p[X]$ is B-smooth, i.e. if all its irreducible factors have degree smaller than B.

1.5.3 Complexity analysis

The main parameter in the presented approaches is this smoothness bound B. To understand the choice of this parameter, we need estimates on the probability that a random element is B-smooth. Such probabilities involve the complexity function L, defined as

$$L_n(\alpha, c) = \exp\left(c(\log n)^{\alpha}(\log\log n)^{1-\alpha}\right).$$

In this notation, α and c are seen as parameters, and the variable is n. It yields a family of functions, interpolating between polynomial (for $\alpha = 0$) and exponential (for $\alpha = 1$) complexity in $\log n$.

Property 1.3.

- $L(\alpha_2, c_2) = o(L(\alpha_1, c_1))$ *if* $\alpha_2 < \alpha_1$ *or* $\alpha_2 = \alpha_1$ *and* $c_2 < c_1$
- $L(\alpha_1, c_1)L(\alpha_2, c_2) = L(\alpha_1, c_1 + o(1))$ *if* $\alpha_1 > \alpha_2$
- $L(\alpha, c_1)L(\alpha, c_2) = L(\alpha, c_1 + c_2)$

We see that the first parameter is the more important for the asymptotic behaviour. For this reason, we often write $L_n(\alpha)$ as a shorthand for $L_n(\alpha, c + o(1))$ for some constant c. Actually, to avoid using Landau notations we even use $L_n(\alpha, c)$ as a shorthand for $L_n(\alpha, c + o(1))$ (this abuse of notation can be a bit weird, as in $C.L_n(\alpha, c) = L_n(\alpha, c)$).

Theorem 1.4 (Canfield-Erdös-Pomerance)**.** *A (uniformly) random integer smaller than x is $L_x(\alpha, c)$-smooth with probability*

$$1/L_x(1-\alpha, (1-\alpha)/c) \text{ as } x \to \infty.$$

We can use this result to derive the asymptotically optimal value of B in the prime field case example. Let $B = L_p(\alpha, c)$. The powers of g are uniformly distributed in $\mathbb{Z}/p\mathbb{Z}$, so according to the above theorem we need on average $L_p(1-\alpha, (1-\alpha)/c)$ tries to obtain one relation (we will neglect the time taken by checking if a number is B-smooth). The number of relations needed is about the size of the factor base $\mathcal{F}$; this is equal to $\pi(B)$, the number of prime numbers smaller than B. So

$$\#\mathcal{F} = \pi(B) \sim \frac{B}{\log(B)} = \frac{L_p(\alpha, c)}{c(\log p)^{\alpha}(\log\log p)^{1-\alpha}} = L_p(\alpha, c + o(1)).$$

This means that the relation step complexity is in $L_p(\alpha, c)L_p(1-\alpha, (1-\alpha)/c)$. This is minimized when $\alpha = 1 - \alpha$, i.e. $\alpha = 1/2$, and then when $c + 1/2c$ is minimal, i.e. for $c = 1/\sqrt{2}$. So the best choice is

$$B \simeq L_p(1/2, 1/\sqrt{2})$$

which yields an asymptotic complexity in $L_p(1/2, \sqrt{2})$ for the relation search. We will see later that the linear algebra step has a quadratic complexity, so the overall complexity is in $L_p(1/2, \sqrt{2})$.

We will not give the details here, but very similar results holds in the small characteristic case; the probability of B-smoothness for random polynomials is given by a theorem of Panario, Gourdon and Flajolet. In the end we obtain the same overall complexity in $L_{p^n}(1/2, \sqrt{2})$.

1.5.4 Sparse linear algebra

An important remark is that the matrix obtained at the end of the relation search is usually extremely sparse: most coefficients are equal to zero. In real-world applications, a typical size for the relation matrix M is several millions rows and columns, yet it contains only a few non-zero coefficients per row. Consequently the index calculus algorithms use sparse linear algebra techniques instead of standard resolution tools (recall that we want to solve an equation of the form $MX = A$ or $MX = 0$). The main ideas are to keep the matrix sparse (this forbids Gauss) and to compute only matrix-vector products, whose cost is only proportional to the number of non-zero entries.

The two principal algorithms for this task are Lanczos's and Wiedemann's; we will only present the latter. For simplicity, we assume that all computations are done modulo a prime r (this can always be achieved thanks to Pohlig-Hellman reduction). Assume that the matrix M is square, of dimension $n \times n$; we want to solve the equation $MX = A$ for some right-hand side A, potentially equal to 0. Let v be a vector of size n; the minimal polynomial of M with respect to v is the smallest degree monic polynomial P such that $P(M)v = 0$.

Suppose we want to solve $MX = A$, $A \neq 0$, and we know the minimal polynomial $\sum_{k=0}^{d} p_k X^k$ of M wrt to A. Then $0 = \sum_{k=0}^{d} p_k M^k A = p_0 A + M(\sum_{k=1}^{d} p_k M^{k-1} A)$, so we can take $X = -(p_0)^{-1} \sum_{k=1}^{d} p_k M^{k-1} A$ (unless $p_0 = 0$, in which case the method fails but M is not invertible). Otherwise, if we want to solve $MX = 0$, $X \neq 0$, we can take a random element w and compute the minimal polynomial P of M wrt to $v = Mw$. Since $0 = P(M)v = P(M)Mw = M(P(M)w)$, we see that $P(M)w$ is a solution (unless it is zero, but then we can start over with some other w).

Thus we just have to compute the minimal polynomial of M wrt some vector v. For that we need some background on linearly recurrent sequences.

Definition 1.5. *A sequence $(u_n)_{n\in\mathbb{N}}$ is a linearly recurrent sequence if there exist a non-zero polynomial $P = \sum_{i=0}^{d} a_i X^i$ such that for all $n \in N$,*

$$\sum_{i=0}^{d} a_i u_{n+i} = 0.$$

It is not too difficult to see that for a given linearly recurrent sequence, the set of all possible polynomials P as in the definition is an ideal. (Sketch of proof: this set is clearly stable under addition and scalar multiplication. Also, if P is in this set, then this also true for XP, since this amounts to replacing n by $n+1$ in the above definition. So it is also true for $X^k P$ for any k, and taking the appropriate sum it is true for the product QP with any polynomial Q). In particular, it makes sense to speak of the minimal polynomial of a linearly recurrent sequence.

Proposition 1.6 (Berlekamp-Massey). *Let (u_n) be a linearly recurrent sequence, whose minimal polynomial is of degree smaller than some integer d. There exists an algorithm which takes as inputs the degree bound d and the values $u_0, u_1, \ldots, u_{2d}$ and outputs the minimal polynomial of the sequence; its complexity is in $O(d^2)$ multiplications.*

Berlekamp-Massey algorithm can be used to compute the minimal polynomial P of M wrt v. For that, we choose a random vector u and compute the sequence of dot products $a_i = u.M^i v$. This sequence is clearly linearly recurring, and its minimal polynomial divides P. So applying Berlekamp-Massey to (a_n) yields a factor P_0 of P. If $P_0 = P$, i.e. if $P_0(M)v = 0$, we are done; otherwise the minimal polynomial of M wrt $P_0(M)v$ is P/P_0, so we can start again with another u and with v replaced by $P_0(M)v$. Repeating this, we obtain finally various factors of P whose product is P.

In the above algorithm, we only compute $O(n)$ dot products and $O(n)$ matrix-vector multiplications and run Berlekamp-Massey a few times (with decreasing degree bound d). Each dot product costs $O(n)$ multiplications, the total cost of the Berlekamp-Massey calls is in $O(n^2)$, and each matrix-vector multiplication is in $O(nc)$ where n is the number of non-zero entries per row. The overall complexity of the linear algebra step with Wiedemann is thus $O(n^2c)$ arithmetic operations, to compare with the $O(n^3)$ complexity of Gauss's algorithm.

Remark: for actual computations, parallelization is very important. The relation search is always straightforward to distribute, but this is not so true for the linear algebra. In particular, Wiedemann algorithm must be adapted in order to be distributed (this is Coppersmith's block Wiedemann algorithm) but this parallelization still requires a lot of bandwidth. For this reason, it is often advantageous to compute many more relations than needed and use extra information to simplify the relation matrix.

1.5.5 State of the art

There have been many works aiming at improving this index calculus method for finite fields, and in particular for prime fields (this is because index calculus is also one of the main methods of factoring large integers). For several years, the best algorithms for computing discrete logarithms in $\mathbb{F}_{p^n}^*$ were the Number Field Sieve (NFS) for large p and small n and the Function Field Sieve (FFS) for small p and large n. Both have a sub-exponential complexity in $L_{p^n}(1/3)$. Instead of trying to factor random elements of $\mathbb{F}_{p^n}$, as in the examples above, these algorithms manage to deal only with elements of small "norm". This greatly improves the smoothness probability, but introduces a tricky "descent step" to recover the actual discrete logarithms.

However, the landscape in the small characteristic case has evolved extremely quickly since 2013. A. Joux, followed by other researchers, showed that it was possible to generate many independent relations from a single one, thus speeding up dramatically the index calculus. Under some heuristics assumptions, when p is smaller than n the most recent algorithm achieves a quasi-polynomial complexity, in $N^{O(\log N)}$ where $N = \log(p^n)$ (this is asymptotically faster than $L_{p^n}(\epsilon)$ for any $\epsilon > 0$). This means that small characteristic fields, and in particular binary fields, are no longer considered as potential settings for the DLP.

When p is greater than n but still small compared to p^n, the new algorithms still beat FFS. Expressing the actual asymptotic complexity requires some care: of course, we consider what happens when the cardinality p^n grows to infinity, but it is important to keep track of the growth rate of p. The main result is that if $p^n \to \infty$ and $p = L_{p^n}(\alpha)$, then the latest algorithm has a complexity in $L_{p^n}(\alpha + o(1))$; this is better that $L(1/3)$ as soon as $\alpha < 1/3$.

In the medium and large characteristic cases (more precisely, when $L_{p^n}(1/3) \leq p \leq L_{p^n}(2/3)$ and when $p \geq L_{p^n}(2/3)$), variants of NFS are still the fastest algorithms. It will be interesting to see if in these two cases, the $L(1/3)$ complexity barrier can be broken in the near future, and if it happens, what are the consequences for integer factorization.

2 Algebraic curves

2.1 Basic algebraic geometry

Algebraic geometry (at its basic level) studies the properties of sets defined by polynomial equations.

Unless otherwise mentionned, all fields considered are either characteristic zero fields, finite fields or algebraic closed fields. If K is a field, we denote $\bar{K}$ its algebraic closure.

We will use without proof the following fact:

Theorem 2.1. *$K[X_1,\dots,X_n]$ is noetherian, i.e. its ideals are finitely generated: for all ideal $\mathcal{I} \subset K[X_1,\dots,X_n]$ there exist $f_1,\dots,f_s \in K[X_1,\dots,X_n]$ such that $\mathcal{I} = (f_1,\dots,f_s)$.*

2.1.1 Algebraic sets

Definition 2.2. *A subset $V \subset K^n$ is an* affine algebraic set *if there exists an ideal $\mathcal{I} \subset K[X_1,\dots,X_n]$ such that*

$$V = \{P = (x_1,\dots,x_n) \in K^n : \forall f \in \mathcal{I},\ f(x_1,\dots,x_n) = 0\}.$$

This is denoted by $V = \mathbb{V}(\mathcal{I})$. If $f_1,\dots,f_s \in K[X_1,\dots,X_n]$ are a set of generators of $\mathcal{I}$, i.e. $\mathcal{I} = (f_1,\dots,f_s)$, then V is the set of solutions of the polynomial system

$$\begin{cases} f_1(x_1,\dots,x_n) = 0 \\ \quad\vdots \\ f_s(x_1,\dots,x_n) = 0 \end{cases}$$

Examples.

- *The unit circle in $\mathbb{R}^2$ is an algebraic set; it is $\mathbb{V}(X^2+Y^2-1)$.*
- *The algebraic set $\mathbb{V}(XZ,YZ) \subset K^3$ is the union of the plane $Z=0$ with the line of equation $\begin{cases} X=0 \\ Y=0 \end{cases}$.*

Note that in general different ideals can define the same algebraic set, e.g. $\mathbb{V}(X) = \mathbb{V}(X^2)$, or in $\mathbb{R}^2$, $\mathbb{V}(1) = \mathbb{V}(X^2+Y^2+1) = \emptyset$. But there is always a largest ideal defining a given algebraic set:

Proposition 2.3. *Let V be an affine algebraic set. The set*

$$\mathbb{I}(V) = \{f \in K[X_1,\dots,X_n] : \forall P = (x_1,\dots,x_n) \in V,\ f(x_1,\dots,x_n) = 0\}$$

is an ideal of $K[X_1,\dots,X_n]$, and $\mathbb{V}(\mathbb{I}(V)) = V$.

Definition 2.4. *An (affine) algebraic set V is* irreducible *if it is not a non-trivial union of two algebraic sets, i.e. for all algebraic sets V_1 and V_2 such that $V = V_1 \cup V_2$, either $V_1 = V$ or $V_2 = V$. An affine* variety *is an irreducible affine algebraic set.*

Examples.

- *The algebraic set $\mathbb{V}(XZ,YZ) \in K^3$ of the previous examples is clearly not irreducible.*
- *A point $(x_1,\dots,x_n)$ is an algebraic set (it is $\mathbb{V}(X_1-x_1,\dots,X_n-x_n)$) and is clearly irreducible.*

Proposition 2.5. *An affine algebraic set V is irreducible if and only if $\mathbb{I}(V)$ is a prime ideal.*

Proof. $\Rightarrow$: we suppose that V is irreducible. Let f, g be two polynomials such that $fg \in \mathbb{I}(V)$. This means that for all $x \in V$ we have $f(x)g(x) = 0$, i.e. $f(x) = 0$ or $g(x) = 0$. So $V \subset \mathbb{V}(f) \cup \mathbb{V}(g)$, and in particular $V = (V \cap \mathbb{V}(f)) \cup (V \cap \mathbb{V}(g))$. But $V \cap \mathbb{V}(f)$ is an algebraic set (it is $\mathbb{V}(\mathbb{I}(V), f)$), and similarly for $V \cap \mathbb{V}(g)$. Since V is irreducible, one of them is equal to V, say $V = V \cap \mathbb{V}(f)$. This implies $V \subset \mathbb{V}(f)$, which means that f vanishes on V, i.e. $f \in \mathbb{I}(V)$.

$\Leftarrow$: suppose that V is not irreducible, say $V = V_1 \cup V_2$ with $V_1 \subsetneq V$, $V_2 \subsetneq V$. Since $V_1 \subsetneq V$, we have $\mathbb{I}(V) \subset \mathbb{I}(V_1)$, and the two ideals are distinct (since otherwise we would have $V = V_1$). So there exists an element $f \in \mathbb{I}(V_1) \setminus \mathbb{I}(V)$. Similarly, there exists $g \in \mathbb{I}(V_2) \setminus \mathbb{I}(V)$. Now for any $x \in V$, we have $f(x) = 0$ (if x is in V_1) or $g(x) = 0$ (if x is in V_2), so $fg(x) = 0$. This means $fg \in \mathbb{I}(V)$, and since neither f nor g is in $\mathbb{I}(V)$, this shows that this ideal is not prime. □

Definition 2.6. *Let V be an affine algebraic set. Its* coordinate ring *is the quotient ring*

$$K[V] = K[X_1, \dots, X_n]/\mathbb{I}(V).$$

If V is a variety, then $K[V]$ is a domain and its fraction ring $K(V) = Frac(K[V])$ is called the function field *of V.*

Remark. *The idea behind this definition is that we want to identify two polynomials if they are equal on V, i.e. if they differ by an element of $\mathbb{I}(V)$. So the coordinate ring is in some sense the ring of polynomial functions on V.*

In the followings, V is an affine variety.

Definition 2.7. *Let $f \in K[V]$ and $P \in V$, and $F \in K[X_1, \dots, X_n]$ an element in the class of f. The* value *of f at P is $f(P) = F(P)$; this is well-defined.*

Let $\phi \in K(V)$ and $P \in V$.

- *If there exist $f, g \in K[V]$ such that $\phi = f/g$ and $g(P) \neq 0$, then ϕ is* regular *at P and its value is $\phi(P) = f(P)/g(P)$.*
- *If there exist $f, g \in K[V]$ such that $\phi = f/g$ and $f(P) \neq 0, g(P) = 0$ then ϕ has a* pole *at P.*
- *If for all $f, g \in K[V]$ such that $\phi = f/g$, one has $f(P) = g(P) = 0$ then ϕ is* undetermined *at P.*

Definition 2.8. *Let P be a point of V. The* local ring *at the point P is the subring of the function field of V defined by*

$$K[V]_P = \{f \in K(V) : \exists g, h \in K[V], f = g/h, h(P) \neq 0\}.$$

In particular, a function $f \in K(V)$ is regular at a point P if $f \in K[V]_P$, and in this case the evaluation of f at P is well-defined.

Definition 2.9. *The dimension of an affine variety is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$, i.e. the largest cardinality of an algebraically independent subset of $\bar{K}(V)$ over $\bar{K}$.*

Examples.

- $\dim \bar{K}^n = n$

- *If $f \in K[X_1, \dots, X_n] \setminus K$, $\dim(V(f)) = n - 1$.*

Definition 2.10. - *V is* non-singular *at $P \in V$ if the Jacobian $\big(\partial f_i/\partial X_j(P)\big)_{1 \le i \le s, 1 \le j \le n}$ has rank $n - \dim(V)$ where $I(V) = \{f_1, \dots, f_s\}$.*

- *V is* smooth *if it is non singular at every point.*

Example. *Let $f \in K[X_1, \dots, X_n] \setminus K$, then $\mathbb{V}(f)$ is singular at P iff*

$$\partial f/\partial X_1(P) = \cdots = \partial f/\partial X_n(P) = 0.$$

In particular, the curve $\mathbb{V}(Y^2 - X^3 - X)$ is smooth at $(0,0)$, but $\mathbb{V}(Y^2 - X^3 - X^2)$ is not.

Definition 2.11. *An ideal $\mathcal{I} \subset \bar{K}[X_1, \dots, X_n]$ is* defined over *K if there exist $f_1, \dots, f_s \in K[X_1, \dots, X_n]$ such that $\mathcal{I} = (f_1, \dots, f_s)$. If $\mathcal{I}$ is defined over K, we set $\mathcal{I}_K = \mathcal{I} \cap K[X_1, \dots, X_n]$; it is an ideal of $K[X_1, \dots, X_n]$, generated by $f_1, \dots, f_s$.*
An affine algebraic set $V \subset \bar{K}^n$ is defined over *K if $\mathbb{I}(V)$ is defined over K; this is denoted by $V_{|K}$. In that case, the set $V(K) = V \cap K^n$ is called the set of K-*rational points *of V.*

Remark. - *If $f_1, \dots, f_s \in K[X_1, \dots, X_n]$ generates the ideal $\mathcal{I}$ defined over K, then $V(K)$ is exactly the set of solutions in K^n of the system $f_1(x_1, \dots, x_n) = \cdots = f_s(x_1, \dots, f_s) = 0$.*

- *If V is defined over K then it is also defined over any larger field L with $K \subset L \subset \bar{K}$. In particular it makes sense to speak of the set $V(L)$ of L-rational points of V.*

Example. *Let $n \ge 3$ be an integer and $V = \mathbb{V}(X^n + Y^n - 1) \subset \bar{\mathbb{Q}}^2$. It is an affine algebraic set defined over $\mathbb{Q}$, and Fermat-Wiles theorem states that the only $\mathbb{Q}$-rational points of V are $\{(1,0),(0,1)\}$ or $\{(\pm 1, 0), (0, \pm 1)\}$.*

2.1.2 Projective algebraic set

We first recall briefly the definitions of projective spaces:

Definition 2.12. *The* projective n-space *over a field K is the set of lines through the origin, or one-dimensional linear subspace, of K^{n+1}. In other words,*

$$\mathbb{P}^n(K) = (K^{n+1} - \{0\})/_\sim$$

where $(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n)$ for any $\lambda \in K^*$. The equivalence class of $(x_0, \dots, x_n)$ is denoted by $[x_0 : \cdots : x_n]$; this notation is called homogeneous *or* projective coordinates*.*

Definition 2.13. *For $0 \le i \le n$, the* affine chart *$U_i \subset \mathbb{P}^n(K)$ is the set $\{[x_0 : \cdots : x_n] : x_i \ne 0\}$. The affine chart U_i is in one-to-one correspondence with the affine n-space via the map $[x_0 : \cdots : x_n] \mapsto (x_0/x_i, \dots, x_{i-1}/x_i, x_{i+1}/x_i, \dots, x_n/x_i)$. Then the set $\{[x_0 : \cdots : x_n] : x_i = 0\}$ is isomorphic to $\mathbb{P}^{n-1}(K)$ and is the* hyperplane at infinity *in U_i.*

Remark. *More generally, if H is a projective hyperplane of $\mathbb{P}^n(K)$, then its complement $\mathbb{P}^n(K) \setminus H$ is an affine chart.*

To define projective algebraic sets of $\mathbb{P}^n$ as an analog of affine sets of K^n, we need first to introduce homogeneous ideals.

Definition 2.14. *A polynomial $f \in K[X_0, \ldots, X_n]$ is called* homogeneous *of degree d if for all $\lambda \in K$, $P(\lambda X_0, \ldots, \lambda X_n) = \lambda^d P(X_0, \ldots, X_n)$. Equivalently, all the monomials of P have total degree d.*
An ideal $\mathcal{I} \subset K[X_0, \ldots, X_n]$ is homogeneous *if it is generated by homogeneous polynomials.*

Definition 2.15.

- *Let $f \in K[X_1, \ldots, X_n]$ a polynomial of total degree d. Then*

  $$f^h = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$$

  is a degree d homogeneous polynomial in $K[X_0, \ldots, X_n]$, called the homogenization *of f (with respect to X_0.*

- *Conversely, if $g \in K[X_0, \ldots, X_n]$ is homogeneous, its* deshomogenization *(with respect to X_0) is $g^* = g(1, X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$.*

Homogenization and deshomogenization are partial inverses : for all f, $(f^h)^* = f$, but for all homogeneous g, $(g^*)^h$ is equal to g only up to multiplication by a power of X_0.

Definition 2.16. *Let $f \in K[X_0, \ldots, X_n]$ a homogeneous polynomial and $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$. We say that f vanishes at P if $f(x_0, \ldots, x_n) = 0$; this is denoted by $f(P) = 0$ and is independent of the choice of projective coordinates for P.*
Let $f, g \in K[X_0, \ldots, X_n]$ two homogeneous polynomials of same degree d and $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ such that g does not vanish at P. Then the value of the rational fraction $\frac{f}{g}$ at P is well-defined and is equal to $\frac{f}{g}(P) = f(x_0, \ldots, x_n)/g(x_0, \ldots, x_n)$.

Remark. *In general, it does not make sense to speak of the value of a polynomial (even homogeneous) at a point $P \in \mathbb{P}^n(K)$.*

Definition 2.17. *A subset $V \in \mathbb{P}^n(K)$ is a* projective algebraic set *if there exists a homogeneous ideal $\mathcal{I} \subset K[X_0, \ldots, X_n]$ such that*

$$V = \{P \in \mathbb{P}^n(K) : f(P) = 0 \textit{ for all homogeneous } f \in \mathcal{I}\}.$$

This is denoted by $V = \mathbb{V}(\mathcal{I})$. If $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ are a set of homogeneous generators of $\mathcal{I}$, then V is the set of points P such that $f_1(P) = \cdots = f_s(P) = 0$.
If V is a projective algebraic set, its associated homogeneous ideal is the ideal $\mathbb{I}(V)$ generated by the set $\{f \in K[X_0, \ldots, X_n] : f \text{ homogeneous}, f(P) = 0\ \forall P \in V\}$. If $\mathbb{I}(V)$ is prime then V is called a projective variety.

Remark. *Contrarily to the affine case, $\mathbb{I}(V)$ is generated by (and thus larger than) the set of homogeneous polynomials that vanish on V. Also, there is no notion of coordinate ring for a projective algebraic set.*

Definition 2.18. *Let V be projective variety. The* function field *of V is defined as*

$$K(V) = \{f/g : f, g \in K[X_0, \ldots, X_n] \textit{ are homogeneous of same degree and } g \notin \mathbb{I}(V)\}/\sim$$

where $f/g \sim f'/g'$ if $fg' - f'g \in \mathbb{I}(V)$.

As in the affine case, a function $\phi \in K(V)$ can be defined, have a pole or be undetermined at a point $P \in V$; in the first case its value $\phi(P)$ is well-defined.

