Codes and modular curves

Alain Couvreur

To cite this version:

Alain Couvreur. Codes and modular curves. Doctoral. Codes and Modular curves, Zurich, Switzerland. 2022, pp.33. hal-03932020

CODES AND MODULAR CURVES

by

Alain Couvreur

Abstract. — These lecture notes have been written for a course at the *Algebraic Coding Theory* (ACT) summer school 2022 that took place in the university of Zurich. The objective of the course propose an in–depth presentation of the proof of one of the most striking results of coding theory: Tsfasman Vlăduţ Zink Theorem, which asserts that for some prime power q, there exist sequences of codes over $\mathbb{F}_q$ whose asymptotic parameters beat random codes.

Contents

Introduction

Algebraic Geometry (AG) codes is a particularly exciting topic lying at the intersection between number theory, algebraic geometry and coding theory. The birth of this research area dates back to the early 80's with the introduction by Goppa [**Gop81**] of a new family of codes obtained by evaluating residues of some differential forms on a given curve. Quickly after, Tsfasman, Vlăduţ, Zink [**TVZ82**] and independently Ihara [**Iha81**] proved the existence of sequences of modular curves and Shimura curves having an excellent asymptotic ratio number of points *v.s.* genus. An immediate but extremely striking corollary is the existence of sequences of codes beating the Gilbert Varshamov bound, in short: codes better than random codes. This remarkable and totally unexpected result turned out to be the first stone of the development of a whole theory: that of AG codes. Surprisingly, a very comparable breakthrough happened in graph theory the late 80's. Indeed, in 1988, Lubotsky, Philips and Sarnak [**LPS88**] and independently Margulis [**Mar88**] used Cayley graphs on quotients of $\mathbf{SL}_2(\mathbb{Z})$ to prove the existence of a family of graphs whose girth, *i.e.* the length of their shortest cycle, exceeds the girth obtained with the probabilistic method. In both situations, coding theory and graph theory, the use of elegant algebraic structures unexpectedly beat random constructions.

The objective of this lecture is to present in an (almost) self-contained presentation, the beginning of this wonderful story: the original proof of Tsfasman, Vlăduţ and Zink Theorem. It should be mentioned that in 1995, Garcia and Stichtenoth [**GS95**] proposed another and somehow more explicit approach to design sequence of curves (actually function fields but the two objects are equivalent) reaching the so-called Drinfeld–Vlăduţ [**VD83**]. It could be considered as strange to present the original proof which turns out to be much more complicated than Garcia and Stichtenoth's one but there are some reasonable motivations for that:

- Tsfasman, Vlăduţ and Zink's proof testifies from the richness of the theory of algebraic geometry codes, with a proof involving deep results from algebraic geometry and number theory.
- This original proof is frequently cited while few references give a complete presentation of it and (in my personal opinion), none of the papers of Tsfasman *et. al.* and Ihara provide an enough detailed proof. In both articles, the proof is made of less than ten lines hiding a huge amount of prerequisites.
- Finally, I wished to give that lecture, because this proof is beautiful and elegant and even if I am not among the mathematicians who do maths *pour la beauté de la chose*(1) it is sometimes pleasant to take the time to appreciate the elegance of some development.

Outline of these notes. — We start in Section 1 with bases on linear codes and their asymptotic behaviour. Section 2 gives an introduction to algebraic curves by providing the necessary material in algebraic geometry. Section 3 introduces algebraic geometry codes and states the main result: Tsfasman–Vlăduţ–Zink Theorem. The remainder of the notes are dedicated to the proof of this statement. Sections 4 and 5 provide further material on elliptic and modular curves respectively. Section 6 concludes the proof.

Acknowledgements. — First, I would like to thank Gianira Alfarano, Karan Khaturia, Alessandro Neri, Violetta Weger, the organisers of the *Algebraic Coding Theory Summer School*(2) 2022 who gave me the motivation to type-write old hand-written notes. I would probably never have found the time to do it if they did not ask me for. Several colleagues spent time to carefully read these notes. In particular, I express a deep gratitude to Elena Berardini, Maxime Bombar, Grégoire Lecerf, Jade Nardi, Christophe Ritzenthaler, Joachim Rosenthal and Gilles Zémor for their relevant comments on the preliminary version of the notes.

The author is funded by the french *Agence nationale de la recherche* for the collaborative project ANR-21-CE39-0009-BARRACUDA.

1. Linear Codes

1.1. Context. — In the sequel we are interested in *linear q–ary codes*, which are linear subspaces of $\mathbb{F}_q^n$. What makes the study hard, but also deeply interesting is that we are not only considering elementary objects such as finite dimensional vector spaces but spaces endowed with a **metric**: the *Hamming metric.* The Hamming distance between two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ is denoted by

$$\mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) \overset{\textbf{def}}{=} \sharp\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}.$$

The *Hamming weight* of a vector is its Hamming distance to the zero vector.

$$\forall \boldsymbol{x} \in \mathbb{F}_q^n, \qquad \mathrm{w_H}(\boldsymbol{x}) \overset{\textbf{def}}{=} \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{0}).$$

1.2. Linear codes. — Unless otherwise specified, a *code* will denote a linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$. The vectors of $\mathcal{C}$ are usually referred to as *codewords.* The *dimension* of $\mathcal{C}$ regarded as an $\mathbb{F}_q$–vector space is always denoted by k and its *minimum distance* denoted by d is defined as

$$d \overset{\textbf{def}}{=} \min_{\substack{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C} \\ \boldsymbol{x} \neq \boldsymbol{y}}} \{\mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y})\} = \min_{\boldsymbol{c} \in \mathcal{C} \setminus \{0\}} \{\mathrm{w_H}(\boldsymbol{c})\},$$

where the last equality is a consequence of the linearity. The *parameters* of a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ refer to the triple n, k, d and is usually denoted as $[n, k, d]_q$, where the cardinality q of the base field is recalled in

[1] Litterally : "for the beauty of the thing"

[2] `https://math.uzh.ch/act/`

subscript. Finally, one can also be interested in the *rate* and *relative distance* of a code, respectively defined and denoted as follows:

$$R \overset{\mathbf{def}}{=} \frac{k}{n} \qquad \text{and} \qquad \delta \overset{\mathbf{def}}{=} \frac{d}{n} \cdot$$

A longstanding problem in coding theory is which kind of triples of parameters $[n, k, d]$ can be achieved? A code will be considered as "good" if both k and d are as close as possible to n. However, many upper bounds exist, the most elementary one being the *Singleton bound* saying that for any code with parameters $[n, k, d]_q$ we have

$$k + d \leqslant n + 1. \tag{1}$$

The rationale behind this question is that both k and d quantify some feature of linear codes. Suppose we are given a *transmission channel*, that can be either a wire or a wireless communication for instance an exchange between electronic devices like between a computer and a WiFi antenna. The rate is nothing but the ratio of information divided by the quantity of data which is actually sent across the channel. Hence, the rate $R = k/n$ quantifies the efficiency of encoding.