Proposition 2.19. *Let K^n be the affine space, that we identify with the affine chart $U_0 \subset \mathbb{P}^n(K)$. Let $V = (f_1, \dots, f_s)$ be an affine algebraic set, where $f_1, \dots, f_s \in K[X_1, \dots, X_n]$. Then $\bar{V} = \mathbb{V}(f_1^h, \dots, f_s^h)$ is the smallest projective algebraic set containing $V \subset U_0 \subset \mathbb{P}^n(K)$, and is called the* projective closure *of V.*
Furthermore, if V is a variety then $\bar{V}$ is also a variety and $K(V) = K(\bar{V})$.

Most properties (smoothness, local ring at P,...) of a projective variety V can be defined in terms of the affine subvariety $V \cap K^n$.

2.2 Curves

Definition 2.20. *A curve is a 1-dimensional variety.*

Example. $y^2 = f(x)$ *defines a plane curve and more precisely:*

- *if* $\deg(f) = 1, 2$*, it is a conic;*
- *if* $\deg(f) = 3, 4$*, it is an elliptic curve;*
- *if* $\deg(f) > 4$*, it is an hyperelliptic.*

Proposition 2.21. *If $\mathcal{C}$ is a curve and $P \in \mathcal{C}$ is a smooth point, then $\bar{K}[\mathcal{C}]_P$ is principal (admitted). Let $t \in \bar{K}[\mathcal{C}]_P$ be a generator of the maximal ideal $m_P = \{f \in \bar{K}[\mathcal{C}]_P : f(P) = 0\}$ of $\bar{K}[\mathcal{C}]_P$. Then t is called a* uniformizer *at the smooth point P.*

Thus, $\bar{K}[\mathcal{C}]_P$ is a *discrete valuation ring*, i.e.

$$\forall f \in \bar{K}[\mathcal{C}]_P, \exists! n \in \mathbb{N}, u \in \bar{K}[\mathcal{C}]_P^\times, f = ut^n;$$

the integer $\mathrm{ord}_P(f) = n$ is called the *order* of f at P.

Given two functions $f, g \in \bar{K}[\mathcal{C}]_P$, we define $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ and thus extend the notion of order to any function of $\bar{K}(V)$. In particular, such a function can no longer be undetermined at a smooth point P and

- if $\mathrm{ord}_P(f) > 0$, then f has a *zero* at P;
- if $\mathrm{ord}_P(f) < 0$, then f has a *pole* at P.

Thus, if $\mathrm{ord}_P(f) \geq 0$, then f is regular at P and $f(P)$ can be computed ; otherwise we write $f(P) = \infty$.

Theorem 2.22. *Let $f \in \bar{K}(\mathcal{C}) \setminus \{0\}$. Then f has a finite number of poles and zeros.*

Example. *Let $E : y^2 = x^3 + x$ be a plane curve and $P = (0, 0) \in E$. Then $ord_P(x) = 2$ and $ord_P(y) = 1$.*
More generally, if $\mathcal{C}$ is a plane curve and P a point on $\mathcal{C}$, then any line which is not a tangent at P gives a uniformizer at P.

2.3 Divisors

Definition 2.23. *The divisor group of a curve $\mathcal{C}$ defined over K is the free abelian group generated by the points of $\mathcal{C}$ over the algebraic closure $\bar{K}$*

$$Div(\mathcal{C}) = \left\{ \sum_{P \in \mathcal{C}(\bar{K})} n_P(P) : n_P \in \mathbb{Z}, n_P = 0 \textit{ for all but finitely many } P \right\}.$$

- *The* degree *of a divisor D is defined by* $\deg(D) = \sum_{P \in \mathcal{C}(\bar{K})} n_P$
- *The divisors of degree* 0 *denoted*

  $$Div^0(\mathcal{C}) = \{D \in Div(\mathcal{C}) : \deg D = 0\}$$

  is a subgroup of $Div(\mathcal{C})$.
- *A divisor $D \in Div(\mathcal{C})$ is defined over K if its image by any automorphism $\sigma \in Gal(\bar{K}/K)$ defined as $D^\sigma = \sum_{P \in \mathcal{C}(\bar{K})} n_P(\sigma(P))$ is equal to D. The corresponding group is denoted $Div_K(\mathcal{C})$.*
- *The* principal divisor *of a function $f \in \bar{K}(\mathcal{C})^*$ is defined as*

  $$\mathrm{div}(f) = \sum_{P \in \mathcal{C}} ord_P(f)(P).$$

  The set of principal divisors of $\mathcal{C}$ is denoted $Princ(\mathcal{C})$.
- *A divisor $D = \sum_{P \in \mathcal{C}(\bar{K})} n_P(P)$ is called an* effective divisor *and denoted $D \geq 0$ if $n_P \geq 0$ for every $P \in \mathbb{C}$. This definition gives an ordering over $Div(\mathcal{C})$ given by $D_1 \geq D_2$ if $D_1 - D_2$ is effective.*
- *We define the* linear equivalence $\sim$ *on $Div(\mathcal{C})$ by $D \sim D'$ if $D = D' + \mathrm{div}(f)$.*

As it is defined, the group $Div(\mathcal{C})$ does not tell anything about the geometry of $\mathcal{C}$. We introduce therefore the Picard's group:

Definition 2.24. *The Picard group of an algebraic curve $\mathcal{C}$ is defined as*

$$Pic^0(\mathcal{C}) = Div^0(\mathcal{C})/\sim$$

where $\sim$ is the linear equivalence between divisors.
The group $Pic^0_K(\mathcal{C})$ is the subgroup of elements of $Pic^0(\mathcal{C})$ fixed by $Gal(\bar{K}/K)$.

Property 2.25. *(admitted)*

- $\deg(\mathrm{div}(f)) = 0$*, so f has the same number of poles and zeros. In particular,*

  $$Princ(\mathcal{C}) \subset \overset{0}{Div}(\mathcal{C}).$$

- $\mathrm{div}(f) = 0 \Leftrightarrow f \in \bar{K}^*$.
- $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$.

Example. *Let K be a field of characteristic different from 2 and $\mathcal{C} : y^2 = (x-e_1)(x-e_2)(x-e_3)$ be a curve defined over K. Then $\operatorname{div}(y) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O})$ and $\operatorname{div}(x - e_i) = 2(P_i) - 2(\mathcal{O})$, where P_i stands for the point of coordinates $(e_i, 0)$. In particular, x/y is a uniformizer at $\mathcal{O}$.*

To a divisor $D \in \operatorname{Div}(\mathcal{C})$, we associate set

$$\mathcal{L}(D) = \{f \in \bar{K}(\mathcal{C})^* : \operatorname{div}(f) \geq -D\} \cup \{0\}.$$

Remark that if $D \geq 0$, then $\mathcal{L}(D)$ is the set of functions of $\mathcal{C}$ whose poles are contained in D.

Property 2.26. *The set $\mathcal{L}(D)$ is a $\bar{K}$-vector space of finite dimension. We note $\ell(D)$ its dimension. Moreover, if D is defined over K, $\mathcal{L}(D)$ admits a basis of functions of $K(\mathcal{C})$.*

Theorem 2.27. *There exists a positive integer $g \in \mathbb{N}$, called the* genus *of $\mathcal{C}$, such that for any $D \in Div(\mathcal{C})$,*

1. $\ell(D) \geq \deg(D) - g + 1$,
2. $\ell(D) = \deg(D) - g + 1$ *if* $\deg D > 2g - 2$.

Look at the given exercises to manipulate Riemann-Roch's theorem...

3 Elliptic and hyperelliptic curves

3.1 Definition and arithmetic

Definition 3.1. *An* elliptic curve *E is a smooth projective curve of genus 1 having a specified base point $\mathcal{O}$ (which is K-rational when $E_{|K}$).*

Theorem 3.2. *The map $\psi_{\mathcal{O}} : E \to Pic^0(E),\ P \mapsto (P) - (\mathcal{O})$ is a bijection.*

Proof. This map is obviously surjective. Now, if $P, Q \in E$ are such that $(P) - (\mathcal{O}) \sim (Q) - (\mathcal{O})$, then $(P) - (Q) \sim 0$ and there exists $f \in \bar{K}(E)$ such that $\operatorname{div}(f) = (P) - (Q)$. But $f \in \mathcal{L}(Q) = \bar{K}$, so that f is a constant and $\operatorname{div} f = 0$. □

The map $\psi_{\mathcal{O}}$ is in fact a group morphism for the chord and tangent group law $\oplus$ defined over E: let $P, Q \in E$ and $\ell, v \in \bar{K}(E)$ such that $\operatorname{div} \ell = (P) + (Q) + (\ominus(P \oplus Q)) - 3(\mathcal{O})$ and $\operatorname{div} v = (P \oplus Q) + (\ominus(P \oplus Q)) - 2(\mathcal{O})$; then $\operatorname{div} \ell/v = (P) + (Q) - (\mathcal{O}) - (P \oplus Q)$ and $(P \oplus Q) - (\mathcal{O}) \sim (P) - (\mathcal{O}) + \sim (Q) - (\mathcal{O})$.

Corollary 3.3. *Let E be an elliptic curve and $D = \sum n_P(P) \in Div(E)$. Then D is principal iff $\sum n_P = 0$ and $\sum [n_P]P = O$.*

Proof. From the definition of the group law on E, we know that $((P) - (O)) + ((Q) - (O)) \sim (P + Q) - (O)$, and thus $(P) + (Q) \sim (P + Q) + (O)$. Similarly $(P) - (Q) \sim (P - Q) - (O)$. Applying this several times we find that $D = \sum n_P(P) \sim (\sum [n_P]P) - (1 - \sum n_P)(O)$. If $\deg D = \sum n_P \neq 0$ then clearly D is not principal. Now if $\sum n_P = 0$: then $D \sim (\sum [n_P]P) - (O)$, which is principal iff $\sum [n_P]P = O$. □

Theorem 3.4. *Let E be an elliptic curve defined over k. Then there exist functions $x, y \in k(E)$ such that $\Phi : E \to \mathbb{P}^2, \phi = [x, y, 1]$ gives an isomorphism between E and the curve given by the Weierstrass equation*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with $a_1, \ldots, a_6 \in k$, such that $\phi(\mathcal{O}) = [0 : 1 : 0]$.

Proof. (Sketch) Riemann-Roch theorem states that $\ell(D) = \deg D$ for all divisor D with positive degree. Thus, using $\ell(d(\mathcal{O})) = d$ for $d = 1, \ldots, 6$, we get that there exists x, y such that

- $\mathcal{L}((\mathcal{O})) = \langle 1 \rangle$;
- $\mathcal{L}(2(\mathcal{O})) = \langle 1, x \rangle$;
- $\mathcal{L}(3(\mathcal{O})) = \langle 1, x, y \rangle$;
- $\mathcal{L}(4(\mathcal{O})) = \langle 1, x, y, x^2 \rangle$;
- $\mathcal{L}(5(\mathcal{O})) = \langle 1, x, y, x^2, xy \rangle$;
- $\mathcal{L}(6(\mathcal{O})) = \langle 1, x, y, x^2, xy, y^2, x^3 \rangle$, so that there is a linear relation between these 7 functions.

□

Proposition 3.5. *An isomorphism between two elliptic curves in Weierstrass form is of the type*

$$\begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases}$$

with $u, r, s, t \in \bar{k}$ and $u \neq 0$. When u, s, r, t belong to k, then the two elliptic curves are k-isomorphic.

Proof. exercise! □

Suppose that $\mathrm{char}(k) \neq 2, 3$, then an elliptic curve E defined over k is (up to isomorphism) of the form, called *Weierstrass reduced equation*,

$$Y^2 = X^3 + AX + B, \text{ where } A, B \in k.$$

We define the j-invariant of E as

$$j(E) = \frac{1728 \cdot 4A^3}{4A^3 + 27B^2}.$$

Proposition 3.6. *Two elliptic curves E and E' are isomorphic if and only if $j(E) = j(E')$.*

Note that in this case, E and E' are not necessarily k-isomorphic. More precisely:

Property 3.7. *Suppose that $j(E) \neq 0, 1728$.*

If E and E' are elliptic curves with the same j-invariant defined over k, then

- *either E and E' are k-isomorphic,*
- *or E and E' are K-isomorphic with K quadratic extension of k; E' is then called a* quadratic twist *of E.*

Proof. We consider the odd characteristic (the proof in the characteristic 2 case is very similar). With obvious notations for equations of E and E', we have

$$\begin{aligned} j(E) = j(E') \quad &\Leftrightarrow \quad \frac{4A^3}{4A^3+27B^2} = \frac{4A'^3}{4A'^3+27B'^2} \\ &\Leftrightarrow \quad A^3B'^2 = A'^3B^2 \end{aligned}$$

Now if there exists an isomorphism between the two reduced Weierstrass equations, then it is necessarily of the form $(x,y) = (u^2x', u^3y')$, so that $A' = A/u^4$ and $B' = B/u^6$. Such an isomorphism exists iff $u^4 = A/A'$ and $u^6 = B/B'$. But this last condition is equivalent to $u^2 = A'B/(AB')$ thanks to the relation $A^3B'^2 = A'^3B^2$. The isomorphism is thus define either on k or on a quadratic extension of k containing $\sqrt{u}$. □

Definition 3.8. *An* imaginary hyperelliptic curve $\mathcal{H} \subset \mathbb{P}^2$ *of genus g defined over a field k is a projective curve with homogeneous equation*

$$Y^2Z^{2g-1} + h_0(X,Z)YZ^g = h_1(X,Z) \qquad (1)$$

where $h_0, h_1 \in k[X,Z]$ are homogeneous with $\deg_X h_1 = \deg h_1 = 2g+1$ and such that the affine part of (1) is smooth.

Remark.

1. *The point $\mathcal{O} = [0:1:0]$ is the unique point at the infinity and this point is not smooth as soon as $g > 1$ (this is not really a problem if you work with the* desingularisation *of $\mathcal{H}$).*

2. *If char(k) $\neq 2$, then it is possible to take $h_0 = 0$. In this case, the function h_1 must have no multiple roots.*

3. *More general hyperelliptic curves occur but are generally not used in HECC (and not treated in this lecture).*

Definition 3.9. *The map $\imath : (x,y) \mapsto (x, -y - h_0(x)), \mathcal{O} \mapsto \mathcal{O}$ is an involution called the* hyperelliptic involution.

In particular,

Proposition 3.10. *An element $D \in Pic^0_k(\mathcal{H})$ has a unique reduced representation*

$$D \sim (P_1) + \cdots + (P_r) - r(\mathcal{O}), \text{ with } r \leq g \text{ and } P_i \neq \imath(P_j), i \neq j.$$

Proof. For existence, see the exercises. Now, if $(P_1)+\cdots+(P_r) - r(\mathcal{O}) \sim (Q_1)+\cdots+(Q_s) - s(\mathcal{O})$ for some integers $r, s \leq g$, then there exists a function f such that $\operatorname{div} f = (P_1) + \cdots + (P_r) + (\imath(Q_1)) + \cdots + (\imath(Q_s)) - (r+s)(\mathcal{O})$. In particular, f has a pole only at $\mathcal{O}$ and is thus a polynomial of degree less than $r + s \leq 2g$. Since $\operatorname{ord}_{\mathcal{O}} y = 2g+1$, $f \in k[x]$ and for each $P \in \operatorname{supp}(\operatorname{div} f)$, we also have $\imath(P) \in \operatorname{supp}(\operatorname{div} f)$. Thus $\{P_i\}_i = \{Q_j\}_j$. □

Definition 3.11. *A divisor $D \in Div^0_k(\mathcal{H})$ is called* semi-reduced *if*

$$D = (P_1) + \cdots + (P_r) - r(\mathcal{O}), \text{ with } P_i \neq \imath(P_j), i \neq j,$$

for some integer r. If we group repeated points together and write

$$D = n_1(Q_1) + \cdots + n_s(Q_s) - r(\mathcal{O})$$

(with $r = \sum_i n_i$ and $n_i > 0$ for all i), the condition becomes $Q_i \neq \imath(Q_j)$ for all $i \neq j$ and $n_i = 1$ if $Q_i = \imath(Q_i)$.

As there is no condition on r, this writing is not unique.

We introduce in the following a convenient representation of the Picard group $\mathrm{Pic}^0(\mathcal{H})$ of an hyperelliptic curve $\mathcal{H}$, which allows to compute the group law algorithmically.

Let $D = (P_1) + \cdots + (P_r) - r(\mathcal{O}) \in \mathrm{Div}^0(\mathcal{H})$ be a semi-reduced divisor. We define the polynomials $u, v \in k[x]$ such that $u(x) = \prod_i (x - x_{P_i})$ and v is the interpolation polynomial such that $v(x_{P_i}) = y_{P_i}$ and $u|(v^2 + vh_0 - h_1)$ (this last condition is only necessary if $P_i = P_j$ for some $i \neq j$).

Reciprocally if $u, v \in k[x]$ are such that $u|(v^2 + vh_0 - h_1)$, it is easy to recover the corresponding semi-reduced divisor. Note however that v is only well-defined modulo u.

More precisely, we have the following proposition which gives us a fine representation of $\mathrm{Pic}^0(\mathcal{H})$:

Proposition 3.12. *The elements of* $Pic^0(\mathcal{H})$ *are in one-to-one correspondence with the set of pairs* $(u, v) \in k[x]^2$ *such that*

- u *is monic and* $\deg u \leq g$
- $\deg v < \deg u$
- $u|(v^2 + vh_0 - h_1)$.

These pairs of polynomials forms the set of k-rational points of an abelian and algebraic variety called the Jacobian variety *of $\mathcal{H}$ and denoted $Jac_{\mathcal{H}}(k)$.*

Note that these pairs of polynomials correspond this time to reduced divisors.

Property 3.13. *The dimension of the variety $Jac_{\mathcal{H}}$ is g. In particular $|Jac_{\mathcal{H}}(\mathbb{F}_q)| \simeq q^g$. More precisely,*

$$(\sqrt{q} - 1)^{2g} \leq \#Jac_{\mathcal{H}}(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g}.$$

It is possible now to describe an algorithm, called *Cantor's algorithm* that computes the addition of two elements of this Jacobian.

Let $D_1 = (u_1, v_1) = \sum_{i=1}^{r_1} (P_i) - r_1(\mathcal{O})$ and $D_2 = (u_2, v_2) = \sum_{i=1}^{r_2} (Q_i) - r_2(\mathcal{O})$ be two reduced divisors. We want to find the unique reduced divisor that is equivalent to $D_1 + D_2$ by computing first the semi-reduced divisor $D_3 \sim D_1 + D_2$ and then by reducing it.

1. Computation of D_3

   (a) If $P_i \neq \imath(Q_j)$ for all i, j, then $D_1 + D_2$ is semi-reduced, so that we can take $u_3 = u_1 u_2$ and v_3 defined modulo $u_1 u_2$ such that

   $$\begin{cases} v_3 = v_1 \bmod u_1 \\ v_3 = v_2 \bmod u_2 \\ u_3 | (v_3^2 + v_3 h_0 - h_1) \end{cases}$$

   Note that the first two equations are coherent, since from hypothesis $v_1 = v_2 \bmod (u_1 \wedge u_2)$, and determine v_3 modulo $u_1 \vee u_2$. The last equation then determines completely $v_3 \bmod u_3$.

(b) If $P_i = \imath(Q_j)$ for some i, j, then x_{P_i} is a root of $d = u_1 \wedge u_2 \wedge (v_1 + v_2 + h_0)$. As we need to remove $(P_i) + (\imath(P_i)) - 2(\mathcal{O})$ from $D_1 + D_2$, we take $u_3 = u_1 u_2 / d^2$ and v_3 such that

$$\begin{cases} v_3 = v_1 \bmod (u_1/d) \\ v_3 = v_2 \bmod (u_2/d) \\ u_3 | (v_3^2 + v_3 h_0 - h_1) \end{cases}$$

and the same remarks as above apply.

2. Reduction of the semi-reduced divisor $D_3 = (u_3, v_3) = (P_1) + \cdots + (P_r) - r(\mathcal{O})$ where $r > g$. The basic idea is to use the equation of the curve to find $D \sim D_3$ such that $|\mathrm{ord}_{\mathcal{O}}(D)| < |\mathrm{ord}_{\mathcal{O}}(D_3)|$ and repeat this operation until $|\mathrm{ord}_{\mathcal{O}}(D)| \leq g$. Let $\tilde{D}$ be the divisor such that $\mathrm{div}(y - v_3) = D_3 + \tilde{D}$, so we have $D_3 \sim -\tilde{D} \sim \imath(\tilde{D})$. It is not difficult to see that $\mathrm{div}(y - v_3)$ is semi-reduced (indeed, the only pole of $y - v_3$ is $\mathcal{O}$, it obviously cannot vanish both in P and $\imath(P)$ if $P \neq \imath(P)$, and one can check that $ord_P(y - v_3) \leq 1$ if $P = \imath(P)$). This implies that $\tilde{D}$, and thus $\imath(\tilde{D})$, are semi-reduced as well. The Mumford representation of $D = \imath(\tilde{D})$ is simply given by

$$u = \frac{(y - v_3)(y + h_0 + v_3)}{u_3} = \frac{h_1 - h_0 v_3 - v_3^2}{u_3}, \qquad v = -v_3 - h_0 \bmod u$$

(up to multiplication by a constant to keep u monic). Since $\deg v_3 < \deg u_3 = r$ and $r > g$, we have $\deg(u) \leq \max(2g+1, g+r-1, 2(r-1)) - r \leq \max(2g+1-r, r-2) \leq \max(g, r-2)$, so we have indeed simplified D_3, and we can continue with D until we obtain a reduced divisor.

Algorithm 1: Cantor's algorithm

```
Input  : $D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ two reduced divisors in the Jacobian $\mathrm{Jac}_{\mathcal{H}}$ of the
         hyperelliptic curve $\mathcal{H} : y^2 + h_0(x)y = h_1(x)$
Output: $D_3 = (u_3, v_3) \sim D_1 + D_2$ reduced divisor
$d \leftarrow u_1 \wedge u_2 \wedge (v_1 + v_2 + h_0)$
$a_1, a_2, a_3 \leftarrow$ Bézout's coefficients such that $d = a_1 u_1 + a_2 u_2 + a_3(v_1 + v_2 + h_0)$
$u_3 \leftarrow u_1 u_2 / d^2$
$v_3 \leftarrow (a_1 u_1 v_2 + a_2 u_2 v_1 + a_3(v_1 v_2 + h_1))/d \bmod u_3$
while $\deg u_3 > g$ do
    $u_3 \leftarrow (h_1 - h_0 v_3 - v_3^2)/u_3$
    $v_3 \leftarrow -v_3 - h_0 \bmod u_3$
return $(u_3/\mathrm{LC}(u_3), v_3)$
```

The asymptotic complexity of this algorithm is obviously in $\tilde{O}(g^3)$ as g and q grows to infinity, but there exist other variant that achieve a better complexity in $\tilde{O}(g^2)$.

Remark. *When taking $g = 1$ in Cantor's algorithm, we recover the classical group law on an elliptic curve.*

3.2 Index calculus on hyperelliptic curves

We apply the outline of section 1.5 to Jacobians of hyperelliptic curves, and consider factor bases of the form (using the Mumford representation of divisors)

$$\mathcal{F} = \{(u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) : \deg u \leq B, \ u \text{ irreducible}\}$$

for some integer B, called the *smoothness bound.* The computation of decompositions then relies on the following easy lemma:

Lemma 3.14. *Let $D = (u, v) \in Div^0_{\mathbb{F}_q}(\mathcal{H})$ be a semi-reduced divisor in Mumford representation. Let $u = \prod_{i=1}^{k} u_i$ be the decomposition of u in irreducible polynomials in $\mathbb{F}_q[x]$, and $v_i = v \bmod u_i$. Then $D = \sum_i D_i$ where $D_i = (u_i, v_i)$.*

This lemma shows that we can express a divisor $D = (u, v)$ as a sum of elements of the factor base $\mathcal{F}$ as soon as u is B-smooth, i.e. it has only irreducible factors of degree smaller than B.

Of course, it is possible to divide the size of $\mathcal{F}$ by 2 using the hyperelliptic involution.

Complexity analysis

Analogously to the finite field case, the probability that a random element of $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ is B-smooth when $B = \lceil \log_q(L_{q^g}(1/2, c)) \rceil$ is bounded from below by $1/L_{q^g}(1/2, 1/2c + o(1))$. In particular, the optimal choice of B when $q \to \infty$ and $g/\log q \to \infty$ is in $\log_q(L_{q^g}(1/2, 1/\sqrt{2}))$ and the total complexity is in $L_{q^g}(1/2, \sqrt{2} + o(1))$.