On the other hand, the minimum distance quantifies how far are words from each other and hence the theoretical ability to recover an original message from a corrupted codeword[(3)].

Finally, suppose that our objective is to correct errors from a given channel. Consider for instance the *q–ary symmetric channel with parameter* $p \in [0, 1 - \frac{1}{q}]$ which takes as input a vector $\boldsymbol{c} \in \mathbb{F}_q^n$ and outputs the vector $\boldsymbol{c} + \boldsymbol{e}$ where $\boldsymbol{e} = (e_1, \dots, e_n)$ and the e_i's are independent random variables over $\mathbb{F}_q$ taking value 0 with probability $1 - p$ and any other value in $\mathbb{F}_q \setminus \{0\}$ with probability $\frac{p}{q-1}$. The average weight of our error vector satisfies

$$\mathbb{E}(\mathrm{w_H}(\boldsymbol{e})) = pn.$$

However, for small values of n, deviations may happen and it is possible that our input vector $\boldsymbol{c}$ is corrupted by much more than $\lfloor pn \rfloor$ errors. Therefore, it is relevant to consider large values of n for which the law of large numbers will assert us that the weight of the error will be close to its expectation.

This last discussion motivates the search of sequences of codes $(\mathcal{C}_s)_{s \in \mathbb{N}}$ with parameters $[n_s, k_s, d_s]$ where

$$\lim_{s \to +\infty} n_s = +\infty$$

and

$$\lim_{s \to +\infty} \frac{k_s}{n_s} = R \qquad \lim_{s \to +\infty} \frac{d_s}{n_s} = \delta.$$

Remark 1. — Usually in the literature, the sequences $(k_s/n_s)_s$ and $(d_s/n_s)_s$ are not supposed to converge and lim sup's are used instead of actual limits.

In this setting, the question of the achievable pairs $(\delta, R) \in [0, 1] \times [0, 1]$ remains open. Some bounds are known:

- Singleton bound immediately entails that $R + \delta \leqslant 1$;
- A more precise bound called *Plotkin bound* entails that $R + \delta \leqslant 1 - \frac{1}{q}$. See for instance [**Cou16**, Chap. 4]
- A principle that "constructing bad codes from good ones is always possible" permits to prove that give an achievable pair (δ, R) any pair (δ', R') with $\delta' \leqslant \delta$ and $R' \leqslant R$ is achievable too.

  Exercise 2. — Prove this last assertion.

- More precisely, it has been proved by Manin [**VM84**], that the frontier between the subdomain of $[0, 1] \times [0, 1]$ of achievable pairs (δ, R) and the non achievable ones is the graph of a continuous function $R = \alpha_q(\delta)$. However, if proving the existence and the continuity of this function α_q is not very hard, having an explicit description of it remains a widely open problem. An upper bound for α_q is given by the minimum of all the known upper bounds on the achievable pairs (δ, R).

[(3)] Here we do not introduce any consideration about practical algorithms to correct errors

- On the other hand a famous result on the average behaviour of random codes referred to as the Gilbert–Varshamov bound asserts that for a random code[4] $\mathcal{C} \subseteq \mathbb{F}_q^n$ with fixed rate R, then for any $\varepsilon > 0$ the probability that the relative distance δ of $\mathcal{C}$ satisfies
$$R \in [1 - H_q(\delta) - \varepsilon, 1 - H_q(\delta) + \varepsilon],$$
goes to 1 when n goes to infinity. The function $H_q(\cdot)$ is the q–ary entropy function defined as
$$H_q : \left\{ \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \left\{ \begin{array}{ccc} -\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x) & \text{if} & x \neq 0,1 \\ 0 & \text{otherwise.} & \end{array} \right. \end{array} \right.$$
In short, the pair (δ, R) for a random sequence satisfies $R = 1 - H_q(\delta)$.

In summary, the unknown function $\delta \mapsto \alpha_q(\delta)$ whose graph is the frontier of the domain of achievable pairs (δ, R) is known to be continuous, to be bounded from below by the Gilbert–Varshamov bound $\delta \mapsto 1 - H_q(\delta)$ and bounded from above by the min of all known upper bounds. For a long time, it has been supposed that Gilbert Varshamov bound was optimal and that somehow, no family of codes could asymptotically beat random codes. A breakthrough is due to Tsfasman, Vlăduţ and Zink [**TVZ82**] who showed that the asymptotic Gilbert Varshamov bound is not always optimal. More precisely, they proved the following statement.

Theorem 3. — *Let $q = p^2$ where p is a prime number. Then for any $R \in [0,1]$, there exists a sequence of codes whose length goes to infinity and whose asymptotic parameters (δ, R) satisfy*
$$R + \delta \geqslant 1 - \frac{1}{p-1}\cdot$$

Remark 4. — Actually, the result holds for any $q = p^{2m}$ where p is prime and $m \geqslant 1$.

Remark 5. — Actually, the result on codes is the corollary of a statement on the existence of a sequence of algebraic curves with specific properties (see further Theorem 41). This statement on curves has proved by Tsfasman, Vlăduţ and Zink in [**TVZ82**] and independently by Ihara in [**Iha81**]. However, Ihara did not rely this result with coding theory while Tsfasman *et. al.* did.

It turns out that, as illustrated by Figures 1 and 2, for $q \geqslant 49$, such codes beat Gilbert Varshamov bound. These codes, are actually far from being random and are constructed using elegant techniques from number theory and algebraic geometry. The objective of these notes is to outline a proof of this incredible result, which is probably one of the major breakthroughs of coding theory.

2. Algebraic curves

The objective of this section is **not** to provide an in depth lecture of algebraic geometry but only to give the minimal prerequisites in algebraic geometry to understand the sequel of these notes. In particular, here most of the proofs will be omitted. I encourage any reader who feels comfortable with algebraic geometry and for whom reading Harsthorne's book [**Har77**] is not harder than reading Harry Potter to **skip** this section for two reasons:

- she/he will not learn anything in it;
- for a reader who feels comfortable with the language of schemes, the contents of this section could appear to be dirty.

If you wish further details on algebraic geometry, I can encourage the following readings depending from your knowledge on the topic:

- Walker's book [**Wal00**] is an excellent first reading if you do not know anything about algebraic geometry and algebraic geometry codes.

[4] This can be formalised as follows, consider the set of all codes of length n and dimension Rn in $\mathbb{F}_q^n$. This set is finite, and let $\mathcal{C}$ be a random variable uniformly distributed over this set.

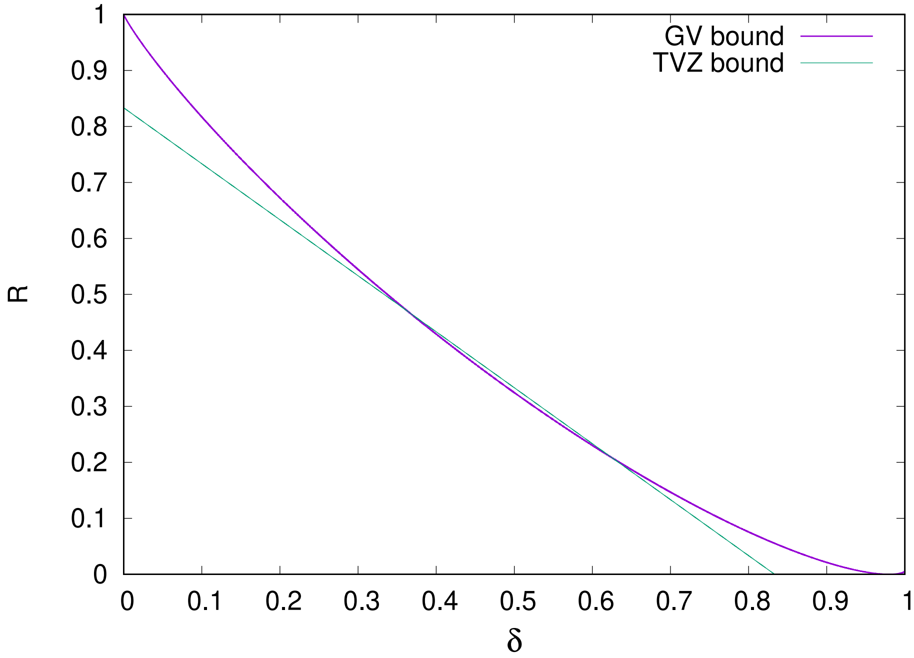

FIGURE 1. The TVZ bound for $q = 49$

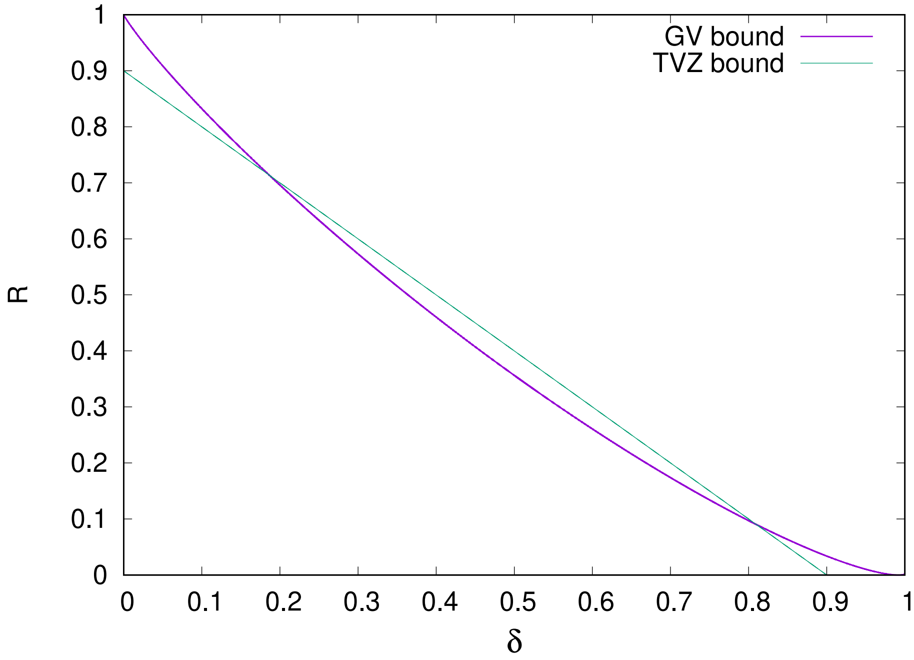

FIGURE 2. The TVZ bound for $q = 121$

- If you do **not** like geometry, Stichtenoth's book [**Sti09**] proposes an excellent introduction to algebraic geometry codes from a purely arithmetic point of view. It provides in particular a different proof of the Tsfasman–Vlăduţ–Zink theorem based on so–called *recursive towers of function fields* which excludes any geometric consideration.

- A more advanced presentation on algebraic geometry codes appears in Tsfasman Vlăduţ and Nogin's book [**TVN07**] and Stepanov [**Ste99**] .
- Finally, the reader interested in discovering algebraic geometry out of the context of algebraic coding theory is encouraged to look (for instance) at the books [**Ful89, Sha94**]. Lorenzini's book [**Lor96**] can be an excellent reading either if you wish a better focus on the arithmetic side.

2.1. Plane curves and functions. — Let $\mathbb{K}$ be a perfect field[(5)] and $\overline{\mathbb{K}}$ be its algebraic closure. We denote by $\mathbb{A}^2(\overline{\mathbb{K}})$ and $\mathbb{P}^2(\overline{\mathbb{K}})$ respectively the affine and projective planes over $\overline{\mathbb{K}}$. An affine *plane curve* $\mathscr{X}$ over $\mathbb{K}$ is the vanishing locus in $\mathbb{A}^2(\overline{\mathbb{K}})$ of a nonzero two variables polynomial $f(x,y) \in \mathbb{K}[x,y]$. Similarly, a *projective plane curve* is the vanishing locus in $\mathbb{P}^2(\overline{\mathbb{K}})$ of a nonzero homogeneous polynomial $F(X,Y,Z) \in \mathbb{K}[X,Y,Z]$. Recall that the projective plane $\mathbb{P}^2(\overline{\mathbb{K}})$ is the set of vectorial lines of $\overline{\mathbb{K}}^3$ or equivalently is the quotient set

$$\mathbb{P}^2(\overline{\mathbb{K}}) \stackrel{\textbf{def}}{=} (\overline{\mathbb{K}}^3 \setminus \{0\})/\overline{\mathbb{K}}^\times,$$

and its elements are represented as triples $(u:v:w)$ with the equivalence relation $(u:v:w) \sim (a:b:c)$ if there exists $\lambda \in \overline{\mathbb{K}}^\times$ such that $u = \lambda a$, $v = \lambda b$ and $w = \lambda c$.