For g small, the situation is quite different and since the former analysis basically suggests $B < 1$ (!...), we take $B = 1$. The factor base has size about q and a divisor gives a relation if and only if the corresponding u polynomial in the Mumford representation is split over $\mathbb{F}_q$, which occurs with a probability in $1/g!$. The relation search has thus a complexity in $\tilde{O}(g!q)$ and the linear algebra is in $\tilde{O}(gq^2)$, giving a total complexity in $\tilde{O}(q^2)$. This is better than generic attacks as soon as $g > 4$. In fact, we can further improve this complexity by using the double large variation technique of Thériault et al., yielding a total complexity in $\tilde{O}(q^{2-2/g})$. Index calculus methods are thus faster than generic algorithms on Jacobian of hyperelliptic curves as soon as $g \geq 3$ and the curves of genera 1 or 2 are currently the best candidates for cryptographic applications.

Example. *Let $\mathcal{H} : y^2 = x^7 + 4x^5 + 3x^3 + 4x^2 + 3x + 4$ be a genus 3 hyperelliptic curve defined over $\mathbb{F}_5$. We take $B = 1$, so the factor base is in one-to-one correspondence with $\mathcal{H}(\mathbb{F}_5) \setminus \{\mathcal{O}\}$.*

1. *The cardinality of $\mathcal{H}(\mathbb{F}_5)$ is equal to 9 and its rational points are $\mathcal{H}(\mathbb{F}_5) = \{(0, \pm 2), (1, \pm 2), (2, \pm 1), (3, \pm 2), \mathcal{O}\}$. The corresponding factor base is*

$$\mathcal{F} = \{(x, \pm 2), (x - 1, \pm 2), (x - 2, \pm 1), (x - 3, \pm 2)\}.$$

2. *We consider the elements $D_0 = (x^3+4x^2+3x+3, x^2+2x+2)$ and $D_1 = (x^3+x^2+4x+2, 2x^2+x+2)$ on the Jacobian of $\mathcal{H}$, which has order 263, and test for relations.*

   - $x^3 + 4x^2 + 3x + 3$ *is not 1-smooth (it is equal to $(x - 3)(x^2 + 2x + 4)$), so D_0 does not give a relation.*
   - $2D_0 = (x^3 + x^2 + 3x + 1, 2x + 1)$ *but $x^3 + x^2 + 3x + 1$ is not split (it is irreducible), so no relation.*
   - ...
   - $5D_0 = (x^3 + 3x^2 + x + 3, 2x^2 + 3x)$ *and $x^3 + 3x^2 + x + 3 = (x - 3)(x - 2)^2$, so we get the relation*

$$5D_0 = (x - 3, 2) + 2(x - 2, 4) = (x - 3, 2) - 2(x - 2, 1).$$

   - ...

We obtain eventually some other relations :

$$\begin{aligned} 7D_0 &= (x,-2)+2(x-3,2) \\ 11D_0 &= (x,2)+(x-3,-2) \\ 13D_0 &= 2(x-2,1) \\ 15D_0 &= (x,-2)+(x-1,2)+(x-2,-1) \\ D_0+D_1 &= (x-1,-2)+2(x-3,2) \end{aligned}$$

3. *The relations can be expressed in matrix form:*

$$\begin{pmatrix} 5 & 0 \\ 7 & 0 \\ 11 & 0 \\ 13 & 0 \\ 15 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -2 & 1 \\ -1 & 0 & 0 & 2 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 \\ -1 & 1 & -1 & 0 \\ 0 & -1 & 0 & 2 \end{pmatrix} \begin{pmatrix} x,2 \\ x-1,2 \\ x-2,1 \\ x-3,2 \end{pmatrix}$$

Note that we have used the hyperelliptic involution to keep only four elements from the factor base. Note also that the relations obtained are not all independent. Using e.g. Gaussian elimination, we find that the vector $v = \begin{pmatrix} 0 & -2 & 0 & 1 & 2 & 2 \end{pmatrix}$ *satisfies* $vM = 0$*, so*

$$0 = \begin{pmatrix} 0 & -2 & 0 & 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 7 & 0 \\ 11 & 0 \\ 13 & 0 \\ 15 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \end{pmatrix} = \begin{pmatrix} 31 & 2 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \end{pmatrix} = 31D_0 + 2D_1,$$

so the discrete log of D_1 *is* $-31.2^{-1} = 116 \bmod 263$.

4 Isogenies between elliptic curves

4.1 Rational maps and morphisms between curves

In all this section, everything is defined over K unless otherwise specified.

Definition 4.1. *Let* $V \subset \mathbb{P}^n(\bar{K})$ *and* $V' \subset \mathbb{P}^m(\bar{K})$ *two varieties.*

- *A* rational map $\phi : V \to V'$ *is the data of* $(f_0, f_1, \ldots, f_m) \in \bar{K}(V)^{m+1} \setminus \{(0,\ldots,0)\}$*, such that for any* $P \in V$ *where all the* f_i *are defined and do not all vanish,* $\phi(P) = [f_0(P) : f_1(P) : \cdots : f_m(P)]$ *belongs to* V'*.*
- *Two* $(m+1)$*-tuples* $(f_0, \ldots, f_m)$ *and* $(f'_0, \ldots, f'_m)$ *define the same rational map if there exists* $g \in \bar{K}(V)^*$ *such that* $f'_i = gf_i$ *for all* i*.*
- *A rational map* $\phi = [f_0 : \cdots : f_m]$ *is defined at a point* $P \in V$ *if there exists* $g \in \bar{K}(V)$ *such that the* gf_i *are all defined and do not all vanish at* P*.*
- *A rational map that is defined everywhere is called a* morphism*.*

- *A morphism $\phi : V \to V'$ is an* isomorphism *if there exists a morphism $\psi : V' \to V$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map (of V' and V respectively).*
- *If V and V' are defined over K, then ϕ is defined over K if it can be expressed as $[f_0 : \cdots : f_m]$ where $f_i \in K(V)$ for all i.*

Note that is also possible to express a rational map $\phi = [F_0, \ldots, F_m]$ with F_i are homogeneous polynomials of same degree d.

In practice we will rather use affine coordinates (so that $f_m = 1$).

Examples.

- *$E : y^2 = x^3 + x^2$, $\phi : E \to \mathbb{P}^1$, $(x, y) \mapsto y/x$. In homogeneous coord, $E : Y^2 Z = X^3 + X^2 Z$ and $\phi([X : Y : Z]) = [Y/X, 1] = [Y, X]$ is a rational map. It is not defined in $[0 : 0 : 1]$ (hence it is not a morphism), but it is defined in $[0 : 1 : 0]$. Let $\psi : \mathbb{P}^1 \to E$, $[S : T] \mapsto [S^2 T - T^3 : S^3 - ST^2 : T^3]$. Then $\psi \circ \phi$ and $\psi \circ \phi$ are the identity wherever they are defined, yet neither is an isomorphism.*
- *Isomorphisms of elliptic curves (as seen in the previous chapter) are indeed isomorphisms.*

Proposition 4.2. *$\phi : C_1 \to C_2$ and $P_1 \in C_1$ smooth point. Then ϕ is defined at P_1.*

Proof. In homogeneous coord., $\phi(P) = [\phi_0(P) : \cdots : \phi_n(P)]$ where $\phi_i \in K(C_1)$. Let t = uniformizer at P_1. Then $\phi_i = t^{\alpha_i} \phi'_i$ where $\alpha_i = ord_{P_1}(\phi_i)$ and $\phi'_i(P_1) \in K^*$. Let $m = \min_i(\alpha_i)$ (can be negative!). Then ϕ is also equal to $[t^{\alpha_0 - m}\phi'_0 : \cdots : t^{\alpha_n - m}\phi'_n]$. $t^{\alpha_i - m}\phi'_i$ has no pole at P_1 and at least one is $\neq 0$ at $P_1 \Rightarrow \phi$ defined at P_1. □

Example. *Note that in the previous example, the rational map was not defined in $(0, 0)$, which was precisely a non smooth point.*

In the following, we assume that all curves are smooth; in particular all rational maps are morphisms.

Definition 4.3. *Let $\phi : C_1 \to C_2$ be a non-constant map and $f \in K(C_2)$. The* pull-back *by ϕ is the field morphism defined by*

$$\phi^*(f) = f \circ \phi \in K(C_1).$$

Theorem 4.4. *The pull-back gives a one-to-one correspondence between the set of non-constant maps from C_1 to C_2 defined over K and the set of field morphisms between the functions field $K(C_2)$ and $K(C_1)$ that fix K:*

$$\begin{array}{ccc} \{ \text{ non-constant maps defined over } K : C_1 \to C_2\} & \to & \{\text{field morphisms fixing } K : K(C_2) \to K(C_1)\} \\ \phi & \mapsto & \phi^* \end{array}$$

Proof. Let $\psi : K(C_2) \to K(C_1)$. Preimage ? Wlog we can assume that $C_2 \subset \mathbb{P}^n$ and $C_2 \not\subset \{x_0 = 0\}$. We look for $\phi = [1 : \phi_1 : \cdots : \phi_n]$ s.t. $\phi^* = \psi$; then necessarily $\phi_i = \frac{x_i}{x_0} \circ \phi = \phi^*(\frac{x_i}{x_0}) = \psi(\frac{x_i}{x_0})$. Conversely, we can check that $\phi = [1 : \psi(\frac{x_1}{x_0}) : \cdots : \psi(\frac{x_n}{x_0})]$ is indeed a non-constant map from C_1 to C_2 such that $\phi^* = \psi$. □

Theorem 4.5 (Admitted)**.** *A map between curves is either constant or surjective.*

Remarks.

- *The map is understood as being from $C_1(\bar{K}) \to C_2(\bar{K})$. This theorem is* not *true if we just consider K-rational points.*

- *A function is also a map to $\mathbb{P}^1$. Thm implies that* $\operatorname{div} f = 0$ *iff f constant.*

Definition 4.6. *The* degree of a morphism *ϕ defined over K is the degree of the corresponding field extension $[K(C_1) : \phi^*(K(C_2))]$ (or 0 if ϕ is constant). The map ϕ is* separable *if the corresponding extension $K(C_1)/\phi^*(K(C_2))$ is separable (i.e. mimimal polynomial of any element has no multiple roots in algebraic closure).*

Remark. *The morphism ϕ is an isomorphism iff* $\deg \phi = 1$. *We have also (and this is admitted) that* $\deg \phi < +\infty$*, and that* $[K(C_1) : \phi^*(K(C_2))] = [\bar{K}(C_1) : \phi^*(\bar{K}(C_2))]$*).*

Some basic properties:

Property 4.7. $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ *and* $\deg(\phi \circ \psi) = \deg \phi \times \deg \psi$.

Proof. First part is immediate. Second part comes from the multiplicativity of field extension degree, and also holds of course if either morphism is constant. □

Our next goal is to define the pullback of a divisor. The main idea is that if $Q \in C_2$ and $D = (Q)$ then $\phi^*((Q)) = \sum_{P \in C_1 \text{ s.t. } \phi(P)=Q} m_P(P)$ where m_P counts the "multiplicity" of P in the pre-image.

Definition 4.8. *The* ramification index *of a curve morphism $\phi : C_1 \to C_2$ at $P \in C_1$ is defined as*

$$e_\phi(P) = ord_P(\phi^* t) \text{ where } t \text{ uniformizer at } \phi(P).$$

The morphism ϕ is unramified *at $P \in C_1$ if $e_\phi(P) = 1$; the morphism ϕ is unramified it is unramified in all points of C_1.*

Property 4.9. *Let $\phi_1 : C_1 \to C_2$ and $\phi_2 : C_2 \to C_3$. Then $e_{\phi_2 \circ \phi_1}(P) = e_{\phi_1}(P).e_{\phi_2}(\phi_1(P))$.*

Proof. Exercice. □

Proposition 4.10 (Admitted)**.**
For all $Q \in C_2$, $\deg \phi = \sum_{P \in \phi^{-1}(\{Q\})} e_\phi(P)$.
If ϕ is separable, then $e_\phi(P) = 1$ for all but finitely many $P \in C_1$.

Example. *Let $E : y^2 = x^3 - x$ (char$K \neq 2, 3$) and $\phi : E \to \mathbb{P}^1$, $(x, y) \mapsto x$. By abuse of notation x also denotes the affine coordinate of $\mathbb{P}^1$, so that $\phi^* x = x$. Then ϕ has degree 2 since $[K(E) : \phi^*(K(\mathbb{P}^1))] = [K(x, y) : K(x)] = 2$.*
Ramification index at $P = (x_P, y_P)$? A uniformizer at $\phi(P)$ is simply $t_{\phi(P)} = x - x_P$, its pullback by ϕ is $\phi^*(t_{\phi(P)}) = x - x_P$. Now at P,

$$(y - y_P + y_P)^2 = (x - x_P + x_P)^3 - (x - x_P + x_P)$$

$$\Rightarrow \quad (y - y_P)^2 + 2y_P(y - y_P) = (x - x_P)^3 + 3x_P(x - x_P)^2 + (3x_P^2 - 1)(x - x_P).$$

If $y_P \neq 0$, $x - x_P$ is a uniformizer at P (and in the local ring, $y - y_P = (x - x_P)\frac{(x-x_P)^2 + 3x_P(x-x_P) + 3x_P^2 - 1}{(y-y_P) + 2y_P}$), so $e_\phi(P) = 1$. If $y_P = 0$, i.e. if $P \in \{(0,0), (1,0), (-1,0)\}$, then a uniformizer at P is y, and in the local ring $(x - x_P) = y^2 / \left((x - x_P)^2 + 3x_P(x - x_P) + 3x_P^2 - 1\right)$, so $ord_P(x - x_P) = 2$ and $e_\phi(P) = 2$. Finally, if $P = O$, then a uniformizer at $\phi(O)$ is $1/x$, it pullback is $1/x$, and $e_\phi(O) = ord_O(1/x) = 2$. Note that the results of the previous proposition are satisfied.

Example. *Let $E : y^2 = x^3 - x$ (char$K \neq 2,3$) and this time $\psi : E \to \mathbb{P}^1$, $(x,y) \mapsto y$. By abuse of notation it is this time y that denotes the affine coordinate of $\mathbb{P}^1$, so that $\psi^* y = y$. Then ψ has degree 3 since $[K(E) : \psi^*(K(\mathbb{P}^1)] = [K(x,y) : K(y)] = 3$. According to Proposition 4.10, ψ is not ramified at $P = (x_P, y_P)$ if the preimage of $\psi(P)$ has three elements, i.e. if the polynomial $x^3 - x - y_P^2$ has simple roots. This is equivalent to saying that the discriminant $(-y_P^2)^2 + 4(-1)^3/27 = y_P^4 - 4/27$ does not vanish (recall that $x^3 + ax + b$ has simple roots iff $b^2 + 4a^3/27 \neq 0$). So ψ is unramified at most points. In fact with what we have done before we see that $y - y_P$ is not a uniformizer iff $3x_P^2 - 1 = 0$, and it is not difficult to obtain that $e_\psi(1/\sqrt{3}, \pm\sqrt{-2/3\sqrt{3}}) = e_\psi(-1/\sqrt{3}, \pm\sqrt{2/3\sqrt{3}}) = 2$, $e_\psi(O) = 3$, and $e_\psi(P) = 1$ everywhere else. Note that $\psi^{-1}(\sqrt{2/3\sqrt{3}}) = \{(-1/\sqrt{3}, \sqrt{2/3\sqrt{3}}), (2/\sqrt{3}, \sqrt{2/3\sqrt{3}})\}$; the ramification index is 2 at the first point and 1 at the second.*

Example. *Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$, $z \mapsto z^n$. This is a degree n morphism ($[K(\mathbb{P}^1) : \phi^*(K(\mathbb{P}^1))] = [K(z) : K(z^n)]$).*
Ramification index at ∞? $\phi(\infty) = \infty$, a uniformizer at ∞ is $1/z$, and $\phi^*(1/z) = 1/z^n$, so $e_\phi(O) = n$. Ramification index at $a \neq \infty$? A uniformizer at $\phi(a) = a^n$ is simply $z - a^n$, its pullback is $z^n - a^n$, which we want to express in term of $z-a$ which is a uniformizer at a. If $a = 0$, then $z^n - 0^n = (z-0)^n$, so $e_\phi(0) = n$. If $a \neq 0$, then $z^n - a^n = (z-a)f_a(z)$ where $f_a(z) = z^{n-1} + az^{n-2} + \cdots + a^{n-2}z + a^{n-1}$. In a, this evaluates as $f_a(a) = na^{n-1}$. If n is coprime to char$K$ or char$K = 0$, then $f_a(a) \neq 0$, so $f_a(z)$ is invertible in the local ring at a, and $e_\phi(a) = 1$. But this is not the case if $n = p^i m$, $p = char(K)$, $p \nmid m$. Then $z^n - a^n = (z^m - a^m)^{p^i} = (z-a)^{p^i}(z^{m-1} + \cdots + a^{m-1})^{p^i}$. The rightmost term no longer vanishes at a (it evaluates as $(ma^{m-1})^{p^i}$), so $e_\phi(a) = p^i$. We can check that the first part of Proposition 4.10 still holds, but not the second one: ϕ is not separable if $p|n$.

Definition 4.11. *Let $\phi : C_1 \to C_2$ be a morphism.*
The pullback of a divisor *$\sum n_Q(Q) \in Div(C_2)$ is defined as $\phi^*(\sum n_Q(Q)) = \sum n_Q \phi^*((Q))$ where*

$$\phi^*((Q)) = \sum_{P \in \phi^{-1}(\{Q\})} e_\phi(P)\,(P).$$

The push-forward of a divisor *$\sum n_P(P) \in Div(C_1)$ is given by*

$$\phi_*(\sum n_P(P)) = \sum n_P(\phi(P)).$$

Property 4.12. *1.* $\deg(\phi^*(D_2)) = \deg(D_2)\deg\phi$

2. $\deg(\phi_*(D_1)) = \deg(D_1)$

3. $\phi_* \circ \phi^*(D_2) = (\deg\phi)D_2$

4. $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$

5. $\phi_*(\mathrm{div}(f))$ *is principal.*

Proof. Exercice, except for 5. (admitted). □

Remark. *If $f \in K(C)$ then f is also a map from C to $\mathbb{P}^1$ and* $\mathrm{div}\, f = f^*((0) - (\infty))$. *Then 1. shows that* $\deg \mathrm{div}\, f = 0$.

In particular ϕ^* maps $Div_K^0(C_2)$ to $Div_K^0(C_1)$ and maps principal divisors to principal divisors, similarly for ϕ_*, so group morphisms:

$$\phi^* : Pic_K^0(C_2) \to Pic_K^0(C_1), \quad \phi_* : Pic_K^0(C_1) \to Pic_K^0(C_2)$$

4.2 Isogenies

Proposition 4.13. *E elliptic curve. Then* $- : \begin{cases} E \to E \\ P \mapsto -P \end{cases}$ *is an isomorphism,* $\tau_Q : \begin{cases} E \to E \\ P \mapsto P+Q \end{cases}$ *is an isomorphism for all* $Q \in E$, $+ : \begin{cases} E \times \cdots \times E \to E \\ (P_1, \ldots, P_n) \mapsto P_1 + \cdots + P_n \end{cases}$ *is a morphism for all* n.

Proof. Clear for $-$, by direct inspection for τ_Q. A bit more complicated for $+$ (ok for $n = 2$, induction for greater n, but requires to know that a product of projective varieties is a projective variety (not so obvious: $\mathbb{P}^n \times \mathbb{P}^m \neq \mathbb{P}^{n+m}$)). □

Corollary 4.14. *The multiplication-by-m map* $[m] : \begin{cases} E \to E \\ P \mapsto P + \cdots + P \end{cases}$ *is a morphism for all* $m \in \mathbb{N}^*$.

If $m < 0$, we set $[m]P = -[-m]P$, and $[0]P = O$, so that $[m]$ is a morphism for all $m \in \mathbb{Z}$ (constant if $m = 0$).

Definition 4.15. *A morphism* $\phi : E_1 \to E_2$ *is an isogeny if* $\phi(O_1) = O_2$.

Examples. 1. *The morphism* $[m]$ *is an isogeny (from E to E) for all* $m \in \mathbb{Z}$. *The composition of two isogenies is an isogeny. If* $\phi : E_1 \to E_2$ *morphism, then* $\tau_{-\phi(O_1)} \circ \phi$ *is an isogeny, so every morphism between elliptic curve is the composition of a translation and an isogeny.*

2. *If* $\phi, \psi : E_1 \to E_2$ *are two isogenies, then the map* $\phi + \psi : P \mapsto \phi(P) + \psi(P)$ *is an isogeny from* E_1 *to* E_2 *(it is indeed a morphism because* $+ : E \times E \to E$ *is a morphism). As a particular case,* $[m] + [n]$ *is obviously an isogeny: it is just* $[m + n]$.

3. *Assume that* char$K \neq 2$. *Let* $E_1 : y^2 = x^3 + ax^2 + bx$ *a non-singular elliptic curve (so* $b \neq 0$ *and* $d = a^2 - 4b \neq 0$*) and* $E_2 : y^2 = x^3 - 2ax^2 + dx$. *Then* $\phi : (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right)$ *is a degree 2 isogeny from* E_1 *to* E_2 *and* $\psi : (x, y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(d-x^2)}{8x^2}\right)$ *is a degree 2 isogeny from* E_2 *to* E_1. *One can check that* $\psi \circ \phi = [2]$ *(on* E_1*) and* $\phi \circ \psi = [2]$ *(on* E_2*). This is actually an example of* dual *isogenies.*

It is clear that $[m](P + Q) = [m]P + [m]Q$, i.e. $[m]$ is a group morphism. But this is actually true for all isogenies!

Theorem 4.16. *Let* $\phi : E_1 \to E_2$ *an isogeny. Then* ϕ *is a group morphism, i.e. for all* $P, P' \in E_1$, $\phi(P + P') = \phi(P) + \phi(P')$ *for the usual elliptic curve law on* E_1 *and* E_2.

This means that a morphism (of varieties) between elliptic curves is a morphism (of groups) if it fixes the point at infinity.

Proof. Remember the bijections (for $i = 1, 2$) $\psi_i : E_i \to Pic^0(E_i)$, $P \mapsto [(P) - (O_i)]$. Then $\psi_2^{-1} \circ \phi_* \circ \psi_1(P) = \psi_2^{-1} \circ \phi_*([(P) - (O_1)]) = \psi_2^{-1}([(\phi(P)) - \phi(O_1)]) = \psi_2^{-1}([(\phi(P)) - (O_2)]) = \phi(P)$. So $\phi = \psi_2^{-1} \circ \phi_* \circ \psi_1$, but ψ_2, ϕ_* and ψ_1 are group morphisms, so ψ is a group morphism. □

Corollary 4.17. *For any* $\phi : E_1 \to E_2$ *isogeny and* $m \in \mathbb{Z}$, $\phi \circ [m] = [m] \circ \phi$.

Indeed, $\phi([m]P) = \phi(P + \cdots + P) = \phi(P) + \cdots + \phi(P) = [m]\phi(P)$. Note that the multiplication-by-m maps on the two sides are on different curves (if $E_1 \neq E_2$).

If $char(K) = p > 0$, a important isogeny is the Frobenius map (very important for point counting !).

Definition 4.18. *Let E of equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a4x + a_6$, $a_1, \ldots, a_6 \in K$, and $\sigma : a \mapsto a^p$ the Frobenius (field-)morphism. We set $E^\sigma : y^2 + a_1^pxy + a_3^py = x^3 + a_2^px^2 + a_4^px + a_6^p$; it is an elliptic curve defined over K, with $j(E^\sigma) = \sigma(j(E))$ and $\Delta(E^\sigma) = \sigma(\Delta(E))$ (so E^σ is non-singular). The Frobenius morphism is*

$$\Phi_p : \begin{cases} E \to E^\sigma \\ (x, y) \mapsto (x^p, y^p) \end{cases}$$

If $q = p^n$ then $\Phi_q = \Phi_p \circ \cdots \circ \Phi_p : E \to E^{\sigma^n}, (x, y) \mapsto (x^q, y^q)$.

It is clearly a rational map, and it is easy to see that $\Phi_p([0 : 1 : 0]) = [0 : 1 : 0]$ indeed. If $K = \mathbb{F}_q$ (where $q = p^n$) then $E^{\sigma^n} = E$ and Φ_q is the identity on $E(\mathbb{F}_q)$ but *not* on E: more precisely, $\Phi_q(P) = P$ iff P is $\mathbb{F}_q$-rational.

Property 4.19. *The Frobenius morphism $\Phi_p : E \to E^\sigma$ is a non separable isogeny of degree p.*

Proof. Since $K(E) = K(x, y)$ where $y^2 = f(x)$ (we assume for simplicity that $p \neq 2$), we have $\Phi_p^*(K(E^\sigma)) = K(x^p, y^p)$.
Then $K(E) = K(x^p, y^p)(x)$: clearly $K(x^p, y^p)(x) = K(x, y^p)$, and $(y^p/f(x)^{(p-1)/2})^2 = f(x)$ so $y = \pm y^p/f(x)^{(p-1)/2} \in K(x, y^p)$, which implies that $K(x, y^p) = K(x, y)$. The extension $K(x^p, y^p)(x)/K(x^p, y^p)$ is now clearly inseparable and of degree p. □

Remark. *The morphism Φ_p is injective, hence bijective (since not constant), but is* not *an isomorphism:* $\deg \Phi_p \neq 1$.