Such an affine (resp. projective) curve is said to be *irreducible* if f (resp. F) is an irreducible polynomial in $\mathbb{K}[x,y]$ (resp. $\mathbb{K}[X,Y,Z]$) and *absolutely irreducible* if f (resp. F) is irreducible when regarded as an element of $\overline{\mathbb{K}}[x,y]$ (resp. $\overline{\mathbb{K}}[X,Y,Z]$).

Example 6. — Suppose $\mathbb{K} = \mathbb{Q}$ and consider the affine curve $\mathscr{X}$ with equation $x^2 - 2y^2 = 0$. This curve is irreducible but **not** absolutely irreducible. Indeed, over $\overline{\mathbb{Q}}$, the equation of the curve factorizes as $(x - \sqrt{2}y)(x + \sqrt{2}y) = 0$ and this factorisation is not defined over $\mathbb{Q}$: the polynomial $x^2 - 2y^2$ is irreducible over $\mathbb{Q}$ but not over $\overline{\mathbb{Q}}$. Geometrically speaking, $\mathscr{X}$ is the union of the two lines with respective equations $x - \sqrt{2}y = 0$ and $x + \sqrt{2}y = 0$. These lines are not defined over $\mathbb{Q}$ but their union is.

Given an affine irreducible plane curve $\mathscr{X}$, the quotient ring $\mathbb{K}[x,y]/(f)$ is integral and its field of fractions $\mathrm{Frac}(K[x,y]/(f))$ is well–defined and referred to as the *function field* of $\mathscr{X}$. In the projective setting, the function field can also be defined as the field of fractions $\frac{A(X,Y,Z)}{B(X,Y,Z)}$ where A, B are homogeneous polynomials of **the same degree** with B is not divisible by F and with the relation:

$$\frac{A(X,Y,Z)}{B(X,Y,Z)} = \frac{C(X,Y,Z)}{D(X,Y,Z)} \quad \text{if} \quad F \text{ divides } (AD - BC).$$

For an affine curve $\mathscr{X}$, elements of $\mathbb{K}[x,y]/(f)$ can be understood as restrictions of polynomial functions to the curve $\mathscr{X}$. Indeed, considering two polynomials $a(x,y), b(x,y) \in \mathbb{K}[x,y]$ regarded as functions $\mathbb{A}^2(\overline{\mathbb{K}}) \to \overline{\mathbb{K}}$, one can consider their restrictions to $\mathscr{X}$ and a well–known result usually called *Hilbert's Nullstellensatz* (see for instance [**Ful89**, § 1.7]) asserts that their restrictions to $\mathscr{X}$ are the same if and only if f divides $a - b$ and hence if and only if they are congruent modulo the ideal spanned by f.

In the projective setting, a homogeneous polynomial cannot be interpreted as a function $\mathbb{P}^2(\overline{\mathbb{K}}) \to \overline{\mathbb{K}}$ since an element of $\mathbb{P}^2(\overline{\mathbb{K}})$ is described by a triple $(u:v:w)$ but also by any other triple $(\lambda u : \lambda v : \lambda w)$ for any $\lambda \in \overline{\mathbb{K}}^\times$. Hence, given a non constant homogeneous polynomial $P \in \mathbb{K}[X,Y,Z]$ of degree $d > 0$, the evaluation cannot make sense since $P(\lambda u, \lambda v, \lambda w) = \lambda^d P(u,v,w)$. Note however that, for such a polynomial, vanishing at a point is a well–defined notion. Moreover, the evaluation of a fraction P/Q of two homogeneous polynomials with the same degree makes sense since

$$\frac{P(\lambda u, \lambda v, \lambda w)}{Q(\lambda u, \lambda v, \lambda w)} = \frac{\lambda^d P(u,v,w)}{\lambda^d Q(u,v,w)} = \frac{P(u,v,w)}{Q(u,v,w)}.$$

This is the reason why we introduce these objects as the good definition of functions on a projective curve.

Remark 7. — Note that we are juggling with $\mathbb{K}$ and $\overline{\mathbb{K}}$. Here it is crucial no notice that the curve is defined as a set of points with coordinates in $\overline{\mathbb{K}}$, while functions, should be rational functions with coefficients in $\mathbb{K}$. On one hand, the function field is defined over $\mathbb{K}$ and describes the arithmetic of the

[(5)] In the sequel the fields of interest will be either $\mathbb{C}$ or finite fields $\mathbb{F}_q$.

curve. On the other hand, when describing a curve as a set of points, considering only the points with coordinates in $\mathbb{K}$ would be too poor: think for instance about the case where $\mathbb{K}$ is a finite field, in this situation the set of points with coordinates in $\mathbb{K}$ is finite and might actually be empty! Then, very different equations may provide the same set of points with coordinates in $\mathbb{K}$ while the sets of points over $\overline{\mathbb{K}}$ will be very different. This explains the rationale behind considering the points with coordinates in $\overline{\mathbb{K}}$.

Remark 8. — Note that when speaking about *functions*, these objects may not be defined everywhere on the curve and may have some poles somewhere. These objects can be understood as the algebraic geometric counterpart of meromorphic functions in complex analysis.

Remark 9. — It is well–known that the projective plane can be covered by affine planes sometimes called *affine charts*. Indeed one can embed the affine plane into $\mathbb{P}^2$ as:

$$\left\{\begin{array}{ccc} \mathbb{A}^2(\overline{\mathbb{K}}) & \longrightarrow & \mathbb{P}^2(\overline{\mathbb{K}}) \\ (x,y) & \longmapsto & (x:y:1) \end{array}\right. \quad \text{or} \quad \left\{\begin{array}{ccc} \mathbb{A}^2(\overline{\mathbb{K}}) & \longrightarrow & \mathbb{P}^2(\overline{\mathbb{K}}) \\ (x,y) & \longmapsto & (x:1:y) \end{array}\right. \quad \text{or} \quad \left\{\begin{array}{ccc} \mathbb{A}^2(\overline{\mathbb{K}}) & \longrightarrow & \mathbb{P}^2(\overline{\mathbb{K}}) \\ (x,y) & \longmapsto & (1:x:y). \end{array}\right.$$

The images of these three embeddings cover the full projective plane. Hence, given a projective curve, one can consider the restriction of the curve on the image of one of the above embeddings and get an affine curve. Practically, starting with a projective curve with equation $F(X,Y,Z)=0$ one can consider for instance the affine curve with equation $F(x,y,1)=0$ but also those with equations $F(x,1,y)=0$ or $F(1,x,y)=0$. Hence, one can deduce affine curves (affine charts) from a given projective curve. On the other hand, starting from an affine curve $\mathscr{X}$ with equation $f(x,y)=0$ the homogeneous polynomial $F(X,Y,Z)$ of degree $\deg f$ such that $f(x,y)=F(x,y,1)$ (such a *homogeneization* is unique, details are left to the reader) is the equation of a curve sometimes referred to as the *projective closure* of $\mathscr{X}$.