Theorem 4.20 (Admitted)**.** *Let $\phi : E_1 \to E_2$ a non-separable isogeny. Then it admits a unique factorization as $\phi = \psi \circ \Phi_{p^n}$ where $\psi : E_1^{\sigma^n} \to E_2$ is separable.*

This theorem is more generally is true if we consider morphisms between arbitrary curves.

Proposition 4.21. *Let $\phi : E_1 \to E_2$ a separable isogeny, then ϕ is unramified. In particular, $|\ker \phi| = |\phi^{-1}(\{O_2\})| = \deg \phi$.*

Proof. Let P_0 be an arbitrary point in E_1. We observe that $\phi = \tau_{-\phi(P_0)} \circ \phi \circ \tau_{P_0}$: indeed, $\tau_{-\phi(P_0)} \circ \phi \circ \tau_{P_0}(P) = \phi(P + P_0) - \phi(P_0) = \phi(P)$ since ϕ is a group morphism. Then using Property 4.9, $e_\phi(O_1) = e_{\tau_{-\phi(P_0)} \circ \phi \circ \tau_{P_0}}(O_1) = e_{\tau_{P_0}}(O_1).e_\phi(\tau_{P_0}(O_1).e_{\tau_{-\phi(P_0)}}(\phi(\tau_{P_0}(O_1))) = e_{\tau_{P_0}}(O_1)).e_\phi(P_0).e_{\tau_{-\phi(P_0)}}(\phi(P_0))$. Since τ_{P_0} and $\tau_{-\phi(P_0)}$ are isomorphisms (of varieties), they are unramified, so $e_\phi(O_1) = e_\phi(P_0)$. This implies that the ramification index is the same everywhere. But the second part of Proposition 4.10 states that ϕ is unramified somewhere, so it is unramified everywhere. Now the first part of the same proposition states that $\deg \phi = \sum_{P \in \ker(\phi)} e_\phi(P) = |\ker \phi|$ since $e_\phi(P) = 1$ for all $P \in E_1$. □

Remark. *As Φ_p is injective, $|\ker \Phi_p| = 1$ and the ramification index of Φ_p is p everywhere.*

Proposition 4.22 (Admitted)**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$, and let m, n be two integers. Then $[m] + [n] \circ \Phi_q : E \to E$ is separable iff $m \wedge q = 1$.*

In particular, the multiplication-by-p map is not separable.

4.3 Torsion points and supersingular curves

Definition 4.23. *For any $m \in \mathbb{N}^*$, the set of m-torsion points of E is $E[m] = \ker[m]$ (it is a subgroup of E). Rational torsion points: $E(K)[m] = E(K) \cap E[m]$.*

Example. *2-torsion points*

- *If char$(K) \neq 2$, E has equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Then $[2]P = O \Leftrightarrow P = -P$. If $P \neq O$, this means that $(x_P, y_P) = (x_P, -y_P)$ so $y_P = 0$ and x_P is a root of $x^3+a_2x^2+a_4x+a_6$. So there are 4 2-torsion points: $E[2] = \{O, (x_1, 0), (x_2, 0), (x_3, 0)\}$ where the x_i's are the roots of $x^3 + a_2x^2 + a_4x + a_6$. As a group, $E[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

- *If char$(K) = 2$ and $j(E) \neq 0$, then E has equation $y^2 + xy = x^3 + a_2x^2 + a_6$. Then $P \in E[2] \Leftrightarrow P = -P \Leftrightarrow P = O$ or $(x_P, y_P) = (x_P, y_P + x_P)$. This last condition is equivalent to $x_P = 0$, which implies $y_P = a_6^{1/2}$. So there are only two 2-torsion points: $E[2] = \{O, (0, a_6^{1/2})\} \simeq \mathbb{Z}/2\mathbb{Z}$.*

- *Finally if char$(K) = 2$ and $j(E) = 0$ then E has equation $y^2 + a_3y = x^3 + a_4x + a_6$. Then $P \in E[2] \Leftrightarrow P = -P \Leftrightarrow P = O$ or $(x_P, y_P) = (x_P, y_P + a_3) \Leftrightarrow P = O$. So there is only one 2-torsion point: $E[2] = \{O\}$.*

Property 4.24. *If m and n are coprime, then $E[mn] \simeq E[m] \times E[n]$*

Proof. Let u, v such that $um+vn = 1$. Then an explicit isomorphism is given by $P \mapsto ([vn]P, [um]P)$; its inverse is $(P_1, P_2) \mapsto P_1 + P_2$. (This is actually a property of abelian groups). □

Theorem 4.25.
- *For all $m \in \mathbb{Z}$, $\deg[m] = m^2$.*
- *Let m be a positive integer, coprime to char(K) if char$(K) \neq 0$. Then $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*
- *If char$(K) = p \neq 0$, then either $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ or $E[p] = \{O\}$. The elliptic curve E is called* ordinary *in the first case,* super-singular *in the second.*

Rk: this is only true when considering points over $\bar{K}$! It is definitely not true for K-rational points. Also, we have seen that it is the case for the 2-torsion.

Proof. The proof of the first point will be admitted for the moment (note that there exists an elementary but computation-heavy proof, that relies on division polynomials and gives an explicit formula for the morphism $[m]$). Note that it is easy to see that $[m]$ is not constant if $m \neq 0$, at least if E is not supersingular in characteristic 2 (hint: restrict to the case m odd and consider the action of $[m]$ on a non-trivial 2-torsion point).
If $p \wedge m = 1$ then $p \nmid m^2$ so $[m]$ is separable (since the degree of a non-separable extension is always a multiple of the characteristic, or see Proposition 4.22). Thus $|E[m]| = \deg[m] = m^2$. The fundamental theorem of abelian groups then implies that $E[m] = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ where $n_1| \dots |n_k$, $n_1 \neq 1$, $n_1 \dots n_k = m^2$ (and necessarily $n_k|m$ since the order of all elements divides m). Then $E[m]$ has a subgroup isomorphic to $(\mathbb{Z}/n_1\mathbb{Z})^k$, which is also a subgroup of $E[n_1]$; if $k > 2$ then $|E[n_1]| > n_1^2$, which is a contradiction. Thus $k = 2$ and $n_1 = n_2 = m$. We will see later the case of $[p]$ (see the proof of Prop. 4.30). □

Super-singular elliptic curves (not to be confused with singular curves!) were once popular candidates for ECC because their cardinality is easy to compute, until it was realized that they are vulnerable to pairing attacks. They are still interesting for pairing-based cryptography (but with adapted security levels).

Easy corollary (or exercise ?): if $p \wedge m = 1$ and $r \in \mathbb{N}^*$, $E[p^r m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p^r m\mathbb{Z}$ if E ordinary or $E[p^r m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ if E supersingular.

4.4 Quotients of elliptic curves and dual isogenies

Let $\phi : E_1 \to E_2$ a non-constant separable isogeny. We know that ϕ is surjective, so as a group, E_2 is isomorphic to the quotient $E_1/\ker\phi$. We can also proceed the other way round:

Theorem 4.26. *Let G be a finite subgroup of an elliptic curve $E_{|K}$. Then there exist an elliptic curve E' and a separable isogeny ϕ such that* $\ker\phi = G$*, and E' and ϕ are unique (up to isomorphisms). If G is defined over K (in the sense that $\sigma(P) \in G$ for all $P \in G$ and all $\sigma \in Gal(\bar{K}/K)$) then E' and ϕ are defined over K.*

The elliptic curve E' is often denoted by E/G. Note that it is always possible to define the quotient E/G as a group; this theorem says that it is the group of points of an elliptic curve. Explicit formulas for E' and ϕ exist (Vélu's formulas).

Proof. (Sketch) Suppose that such a ϕ and E' exist. If f is in $\bar{K}(E')$, then for any $P \in G$ and any $Q \in E$, $\tau_P^*(\phi^*(f))(Q) = f(\phi(P+Q)) = f(\phi(P)+\phi(Q)) = f(\phi(Q)) = \phi^*(f)(Q)$, so $\tau_P^*(\phi^*(f)) = \phi^*(f)$. This means that the subfield $\phi^*(\bar{K}(E'))$ is invariant by τ_P^* for any $P \in G$ (note that since the translation by P is an isomorphism, τ_P^* is an automorphism of $\bar{K}(E)$).
So we consider the subfield $\bar{K}(E)^G = \{f \in \bar{K}(E) : \tau_P^*(f) = f \ \forall P \in G\}$. This is the function field of a curve C, and the inclusion $\bar{K}(E)^G \subset \bar{K}(E)$ gives a morphism $\phi : E \to C$. It remains to check that C is indeed an elliptic curve and that ϕ is indeed an isogeny such that $\ker\phi = G$. □

This is an efficient tool to construct separable isogenies. For instance, let ℓ be a prime number coprime to q. If $E_{|\mathbb{F}_q}$ is a given elliptic curve, what is the number of degree ℓ isogenies (defined over $\mathbb{F}_q$) starting from E? The above theorem states that such isogenies are in bijection with the cyclic subgroups of $E[\ell]$ that are globally invariant under the action of the Frobenius map Φ_q. This is an important tool of the SEA point counting algorithm.

Corollary 4.27. *Let $\phi_1 : E \to E_1$ and $\phi_2 : E \to E_2$ two separable isogenies such that* $\ker\phi_1 = \ker\phi_2$*. Then there exists an isomorphism $\psi : E_1 \to E_2$ such that $\phi_2 = \psi \circ \phi_1$.*

Let $\phi : E_1 \to E_2$ be an isogeny; it can be identified with the push-forward $\phi_* : Pic^0(E_1) \to Pic^0(E_2)$. But we have seen that there is also a pull-back map $\phi^* : Pic^0(E_2) \to Pic^0(E_1)$. This means that we can construct a map $\hat{\phi} = \psi_1^{-1} \circ \phi^* \circ \psi_2 : E_2 \to E_1$ (where ψ_i is the bijection $E_i \to Pic^0(E_i)$, $P \mapsto [(P) - (O_i)]$). Then $\phi \circ \hat{\phi} = \psi_1^{-1} \circ \phi_* \circ \phi^* \circ \psi_2 = [\deg\phi]$ (cf Property 4.12). But it is not clear that $\hat{\phi}$ is a rational map (i.e. is given by rational functions)...

Theorem 4.28. *Let $\phi : E_1 \to E_2$ be a non constant isogeny. Then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$, called the* dual isogeny *of ϕ, such that $\phi \circ \hat{\phi} = [\deg\phi]$. It satisfies the following properties:*

- $\widehat{\phi_1 \circ \phi_2} = \hat{\phi}_2 \circ \hat{\phi}_1$
- $\hat{\phi} \circ \phi = [\deg \phi]$

Proof. Uniqueness is not difficult: if ψ and ψ' are two isogenies such that $\phi \circ \psi = \phi \circ \psi' = [\deg \phi]$, then $0 = \phi \circ \psi - \phi \circ \psi' = \phi \circ (\psi - \psi')$ (this last equality holds because ϕ is an isogeny); by multiplicativity of the degree, $\deg \phi \times \deg(\psi - \psi') = 0$ so $\deg(\psi - \psi') = 0$ and $\psi - \psi' = 0$, i.e. $\psi = \psi'$.
For the first property, observe that $(\phi_1 \circ \phi_2) \circ (\hat{\phi}_2 \circ \hat{\phi}_1) = \phi_1 \circ (\phi_2 \circ \hat{\phi}_2) \circ \hat{\phi}_1 = \phi_1 \circ [\deg \phi_2] \circ \hat{\phi}_1 = [\deg \phi_2] \circ \phi_1 \circ \hat{\phi}_1$ (cf Corollary 4.17) $= [\deg \phi_2] \circ [\deg \phi_1] = [\deg \phi_2 \times \deg \phi_1] = [\deg(\phi_1 \circ \phi_2)]$, so by uniqueness $\widehat{\phi_1 \circ \phi_2} = \hat{\phi}_2 \circ \hat{\phi}_1$.
Second property: $\phi \circ (\hat{\phi} \circ \phi) = (\phi \circ \hat{\phi}) \circ \phi = [\deg \phi] \circ \phi = \phi \circ [\deg \phi]$, and since ϕ is not constant we obtain that $\hat{\phi} \circ \phi = [\deg \phi]$.
Existence (useful?) □

By convention, the dual of the constant (zero) isogeny $E_1 \to E_2$ is the zero isogeny $E_2 \to E_1$.

Corollary 4.29. *The relation "being (K-)isogenous" is an equivalence relation on the set of elliptic curves (defined over K), where E_1 is isogenous to E_2 iff there exists a non-constant isogeny (defined over K) $\phi : E_1 \to E_2$.*

Proof. Reflexivity and transitivity are obvious, and the symmetry follows from the existence of dual isogenies. □

Proposition 4.30. *Let $V_p : E^\sigma \to E$ be the dual of the Frobenius isogeny Φ_p. Then V_p is separable iff E is ordinary.*

V_p is sometimes called the *Verschiebung* ("shift").

Proof. By definition, $V_p \circ \Phi_p = [\deg \Phi_p] = [p]$. Since $\deg[p] = p^2$ (see Theorem 4.25), by multiplicativity of the degree we find that $\deg V_p = p$. If V_p is separable then $|\ker V_p| = \deg V_p = p$, and since Φ_p is injective, $|\ker[p]| = p$ (ordinary case). If V_p is not separable then according to Theorem 4.20, there exists an isogeny ψ such that $V_p = \psi \circ \Phi_p$, and by looking at the degree we see that ψ is an isomorphism. So V_p is injective, and so is $[p]$, hence $E[p] = \{O\}$ (supersingular case). □

Note this proof shows that if E is supersingular then it is isomorphic to E^{σ^2}. As a consequence, the j-invariant of a supersingular elliptic curve always lies in $\mathbb{F}_{p^2}$.

For general knowledge, we state without proof the following result:

Theorem 4.31. *Two elliptic curves E_1 and E_2 defined over $\mathbb{F}_q$ are isogenous iff $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$.*

We will see more properties of the dual isogeny once we have defined pairings on elliptic curves.

5 Pairings

5.1 Weil reciprocity

Let C be a smooth algebraic curve.

Definition 5.1. *Let $D = \sum n_P(P) \in Div(C)$. The* support *of D is $Supp(D) = \{P \in C : n_P \neq 0\}$. Let $f \in \bar{K}(C)^*$ a function such that $Supp(\mathrm{div}(f)) \cap Supp(D) = \emptyset$ (i.e. $ord_P(f) = 0$ whenever $n_P \neq 0$). Then*

$$f(D) = \prod f(P)^{n_P}.$$

This is a well-defined element of $\bar{K}^*$ precisely because the supports are disjoint. Clearly, $(fg)(D) = f(D)g(D)$ and $f(D_1 + D_2) = f(D_1)f(D_2)$ (provided all supports are disjoint). Also, if C is defined over K, $f \in K(C)$ and $D \in Div_K(C)$ then $f(D) \in K^*$.

Theorem 5.2 (Weil reciprocity)**.** *Let $f, g \in \bar{K}(C)^*$ two functions such that $Supp(\mathrm{div}(f)) \cap Supp(\mathrm{div}(g)) = \emptyset$. Then*

$$f(\mathrm{div}\, g) = g(\mathrm{div}\, f).$$

Proof. We will just prove it for $C = \mathbb{P}^1$ (it is in fact always possible to reduce to that case but we will not do it here). Then $f = c\prod_i (x - a_i)^{n_i}$ and $g = d\prod_j (x - b_j)^{m_j}$. Their divisors are $\mathrm{div}\, f = \sum_i n_i(a_i) - (\sum_i n_i)(\infty)$ and $\mathrm{div}\, g = \sum_j m_j(b_j) - (\sum_j m_j)(\infty)$. Since the supports of these divisors have to be disjoint, we have $a_i \neq b_j\ \forall i, j$ and either $\sum_i n_i = 0$ or $\sum_j m_j = 0$; wlog we can assume that the former is true. Then $f(\mathrm{div}\, g) = \prod_j f(b_j)^{m_j}.f(\infty)^{-\sum_j m_j} = \prod_j (c\prod_i (b_j - a_i)^{n_i})^{m_j}.c^{-\sum_j m_j} = \prod_{i,j}(b_j - a_i)^{n_i m_j}$ and $g(\mathrm{div}\, f) = \prod_i g(a_i)^{n_i} = \prod_i (d\prod_j (a_i - b_j)^{m_j})^{n_i} = d^{\sum_i n_i}\prod_{i,j}(a_i - b_j)^{m_j n_i} = d^{\sum_i n_i}(-1)^{\sum_{i,j} n_i m_j}\prod_{i,j}(b_j - a_i)^{n_i m_j} = \prod_{i,j}(b_j - a_i)^{n_i m_j}$ since $\sum_i n_i = 0$. □

5.2 The Weil pairing

Let E be an elliptic curve defined over K and let m be an integer coprime to $char(K)$. Our goal is to define a map $E[m] \times E[m] \to \bar{K}$. We start as follows: let P and Q be two m-torsion points, and let D_P and D_Q be two divisors with disjoint supports such that $D_P \sim (P) - (O)$ and $D_Q \sim (Q) - (O)$ (a simple way of doing so is for instance to take $D_P = (P) - (O)$ and $D_Q = (Q + R) - (R)$ for some $R \in E$). Then according to Corollary 3.3, $mD_P \sim m(P) - m(O)$ is principal; let $f_P \in \bar{K}(E)$ be a function such that $\mathrm{div}\, f_P = mD_P$. Similarly, let f_Q be a function such that $\mathrm{div}\, f_Q = mD_Q$. Finally, we define the m-th *Weil pairing* of P and Q as

$$e_m(P, Q) = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

Proposition 5.3.

- *The Weil pairing $e_m(P, Q)$ is well-defined, i.e. does not depend of the choices of D_P, D_Q, f_P and f_Q.*
- *For any $P, Q \in E[m]$, $e_m(P, Q)^m = 1$.*

Proof. First, any function whose divisor is mD_P is of the form cf_P, $c \in \bar{K}^*$, and $(cf_P)(D_Q) = c^{\deg D_Q} f_P(D_Q) = f_P(D_Q)$ since $\deg D_Q = 0$. So the choice of the function f_P is irrelevant, and similarly for f_Q. Now if we replace D_P by a linearly equivalent divisor $D'_P = D_P + \mathrm{div}\, g$, then $mD'_P = mD_P + m\ \mathrm{div}\, g = \mathrm{div}(f_P g^m)$, so f_P is also replaced by $f'_P = f_P g^m$. Now

$$\frac{f'_P(D_Q)}{f_Q(D'_P)} = \frac{(f_P g^m)(D_Q)}{f_Q(D_P + \mathrm{div}\, g)} = \frac{f_P(D_Q)g^m(D_Q)}{f_Q(D_P)f_Q(\mathrm{div}\, g)} = e_m(P, Q)\frac{g(mD_Q)}{f_Q(\mathrm{div}\, g)} = e_m(P, Q)\frac{g(\mathrm{div}\, f_Q)}{f_Q(\mathrm{div}\, g)}$$

which is equal to $e_m(P,Q)$ according to Weil reciprocity law. The final value is then independent of the choice of D_P, and the same is of course true for D_Q.
The second statement also follows from Weil reciprocity law:

$$e_m(P,Q)^m = \frac{f_P(D_Q)^m}{f_Q(D_P)^m} = \frac{f_P(mD_Q)}{f_Q(mD_P)} = \frac{f_P(\operatorname{div} f_Q)}{f_Q(\operatorname{div} f_P)} = 1.$$

□

Exercice: let $P,Q \in E[m]$ and f_P, f_Q two functions such that $\operatorname{div} f_P = m(P) - m(O)$ and $\operatorname{div} f_Q = m(Q) - m(O)$. Show that

$$e_m(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \frac{f_Q(-S)}{f_Q(P-S)}$$

for any $S \notin \{O, P, -Q, P-Q\}$ (hint: apply the definition with $D_P = (P-S) - (-S)$ and $D_Q = (Q) - (O)$, and observe that $D_P = \tau_S^*((P) - (O))$).

We will denote by μ_m the set $\{\zeta \in \bar{K} : \zeta^m = 1\}$ of the m-th roots of unity; since m is coprime to $charK$ this is a cyclic group of cardinality m.

Proposition 5.4. *The Weil pairing $e_m : E[m] \times E[m] \to \mu_m \subset \bar{K}$ satisfies the following properties:*

- *Alternativity: $e_m(P,Q) = e_m(Q,P)^{-1}$ for all $P,Q \in E[m]$*
- *Bilinearity: $e_m([a]P_1+[b]P_2, Q) = e_m(P_1,Q)^a e_m(P_2,Q)^b$, and $e_m(P,[a]Q_1+[b]Q_2) = e_m(P,Q_1)^a e_m(P,Q_2)^b$ (for all...)*
- *Non-degeneracy: $\forall P \in E[m] \setminus \{O\}$, $\exists Q \in E[m]$ such that $e_m(P,Q) \neq 1$.*

Proof. The first point is obvious from the definition. Then linearity on the right side is an immediate consequence of linearity on the left side. Now as in the definition of the Weil pairing, let $D_1 \sim (P_1) - (O)$ and $D_2 \sim (P_2) - (O)$ such that their supports is disjoint from the one of $D_Q \sim (Q) - (O)$, and let f_1, f_2, f_Q be such that $\operatorname{div} f_i = mD_i$ and $\operatorname{div} f_Q = mD_Q$. Then $D' = aD_1 + bD_2$ is linearly equivalent to $([a]P_1 + [b]P_2) - (O)$, its support is disjoint from $SuppD_Q$, and $mD' = \operatorname{div}(f')$ where $f' = f_1^a f_2^b$. So

$$e_m([a]P_1 + [b]P_2, Q) = \frac{f'(D_Q)}{f_Q(D')} = \frac{(f_1^a f_2^b)(D_Q)}{f_Q(aD_1 + bD_2)} = \frac{f_1(D_Q)^a f_2(D_Q)^b}{f_Q(D_1)^a f_Q(D_2)^b} = e_m(P,Q_1)^a e_m(P,Q_2)^b.$$

Non-degeneracy is harder and will be admitted. □

Corollary 5.5. *There exist $P,Q \in E[m]$ such that $e_m(P,Q)$ is a primitive m-th root of unity. In particular, if $E[m] \subset E(K)$ then $\mu_m \subset K$.*

Proof. Let P,Q such that $E[m] = \langle P,Q \rangle$ and $\zeta = e_m(P,Q)$. If ζ is not primitive, i.e. $\zeta^d = 1$ for $d|m$, $d \neq m$, then the bilinearity implies that $e_m([d]P,R) = 1$ for all $R \in E[m]$, which contradicts the non-degeneracy. Now if $E[m] \subset E(K)$, then D_Q and D_P can be chosen in $Div_K(E)$, similarly f_P and f_Q can be chosen in $K(E)$, so that $e_m(P,Q) \in K^*$. □

Corollary 5.6. *$E(F_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ where $n_1|n_2$ and $n_1|q-1$.*

Proof. The fundamental theorem of abelian groups and Theorem 4.25 already imply that $E(F_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with $n_1|n_2$ and $p \wedge n_1 = 1$. Now $E[n_1] \subset E(F_q)$, so μ_{n_1} is a subgroup of $\mathbb{F}_q^*$. (Note that $n_1 = 1$ is permitted). □

Alternativity (and non-degeneracy) can be useful to test if two points $P_1, P_2 \in E[m]$ belong to a common cyclic subgroup of $E[m]$: it is the case iff $e_m(P_1, P_2) = 1$. But it also means that there are no cyclic subgroups of $E[m]$ on which e_m is non trivial.

5.3 The Tate pairing

For practical applications, the Tate-Lichtenbaum pairing (or Tate pairing for short) is a second pairing which is more often used; we will see that it can be computed approximately twice as fast as the Weil pairing.