A crucial fact is that a curve and its projective closure share a common object : **their function field remains the very same one**.

2.2. Points. — A *point* of $\mathscr{X}$ is an element $(a,b)\in\mathbb{A}^2(\overline{\mathbb{K}})$ (resp. $(u:v:w)\in\mathbb{P}^2(\overline{\mathbb{K}})$) such that $f(a,b)=0$ (resp. $F(u,v,w)=0$). A point is said to be *a rational point* or a $\mathbb{K}$–point if its coordinates all lie in $\mathbb{K}$. More generally, given an extension $\mathbb{L}/\mathbb{K}$, one can define the notions of $\mathbb{L}$–points of $\mathscr{X}$. The set of $\mathbb{K}$–points or $\mathbb{L}$–points of $\mathscr{X}$ respectively denoted by $\mathscr{X}(\mathbb{K})$ and $\mathscr{X}(\mathbb{L})$. One of topics of interest for us in the sequel is the case $\mathbb{K}=\mathbb{F}_q$. In this situation, one sees easily that $\mathscr{X}(\mathbb{F}_q)$ is finite. Indeed, it is a subset of $\mathbb{A}^2(\mathbb{F}_q)$ or $\mathbb{P}^2(\mathbb{F}_q)$ which are both finite sets. On the other hand $\mathscr{X}$ has been defined as a set of $\overline{\mathbb{K}}$–points that we sometimes call the *geometric points* in the sequel, hence we can also denote it as $\mathscr{X}(\overline{\mathbb{K}})$ when we wish to emphasize that we are interested in *any* possible point.

Given an affine (resp. projective) curve $\mathscr{X}$ defined by the equation $f(x,y)=0$ (resp. $F(X,Y,Z)=0$) over a field $\mathbb{K}$, a point $P\in\mathscr{X}(\overline{\mathbb{K}})$ with coordinates (x_P,y_P) (resp. $(u_P:v_P:w_P)$) is said to be *singular* if

$$\frac{\partial f}{\partial x}(x_P,y_P)=\frac{\partial f}{\partial y}(x_P,y_P)=0$$

resp.

$$\frac{\partial F}{\partial X}(u_P,v_P,w_P)=\frac{\partial F}{\partial Y}(u_P,v_P,w_P)=\frac{\partial F}{\partial Z}(u_P,v_P,w_P)=0.$$

A non singular point is said to be *regular*. A curve without singular points is said to be *regular* or *smooth*. On the other hand a curve having at least one singular point is said to be *singular*. It can be proved that the set of singular points of a curve is always finite.

From now on, unless otherwise specified, **any *curve* is smooth projective and absolutely irreducible.**

2.3. Galois action on points. — Recall that, for the sake of simplicity, we restrict the definitions to the case where the base field $\mathbb{K}$ is perfect. This is not a strong restriction for the subsequent purpose where $\mathbb{K}$ will always be either finite or of characteristic zero.

Given a curve $\mathscr{X}$ defined over $\mathbb{K}$, any point $P\in\mathscr{X}(\overline{\mathbb{K}})$ has coordinates (x_P,y_P) (or $(u_P:v_P:w_P)$ in the projective setting). These coordinates being in $\overline{\mathbb{K}}$ while $\mathscr{X}$ is defined by polynomial equations with coefficients in $\mathbb{K}$, there is a natural action of $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ on points of $\mathscr{X}$. Note that the coordinates of P

are algebraic over $\mathbb{K}$ and hence generate a finite extension of $\mathbb{K}$ usually denoted $\mathbb{K}(P)$. Therefore, even if $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ may be a complicated object (a profinite group), P is stabilized by $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K}(P))$ and hence the orbit of P is a finite set which is nothing but the orbit of P under the action of the finite group $\mathrm{Gal}(\mathbb{K}(P)'/\mathbb{K})$, where $\mathbb{K}(P)'$ is the Galois closure of $\mathbb{K}(P)$ over $\mathbb{K}$.

Definition 10. — Let $\mathbb{K}$ be a perfect field, a *closed point* of a curve $\mathscr{X}$ defined over $\mathbb{K}$ is the orbit of a geometric point $P \in \mathscr{X}(\overline{\mathbb{K}})$ under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$.

The number of elements in such an orbit is referred to as the *degree* of the closed point. It is also the extension degree $[\mathbb{K}(P) : \mathbb{K}]$. A rational point is always closed since it is fixed by any element of the absolute Galois group and hence it equals to its own orbit under this group action.

Remark 11. — If you prefer the language of number theory, closed points are nothing but the geometric analogue of the *places* of the function field $\mathbb{K}(\mathscr{X})$.

Example 12. — Consider the case $\mathbb{K} = \mathbb{Q}$ and the affine curve $\mathscr{C}$ with equation $x^2 + y^2 - 1 = 0$ (a circle). The point with coordinates $(1, 0)$ is a rational point of $\mathscr{X}$, *i.e.* an element of $\mathscr{C}(\mathbb{Q})$. The complex point $(2, \sqrt{3}i)$, (where $i^2 = -1$), is a geometric point of $\mathscr{C}$, *i.e.* an element of $\mathscr{C}(\mathbb{C})$. Finally, $\{(2, i\sqrt{3}), (2, -i\sqrt{3})\}$ is a closed point of degree 2 of $\mathscr{C}$.