Let E be an elliptic curve defined over K, m an integer coprime to $char(K)$, $P \in E(K)[m]$ and $Q \in E(K)$. As for the Weil pairing, we consider divisors $D_P \sim (P) - (O)$ and $D_Q \sim (Q) - (O)$ defined over K, and a function $f_P \in K(E)^*$ such that $\operatorname{div} f_P = mD_P$. The Tate pairing of P and Q is simply defined as

$$\tau_m(P, Q) = f_P(D_Q).$$

Is it well-defined? Since $\deg D_Q = 0$, this value does not depend of the choice of f_P. But if we replace D_P by $D_P + \operatorname{div} g$, then f_P is replaced by $f'_P = f_P g^m$, and

$$f'_P(D_Q) = (f_P g^m)(D_Q) = f_P(D_Q)(g(D_Q))^m = \tau_m(P, Q)(g(D_Q))^m.$$

Similarly, if we replace D_Q by $D'_Q = D_Q + \operatorname{div} g$, then

$$f_P(D'_Q) = f_P(D_Q + \operatorname{div} g) = f_P(D_Q) f_P(\operatorname{div} g) = \tau_m(P, Q) g(\operatorname{div} f_P) = \tau_m(P, Q) g(mD_P) = \tau_m(P, Q)(g(D_P))^m.$$

So we see that it is defined only up to a m-th power: $\tau_m : E(K)[m] \times E(K) \to K^*/(K^*)^m$. We can now show as we have done for Weil that τ_m is bilinear:

$$\tau_m([a]P_1 + [b]P_2, [c]Q_1 + [d]Q_2) = \tau_m(P_1, Q_1)^{ab} \tau_m(P_1, Q_2)^{ad} \tau_m(P_2, Q_1)^{bc} \tau_m(P_2, Q_2)^{bd}$$

But then it is not necessarily non-degenerate: if $Q = E(K)$ is equal to $[m]Q'$, $Q' \in E(K)$, then for all $P \in E(K)[m]$, $\tau_m(P, Q) = \tau_m(P, [m]Q') = \tau_m(P, Q')^m = 1$ in $K^*/(K^*)^m$. Thus the second factor will be considered modulo multiple of m, i.e. in the quotient $E(K)/[m]E(K)$.

Proposition 5.7. *The Tate pairing is a well-defined bilinear map*

$$\begin{array}{rcl} \tau_m : E(K)[m] \times E(K)/[m]E(K) & \to & K^*/(K^*)^m \\ (P, Q) & \mapsto & f_P(D_Q) \end{array}$$

Note that it is very possible that either of $E(K)[m]$, $E(K)/[m]E(K)$ and $K^*/(K^*)^m$ can be a trivial group, so that τ_m is constant...

If $K = \mathbb{F}_q$ is a finite field then we can say more about the Tate pairing. Assume for simplicity that m is prime. Then $(\mathbb{F}_q^*)^m \neq \mathbb{F}_q^*$ iff $x \mapsto x^m$ is not surjective iff $x \mapsto x^m$ is not injective (since the field is finite) iff $m|(q-1)$. If this is not the case, in order to obtain a non-trivial pairing we must consider an extension $\mathbb{F}_{q^k}$ such that $m|(q^k - 1)$.

Definition 5.8. *Let $E_{|\mathbb{F}_q}$ be an elliptic curve and m an integer coprime to p. The* embedding degree *(relative to m and q) is the smallest positive integer k such that $m|(q^k - 1)$.*

Rk: k is actually the multiplicative order of q modulo m, so $k|\varphi(m) = m - 1$. This means that for "random" m and q, we can expect k to be of the order of m.

Property 5.9. *If $m|(q^k-1)$, then the map $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^m \to \mathbb{F}_{q^k}^*, \bar{x} \mapsto x^{(q^k-1)/m}$ is injective, and its image is μ_m.*

Proof. Exercise. □

Thus we can get rid of the quotient by doing a final exponentiation.

Definition 5.10. *The modified Tate pairing is the map*

$$\begin{aligned}\langle .,.\rangle_m : E(\mathbb{F}_{q^k})[m] \times E(\mathbb{F}_{q^k})/[m]E(\mathbb{F}_{q^k}) &\to \mu_m \subset \mathbb{F}_{q^k}^* \\ (P,Q) &\mapsto f_P(D_Q)^{(q^k-1)/m}\end{aligned}$$

Note: this final exponentiation is also important for security reasons (it conceals the actual representative of the coset in $K^*/(K^*)^m$).

Theorem 5.11 (Admitted)**.** *Let $m \neq p$ be a prime number such that $m|E(\mathbb{F}_q)$ and k the corresponding embedding degree. The (modified) Tate pairing*

$$\langle .,.\rangle_m : E(\mathbb{F}_{q^k})[m] \times E(\mathbb{F}_{q^k})/[m]E(\mathbb{F}_{q^k}) \to \mu_m \subset \mathbb{F}_{q^k}^*$$

is non degenerate, i.e. for all $P \in E(\mathbb{F}_{q^k})[m]$, $P \neq O$, there exists $Q \in E(\mathbb{F}_{q^k})$ such that $\langle P,Q\rangle_m \neq 1$, and for all $Q \in E(\mathbb{F}_{q^k})$, $Q \notin [m]E(\mathbb{F}_{q^k})$, there exists $P \in E(\mathbb{F}_{q^k})[m]$ such that $\langle P,Q\rangle_m \neq 1$.

The same result is of course true for the original pairing.

We would also like to simplify the second group, and this is usually possible:

Proposition 5.12. *Assume that $E(\mathbb{F}_{q^k})[m^2] = E(\mathbb{F}_{q^k})[m]$, i.e. there are no $\mathbb{F}_{q^k}$-rational points of order exactly m^2. Then the map*

$$E(\mathbb{F}_{q^k})[m] \to E(\mathbb{F}_{q^k})/[m]E(\mathbb{F}_{q^k})$$

that sends a m-torsion point to its equivalence class is a bijection.

Proof. We consider first the multiplication-by-m map $[m] : E(K) \to E(K)$. It image is precisely $[m]E(K)$ and its kernel $E(K)[m]$, so there is an isomorphism $E(K)/E(K)[m] \simeq [m]E(K)$. Hence $|[m]E(K)| = |E(K)|/|E(K)[m]|$, which implies that $|E(K)[m]| = |E(K)|/|[m]E(K)|$, i.e. $E(K)[m]$ and $E(K)/[m]E(K)$ have the same cardinality (note that this is always true as sons as $E(K)$ is finite). Thus the map $E(K)[m] \to E(K)/[m]E(K)$ is an isomorphism iff it is injective. Its kernel is exactly $E(K)[m] \cap [m]E(K)$, i.e. the set of m-torsion points that are also multiple of m, and this is $\{O\}$ if there are no points of order m^2. □

The assumption of this proposition is satisfied in many situations relevant for cryptography, so we obtain as for the Weil pairing a bilinear map $E(K)[m] \times E(K)[m] \to \mu_m$.

Note: other pairings exist (Ate, eta,...) and are sometimes more suitable for crypto applications.

Exercise: let $E|\mathbb{F}_q$ be an elliptic curve such that $|E(\mathbb{F}_q)| = q-1$, and assume that $q-1$ is almost prime, i.e. is of the form cm where m is a prime and c is a small cofactor. Show that there is a non-degenerate bilinear *self-pairing* $G_1 \times G_1 \to G_2$ where G_1 is a cyclic order m subgroup of E and G_2 is a cyclic order m subgroup of $\mathbb{F}_q^*$. Such "trace 2" curves are interesting but difficult to come by.

5.4 Miller's algorithm

To compute the Weil or Tate pairing, we need to compute expressions of the form $f_P(Q+S)/f_P(S)$ where f_P is a function such that $\operatorname{div} f_P = m(P) - m(O)$. In order to achieve this, we compute by induction functions f_i such that

$$\operatorname{div} f_i = (i(P) - i(O)) - (([i]P) - (O)) = i(P) - ([i]P) - (i-1)(O).$$

Assume such functions f_i and f_j are known. Then $\operatorname{div} f_i f_j = (i+j)(P) - ([i]P) - ([j]P) - (i+j-2)(O)$, which is not far from what we want for $\operatorname{div} f_{i+j}$. Let $\ell_{i,j}$ be the equation of the straight line through $[i]P$ and $[j]P$ (or the tangent if both points are equal) and v_{i+j} the equation of the vertical line through $[i+j]P$. Then $\operatorname{div} \ell_{i,j} = ([i]P) + ([j]P) + ([-i-j]P) - 3(O)$ and $\operatorname{div} v_{i+j} = ([i+j]P) + ([-i-j]P) - 2(O)$, so that

$$\begin{aligned}\operatorname{div} f_i f_j \ell_{i,j}/v_{i+j} &= (i+j)(P) - ([i]P) - ([j]P) - (i+j-2)(O) \\ &\quad +([i]P) + ([j]P) + ([-i-j]P) - 3(O) \\ &\quad -([i+j]P) - ([-i-j]P) + 2(O) \\ &= (i+j)(P) - ([i+j]P) - (i+j-1)(O)\end{aligned}$$

so we can take $f_{i+j} = \frac{f_i f_j \ell_{i,j}}{v_{i+j}}$. Thus we can compute $f_P = f_m$ starting from $f_1 = 1$ with a double-and-add algorithm. In practice, computing the rational function f_P is out of the question, but we will evaluate all expressions at Q (or $Q+S$, or S) throughout.

Algorithm 2: Miller's algorithm

```
Input  : $E$, $m = (m_l ... m_0)_2 \in \mathbb{N}^*$, $P \in E[m]$, $Q \in E$
Output: $f_P(Q)$ where div $f_P = m(P) - m(O)$
$T \leftarrow P$, $f \leftarrow 1$
for $k = l - 1$ down to 0 do
    $\ell \leftarrow$ tangent at $T$
    $v \leftarrow$ vertical line at $[2]T$
    $T \leftarrow [2]T$
    $f \leftarrow f^2 \ell(Q)/v(Q)$
    if $m_k = 1$ then
        $\ell \leftarrow$ line through $T$ and $P$
        $v \leftarrow$ vertical line at $T + P$
        $T \leftarrow T + P$
        $f \leftarrow f \ell(Q)/v(Q)$
return $f$
```

Rk: the algorithm fails if Q is a zero of ℓ or v at some step, i.e. if $Q = \pm T$ at some step. So there are approximately $O(\log m)$ inputs for which Miller's algorithm fails, but this can be easily detected. Then one can either change the parameters, work with another linearly divisor, or use another addition chain.

Improvements (important!):

- use ℓ and v to compute $[2]T$ or $T+P$ (this is a no-brainer)
- postpone all divisions until the end by computing numerators and denominators separately

- still less divisions: use projective coordinates for T (but not for P or Q)
- if the goal is to compute something like $f_P(Q+S)/f_P(S)$, adapt the algorithm to do it in one pass
- security check: $T=O$ at the end if the order of P is correct

Complexity: $\log m$ steps. If P and Q are in $E(\mathbb{F}_{q^k})$ then each step costs $O((\log(q^k))^3)$ (because of the division required for ℓ), so total in $O(\log m\, k^3 \log^3 q)$. But if only Q is in $E(\mathbb{F}_{q^k})$ and $P \in E(\mathbb{F}_q)[m]$, then there is only one division in $\mathbb{F}_{q^k}$ at the end, and the complexity reduces to $O(\log m(\log^3 q + \log^2(q^k))) = O(\log m \log^2 q(\log q + k^2)))$. (Note that $\log m \approx \log q$ in most applications).

Rk: the complexity is exponential in the size of k. This means that this computation is feasible only if k is not too big. But we have seen that for "random" parameters, k is expected to have approximately the same size as m. If m is close to $E(\mathbb{F}_q) \approx q$, then the Weil or Tate pairing cannot be computed! (The result which lies in $\mu_m \subset \mathbb{F}_{q^k}$ could not be expressed anyway.)

Rk: the function f_P returned by Miller's algorithm has an interesting property. In the local ring at O, a preferred uniformizer is $z = x/y$, and since $ord_O(f_P) = -m$, $f_0 = (x/y)^m f_P$ is defined at O and satisfies $f_0(O) \neq 0$. If all line equations in the algorithm are taken of the form $y - \lambda x - \mu = 0$ or $x - x_0 = 0$, then f_P is *normalized* at infinity, i.e. $f_0(O) = 1$. This allows to simplify some computations:

Proposition 5.13. *Let $P \in E(\mathbb{F}_{q^k})[m] \setminus \{O\}$ and $Q \in E(\mathbb{F}_{q^k}) \setminus \{O, P\}$. If f_P satisfies $\operatorname{div} f_P = m(P) - m(O)$ and is normalized at infinity, then*

$$\langle P, Q\rangle_m = f_P(Q)^{(q^k-1)/m}.$$

If Q is a m-torsion point and f_Q satisfies $\operatorname{div} f_Q = m(Q) - m(O)$ and is normalized at infinity, then

$$e_m(P,Q) = (-1)^m \frac{f_P(Q)}{f_Q(P)}.$$

These formulas are always use in practice since they speed up the computations.

Proof. For Tate: we know that $\langle P, Q\rangle_m = (f_P(Q+S)/f_P(S))^{(q^k-1)/m} = (f_P \circ \tau_Q(S)/f_P(S))^{(q^k-1)/m}$. The divisor of $f_P \circ \tau_Q / f_P$ is $\operatorname{div} f_P \circ \tau_Q / f_P = \tau_Q^* \operatorname{div}(f_P) - \operatorname{div} f_P = m(P-Q) - m(-Q) - m(P) + m(O)$. Let ℓ be the line (of equation $y - \lambda x - \mu = 0$) through P and $-Q$ and v the vertical line (of equation $x - x0 = 0$) through $P-Q$. Then $\operatorname{div} \ell/v = (P) + (-Q) + (Q-P) - 3(O) - (P-Q) - (Q-P) + 2(O) = (P) + (-Q) - (P-Q) - (O)$. In particular, $f_P \circ \tau_Q / f_P$ and $(v/\ell)^m$ have the same divisor, so there exists $c \in \mathbb{F}_{q^k}$ such that $f_P \circ \tau_Q / f_P = c(v/\ell)^m$. The $(v/\ell)^m$ part is the one that has a pole in O but since it is a m-th power this does not impact the final resut. More precisely,

$$\langle P, Q\rangle_m = (f_P \circ \tau_Q(S)/f_P(S))^{(q^k-1)/m} = (c(v(S)/\ell(S))^m)^{(q^k-1)/m} = c^{(q^k-1)/m}.$$

Now c is the value of the constant map $f_P \circ \tau_Q \times (\ell/v)^m / f_P$, that we want to evaluate at O. Since f_P and $(\ell/v)^m$ have both a normalized pole of order m at O, their quotient is a defined function at O with value 1, and thus $c = f_P \circ \tau_Q(O) = f_P(Q)$.

For Weil: we have seen (in exercise) that $e_m(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \frac{f_Q(-S)}{f_Q(P-S)}$. In particular, the function $(f_P \circ \tau_Q \times f_Q \circ [-1])/(f_P \times f_Q \circ \tau_P \circ [-1])$ is constant. At the point at infinity O, $f_P \circ \tau_Q$ and $f_Q \circ \tau_P \circ [-1]$ are defined and do not vanish, and f_P and f_Q have a normalized pole of order m. This means that $f_Q = (x/y)^{-m}(1+f_1)$ where $f_1(O) = 0$. So $f_Q \circ [-1] = (-x/y)^{-m}(1 + f_1 \circ [-1]) = (-1)^m (x/y)^{-m}(1 + f_1 \circ [-1])$. Evaluating everything in O, we obtain $e_m(P,Q) = (-1)^m f_P(Q)/f_Q(P)$. □

Toy example: $E : y^2 = x^3 + 7$ over $\mathbb{F}_{13}$. Then $E(\mathbb{F}_{13}) \simeq \mathbb{Z}/7\mathbb{Z}$; we take of course $m = 7$, and $k = 2$ (since $7 \nmid (13-1)$, but $13^2 - 1 = 168 = 7 \times 24$). Let $P = (11, 5) \in E$, we can compute f_P with Miller's algorithm. For reference, the tangent at (x_T, y_T) is $y - \frac{3x_T^2}{2y_T}(x - x_T) - y_T$ and the line through (x_T, y_T) and P is $y - \frac{5-y_T}{11-x_T}(x - x_T) - y_T$.

- first step: $\ell = y + 4x + 1$, $v = x - 7$, $T = [2]P = (7, 5)$, $f = \frac{y+4x+3}{x-7}$
- second step: $\ell = y + 8$, $v = x - 8$, $T = [3]P = (8, 8)$, $f = \frac{(y+4x+3)(y+8)}{(x-7)(x-8)}$
- third step: $\ell = y + x + 10$, $v = x - 11$, $T = [6]P = (11, 8)$, $f = \frac{(y+4x+3)^2(y+8)^2(y+x+10)}{(x-7)^2(x-8)^2(x-11)}$
- fourth step: $\ell = x - 11$, $v = 1$, $T = [7]P = O$, $f = \frac{(y+4x+3)^2(y+8)^2(y+x+10)}{(x-7)^2(x-8)^2}$

Of course, this should be evaluated at each step. Now, we find that $E(\mathbb{F}_{13^2}) \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/21Z$. Let $Q = (4, 7t + 10) \in E(\mathbb{F}_{13^2})[7]$, where $t \in \mathbb{F}_{13^2}$ is such that $t^2 + t - 1 = 0$. Then $f_P(Q) = 7t + 5$, and $\langle P, Q\rangle_7 = (7t + 5)^{24} = 5t$.

5.5 The embedding degree

We recall that the embedding degree (relative to m and q) is the smallest integer k such that $m|q^k - 1$. If E is defined over $\mathbb{F}_q$ and m is a (the) large prime divisor of $|E(\mathbb{F}_q)|$ then k is sometimes referred to by abuse of language as the embedding degree of E. This is the degree of the smallest field extension of $\mathbb{F}_q$ which contains the group μ_m of m-th roots of unity, so controls in which field the pairing will have values. But it is also related to the field extension over which E has m-torsion points.

Proposition 5.14. *Let $E_{|\mathbb{F}_q}$ an elliptic curve, $m \neq p$ a prime, and k its embedding degree.*

- *If $|E(\mathbb{F}_{q^n})[m]| = m^2$ then $\mu_m \subset \mathbb{F}_{q^n}$, i.e. $k|n$ (Weil).*
- *Conversely, if $m||E(\mathbb{F}_q)|$ and $k > 1$, then $|E(\mathbb{F}_{q^k})[m]| = m^2$ (Balasubramanian-Koblitz).*

We have already seen the first point, which results from the non degeneracy of the Weil pairing. The second point is interesting: it means that if E has $\mathbb{F}_q$-rational m-torsion point, then $\mathbb{F}_{q^k}$ is the smallest extension over which its full m-torsion is defined (provided $k > 1$). Note that in applications, the hypothesis $m||E(\mathbb{F}_q)|$ is always satisfied, and very often $m^2 \nmid |E(\mathbb{F}_q)|$. If $k > 1$ then $m^2||E(\mathbb{F}_{q^k})|$ but also very often $m^3 \nmid E(\mathbb{F}_{q^k})$, in which case Proposition 5.12 applies.

In practice, computations are only possible if k is small, which is *not* typically the case. An important exception consists of supersingular curves.

Theorem 5.15 (Admitted). *Let E be supersingular elliptic curve defined over $\mathbb{F}_{p^d}$, and m a prime different from p such that $E(\mathbb{F}_{p^d})[m] \neq O$ (i.e. $m||E(\mathbb{F}_{p^d})$).*

- *If $p = 2$ then $k \leq 4$;*
- *if $p = 3$ then $k \leq 6$;*
- *if $p \geq 5$ then $k \leq 3$; if furthermore $d = 1$ then $k \leq 2$.*

All the above bounds on k are sharp, i.e. the upper bounds can be obtained for some choices of $\mathbb{F}_{p^d}$, E and m.

Other families of "pairing-friendly" curves (i.e. curves with a prescribed small embedding degree) have been discovered these last years (MNT curves, BN curves, etc) but this is still an active domain of research.

5.6 Self-pairing and distortion maps

In ECC, since the main problem is the DLP, the focus is essentially on cyclic (sub)groups. If $E_{|\mathbb{F}_q}$ is an elliptic curve used in cryptography, then we are principally interested in its subgroup G of large prime order m, generated by a point $P \in E(\mathbb{F}_q)$. Then $G \subset E[m]$, but $E[m]$ is not cyclic, and except in special cases $E(\mathbb{F}_{q^k})[m]$ is not cyclic either. So for applications we would like to have a bilinear, non-degenerate pairing $G \times G \to \mu_m$. This is generally not directly possible: the Weil pairing is alternating so is automatically trivial when restricted to $G \times G$; for the Tate pairing, $\langle P, P\rangle_m \in \mathbb{F}_q^* \cap \mu_m = \{1\}$ if $k > 1$. So in general (and with the exception of the trace 2 curves), we have to consider a second cyclic subgroup $G' \subset E(\mathbb{F}_{q^k})[m]$ (or $\subset E(\mathbb{F}_{q^k})/[m]E(\mathbb{F}_{q^k})$) of order m to obtain a restricted bilinear pairing

$$G \times G' \to \mu_m \subset \mathbb{F}_{q^k}^*$$

which is not degenerate.

A possible workaround is the use of distortion maps, introduced by Verheul. If ϕ is an endomorphism of E (i.e. an isogeny $E \to E$), then for any $Q \in E[m]$, $\phi(Q) \in E[m]$ (this is because $\phi \circ [m] = [m] \circ \phi$). Suppose there exists an endomorphism ϕ such that $\phi(P) \in E[m] \setminus G$. Then we can construct a non-degenerate self-pairing

$$\begin{array}{rcl} G \times G & \to & \mu_m \\ (P_1, P_2) & \mapsto & e_m(P_1, \phi(P_2)) \end{array}$$

Such an endomorphism ϕ is called a *distortion map*; distortion maps always exist if E is supersingular.

If $k > 1$ and ϕ is a distortion map, then $\phi(P) \in E(\mathbb{F}_{q^k}) \setminus E(\mathbb{F}_q)$. Let Φ_q be the q-th Frobenius; it is also an endomorphism of E. Then $\phi \circ \Phi_q(P) = \phi(P)$ but $\Phi_q \circ \phi(P) \neq \phi(P)$ since P is $\mathbb{F}_q$-rational but $\phi(P)$ is not. We will see later that this fact (that there exist two endomorphisms of E that do not commute) implies that E is supersingular.

Example: let $E : y^2 = x^3 + ax$ be an elliptic curve defined over $\mathbb{F}_p$, $p \equiv 3 \bmod 4$. Then -1 is not a square in $\mathbb{F}_p$. Let $i \in \mathbb{F}_{p^2}$ be such that $i^2 = -1$; a distortion map for E is given by $\phi : (x, y) \mapsto (-x, iy)$.

5.7 Transfer of DLP and security implications

As seen in Elbaz-Vincent's lectures, pairings have a constructive and a destructive aspect in cryptology. They allow new asymmetric protocols (IBE, short signatures, etc) but they can also threaten the DLP.

More precisely, let $E_{|\mathbb{F}_q}$ be an elliptic curve and let $G \subset E(\mathbb{F}_q)$ be a prime order m subgroup. Suppose we want to use the DL in G as a cryptographic primitive, so m is large enough to prevent generic attacks. But we can use pairings to transfer the DLP from G to $\mathbb{F}_{q^k}^*$. Let d be a secret integer, $P_0 \in G \setminus \{O\}$, and $P_1 = [d]P_0$. Since $G \subset E[m]$, and because of the non-degeneracy, there exists Q in

$E(\mathbb{F}_{q^k})[m]$ (resp. in $E(\mathbb{F}_{q^k})/[m]E(\mathbb{F}_{q^k})$) such that $e_m(P_0, Q) \neq 1$ (resp. $\langle P_0, Q\rangle_m \neq 1$). Then

$$e_m(P_1, Q) = e_m([d]P_0, Q) = e_m(P_0, Q)^d.$$

So d can be recovered (at least theoretically) by solving the DLP in $\mathbb{F}_{q^k}^*$. In particular, the DLP in G is no more difficult than the DLP in $\mathbb{F}_{q^k}^*$! This is very important because for finite fields, index calculus attacks have a subexponential complexity, in $L_{q^k}(1/3)$, whereas generic attacks have complexity in $O(\sqrt{m})$. In particular, if m is close to q and k is small, then $L_{q^k}(1/3) \ll \sqrt{m}$, so the DLP on G is much less secure than expected.

Security implications:

- For non-pairing based ECC, setup: $E_{|\mathbb{F}_q}$, $G \subset E(\mathbb{F}_q)$ subgroup of large prime order m. In order to be safe against this transfer by pairing it is enough to check that the embedding degree k is large (which is very often the case anyway). Do not use supersingular curves.

- For pairing-based ECC, setup: $E_{|\mathbb{F}_q}$, $G \subset E(\mathbb{F}_q)$ subgroup of large prime order m, $G' \subset E(\mathbb{F}_{q^k})$ (or $E(\mathbb{F}_{q^k})/[m]E(\mathbb{F}_{q^k})$) another order m subgroup, pairing $G \times G' \to \mu_m \subset \mathbb{F}_{q^k}$. The embedding degree must not be too large, but the DLP must be hard both in G and in $\mathbb{F}_{q^k}^*$. More precisely, to achieve a security level of s bits, m (and hence q) must be larger than 2^{2s}, and q^k must be large enough so that $L_{q^k}(1/3) > 2^s$; for a given k this gives a second lower bound on q. For efficiency it is better if the bounds on q and m are close (smaller key sizes), so there is a best choice of k for each security level. This optimal k increases with the security level, and this motivates the search for pairing-friendly curves other than supersingular curves which are limited to $k = 6$.

Security			$\vert q\vert_2$ for $k =$								
level (in bits)	$\vert m\vert_2$	$\vert q^k\vert_2$	2	3	4	6	8	10	12	20	30
64	128	816	408	272	204	**136**	102	82	68	41	27
80	160	1248	624	416	312	208	**156**	125	104	62	42
96	192	1776	888	592	444	296	**222**	177	148	89	52
112	224	2432	1216	811	608	405	304	**243**	203	122	81
128	256	3248	1624	1083	812	541	406	325	**271**	162	108
192	384	7936	3968	2645	1984	1323	992	794	661	**397**	265
256	512	15424	7712	5141	3856	2571	1928	1542	1285	771	**514**

5.8 Isogenies and pairings

Proposition 5.16 (Admitted)**.** *Let $\phi : E_1 \to E_2$ an isogeny and m an integer coprime to char$K$. Then for any $P \in E_1[m]$ and $Q \in E_2[m]$,*

$$e_m(\phi(P), Q) = e_m(P, \hat{\phi}(Q)).$$

Note that the two pairings take place on different curves: E_2 for the left-hand side and E_1 for the right-hand side.

Corollary 5.17.

- *Let ψ, ϕ two isogenies $E_1 \to E_2$. Then $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$.*

- $\widehat{[n]} = [n]$ *for any $n \in \mathbb{Z}$.*

- $\deg[n] = n^2$

- $\hat{\hat{\phi}} = \phi$
- $\deg \hat{\phi} = \deg \phi$

Proof. Let P be any point of $E_2[m]$ where m is coprime to $charK$. Then for any $Q \in E_1[m]$, $e_m(Q, \widehat{\psi + \phi}(P)) = e_m((\psi + \phi)(Q), P) = e_m(\psi(Q), P)e_m(\phi(Q), P) = e_m(Q, \hat{\psi}(P))e_m(Q, \hat{\phi}(P)) = e_m(Q, (\hat{\psi} + \hat{\phi})(P))$. In particular, $e_m(Q, (\widehat{\psi + \phi} - \hat{\psi} - \hat{\phi})(P)) = 1$ for all $Q \in E_1[m]$. The non-degeneracy of the Weil pairing then implies that $(\widehat{\psi + \phi} - \hat{\psi} - \hat{\phi})(P) = O$. In other words, any point of E_2 whose order is coprime to $charK$ is in $\ker(\widehat{\psi + \phi} - \hat{\psi} - \hat{\phi})$, which is thus infinite. But a non-constant isogeny has a finite kernel, so $\widehat{\psi + \phi} - \hat{\psi} - \hat{\phi} = 0$, i.e. $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$. Now it is clear that $\widehat{[1]} = [1]$, so an immediate induction using the previous point yields $\widehat{[n]} = [n]$ for any $n \in \mathbb{Z}$. In particular, and by definition of the dual isogeny, $[\deg[n]] = [n] \circ \widehat{[n]} = [n] \circ [n] = [n^2]$, so $\deg[n] = n^2$.
For the last two points: we know that $\phi \circ \hat{\phi} = [\deg \phi]$. So $\widehat{\phi \circ \hat{\phi}} = \hat{\hat{\phi}} \circ \hat{\phi} = \widehat{[\deg \phi]} = [\deg \phi] = \phi \circ \hat{\phi}$, thus $\hat{\hat{\phi}} = \phi$. It follows that $[\deg \phi] = \phi \circ \hat{\phi} = \hat{\hat{\phi}} \circ \hat{\phi} = [\deg \hat{\phi}]$, so $\deg \hat{\phi} = \deg \phi$. □

Rk: this gives a second proof of the fact that $\deg[n] = n^2$. Except that it relies on the Weil pairing, and the proof of its non degeneracy requires some knowledge about the structure of the n-torsion, which in our case came from knowing the degree of $[n]$... But there is a way of making this work.

6 Point counting

6.1 The endomorphism ring

Definition 6.1. *An* endomorphism *of an elliptic curve E is an isogeny from $E \to E$. We denote by $End_K(E)$ the set of all endomorphisms of E defined over K, and $End(E) = End_{\bar{K}}(E)$.*

Proposition 6.2. *$End(E)$ (resp. $End_K(E)$) is a characteristic zero domain for the operations $+$ and $\circ$, with an anti-involution $\widehat{\ }$.*

Proof. Clearly $(End(E), +)$ is a group and $\circ$ is a well-defined composition law. Now $(\phi_1 + \phi_2) \circ \psi = \phi_1 \circ \psi + \phi_2 \circ \psi$ by definition, and $\psi \circ (\phi_1 + \phi_2) = \psi \circ \phi_1 + \psi \circ \phi_2$ because ψ group morphism, so $(End(E), +, \circ)$ is a ring. It is a domain since if $\phi \circ \psi = 0$, then $0 = \deg(\phi \circ \psi) = \deg \phi \times \deg \psi$, so either $\deg \phi = 0$ or $\deg \psi = 0$, i.e. $\phi = 0$ or $\psi = 0$.
To say that $char(End(E)) = 0$ means that the map $\mathbb{Z} \to End(E)$, $m \mapsto [m]$ is injective; equivalently, $[m]$ is not constant for any $m > 0$, and we have proved that before.
Finally, $\widehat{\ }$ is indeed an anti-involution since it sends endomorphisms to endomorphisms (clear), $\hat{\hat{\phi}} = \phi$, $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$ and $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$ □

So $\mathbb{Z} \subset End_K(E)$ for any elliptic curve E. If $char(K) = 0$, usually there exist no other endomorphisms; if $End(E) \neq \mathbb{Z}$ then E is said to have complex multiplication. Complex multiplication is an important topic for constructing curves (over finite fields) with subgroups of prescribed large prime order. If E is defined over a finite field $K = \mathbb{F}_q$ then $\Phi_q \in End_K(E)$ and one can show that $End_K(E)$ is always bigger than $\mathbb{Z}$ (even in the uncommon case where $\Phi_q = [\sqrt{q}] \in \mathbb{Z}$).

Rk: we have seen with the distortion maps examples where $End(E)$ is strictly larger that $End_K(E)$. But if E is defined over $\mathbb{F}_q$, we have showed that $End(E) \neq End_{\mathbb{F}_q}(E)$ implies that $End(E)$ is not commutative, which only happens in the supersingular case.

6.2 Trace and characteristic polynomial

A very important result is that it is possible to define a degree 2 characteristic polynomial for any element of $End(E)$. When applied to Φ_q, this will be the basis of every point-counting algorithm.

Theorem 6.3. *Let $\phi \in End(E)$. Then ϕ satisfies the relation*

$$\phi \circ \phi - [\mathrm{tr}(\phi)] \circ \phi + [\deg \phi] = 0$$

where the integer $\mathrm{tr}(\phi) \in \mathbb{Z}$*, called the* trace *of ϕ, is given by* $\mathrm{tr}(\phi) = 1 + \deg \phi - \deg([1] - \phi)$*.*

This formula is often shortened as $\phi^2 - \mathrm{tr}(\phi)\phi + \deg \phi = 0$. The polynomial $X^2 - \mathrm{tr}(\phi)X + \deg \phi$ is called the *characteristic polynomial* of ϕ.

Proof. Let m be a prime different from $charK$. Then $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$; in other words, $E[m]$ is a $\mathbb{Z}/m\mathbb{Z}$-vector space of dimension 2. Now if $P \in E[m]$, then $[m]\phi(P) = \phi([m]P) = O$, so ϕ can be restricted as a map $\phi_m : E[m] \to E[m]$, and it is easy to check that this map is actually $\mathbb{Z}/m\mathbb{Z}$-linear. If we choose a basis $\{P_1, P_2\}$ of $E[m]$, then ϕ_m can represented by a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/m\mathbb{Z})$. First-year linear algebra states that ϕ_m is annihilated by its characteristic polynomial $X^2 - \mathrm{tr}(\phi_m)X + \det(\phi_m)$ where $\det(\phi_m) = \det(M) \in \mathbb{Z}/m\mathbb{Z}$ and $\mathrm{tr}(\phi_m) = \mathrm{tr}(M) \in \mathbb{Z}/m\mathbb{Z}$. So if we identify elements of $\mathbb{Z}/m\mathbb{Z}$ with their representatives in $\mathbb{Z}$, then for all $P \in E[m]$, $\phi(\phi(P)) - [\mathrm{tr}(\phi_m)]\phi(P) + [\det \phi_m]P = O$.

The next step is to show that $\det(\phi_m) \equiv \deg(\phi) \bmod m$, using the Weil pairing. Indeed,

$$\begin{aligned} e_m(P_1, P_2)^{\deg \phi} &= e_m([\deg \phi]P_1, P_2) = e_m((\hat{\phi} \circ \phi)(P_1), P_2) = e_m(\phi(P_1), \phi(P_2)) \\ &= e_m([a]P_1 + [c]P_2, [b]P_1 + [d]P_2) = e_m(P_1, P_1)^{ab} e_m(P_1, P_2)^{ad} e_m(P_2, P_1)^{bc} e_m(P_2, P_2)^{bd} \\ &= e_m(P_1, P_2)^{ad-bc} = e_m(P_1, P_2)^{\det(\phi_m)}. \end{aligned}$$

Since $e_m(P_1, P_2)$ is a primitive m-th root of unity, this shows that $\deg \phi \equiv \det(\phi_m) \bmod m$ for every prime $m \neq charK$ and every endormorphism of E.
Now an elementary calculation shows that if M is a 2×2 matrix, then $\mathrm{tr}(M) = 1 + \det(M) - \det(I - M)$ and the same result is of course true for an endomorphism of a dimension 2 vector space. So $\mathrm{tr}(\phi_m) = 1 + \det(\phi_m) - \det(Id - \phi_m) = 1 + \det(\phi_m) - \det(([1] - \phi)_m) \equiv 1 + \deg(\phi) - \deg([1] - \phi) \bmod m$, thus $\mathrm{tr}(\phi_m) \equiv \mathrm{tr}(\phi) \bmod m$.
Thus for any prime $m \neq charK$ and for any $P \in E[m]$, $\phi(\phi(P)) - [\mathrm{tr}(\phi_m)]\phi(P) + [\det \phi_m]P = O$. This means that the kernel of $\phi \circ \phi - [\mathrm{tr}(\phi)] \circ \phi + [\deg \phi]$ contains $E[m]$ for all primes $m \neq charK$, so $\phi \circ \phi - [\mathrm{tr}(\phi)] \circ \phi + [\deg \phi]$ has a infinite kernel and is thus the constant map 0. □

6.3 Cardinality of an elliptic curve

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. We already know that $E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ where $n_1 | n_2$ and $n_1 | (q - 1)$, but this does not give much information about the cardinality of $E(\mathbb{F}_q)$.

For cryptography applications, it is extremely important to know the number of points of $E(\mathbb{F}_q)$ and to know if this cardinality is divisible by a large prime.

A rough estimate is that the number of point of $E(\mathbb{F}_q)$ should be close to q. For any $x \in \mathbb{F}_q$, if x^3+ax+b is a square then this gives two points on the curve (exceptionally one), and if x^3+ax+b is not a square then this gives zero point. Since there is the same number of squares and non-squares in $\mathbb{F}_q$, we can expect to have on average one point on the curve for each value of $x \in \mathbb{F}_q$, so about q points. We will see that this estimate is in fact surprisingly accurate.

Proposition 6.4.
$E(\mathbb{F}_q) = \ker([1]-\Phi_q)$, and $|E(\mathbb{F}_q)| = \deg([1]-\Phi_q) = q+1-\operatorname{tr}(\Phi_q)$.

Proof. We know that a point $P \in E$ is F_q-rational iff it is invariant by Frobenius, i.e. iff $\Phi_q(P) = P$. So $P \in E(\mathbb{F}_q) \Leftrightarrow P - \Phi_q(P) = O \Leftrightarrow P \in \ker([1]-\Phi_q)$. Now $[1]-\Phi_q$ is separable according to 4.22, so $|E(\mathbb{F}_q)| = |\ker([1]-\Phi_q)| = \deg([1]-\Phi_q)$. Now by definition, $\operatorname{tr}(\Phi_q) = 1+\deg(\Phi_q)-\deg([1]-\Phi_q)$, which gives immediately $|E(\mathbb{F}_q)| = q+1-\operatorname{tr}(\Phi_q)$ (we recall that $\deg\Phi_p = p$ (Property 4.19), so by multiplicativity of the degree $\deg\Phi_q = q$). □

Corollary 6.5. *If E_1 and E_2 are two isogenous curves defined over $\mathbb{F}_q$ then $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$.*

Rk: here isogenous = $\mathbb{F}_q$-isogenous. We have already mentioned that the converse is also true.

Proof. Let $\phi : E_1 \to E_2$, $(x,y) \mapsto (\phi_1(x,y), \phi_2(x,y))$ be a non-constant isogeny defined over $\mathbb{F}_q$. Let Φ_q^1, resp. Φ_q^2, be the Frobenius endomorphism of E_1, resp. E_2. Then $\phi\circ\Phi_q^1(x,y) = (\phi_1(x^q,y^q), \phi_2(x^q,y^q)) = (\phi_1(x,y)^q, \phi_2(x,y)^q)$ since ϕ_1 and ϕ_2 are rational fractions with coefficients in $\mathbb{F}_q$. So $\phi\circ\Phi_q^1 = \Phi_q^2\circ\phi$. In particular, $\deg\phi \times \deg([1]-\Phi_q^1) = \deg(\phi\circ([1]-\Phi_q^1)) = \deg(\phi - \phi\circ\Phi_q^1) = \deg(\phi - \Phi_q^2\circ\phi) = \deg(([1]-\Phi_q^2)\circ\phi) = \deg([1]-\Phi_q^2)\times\deg(\phi)$, which gives $\deg([1]-\Phi_q^1) = \deg([1]-\Phi_q^2)$. □

Theorem 6.6 (Hasse's bound)**.** *$-2\sqrt{q} \le \operatorname{tr}(\Phi_q) \le 2\sqrt{q}$. In particular,*

$$q+1-2\sqrt{q} \le |E(\mathbb{F}_q)| \le q+1+2\sqrt{q}.$$

Proof. Let $\chi(X) = X^2 - \operatorname{tr}(\Phi_q)X + q$ be the characteristic polynomial of Φ_q. In order to prove Hasse's bound, it is enough to show that $\chi(x) \ge 0$ for all $x \in \mathbb{Q}$, since this implies that its discriminant $(\operatorname{tr}\Phi_q)^2 - 4q$ is non-positive.
Let $\frac{a}{b} \in \mathbb{Q}$. For any prime $m \ne p$, we know that $\chi(X)$ is equal modulo m to the characteristic polynomial of $(\Phi_q)_m$, i.e. $\chi(X) \equiv \det((\Phi_q)_m - X\,Id) \bmod m$. So modulo m, $\chi(\frac{a}{b}) \equiv \det((\Phi_q)_m - \frac{a}{b}Id) \equiv \frac{1}{b^2}\det(b(\Phi_q)_m - a\,Id) \equiv \frac{1}{b^2}\deg([b]\circ\Phi_q - [a]) \bmod m$. Since this is true for all prime $m \ne p$, we deduce that $\chi(\frac{a}{b}) = \deg([b]\circ\Phi_q - [a])/b^2$, so $\chi(\frac{a}{b}) \ge 0$. □

Rk: more generally, this proof shows that the characteristic polynomial of any endomorphism has a non-positive discriminant. In particular, $|\operatorname{tr}\phi| \le 2\sqrt{\deg\phi}$ for any $\phi \in End(E)$.

Rk: because of its importance, the trace of the Frobenius endomorphism is often simply called the trace of E.

Proposition 6.7. *Let $E_{|\mathbb{F}_q}$ be an elliptic curve and let t_k be the trace of $\Phi_{q^k} = (\Phi_q)^k$, so that the cardinality of $E(\mathbb{F}_{q^k})$ is q^k+1-t_k. Then the sequence (t_k) satisfies the relation*

$$t_{k+2} = t\,t_{k+1} - q\,t_k, \qquad t_1 = t = \operatorname{tr}(\Phi_q),\ t_0 = 2.$$

If α and β are the two roots (in $\mathbb{C}$) of the characteristic polynomial X^2-tX+q of Φ_q, then $t_k = \alpha^k+\beta^k$.

Rk: this is exactly what would happen if Φ_q were a linear endomorphism of a dimension 2 vector space over $\mathbb{Q}$ (or $\mathbb{R}$, or $\mathbb{C}$); then α and β would be its two eigenvalues.

Rk: this theorem allows to compute very efficiently $E(\mathbb{F}_{q^k})$ as soon as $E(\mathbb{F}_q)$ is known.

Proof. It is an easy exercise to show that if $M \in M_2(K)$ (for any field K), then $\text{tr}(M^{k+2}) = \text{tr}(M)\text{tr}(M^{k+1}) - \det(M)\text{tr}(M^k)$ (either by induction and direct computation or by considering eigenvalues in $\bar{K}$), and of course $\text{tr}(M^0) = 2$. Naturally, this also holds for any endomorphism of a dimension 2 vector space, and in particular this is satisfied by $(\Phi_q)_m$ (and in fact by ϕ_m for any $\phi \in End(E)$). This implies that the relation $t_{k+2} = t\,t_{k+1} - q\,t_k,\ t_1 = t = \text{tr}(\Phi_q),\ t_0 = 2$ is true modulo m for any prime $m \neq p$, so it is true in $\mathbb{Z}$. The second part of the statement is an elementary result about sequences satisfying this kind of recurrence formula. □

Rk: the proof actually shows that $\text{tr}(\phi^{k+2}) = \text{tr}(\phi)\text{tr}(\phi^{k+1}) - \deg(\phi)\text{tr}(\phi^k)$ for any $\phi \in End(E)$.

Proposition 6.8. *$E_{|\mathbb{F}_q}$ is supersingular if and only if $p|\text{tr}(\Phi_q)$.*

Proof. We start by a preliminary result. We have seen that $t_{k+2} = t\,t_{k+1} - q\,t_k$, so modulo p, $t_{k+2} \equiv t\,t^{k+1}$, i.e. for $k > 0$ the sequence (t_k) is geometric mod p and thus $t_k \equiv t^k \bmod p$.
Suppose now that E is ordinary, i.e. $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$. Let $\mathbb{F}_{q^n}$ be the extension of $\mathbb{F}_q$ generated by the coordinates of the p-torsion points, so that $E(\mathbb{F}_{q^n})[p] = E[p]$. Then p divides $|E(\mathbb{F}_{q^n})| = q^n + 1 - t_n$, so modulo p, $t_n \equiv t^n \equiv 1$. This implies that $t \not\equiv 0 \bmod p$.
Conversely, suppose that $t \not\equiv 0 \bmod p$. Then $t_{p-1} \equiv t^{p-1} \equiv 1 \bmod p$, so $|E(\mathbb{F}_{q^{p-1}})| = q^{p-1} + 1 - t_{p-1}$ is dividable by p, and thus $E(\mathbb{F}_{q^{p-1}})[p] \neq \{O\}$, i.e. E is ordinary. □

Rk: as a byproduct of the proof we obtain that the degree of the smallest extension over which the p-torsion is defined is the multiplicative order of $\text{tr}(\Phi_q)$ in $\mathbb{F}_p^*$.

Exercise: show that if E is defined over a prime field $\mathbb{F}_p$ with $p \geq 17$ and is supersingular then $|E(\mathbb{F}_p)| = p + 1$ (we will see below a more precise statement).

Theorem 6.9. *Let $q = p^d$ be a prime power. Then for any $t \in \mathbb{Z}$ such that $|t| \leq 2\sqrt{q}$ and $p \nmid t$, there exists an elliptic curve E defined over $\mathbb{F}_q$ whose trace is t.*

The curve E can be constructed (at least theoretically) by the complex multiplication method.

Theorem 6.10 (Admitted)**.** *The following table lists all possible traces of supersingular curves (and the associated embedding degree).*

t	$q = p^d$	k
0	d *odd* d *even and* $p \not\equiv 1 \bmod 4$	2
$\pm 2\sqrt{q} = \pm 2p^{d/2}$	d *even*	1
$\pm\sqrt{q} = \pm p^{d/2}$	d *even and* $p \not\equiv 1 \bmod 3$	3
$\pm\sqrt{2q}$	$p = 2$ *and* d *odd*	4
$\pm\sqrt{3q}$	$p = 3$ *and* d *odd*	6

(Note: in the third case, the group of m-th roots of unity in which the pairings have values is actually included in the subfield $\mathbb{F}_{q^{3/2}}$ of $\mathbb{F}_{q^3}$).

For ECC, we need elliptic curves defined over finite fields whose cardinality is dividable by a large prime m (and for key size / bandwidth issues, the smaller the cofactor the better). There are basically four possible approaches:

1. Choose a supersingular curve with a relevant cardinality (for instance, find a prime p in the appropriate range such that $(p+1)/2$ is prime and choose E defined over $\mathbb{F}_p$ with $t=0$). Because of pairing attacks, this approach is not recommended anymore, except for pairing-based cryptography (and with special care concerning the key size; actually, only the $k=6$ case seems still relevant today).

2. Choose a curve E defined over a small field $\mathbb{F}_q$ and an integer d such that $E(\mathbb{F}_{q^d})$ has a subgroup of large prime order (such a curve is called a Koblitz curve or a subfield curve). The cardinality of $E(\mathbb{F}_q)$ can be computed by exhaustive search, and the cardinality of $E(\mathbb{F}_{q^d})$ follows easily from Proposition 6.7. Note that $E(\mathbb{F}_q)$ is then a subgroup of $E(\mathbb{F}_{q^d})$ and its cardinality appears automatically in the cofactor of m. Also, it is better if d is prime, since otherwise $E(\mathbb{F}_{q^{d'}})$ is a subgroup of $E(\mathbb{F}_{q^d})$ for all divisors d' of d, which means that m has an important cofactor.
   Example: $E : y^2 + xy = x^3 + 1$, defined over $\mathbb{F}_2$. Then $|E(\mathbb{F}_{2^{131}})|$ is 4 times a 129-bit prime (this is the Certicom ECC2K-130 challenge).
   Curves of this type are usually not recommended today for the following reasons:

   - The existence of a non-trivial group automorphism (namely, Φ_q) improves somehow the efficiency of generic attacks. But note that it also allows to speed up the computation of the scalar multiplication, which is very interesting since this is the main operation used in ECC.
   - If we want $E(\mathbb{F}_q)$ to be small then there are very few curves to choose from.
   - Koblitz curves are in some sense "special" and possess an additional structure. It is conceivable that in the future, a newly discovered attack can use this additional structure to target all these curves .

3. One can first choose m and then find with the complex multiplication method a curve having a subgroup of this order. The advantage is that m is known in advance, the drawbacks are that finding the curve is not as fast as with the previous methods, and all curves constructed in that way have a "special" property: the "fundamental discriminant" of their endomorphism ring is small. As before, this may give rise in the future to a new attack.

4. One can choose a curve at random, compute its cardinality and repeat until one with a large prime order subgroup is found. Curves constructed that way are considered to be safe, at least when defined over a prime field or a binary field of the type $\mathbb{F}_{2^d}$, d prime. However, finding a correct curve is slower than with the previous methods and requires an efficient point counting algorithm. Fortunately, such algorithms do exist now. But one cannot hope to find a pairing-friendly curve with this method.

Exercise: let $E_{|\mathbb{F}_q}$ be an elliptic curve such that $j(E) \notin \{0, 1728\}$ (and $p \geq 5$), and denote by t its trace, so that $|E(\mathbb{F}_q)| = q + 1 - t$. Let E' be the quadratic twist of E, i.e. E' is isomorphic to E over $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$. Show that the cardinality of $E'(\mathbb{F}_q)$ is $q + 1 + t$.

Exercise: how many Koblitz curves are there over $\mathbb{F}_{2^{131}}$? What are their cardinalities?

Exercise: Devise a point counting algorithm whose complexity is in $O(q)$ operations in $\mathbb{F}_q$.

Exercise: Assume that the cardinality of $E(\mathbb{F}_q)$ is a prime. Devise a (probabilistic) point counting algorithm whose complexity is in $O(q^{1/2})$ operations in $\mathbb{F}_q$.

Exercise: Assume that the cardinality of $E(\mathbb{F}_q)$ is a prime. Devise a (probabilistic) point counting algorithm whose complexity is in $O(q^{1/4})$ operations in $\mathbb{F}_q$ (hint: think baby-step giant-step). Can it be adapted to the case where $E(\mathbb{F}_q)$ is only assumed to be cyclic? More difficult: can it be adapted to the general case?