2.4. Maps between curves. — As usually in algebra, once structures have been introduced: for instance groups, rings, modules, etc., one introduces morphisms between these objects. In the case of curves, we are interested in two kinds of maps referred to as *morphisms* and *rational maps.* A *rational map* between two affine (resp. projective) curves $\mathscr{X}, \mathscr{Y}$ contained in $\mathbb{A}^2$ (resp. $\mathbb{P}^2$) is a map:

$$\varphi : \left\{ \begin{array}{ccc} \mathscr{X} & \dashrightarrow & \mathscr{Y} \\ (x, y) & \longmapsto & (\varphi_1(x, y), \varphi_2(x, y)) \end{array} \right.$$

resp.

$$\psi : \left\{ \begin{array}{ccc} \mathscr{X} & \dashrightarrow & \mathscr{Y} \\ (u : v : w) & \longmapsto & (\psi_1(u, v, w), \psi_2(u, v, w), \psi_3(u, v, w)). \end{array} \right.$$

where ϕ_1, ϕ_2 (resp. ψ_1, ψ_2, ψ_3) are elements of $\mathbb{K}(\mathscr{X})$ (and, in the projective setting, at least one of the three functions ψ_1, ψ_2, ψ_3 is nonzero). The dashed arrow $\dashrightarrow$ is here to emphasize the fact that this map is not defined at every point but only on a subset[(6)]. For affine curves, at any point where φ_1, φ_2 have no pole, the map is defined and said to be *regular.* For projective curves, at any point P where for some $\eta \in \mathbb{K}(\mathscr{X})^\times$, $\eta\psi_1, \eta\psi_2, \eta\psi_3$ have no pole at P and are not simultaneously vanishing, the map ψ is well–defined and said to be *regular* at P. A rational map between two curves $\mathscr{X} \dashrightarrow \mathscr{Y}$ is said to be *regular* if it is regular at any point of $\mathscr{X}$.

A rational map $\varphi : \mathscr{X} \dashrightarrow \mathscr{Y}$ induces a field extension the other way around $\mathbb{K}(\mathscr{Y}) \hookrightarrow \mathbb{K}(\mathscr{X})$ which is defined as follows:

$$h \in \mathbb{K}(\mathscr{Y}) \longmapsto h \circ \varphi \in \mathbb{K}(\mathscr{X}).$$

The *degree* of φ is defined as the degree of this field extension.

Example 13. — Back to example 12. The map

$$\left\{ \begin{array}{ccc} \mathscr{C} & \dashrightarrow & \mathbb{P}^1 \\ (x, y) & \longmapsto & (x : 1) \end{array} \right. \tag{2}$$

is a rational map. It is also possible to construct a rational map $\mathbb{P}^1 \to \mathscr{C}$ as

$$\left\{ \begin{array}{ccc} \mathbb{P}^1 & \dashrightarrow & \mathscr{C} \\ (u : v) & \longmapsto & \left(\frac{v^2 - u^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2}\right) \end{array} \right. . \tag{3}$$

Note that these two maps are not inverses to each other.

Finally, the following statements are well–known. Their proofs are omitted.

[(6)] This subset turns out to be dense for a suitable topology called *Zariski topology*

Proposition 14. — *Let $h : \mathscr{X} \to \mathscr{Y}$ be a rational map between two smooth projective absolutely irreducible curves $\mathscr{X}, \mathscr{Y}$.*

(i) if $\mathscr{X}$ is smooth, then h is regular;

(ii) if h is non constant, then it is surjective.

2.5. Valuations. — Recall that a *local ring* is a ring having a unique maximal ideal. The term *local* comes precisely from the fact that many such rings may be understood as rings of functions characterized by a local property. For instance, given an affine curve $\mathscr{X}$ and a rational point P with coordinates (x_P, y_P), the ring $\mathcal{O}_{\mathscr{X},P}$ defined as the subring of $\mathbb{K}(\mathscr{X})$ of functions which are regular (*i.e.* have no pole) at P. Namely

$$\mathcal{O}_{\mathscr{X},P} \stackrel{\mathbf{def}}{=} \left\{ \frac{a(x,y)}{b(x,y)} \in \mathbb{K}(\mathscr{X}) \;\middle|\; b(x_P,y_P) \neq 0 \right\}.$$

One can prove that this ring is a local one whose maximal ideal is the ideal:

$$\mathfrak{m}_{\mathscr{X},P} \stackrel{\mathbf{def}}{=} \left\{ \frac{a(x,y)}{b(x,y)} \in \mathbb{K}(\mathscr{X}) \;\middle|\; b(x_P,y_P) \neq 0 \text{ and } a(x_P,y_P) = 0 \right\}.$$

When the point P is smooth, the ring $\mathcal{O}_{\mathscr{X},P}$ is known to be a discrete valuation ring, which means that the maximal ideal $\mathfrak{m}_{\mathscr{X},P}$ is principal and that, given a generator t of this maximal ideal, for any nonzero element $a \in \mathcal{O}_{\mathscr{X},P}$, there exists a non negative integer n and an element $\varphi \in \mathcal{O}_{\mathscr{X},P}^{\times}$ such that $a = \varphi t^n$. Such a generator t of $\mathfrak{m}_{\mathscr{X},P}$ is called a *local parameter* (or sometimes a *uniformising parameter*) at P. Moreover, the integer n does not depend on the choice of the generator t and is referred to as the *valuation* of a at P and denoted as $v_P(a)$. Next, one can easily prove that $\mathbb{K}(\mathscr{X})$ is nothing but the field of fractions of $\mathcal{O}_{\mathscr{X},P}$. Then, any function $h \in \mathbb{K}(\mathscr{X})$ can be written as $h = \frac{h_1}{h_2} \in \mathbb{K}(\mathscr{X}) \setminus \{0\}$, where $h_1, h_2 \in \mathcal{O}_{\mathscr{X},P}$ and the valuation of h at P will be defined as

$$v_P(h) = v_P(h_1) - v_P(h_2).$$

In summary, we introduced a map

$$v_P : \mathbb{K}(\mathscr{X}) \setminus \{0\} \to \mathbb{Z}$$

and this map is known to satisfy the following properties,

- $\forall a, b \in \mathbb{K}(\mathscr{X}) \setminus \{0\}$, $v_P(ab) = v_P(a) + v_P(b)$;
- $\forall a, b \in \mathbb{K}(\mathscr{X}) \setminus \{0\}$, $v_P(a+b) \geqslant \min\{v_P(a), v_P(b)\}$ and equality holds when $v_P(a) \neq v_P(b)$.

Finally, it should be emphasized that, even if we defined the notion at a rational point, one can actually extend the notion to any geometric point by replacing $\mathbb{K}(\mathscr{X})$ by $\overline{\mathbb{K}}(\mathscr{X})$, *i.e.* the field of rational functions on $\mathscr{X}$ with coefficients in $\overline{\mathbb{K}}$. Therefore, the valuation may be defined at any possible point.

2.6. Divisors. — A fundamental object when studying the geometry and arithmetic of a curve is divisors which somehow are the curve/function fields counterpart of fractional ideals in the theory of number fields.

Given a **smooth** curve $\mathscr{X}$ over a perfect field $\mathbb{K}$, a (geometric) *divisor* is a formal $\mathbb{Z}$–linear combination of geometric points of $\mathscr{X}$. A divisor is said to be *rational* if it is globally invariant under the action of $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$. Equivalently, it is a formal sum of closed points of $\mathscr{X}$.

Hence a divisor G on $\mathscr{X}$ can be represented as

$$G = n_1 P_1 + \cdots + n_r P_r, \tag{4}$$

where the n_i's are integers and the P_i's are geometric points of $\mathscr{X}$. The set $\{P_1, \ldots, P_r\}$ is referred to as the *support* of G. The divisor is rational if for any $i, j \in \{1, \ldots, r\}$ such that P_i, P_j are in the same orbit under the action of $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$, then $n_i = n_j$.

Remark 15. — We emphasize that a sum of rational points yields a rational divisor but the converse is false. A rational divisor may be a sum of non rational points. See the subsequent Example 16.

Example 16. — Back to the curve of Example 12 defined over $\mathbb{Q}$ with equation $x^2 + y^2 - 1 = 0$, consider the points $P = (\frac{1}{2}, \frac{\sqrt{3}}{2})$, $P' = (\frac{1}{2}, -\frac{\sqrt{3}}{2})$ and $Q = (1, 0)$. Then, $aP + bP' + cQ$ is a rational divisor on the curve if and only if $a = b$.

The group of divisors is equipped with a partial order relation denoted $\leqslant$ and defined as follows. Given two divisors

$$G = \sum_{P \in \mathscr{X}(\overline{\mathbb{K}})} n_P P \quad \text{and} \quad G' = \sum_{P \in \mathscr{X}(\overline{\mathbb{K}})} n'_P P,$$

we say that $G \leqslant G'$ if

$$\forall P \in \mathscr{X}(\overline{\mathbb{K}}),\ n_P \leqslant n'_P.$$

In particular, a divisor G is said to be *positive* if $G \geqslant 0$, where 0 denotes the zero divisor.

Given a divisor G as in (4), its *degree* is defined as

$$\deg G \stackrel{\text{def}}{=} n_1 + \cdots + n_r.$$

Given a function $f \in \mathbb{K}(\mathscr{X}) \setminus \{0\}$, one can associate its divisor denoted (f) and defined as

$$(f) \stackrel{\text{def}}{=} \sum_{P \in \mathbb{K}(\mathscr{X})} v_P(f) P. \tag{5}$$

Such a divisor is called a *principal divisor.*

Remark 17. — For such an object to be a divisor, we need to show that the sum (5) is finite, *i.e.* that the n_P's are all zero but a finite number of them. This is actually due to a well–known fact appearing in the next statement whose proof is omitted.

Proposition 18. — *A nonzero rational function on a curve has only a finite number of zeroes and poles.*

Remark 19. — It is worth noting that a principal divisor is rational. Indeed, one can first note that, since $f \in \mathbb{K}(\mathscr{X})$ and hence has its coefficients in $\mathbb{K}$, then for any geometric point $P \in \mathscr{X}(\overline{\mathbb{K}})$ and any $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ then $v_P(f) = v_{\sigma(P)}(f)$.

The following very classical statement is crucial in the sequel.

Proposition 20. — *The degree of principal divisor is always* 0.

We finish this discussion with a statement that we admit and which will be useful later.

Proposition 21. — *A principal divisor (f) associated to $f \in \mathbb{K}(\mathscr{X})^\times$ is zero if and only if f is constant.*

2.7. Genus and Riemann–Roch Theorem. — The most elementary curve one may define is the affine line $\mathbb{A}^1$ and its projective closure being the projective line $\mathbb{P}^1$. Regular functions on $\mathbb{A}^1$ are nothing but univariate polynomials. Regarding such a polynomial $h(x) \in \mathbb{K}[x]$ as rational function on $\mathbb{P}^1$, it has a pole at the point "at infinity", *i.e.* the points with homogeneous coordinates $(1 : 0)$ and one can prove that the valuation at this pole is nothing but $-\deg h$.

Therefore, the space $\mathbb{K}[x]_{\leqslant n}$ of polynomials of degree less than or equal to n can be (with enough pedantry) defined as the space of rational functions on $\mathbb{P}^1$ which are regular everywhere on an affine chart and with valuation larger than or equal to $-n$ at the point at infinity. Denoting by P_∞ this point at infinity, then the space $\mathbb{K}[x]_{\leqslant n}$ can be regarded as the space of rational functions $h \in \mathbb{K}(\mathbb{P}^1)$ which are either 0 or such that

$$(h) \geqslant -nP_\infty.$$

As the following definition suggests, Riemann–Roch spaces are generalisations for curves of the spaces $\mathbb{K}[x]_{\leqslant n}$.

Definition 22 **(Riemann–Roch space).** — Let $\mathscr{X}$ be a smooth projective absolutely irreducible curve over $\mathbb{K}$ and G be a rational divisor on X. Then the *Riemann–Roch space associated to* G is defined as

$$L(G) \stackrel{\text{def}}{=} \{h \in \mathbb{K}(\mathscr{X}) \mid (h) + G \geqslant 0\} \cup \{0\}.$$

This is a vector space over $\mathbb{K}$.

Remark 23. — According to the previous discussion, on $\mathbb{P}^1$, we have $L(nP_\infty) \simeq \mathbb{K}[x]_{\leqslant n}$.

The following statement summarises some properties of Riemann–Roch spaces.

Proposition 24. — *(i) A Riemann–Roch space is a vector space over $\mathbb{K}$ of finite dimension;*
(ii) For any rational divisor $G < 0$, we have $L(G) = \{0\}$;
(iii) For any rational divisor G, we have $\dim_{\mathbb{K}} L(G) \leqslant \deg G + 1$.

With the above statement at hand, we can introduce a fundamental invariant of a curve: its *genus*. There are dozens of manners to define this object but none of them is trivial. The one given in these notes is far from being satisfying since it is clearly not intuitive. However, it permits to define the object with a minimal amount of material.

Definition 25 **(Genus of a curve).** — Let $\mathscr{X}$ be a smooth projective absolutely irreducible curve. The *genus* of $\mathscr{X}$ is defined as

$$g = 1 - \min_{D}\{\dim_{\mathbb{K}} L(D) - \deg D\},$$

where D ranges over all the divisors of $\mathscr{X}$.

Remark 26. — Proposition 24 (iii) asserts that the involved minimum exists and that the genus is nonnegative.

Exercise 27. — Prove the statement of Remark 26.

Exercise 28. — Using Definition 25, prove that the genus of the projective line $\mathbb{P}^1$ is zero.