7 SEA algorithm

7.1 Division polynomials

Division polynomials are used to characterize the m-torsion points and also to give an expression of the multiplication-by-m map. For concision we will leave aside the characteristic 2 and 3 cases.

Some examples first: let $E : y^2 = x^3 + ax + b$. Then $P = (x, y)$ is in $E[2]$ iff $y = 0$, or equivalently iff $x^3 + ax + b = 0$.
For $m = 3$, we know that $P \in E[3]$ iff it is an inflection point. Assume for simplicity that we are working over $\mathbb{R}$; then $P = (x, y)$ is an inflection point if the second derivative of $y = \sqrt{x^3 + ax + b}$ vanishes. A short computation yields $2y' = (3x^2+a)(x^3+ax+b)^{-1/2}$, and $4y'' = \left(12x(x^3 + ax + b) - (3x^2 + a)^2\right)(x^3+ax + b)^{-3/2}$. So $P = (x, y) \in E[3] \Leftrightarrow 12x(x^3 + ax + b) - (3x^2 + a)^2 = 0 \Leftrightarrow 3x^4 + 6ax^2 + 12bx - a^2 = 0$. One can check that this also holds over any base field.
For $m = 4$, we know that $P \in E[4]$ iff $[2]P \in E[2]$. Using the duplication formula and the characterization of 2-torsion points, it is not difficult to find a polynomial vanishing exactly on the 4-torsion points of $E \setminus \{O\}$.

We now consider the family (ψ_m) of polynomials in $\mathbb{Z}[x, y, a, b]$, defined by the following recurrence formula:

$$\begin{aligned}
&\psi_1 = 1 \qquad \psi_2 = 2y \\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2 \\
&\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 && (m \geq 2) \\
&\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/2y && (m \geq 3)
\end{aligned}$$

It is easy to check by induction that ψ_{2m} is indeed a polynomial (despite the division by $2y$), that $\psi_m \in \mathbb{Z}[x, y^2, a, b]$ if m is odd, and that $\psi_m \in 2y\mathbb{Z}[x, y^2, a, b]$ if m is even. Replacing y^2 by $x^3 + ax + b$ everywhere, we now consider ψ_m (resp. $\psi_m/2y$ if m even) as polynomials in $\mathbb{Z}[x, a, b]$, and as such,

$$\psi_m = \begin{cases} mx^{(m^2-1)/2} + \dots & \text{if } m \text{ odd} \\ y(mx^{(m^2-4)/2} + \dots) & \text{if } m \text{ even} \end{cases}$$

Theorem 7.1 (Admitted). *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve and $m \in \mathbb{N}^*$. Then*

$$P \in E[m] \setminus \{O\} \Leftrightarrow \psi_m(P) = 0,$$

and for any $P = (x_0, y_0) \in E$,

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

where $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$ and $\omega_m = (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/4y$.

Of course, in this statement all coefficients are reduced modulo the characteristic of the field. This theorem gives an explicit expression for the multiplication-by-m map and can be used to show that $\deg[m] = m^2$, but in practice this is *not* how one computes $[m]P$ for a given point P.

7.2 Schoof's algorithm

To find the number of $\mathbb{F}_q$-rational points of an elliptic curve E, the idea of Schoof is quite simple:

1. compute t_ℓ, the trace of Φ_q modulo ℓ, for many different primes ℓ;
2. use the chinese remainder theorem to recover $\mathrm{tr}\Phi_q$ from the t_ℓ.

We start with the second step. Thanks to Hasse's bound, we know that $-2\sqrt{q} \leq t \leq 2\sqrt{q}$. Thus it is enough to know t modulo primes $\ell_1, \ldots, \ell_n$ such that $\prod_i \ell_i \geq 4\sqrt{q}$. In practice, it may be faster to consider a smaller set of primes and use a baby-step giant-step approach to find the correct cardinality.

The difficulty is of course in the first step (apart from the computation of t_2, which we leave as an exercise). We know that t_ℓ is such that

$$\Phi_q^2(P) + [q_\ell]P = [t_\ell]\Phi_q(P)$$

for any $P \in E[\ell]$, with $q_\ell \equiv q \bmod \ell$. Since the non-trivial ℓ-torsion points are exactly the zeroes of the division polynomial ψ_ℓ, this means that

$$(X^{q^2}, Y^{q^2}) + [q_\ell](X, Y) \equiv [t_\ell](X^q, Y^q) \bmod (\psi_\ell(X), Y^2 - X^3 - aX - b).$$

The left-hand term is computed using modular exponentiation and the formula from Theorem 7.1 for $[q_\ell]$. We then test all possible values of t_ℓ until the correct one is found (in fact we just have to check equality for the abscissae and $t_\ell \in [0, \ell/2]$, and then pick the correct sign by looking at the y-coordinate). Note that for most primes, the ℓ-torsion points are not in $E(\mathbb{F}_q)$, so we cannot test the above equality on a rational point.

Example: let $E : y^2 = x^3 + 184x + 896$ be an elliptic curve defined over $\mathbb{F}_p$ where $p = 1009$.

We will not develop this here, but one can show that complexity of Schoof's algorithm is in $O((\log q)^8)$ (as compared to $O(q^{1/4})$ for the BSGS-style approach). The main drawback of this algorithm is that the degree of the division polynomials grows quickly (in $O(\ell^2)$), so computing modulo ψ_ℓ is the time-consuming step. We will see that it is actually possible to work modulo smaller polynomials, of degree $(\ell - 1)/2$.

7.3 Modular polynomials

The improvements to Schoof's algorithm rely on a more careful study of the action of the Frobenius morphism Φ_q on the space of ℓ-torsion points, which in turn is related to the existence of ℓ-isogenies (i.e. isogenies of degree ℓ) defined over $\mathbb{F}_q$ (see Theorem 4.26 and the discussion that follows). The modular polynomials are a powerful tool for doing so.

Theorem 7.2 (Admitted). *Let ℓ be a prime number. There exists a symmetric polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$, called the ℓ-th (classical) modular polynomial, such that for any ordinary elliptic curves E_1, E_2 defined over $\mathbb{F}_{p^d}$ with $p \neq \ell$ and $j(E_1), j(E_2) \notin \{0, 1728\}$,*

$$\Phi_\ell(j(E_1), j(E_2)) = 0 \bmod p \Leftrightarrow E_1 \text{ is } \ell\text{-isogenous over } \mathbb{F}_{p^d} \text{ to } E_2 \text{ or its quadratic twist.}$$

Thus in order to find the elliptic curves that are ℓ-isogenous to E, one can solve the equation $\Phi_\ell(X, j(E)) = 0$ in $\mathbb{F}_q$ or its algebraic closure. But we know from Theorem 4.26 and its corollary 4.27 that the isogenies of degree ℓ starting from E are in one-to-one correspondence with the subgroups of cardinality ℓ of E. Such a subgroup is obviously included in $E[\ell]$; actually, using the $\mathbb{Z}/\ell\mathbb{Z}$-vector space structure of $E[\ell]$, it is a dimension 1 linear subspace. Now $E[\ell]$ has exactly $\ell + 1$ dimension 1 linear subspaces, so there are exactly $\ell + 1$ isogenies of degree ℓ (defined over $\overline{\mathbb{F}_q}$) starting from E. This means that $\Phi_\ell(X, Y)$ has degree $\ell + 1$ (in each variable).

Modular polynomials can be computed using complex analysis techniques that are beyond the scope of these lectures. Their main drawbacks are that their coefficients grow extremely fast: just to give an example,

$$\begin{aligned}\Phi_3(X,Y) = X^4 + Y^4 - X^3Y^3 + 2232(X^3Y^2 + X^2Y^3) - 1069956(X^3Y + XY^3) + 36864000(X^3 + Y^3)\\ + 2587918086X^2Y^2 + 8900222976000(X^2Y + XY^2) + 452984832000000(X^2 + Y^2)\\ - 770845966336000000XY + 1855425871872000000000(X + Y).\end{aligned}$$

A workaround is to use other types of modular polynomials, with less nice properties but smaller coefficients, such as the so-called canonical modular polynomials:

Theorem 7.3. *Let ℓ be a prime number. There exists a polynomial $\Phi_\ell^c(X, Y) \in \mathbb{Z}[X, Y]$, called the ℓ-th canonical modular polynomial, such that for any $j \in \mathbb{F}_q \setminus \{0, 1728\}$, $q = p^d$, $p \neq \ell$,*

1. *if $\Phi_\ell(X, j)$ factorizes in $\mathbb{F}_q[X]$ as $\prod_{i=1}^k P_i(X)$, then $\Phi_\ell^c(X, j)$ factorizes as $\prod_{i=1}^k Q_i(X)$ with $\deg Q_i = \deg P_i$;*
2. *if $f \in \mathbb{F}_q$ is a root of $\Phi_\ell^c(X, j)$ and $j' \in \mathbb{F}_q$ is a root of $\Phi_\ell^c(\ell^{12/\gcd(12,\ell-1)}/f, Y)$, then $\Phi_\ell(j', j) = 0$.*

These polynomials have much smaller coefficients than the classical modular polynomials; for instance,

$$\Phi_3^c(X, Y) = X^4 + 36X^3 + 270X^2 - XY + 756X + 729$$

This means that they can be precomputed easily, or even better, directly downloaded from some database (e.g. with PARI/GP one just has to install the package `seadata.tgz`).

7.4 The improvements of Elkies and Atkin

We recall that our goal is to compute t_ℓ, the trace of Φ_q modulo a prime ℓ, for an ordinary elliptic curve E. This is exactly the trace of Φ_q considered as a $\mathbb{Z}/\ell\mathbb{Z}$-linear transformation of $E[\ell]$. So we begin by looking more precisely at the different possibilities for the action of Φ_q on $E[\ell]$:

1. Φ_q has one dimension 2 eigenspace (i.e. it acts as multiplication by a scalar λ on $E[\ell]$). Then each of the $\ell + 1$ dimension 1 linear subspaces is (globally) invariant by Φ_q. Consequently, there are $\ell + 1$ $\mathbb{F}_q$-rational isogenies of degree ℓ starting from E, and the modular polynomial $\Phi_\ell(X, j(E))$ splits completely over $\mathbb{F}_q$.
   In this case, the characteristic polynomial of Φ_q on $E[\ell]$ is $(X - \lambda)^2 = X^2 - t_\ell X + q_\ell$, so $q_\ell \equiv q \bmod \ell$ is a square in $\mathbb{Z}/\ell\mathbb{Z}$ and $t_\ell = \pm 2(q_\ell)^{1/2}$.
2. Φ_q has two dimension 1 eigenspaces (i.e. it is diagonalizable but not a homothety). Then they are the only dimension 1 subspaces globally invariant, so there are only two $\mathbb{F}_q$-rational ℓ-isogenies starting from E and $\Phi_\ell(X, j(E))$ has exactly two roots in $\mathbb{F}_q$.

3. Φ_q has one dimension 1 eigenspace (i.e. it is trigonalizable but not diagonalizable). Then it is the only dimension 1 subspace globally invariant, so $\Phi_\ell(X, j(E))$ has exactly one root in $\mathbb{F}_q$. As in the first case, the characteristic polynomial of Φ_q on $E[\ell]$ is $(X - \lambda)^2$, so $t_\ell = \pm 2(q_\ell)^{1/2}$.

4. Φ_q has no non-trivial eigenspace. Then no dimension 1 linear subspace of $E[\ell]$ is globally invariant by Φ_q, so $\Phi_\ell(X, j(E))$ has no root in $\mathbb{F}_q$.

In the last case (corresponding to an irreducible characteristic polynomial modulo ℓ), ℓ is said to be an *Atkin prime*; it is called an *Elkies prime* otherwise. Note that the first and third case are quite special and rarely happen, whereas the two other cases are approximately equally frequent. Also, $E[\ell]$ almost never contains non-trivial rational points; it occurs only when 1 is a eigenvalue of Φ_q. Now a key observation is that we can determine what is the case just by looking at the factorization of $\Phi_\ell(X, j(E))$, (or more practically of $\Phi_\ell^c(X, j(E))$), for which there exist efficient algorithms.

Suppose first that ℓ is an Atkin prime. To say more, we need to study in more depth the relation between the action of the Frobenius map on $E[\ell]$ and the factorization pattern of $\Phi_\ell(X, j(E))$ (resp. $\Phi_\ell^c(X, j(E))$). The discussion above can actually be applied to any power Φ_{q^k} of the Frobenius morphism. It implies that over any extension $\mathbb{F}_{q^k}$, $\Phi_\ell(X, j(E))$ has either zero, one, two or $\ell+1$ roots, and this restricts the possible factorization of $F(X) = \Phi_\ell(X, j(E))$. Indeed, let r be the smallest degree of the irreducible factors of $F(X)$ in $\mathbb{F}_q[X]$ ($r > 1$ since by assumption $F(X)$ has no root in $\mathbb{F}_q$), and let n be the number of the degree r factors. Then over $\mathbb{F}_{q^r}$, all the degree r factors split, so $F(X)$ has exactly nr roots in $\mathbb{F}_{q^r}$. This means that either $r = 2$ and $n = 1$, or $nr = \ell + 1$. To distinguish between these two possibilities, we look at the characteristic polynomial $X^2 - t_\ell X + q_\ell$ of Φ_q on $E[\ell]$. Since we are in the Atkin case, it is irreducible over $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$; its roots λ and μ belong to $\mathbb{F}_{\ell^2}$ and are conjugated by the ℓ-th Frobenius, i.e. $\lambda^\ell = \mu$, $\mu^\ell = \lambda$. But the characteristic polynomial of Φ_q^r, which is $(X - \lambda^r)(X - \mu^r)$, splits over $\mathbb{F}_\ell$ (and r is the smallest integer for which this is the case). So λ^r belongs to $\mathbb{F}_\ell$, thus $\lambda^r = (\lambda^r)^\ell = (\lambda^\ell)^r = \mu^r$. The two eigenvalues of Φ_q^r are equal, so we are in the case where $F(X)$ splits completely and $nr = \ell + 1$.

It is easy to compute r: it is the smallest divisor of $\ell+1$ such that $gcd(X^{q^r} - X, F(X)) \neq 1$. Then we know that $q_\ell^r = \lambda^r \mu^r = \lambda^{2r}$, and from this relation we can obtain a (hopefully small) list of possible values for t_ℓ. More precisely:

- If r is odd, since λ^{2r} is a square then q_ℓ is square modulo ℓ, i.e. $q_\ell = u^2$ for some $u \in \mathbb{F}_\ell$. So $\lambda^r = \pm u^r = (\pm u)^r$; we can choose u so that $\lambda^r = u^r$. This implies that $\lambda = u\zeta$ where $\zeta \in \overline{\mathbb{F}_\ell}$ is a r-th root of unity. Let s be the order of ζ; it divides r, and $\lambda^s = u^s$ lies in $\mathbb{F}_\ell$. Since r is the smallest integer such that $\lambda^r \in \mathbb{F}_\ell$, this means that $s = r$, i.e. ζ is a primitive r-th root of unity. Finally, $t_\ell = \lambda + q_\ell/\lambda = u(\zeta + \zeta^{-1})$; this is usually stated as
$$t_\ell^2 = q_\ell(\zeta + \zeta^{-1})^2, \quad \zeta \text{ primitive } r\text{-th root of unity.}$$
There are $\varphi(r)$ possible choices for ζ (where φ it the Euler totient); by symmetry this gives only $\varphi(r)/2$ possibilities for $(\zeta + \zeta^{-1})$. With the indeterminacy of the sign of u, we obtain $\varphi(r)$ candidates for the value of t_ℓ.

- If r is even: from $\lambda^{2r} = q_\ell^r$ we deduce that $\lambda^2 = q_\ell \xi$ where $\xi \in \overline{\mathbb{F}_\ell}$ is a r-th root of unity. Let s be the order of ξ; it divides r, and $\lambda^{2s} = q_\ell^s \in \mathbb{F}_\ell$ so $r|2s$. This shows that $s = r$ or $s = r/2$. So $\xi = \zeta^2$ where ζ is a primitive r-th or $2r$-th root of unity, and similarly to the previous case we obtain
$$t_\ell^2 = q_\ell(\zeta + \zeta^{-1})^2, \quad \zeta \text{ primitive } r\text{-th or } 2r\text{-th root of unity,}$$

or equivalently,

$$t_\ell^2 = q_\ell(\xi + \xi^{-1} + 2), \quad \xi \text{ primitive } r/2\text{-th or } r\text{-th root of unity.}$$

Note that if $\ell \equiv 3 \bmod 4$, it it possible to tell if ζ is a r-th or $2r$-th primitive root (see exercise below). In any case, there are either $\varphi(r)$ or $2\varphi(r)$ candidates for the value of t_ℓ.

Note that r divides $l^2 - 1$, so the r-th roots are included in $\mathbb{F}_{l^2}$. Once the possible values of t_ℓ are computed, we store this partial information for the final CRT phase; we do not try to obtain the exact value.

Let now ℓ be an Elkies prime. Then $E[\ell] = V_\lambda \oplus V_\mu$, where λ and μ are the two distinct eigenvalues of Φ_q and V_λ and V_μ are the corresponding eigenspaces (this is for the second case above; the two remaining cases can be dealt similarly) . If we can find λ, then we can easily recover $t_\ell = \lambda + \mu = \lambda + q_\ell/\lambda$. Let $x(V_\lambda) = \{x(P) : P \in V_\lambda, P \neq O\}$ and $g(X) = \prod_{x \in x(V_\lambda)}(X - x)$. This is a non-trivial factor of the ℓ-th division polynomial ψ_ℓ, and $g(X) \in \mathbb{F}_q[X]$ because V_λ is globally invariant by Φ_q. Now since for any $P \in V_\lambda$, $\Phi_q(P) = [\lambda]P$, we obtain that

$$(X^q, Y^q) = [\lambda](X, Y) \bmod (g(X), Y^2 - X^3 - aX - b).$$

If we know $g(X)$, we can find λ as in Schoof's algorithm, by testing all possible values; the main advantage is that we now work modulo a polynomial of degree $(\ell - 1)/2$ instead of a degree $(\ell^2 - 1)/2$.

The computation of $g(X)$ is quite involved and is the major contribution of Elkies (with improvements of Couveignes for small characteristics). Very briefly, we start by computing a root j' of $\Phi_\ell(X, j(E))$. Elkies gives a formula for the elliptic curve E' with $j(E') = j'$ which is ℓ-isogenous to E (the difficulty is not to find a curve whose j-invariant is j', but to tell if this is this curve or its twist that is isogenous to E). The hardest step is then to obtain $g(X)$, which characterizes the elements of the kernel of the ℓ-isogeny $E \to E'$, and this can be done using formulas stemming from complex analysis (at least when the characteristic is large enough). The details of these computations are outside the scope of these lectures anyway.

In a final phase, the partial informations collected about the trace of the Frobenius map are combined. The tricky part is obviously to use the list of possible values from each Atkin prime (and in fact a slower alternative is to only work with Elkies primes). In Atkin's "Match and Sort" algorithm, a baby-step giant-step approach is further used, but the fastest method to recover the only solution in the Hasse's bound of all the congruence relations is Lercier's "Chinese and Match" algorithm. The overall complexity of the SEA algorithm is in $O((\log q)^5)$, as compared to $O((\log q)^8)$ for Schoof's original algorithm.

Note: an interesting feature of the SEA algorithm is that it allows an "early abort" strategy. In most applications, the goal of point counting is to check that $|E(\mathbb{F}_q)|$ is prime or is divisible by a large prime, with a small cofactor. In particular, it should not be divisible by too many small primes ℓ. But if $\ell || E(\mathbb{F}_q)|$, then $t_\ell \equiv p + 1 \bmod \ell$, and this can be tested during the execution (at least if ℓ is Elkies). If this happens too often, we can stop the algorithm and test a new curve.

Note: for elliptic curves defined over (large) finite fields of small characteristic, there exist more efficient point counting algorithms (but with the same asymptotic complexity). In the important case of binary fields, the arithmetic-geometric mean (AGM) algorithm of Mestre is usually the fastest one.

Exercise: let ℓ be an Atkin prime for an elliptic curve E, and $\lambda \in \mathbb{F}_{\ell^2}$ a root of the (irreducible) characteristic polynomial $X^2 + t_\ell X + q_\ell \in \mathbb{F}_\ell[X]$. We keep the notations introduced above.

1. Show that if r is even, then λ^r is not a square in $\mathbb{F}_\ell$.

2. Show that if $\ell \equiv 1 \bmod 4$ and q is a quadratic residue modulo ℓ, then r is odd. How can this be used to speed up the SEA algorithm?

3. Assume that r is even and $\ell \equiv 3 \bmod 4$. Explain how to tell if $\lambda^r = q_\ell^{r/2}$ or $\lambda^r = -q_\ell^{r/2}$. Show that $s = r/2$ in the first case and $s = r$ in the second, and that this gives $\varphi(r)$ choices for t_ℓ in both cases.

4. Prove the formula: $(-1)^{(\ell+1)/r} = \left(\frac{q}{\ell}\right)$

Part II

Gröbner basis

8 Motivation

Gröbner bases are a powerful tool for computations based on the resolution of polynomial systems in several variables. In this sense, they generalise operations such as the Euclidean division in the ring $K[X_1, \ldots, X_n]$, the extended Euclid algorithm (only available in one variable), or Gaussian elimination (for linear systems in several variables). For a given $I = \langle f_1, \ldots, f_k \rangle$ ideal of $K[X_1, \ldots, X_n]$, Gröbner bases allow to address the classical following problems:

- Membership problem: determine if $f \in K[X_1, \ldots, X_n]$ belongs to I;
- Efficient computations in $K[X_1, \ldots, X_n]/I$;
- Implicitation of a curve or a parametrized surface;
- Computation of solutions of polynomial systems in several variables over finite fields:
  - multivariate cryptography and cryptanalysis of HFE
  - index calculus over elliptic and hyperelliptic curves...

Note that for example, the upper bounds on the complexity of the Ideal membership problem are at least exponential (this problem belongs to the family of EXPSPACE complete problems). There also exist examples of Gröbner basis computations where the complexity is doubly exponential in the number of variables of the polynomials generating the ideal! Nevertheless, we will give examples of ideal families where computations are more feasible.

8.1 Multivariate cryptography

Secret key:

- a map $F : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n, (x_1, \dots, x_n) \mapsto (f_1(x_1, \dots, x_n), \dots, f_n(w_1, \dots, x_n))$ given by a collection of n polynomials in n variables; F has to be easily invertible
- S and T two invertible $n \times n$ matrices over $\mathbb{F}_q$.

Public key:
$PK = T \circ F \circ S = (PK_1(x_1, \dots, x_n), \dots, PK_n(x_1, \dots, x_n))$ a system of random-looking multivariate polynomials.

Encryption of $\underline{x}$: evaluation $\underline{c} = PK(\underline{x})$
Decryption: invert T then F then S

The security of such systems rely on the fact that solving multivariate polynomial equations is difficult (NP-complete in general and random instances are difficult). The hope is that $PK = T \circ F \circ S$ is random enough (S and T hide the structure of F) and thus hard to invert.

8.2 HFE: Hidden Field equations

This encryption scheme (also used for digital signature) has been introduced by Patarin in 1996 and is certainly the most well-known multivariate cryptosystem. It is a generalisation of the Matsumoto-Imaï scheme (1988), whose core idea is to use the isomorphism between $(\mathbb{F}_q)^n$ and $\mathbb{F}_{q^n}$ and the Frobenius map $\Phi_q \in \mathrm{Aut}(\mathbb{F}_{q^n})$ to construct F.

The scheme has the same basic building blocks as any multivariate cryptosystems:

- Take for F a polynomial $P = \sum_{i,j} a_{ij} X^{q^i + q^j} + \sum_i b_i X^{q^i} + c$, where $a_{ij}, b_i, c \in \mathbb{F}_{q^n}$ with a small degree D, so that the solutions of an equation of the form $P(x) = y$ can easily be found over $\mathbb{F}_{q^n}$.
- Consider a $\mathbb{F}_q$-basis $(\theta_1, \dots, \theta_n)$ of $\mathbb{F}_{q^n}$ and polynomials $p_1, \dots, p_n \in \mathbb{F}_q[X]$ such that

  $$P(x_1\theta_1 + \dots + x_n\theta_n) = p_1(x_1, \dots, x_n)\theta_1 + \dots + p_n(x_1, \dots, x_n)\theta_n.$$

  The important point here is that the polynomials p_i have degrees much smaller than D. More precisely, since the i-th power Φ_q^i of the Frobenius is linear over $\mathbb{F}_q$, and because of the shape of F, the polynomials p_i are quadratic over $\mathbb{F}_q$.
- Take for S, T affine (instead of linear) transformations of $\mathbb{F}_q$, i.e. composed of one invertible matrix of $\mathcal{M}_n(\mathbb{F}_q)$ and one vector of $\mathbb{F}_q^n$ each.

Tiny example over $\mathbb{F}_8 = \mathbb{F}_2[t]/(t^3 + t + 1)$:

$$\begin{aligned}
X^5 &= (x_0 + x_1 t + x_2 t^2)^5 \\
&= (x_0 + x_1 t + x_2 t^2)^4 (x_0 + x_1 t + x_2 t^2) \\
&= (x_0 + x_1 t^4 + x_2 t^8)(x_0 + x_1 t + x_2 t^2) \\
&= (x_0 + x_1(t + t^2) + x_2 t)(x_0 + x_1 t + x_2 t^2) \\
&= (x_0^2 + x_1^2 + x_1 x_2 + x_2^2) + (x_0 x_2 + x_1^2 + x_2^2)t + (x_0 x_2 + x_1^2 + x_0 x_1)t^2 \\
&= (x_0 + x_1 + x_1 x_2 + x_2) + (x_0 x_2 + x_1 + x_2)t + (x_0 x_2 + x_1 + x_0 x_1)t^2
\end{aligned}$$

thus $F_1 = x_0 + x_1 + x_2 + x_1x_2$, $F_2 = x_1 + x_2 + x_0x_2$ and $F_3 = x_1 + x_0x_2 + x_0x_1$.

The public key size depends on the number of coefficients of the public polynomials, i.e. $n(n+1)(n+2)/2 = O(n^3)$. The private key size depends on the number of coefficients in the private polynomial P and the affine transformations S and T, it is usually much smaller than the public key. In practice, we always take $q = 2$; for example, for $D = 257$ and $n = 129$ the private key has size 4.7 kB and the public key 134 kB.

Remarks:

1. The encryption part is the easiest one; we basically need to evaluate polynomials (no division nor exponentiation are required for this step). The decryption step is more expensive: we need to solve the equation $P(x) = y$ for a given y (inversion of T and S are immediate); hopefully there are efficient algorithms to do the job. Note however that since the degree of P is D, we can expect up to D solutions for this equation, which is somehow inappropriate for decryption. Thus, a redundancy r is added in practice to be sure to find the correct solution.

2. This scheme can be used as well for signature using the trapdoor $k = (S, P, T)$; we then need to add a padding to the message to sign, since P is not surjective.

The attack proposed by Faugère and Joux on HFE in 2002 was basically to solve directly the quadratic equations using computations of Gröbner bases

$$\begin{array}{rcl} y_1 & = & p_1(x_1, \dots, x_n) \\ & \vdots & \\ y_n & = & p_n(x_1, \dots, x_n). \end{array}$$

They actually broke the HFE challenge proposed by Patarin with parameters $q = 2$, $n = 80$ and $d = 96$ in only 96 hours. With this attack, Gröbner bases rose to fame in the cryptographic community, giving birth to algebraic cryptanalysis.

9 Division of multivariate polynomials

Goal: find an analogue in $K[X_1, \dots, X_n]$ of the Euclidean division in $K[X]$. But instead of dividing a polynomial by another, we divide a polynomial $f \in K[X_1, \dots, X_n]$ by a *family* of polynomials $G = \{g_1, \dots, g_s\}$.

9.1 Monomial orders

Definition 9.1. *An admissible monomial order $\preccurlyeq$ over $\mathbb{K}[X_1, \dots, X_n]$ is an order relation on the set of monomials of $\mathbb{K}[X_1, \dots, X_n]$, which is*

1. *total*

2. *compatible with the multiplication of $\mathbb{K}[X_1, \dots, X_n]$: if m_1 and m_2 are two monomials s.t. $m_1 \preccurlyeq m_2$, then $m_1m_3 \preccurlyeq m_2m_3$ for all monomial m_3*

3. *a well-ordering: a non-empty set of monomials always admits a minimal element for $\preccurlyeq$ (or equivalently, assuming 2., every monomial m must satisfy $1 \preccurlyeq m$).*

Examples:

1. The *lexicographic order* $lex_{X_1>X_2>\ldots>X_n}$: $X^\alpha <_{lex} X^\beta$ if $\alpha - \beta = (\alpha_1, \ldots, \alpha_n) - (\beta_1, \ldots, \beta_n) = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ is such that the first non-zero $\alpha_i - \beta_i$ starting from the left is negative.
   Ex: $X_1 >_{lex} X_2^4$

2. The *graded lexicographic order* $glex_{X_1>X_2>\ldots>X_n}$: graded first by degree and then by $lex_{X_1>X_2>\ldots>X_n}$.
   Ex : $X_1^4 >_{glex} X_2^4 >_{glex} X_1$

3. The *graded reverse lexicographic order* $grevlex_{X_1>X_2>\ldots>X_n}$: graded first by degree and then by $lex_{X_1>X_2>\ldots>X_n}$ "inverted" → the minimal monomial is the one containing the biggest power of X_n, then of X_{n-1}...
   Ex : $X_2^4 >_{grevlex} X_1X_3$ but $X_1^2X_2^2X_3 >_{grevlex} X_1^3X_3^2$

Note that the reverse lexicographic order is *not* a monomial order: it is not a well-ordering.

Let $\prec$ a given monomial order over the set of monomials of $\mathbb{K}[X_1, \ldots, X_n]$.

Definition 9.2. *Let $f = \sum_\alpha c_\alpha X^\alpha$ a non-zero polynomial of $\mathbb{K}[X_1, \ldots, X_n]$ and $\gamma = \max_\prec\{\alpha \in \mathbb{N}^n : c_\alpha \neq 0\}$ the multi-degree of the largest monomial of f for the order $\prec$.*

1. *The leading monomial of f is $\mathrm{lm}(f) = X^\gamma$.*

2. *The leading coefficient of f is $\mathrm{lc}(f) = c_\gamma$.*

3. *The leading term of f is $\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f) = c_\gamma X^\gamma$.*

The tail *of the polynomial f is the polynomial obtained by omitting the leading term of f.*

9.2 Division algorithm in several variables

As the ring $\mathbb{K}[X_1, \ldots, X_n]$ is not principal, it is natural to consider the division of a given polynomial f with respect to a list of polynomials $\{g_1, \ldots, g_s\}$ (and not anymore wrt one polynomial as in Euclidean division) such that

$$f = q_1g_1 + \cdots + q_sg_s + r \text{ with } \begin{cases} \mathrm{lm}(q_ig_i) \preccurlyeq \mathrm{lm}(f), \\ r = 0 \text{ or } [\forall m \text{ monomial of } r,\ \forall i \in [\![1; s]\!],\ \mathrm{lm}(g_i) \nmid m]. \end{cases} \tag{2}$$

This division is easily obtained with the following algorithm; the termination is guaranteed since the leading monomial sequence of f is strictly decreasing and $\prec$ is an admissible order.

Example: Let $f(X_1, X_2) = X_1^2X_2 + X_1X_2^2 + X_2^2$ the polynomial we want to divide by $G = \{X_1X_2 - 1, X_2^2 - 1\}$

Algorithm 3: Division algorithm in $\mathbb{K}[X_1,\dots,X_n]$.

```
Input  : $f$, $G = \{g_1,\dots,g_s\}$, $\prec$
Output: the remainder $r$ and $\{q_1,\dots,q_s\}$ the quotients as in (2)
$r \leftarrow 0$, $q_i \leftarrow 0$ for $i = 1,\dots,s$
while $f \neq 0$ do
    $i \leftarrow 1$
    while $i \leq s$ do
        if $\mathrm{lm}(g_i)|\mathrm{lm}(f)$ then
            $f \leftarrow f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g_i)} g_i$,    $q_i \leftarrow q_i + \frac{\mathrm{lt}(f)}{\mathrm{lt}(g_i)}$
            if $f = 0$ then return $r$ and $\{q_1,\dots,q_s\}$

            $i \leftarrow 1$
        else $i \leftarrow i + 1$

    $r \leftarrow r + \mathrm{lt}(f)$
    $f \leftarrow f - \mathrm{lt}(f)$
return $r$ and $\{q_1,\dots,q_s\}$
```

for the $\prec_{lex}$ order.

	X_1X_2-1	X_2^2-1	r
$X_1^2X_2 + X_1X_2^2 + X_2^2$	X_1	0	0
$-X_1^2X_2 + X_1$			
$X_1X_2^2 + X_1 + X_2^2$	X_1+X_2	0	0
$-X_1X_2^2 + X_2$			
$[X_1] + X_2^2 + X_2$	X_1+X_2	0	X_1
$X_2^2 + X_2$	X_1+X_2	1	
$-X_2^2 + 1$			
$[X_2] + 1$	X_1+X_2	1	X_1+X_2
$[1]$	X_1+X_2	1	X_1+X_2+1

Thus the division of f by $G = \{X_1X_2 - 1, X_2^2 - 1\}$ is $f = (X_1+X_2)\cdot[X_1X_2-1] + [X_2^2-1] + (X_1+X_2+1)$. If one reverts the order of the polynomials in G, then

	X_2^2-1	X_1X_2-1	r
$X_1^2X_2 + X_1X_2^2 + X_2^2$	0	X_1	0
$-X_1^2X_2 + X_1$			
$X_1X_2^2 + X_1 + X_2^2$	X_1	X_1	0
$-X_1X_2^2 + X_1$			
$[2X_1] + X_2^2$	X_1	X_1	$2X_1$
X_2^2	X_1+1	X_1	$2X_1$
$-X_2^2 + 1$			
$[1]$	X_1+1	X_1	$2X_1+1$

Thus, $f = (X_1+1)\cdot[X_2^2-1] + (X_1)\cdot[X_1X_2-1] + (2X_1+1)$.

Remarks:

1. The remainder $\overline{f}^G$ depends on the order of the polynomials in G.
2. Clearly if $\overline{f}^G = 0$, then f belongs to the ideal generated by the family G. The converse is not true in general and will be verified only if G is a good set of generators of the ideal; in particular for this specific system the condition that f belongs to the ideal is equivalent to the cancellation of the remainder and the order of the polynomials in G does not matter.

10 Gröbner bases

Let $\prec$ be a monomial order.

Definition 10.1. *An ideal* $I \subset \mathbb{K}[X_1, \ldots, X_n]$ *is called a* monomial ideal *if there exists a generating family composed of monomials.*
The initial ideal *of an ideal* I *is the monomial ideal given by*

$$\mathrm{lt}(I) = \langle \mathrm{lm}(f) : f \in I \rangle.$$

In particular, a monomial m *belongs to* $\mathrm{lt}(I)$ *iff there exists* $f \in I$ *s.t.* $m = \mathrm{lm}(f)$.

Remark: for $I = \langle f_1, \ldots, f_s \rangle$, then necessarily $\langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s) \rangle \subset \mathrm{lt}(I)$, but the inclusion is strict in general. Example: let $I = \langle X_1 - X_2, X_1 - X_2^2 \rangle \subset \mathbb{R}[X_1, X_2]$ ideal with lexicographic order, then $\mathrm{lt}(I) = \langle X_1, X_2^2 \rangle \neq \langle X_1 \rangle$. However one has the following property

Property 10.2. *Let* $I \subset \mathbb{K}[X_1, \ldots, X_n]$ *an ideal. Then for every ideal* $J \subset I$*, if* $\mathrm{lt}(J) = \mathrm{lt}(I)$ *then* $J = I$.

Proof. Assume by contradiction that $J \neq I$, and let f be an element of $I \setminus J$ such that $\mathrm{lm}f = \min_{\prec}\{\mathrm{lm}g : g \in I \setminus J\}$; such an f exists because $\prec$ is a well-order. Then $\mathrm{lm}f \in \mathrm{lt}I = \mathrm{lt}J$, so there exists $p \in J$ such that $\mathrm{lm}f = \mathrm{lm}p$. Then $f' = f - \frac{\mathrm{lc}f}{\mathrm{lc}p}p$ lies in I (since f and p are in I) but not in J (otherwise f would be in J), and $\mathrm{lm}f' \prec \mathrm{lm}f$, which is a contradiction. □

Definition 10.3. *A Gröbner basis of* I *is a family* $G = \{g_1, \ldots, g_s\}$ *of polynomials of* I *such that* $\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle = \mathrm{lt}(I)$.

The existence of such a family is clear: the initial ideal $\mathrm{lt}(I)$ is finitely generated by some monomials $m_1, \ldots, m_s$, and for each of them there exist $g_i \in I$ such that $m_i = \mathrm{lt}(g_i)$. The family $G = \{g_1, \ldots, g_s\}$ is then a Gröbner basis of I. The previous property implies that every Gröbner basis is indeed a basis of the ideal.

Example. *Let* $I \subset \mathbb{R}[X_1, X_2, X_3]$ *the ideal given by*

$$I = \langle X_1^2 + X_2^2 + X_3^2 - 25, X_1^2 - X_2^2 - (X_3 - 4)^2 + 9, (X_1 - 3)^2 + X_2^2 - 10 \rangle.$$

We can easily check that $G = \{X_1^2 + 4X_3 - 16, X_2^2 - 6X_1 - 4X_3 + 15, X_3^2 + 6X_1 - 24\}$ *is a Gröbner basis of* I *for* $grevlex_{X_1 \succ X_2 \succ X_3}$.

The division operation then provides a valid test for ideal membership:

Property 10.4. *Let* $G = \{g_1, \ldots, g_s\}$ *a Gröbner basis of the ideal* I *and* $f \in \mathbb{K}[X_1, \ldots, X_n]$. *Then there exists a unique polynomial* r *such that*

1. *no terms of r are divisible by a monomial of* $\mathrm{lt}(G) = \{\mathrm{lm}(g_1), \dots, \mathrm{lm}(g_s)\}$ *;*
2. *the polynomial $f - r$ belongs to I.*

Proof. exercise! □

The remainder r does not depend anymore on the order of the polynomials in G; it is denoted $\overline{f}^G$ and called the *normal form* of f modulo G.

A Gröbner basis is not necessarily unique for a given ideal: some polynomials of the basis can be redundant in the sense that their leading monomial is divisible by the leading monomial of another element of the Gröbner basis. By eliminating such polynomials and normalizing the remaining polynomials in the basis, we obtain a *minimal* Gröbner basis:

Definition 10.5. *A* minimal *Gröbner basis of an ideal I is a Gröbner basis G of I such that*

1. $\forall g \in G$, $\mathrm{lc}(g) = 1$ *;*
2. $\forall g, g' \in G, g \neq g'$, $\mathrm{lm}(g) \nmid \mathrm{lm}(g')$.

In particular, minimal Gröbner bases have the same cardinality. The unicity can be obtained by introducing more restrictive conditions:

Definition 10.6. *A* reduced *Gröbner basis of an ideal I is a Gröbner basis G of I such that*

1. $\forall g \in G$, $\mathrm{lc}(g) = 1$ *;*
2. $\forall g, g' \in G, g \neq g'$, *there is no monomial of g divisible by* $\mathrm{lm}(g')$.

11 Application to the resolution of multivariate polynomial system

Goal: determine (or at least give a nice description) of the solutions of a given polynomial system $f_1, \dots, f_s \in K[X_1, \dots, X_n]$.

Definition 11.1. *Let $I \subset \mathbb{K}[X_1, \dots, X_n]$ an ideal. For $k \in [\![1; n]\!]$, we consider the k-*th elimination ideal $I_k = I \cap \mathbb{K}[X_k, \dots, X_n]$.

It is clear that I_k is indeed an ideal of $\mathbb{K}[X_k, \dots, X_n]$. The knowledge of the elimination ideals allows then to obtain some sort of triangularisation of the system associated to the ideal I, which somehow corresponds to the output of the Gauss algorithm for linear polynomials.

Proposition 11.2. *Let I be an ideal of $\mathbb{K}[X_1, \dots, X_n]$ and G a Gröbner basis of I for the lexicographic order. Then for all $k \in [\![1; n]\!]$, $G \cap \mathbb{K}[X_k, \dots, X_n]$ is a Gröbner basis of I_k for the lexicographic order.*

Proof. If $f \in I_k$, then there exists $g \in G$ such that $\mathrm{lt}(g) | \mathrm{lt}(f)$. In particular, $\mathrm{lt}(g) \in \mathbb{K}[X_k, \dots, X_n]$ and $g \in \mathbb{K}[X_k, \dots, X_n]$ (since the order is the lexicographic one). We then conclude with the property 10.2. □

When the considered system has only a finite number of solutions, we usually get a Gröbner basis for the lexicographic order which has a nice shape

Proposition 11.3 (Shape Lemma)**.**
Let $I \subset \mathbb{K}[X_1, \dots, X_n]$ be a radical ideal of dimension 0 and degree d, i.e. the quotient $\mathbb{K}[X_1, \dots, X_n]/I$ has dimension d as a K-vector space. Then, up to a linear change of coordinates, the Gröbner basis of I for the lex order has the following shape:

$$\{X_1 - g_1(X_n) \ , \ \dots \ , \ X_{n-1} - g_{n-1}(X_n) \ , \ g_n(X_n)\}$$

where g_n is a univariate polynomial of degree d and $g_1, \dots, g_{n-1}$ are univariate polynomials of degree strictly smaller than d.

Thus knowing the lex Gröbner basis of 0-dimensional ideal, it is easy to compute the solutions of the corresponding system: the n-th elimination ideal is principal, thus generated by a polynomial g_n which roots can be efficiently computed; evaluating X_n in such roots in I_{n-1} allows to deduce easily the corresponding values for X_{n-1}, and so on...

Remarks:

- as the computation of a lex Gröbner basis is (very!) expensive in practice, a possible strategy is to first compute a grevlex Gröbner basis and then use a changing order algorithm such as FGLM...
- in the specific case of finite fields, use field equations to reduce the degree of the intermediate equations (only in small characteristic, like in HFE)

12 Gröbner basis computation algorithms

Gröbner bases are first introduced by Buchberger in 1965 in his PhD thesis, where he gives a criterion that determines if a given set of polynomial forms a Gröbner basis. An algorithm for the computation of Gröbner basis can also directly be deduced from this criterion.

12.1 The Buchberger criterion

Let $\prec$ a admissible monomial order.

The computation of the syzygy of two polynomials basically consists in finding the simplest monomial combination that cancels the leading term of these polynomials:

Definition 12.1. *Let g_1, g_2 two polynomials of $\mathbb{K}[X_1, \dots, X_n]$. We denote $S(g_1, g_2)$ the syzygy of g_1, g_2 defined by*

$$S(g_1, g_2) = u_1 g_1 - u_2 g_2$$

where $lcm = \mathrm{lm}(g_1) \vee \mathrm{lm}(g_2)$ and $u_i = \frac{lcm}{\mathrm{lt}(g_i)}$ for $i = 1, 2$.

We have seen in section 10 that $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of an ideal I if $I = \langle g_1, \ldots, g_s\rangle$ and $\mathrm{lt}(G) = \mathrm{lt}(I)$. In particular, to check if a given family of polynomials $\{f_1, \ldots, f_r\}$ is a Gröbner basis of $\langle f_1, \ldots, f_r\rangle$, we can consider the polynomials $S(f_i, f_j)$, whose leading terms are not trivially in $\langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_r)\rangle$. These polynomials are of course in the ideal generated by $\{f_1, \ldots, f_r\}$, and if the division of one of these $S(f_i, f_j)$ by $\{f_1, \ldots, f_r\}$ is not equal to 0, then $\{f_1, \ldots, f_r\}$ is not a Gröbner basis. This is the main idea of the following theorem:

Theorem 12.2 (Buchberger (admitted)).
A family $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}[X_1, \ldots, X_n]$ is a Gröbner basis of the ideal I generated by G if and only if for every couple $(i, j) \in [\![1; s]\!]^2$, the remainder in the division of $S(g_i, g_j)$ by G, noted $\overline{S(g_i, g_j)}^G$, is equal to 0.

Example: let $f_1 = X_1X_2 - X_1X_3$, $f_2 = X_1^2X_3 - X_3^3$ and $f_3 = X_2X_3^2 - X_3^3$ polynomials of $\mathbb{K}[X_1, X_2, X_3]$ where $\mathbb{K}$ is a field. The family $G = \{f_1, f_2, f_3\}$ is a Gröbner basis for $grevlex_{X_1 \succ X_2 \succ X_3}$:
$S(f_1, f_2) = X_1X_3f_1 - X_2f_2 = -X_3f_2 + X_3f_3 \Rightarrow \overline{S(f_1, f_2)}^G = 0,$
$S(f_1, f_3) = X_3^2f_1 - X_1f_3 = 0 \Rightarrow \overline{S(f_1, f_3)}^G = 0,$
$S(f_2, f_3) = X_2X_3f_2 - X_1^2f_3 = X_3^2f_2 - X_3^2f_3 \Rightarrow \overline{S(f_2, f_3)}^G = 0.$

12.2 Basic version of the Buchberger's algorithm

From Buchberger's theorem, we easily deduce the following algorithm:

Algorithm 4: Basic version of Buchberger's algorithm

```
Input  : $I = \langle f_1, \ldots, f_k\rangle \subset \mathbb{K}[X_1, \ldots, X_n]$
Output: $G$ GB of $I$
$G \leftarrow \{f_1, \ldots, f_k\}$
CP $\leftarrow \{S(f_i, f_j), 1 \leq i < j \leq k\}$
while $CP \neq \emptyset$ do
    choose $s \in$ CP and remove it from CP
    $r \leftarrow \overline{s}^G$
    if $r \neq 0$ then
        CP $\leftarrow$ CP $\cup \{S(g, r) : g \in G\}$
        $G \leftarrow G \cup \{r\}$
return G
```

We can check without difficulty that the property that the ideal I is generated by G is a loop invariant. At each iteration of the loop, either the initial ideal of I increases, or it remains constant but the number of syzygies decreases. Since an increasing sequence of ideals is ultimately stationary (noetherianity), this proves that the algorithm terminates. At the end, every syzygy necessarily reduces to 0 in G and the algorithm returns a Gröbner basis of I.

Remarks: even if the algorithm is very simple, it already raises some implementation questions, as for example the choice of the couple of polynomials during the loop, or the choice of the order of the polynomials in G for the division operation. Of course, these choices have no impact on the result but they can greatly improve the performances of the algorithm. See the book of Cox, Little and O'Shea for more details.

12.3 The problem of the reductions to zero

The most consuming step of Buchberger's algorithm is the computation of the reduction of the syzygies. However, in practice we can observe that most of the time, these reductions are equal to zero! It is thus natural to try to lessen the number of couples to consider.

A first idea consists in minimizing the number of polynomials in the basis G, by eliminating the redundant polynomials at each step (exercise). Performances can also be greatly improved by using two criteria of Buchberger, that allow to skip directly some non useful syzygies.

Property 12.3 (Buchberger's criteria).
Let $G \subset \mathbb{K}[X_1, \ldots, X_n]$ and f, g, h polynomials in G.

1. First criterion: *If* $\mathrm{lm}(f) \wedge \mathrm{lm}(g) = 1$ *(f and g are called* foreign *polynomials), then* $\overline{S(f,g)}^{\{f,g\}} = 0$.
2. Second criterion : *If* $S(f,g) = o_G(\mathrm{lm}(f) \vee \mathrm{lm}(g))$ *and* $S(f,h) = o_G(\mathrm{lm}(f) \vee \mathrm{lm}(h))$ *and if* $\mathrm{lm}(f) \mid (\mathrm{lm}(g) \vee \mathrm{lm}(h))$*, then* $S(g,h) = o_G(\mathrm{lm}(g) \vee \mathrm{lm}(h))$*, where the notation* $p = o_G(m)$ *signifies* $\exists u_1, \ldots, u_s \in K[X_1, \ldots X_n]$ *s.t.* $\begin{cases} p = \sum u_i g_i \\ \mathrm{lm}(u_i g_i) < m \end{cases}$

The second criterion can be interpreted in the following way: if the couples (f,g) and (f,h) have already been considered during the algorithm, then the couple (g,h) is not useful as soon as the leading term of f divides the lcm of the leading terms of g and h.

The implementation of these two criteria is not obvious, we refer to the paper of Gebauer and Möller for a thorough analysis.

12.4 Other Gröbner basis computation algorithms

There exist essentially two family of Gröbner basis computation algorithms: the first one starts from the original Buchberger's algorithm and the second one relies on the theory of elimination and resultants and makes extensive use of Macaulay matrices and Gaussian elimination. Just to mention a few:

1. F4 and F5 are two algorithms proposed by Faugère in 1999 and 2002, which are improvement of Buchberger's algorithm: the first one uses linear algebra to parallelize the computations of the reductions and also store some computations to accelerate the following ones, whereas the second provides a new criterion that allows to avoid more reductions to zero.
2. Lazard's algorithm, XL, MXL... which are based on linearisation techniques.