Note that the effective computation of the genus is not a simple task. However, for smooth plane curves of degree d, there is a closed formula (see [**Ful89**, Prop. VIII.5]):

$$g = \frac{(d-1)(d-2)}{2}\cdot$$

This permits in particular to prove that the projective line and smooth conics have genus 0.

Remark 29. — The notion of genus can actually be defined for singular curves. In this context, two distinct invariants respectively called *arithmetic genus* and *geometric genus* can be defined. These two invariants coincide when the curve is smooth.

We conclude this section with Riemann–Roch Theorem, which is a crucial statement in the theory of algebraic curves. This statement is admitted and we refer the reader to Fulton [**Ful89**] or Stichtenoth's [**Sti09**] book for a proof. The first part of the statement is actually a straightforward consequence of the definition we gave for the genus (Definition 25).

Theorem 30 **(Riemann–Roch Theorem).** — *Let $\mathscr{X}$ be a smooth absolutely irreducible curve of genus g over $\mathbb{K}$ and G be a rational divisor on $\mathscr{X}$. Then*

$$\dim_{\mathbb{K}} L(G) \geqslant \deg G + 1 - g$$

and equality holds when $\deg G > 2g - 2$.

2.8. The Riemann–Hurwitz formula. — The last statement that will be useful in the sequel is Riemann–Hurwitz formula which relates the genera of two smooth projective absolutely irreducible curves $\mathscr{X}, \mathscr{Y}$ linked by a non constant rational map $\varphi : \mathscr{X} \dashrightarrow \mathscr{Y}$. Recall that, according to Proposition 14, such a map is regular and surjective. Denoting by δ its degree (see § 2.4 for the definition of degree), consider any geometric point $P \in \mathscr{Y}(\overline{\mathbb{K}})$. Then one can prove that $\varphi^{-1}(\{P\})$ is a finite subset of $\mathscr{X}(\overline{\mathbb{K}})$ and that for any P but finitely many of them the cardinality of $\phi^{-1}(\{P\})$ always equals δ.

The finite number of points of $\mathscr{Y}(\overline{\mathbb{K}})$ where this no longer holds are called *ramified points.* Given $Q \in \mathscr{X}(\overline{\mathbb{K}})$, $P = \varphi(Q)$ and t a local parameter at P, the *ramification index of* Q is defined as

$$e_Q \overset{\mathbf{def}}{=} v_Q(t \circ \varphi),$$

$t \circ \varphi$ being an element of $\mathbb{K}(\mathscr{X})$. It can be proved that this definition does not depend on the choice of the local parameter t at P. According to the previous definition, for any point $Q \in \mathscr{X}(\overline{\mathbb{K}})$ but finitely many of them, we have $e_Q = 1$.

Here we have the material to state Riemann–Hurwitz formula.

***Theorem 31* (Riemann–Hurwitz formula (Tame version)).** — *Let $\mathscr{X}, \mathscr{Y}$ be two smooth projective absolutely irreducible curves over $\mathbb{K}$ and $\varphi : \mathscr{X} \dashrightarrow \mathscr{Y}$ be a rational map. Suppose that for any $Q \in \mathscr{Y}(\overline{\mathbb{K}})$, the ramification index e_Q is prime to the characteristic of $\mathbb{K}$. Then, the genera $g_{\mathscr{X}}, g_{\mathscr{Y}}$ of $\mathscr{X}, \mathscr{Y}$ are related by the following formula.*

$$(2g_{\mathscr{X}} - 2) = \deg \varphi \cdot (2g_{\mathscr{Y}} - 2) + \sum_{Q \in \mathscr{Y}(\overline{\mathbb{K}})} (e_Q - 1).$$

Remark 32. — According to the previous discussion, the terms of the sum in the above formula are all zero but a finite number of them.

Remark 33. — The assumption "ramification indexes are prime to the characteristic" can be discarded at the cost of replacing the term $\sum(e_Q - 1)$ by a more complicated one. See [**Sti09**, Thm. 3.4.13].

This formula is particularly useful since many curves $\mathscr{X}$ are described by a morphism $\mathscr{X} \to \mathbb{P}^1$. Since $\mathbb{P}^1$ is known to have genus 0, the genus of $\mathscr{X}$ can be deduced from the knowledge of the degree of this map and the ramification indexes.

Example 34. — Consider the map (2) of Example 13 but here we regard the curve $\mathscr{C}$ as a curve over $\mathbb{C}$. One sees that any point $P = (t : 1) \in \mathbb{P}^1(\mathbb{C})$ has 2 preimages by the map if $t \notin \{-1, 1\}$ and only one if $t \in \{-1, 1\}$. Therefore, there are two ramified points both with ramification index 2 (one can show that the map does not ramify at infinity). Moreover, the map has degree 2. Then, Riemann–Hurwitz formula yields

$$2g_{\mathscr{C}} - 2 = 2(2g_{\mathbb{P}^1} - 2) + 2.$$

Since $g_{\mathbb{P}^1} = 0$, we deduce that $g_{\mathscr{C}} = 0$ too.

2.9. What about non plane curves? — A last important fact is that some curves are not plane and may be contained in $\mathbb{P}^N$ for $N > 2$. It is actually important in the sequel since we are searching for smooth curves $\mathscr{X}$ over a finite field $\mathbb{F}_q$ with $\sharp\mathscr{X}(\mathbb{F}_q)$ arbitrarily large. Since $\sharp\mathbb{P}^2(\mathbb{F}_q)$ is finite (and equal to q^2+q+1) such a curve may not be embeddable in $\mathbb{P}^2$ and requires a larger dimensional ambient space. So, the question is... what remains true when considering curves in $\mathbb{P}^N$ with $N > 2$? and actually, how are such objects defined?

We define a projective subvariety of $\mathbb{P}^N$ as the common vanishing locus of the elements of a homogeneous ideal $I \subseteq \mathbb{K}[X_0, \dots, X_N]$. If this ideal is prime, then the variety will be said to be *irreducible* and in this setting, the function field of the variety can be defined in the very same manner as in the plane case. Then, the *dimension* of the variety can be defined as the transcendence degree of the function field over $\mathbb{K}$. A curve will be a variety of dimension 1. Smoothness can be defined very similarly by requiring a non simultaneous vanishing of all the partial derivatives with respect to the $N + 1$ variables. All the other objects, rational maps, valuations, divisors, Riemann–Roch spaces can be defined in the very same manner at the cost of heavier notation. Finally all the previous statements on plane curves actually hold for any curve.

3. Algebraic geometry codes

Now, we have the necessary material to define algebraic geometry (AG) codes. Before, let us recall the definition of Reed–Solomon codes that AG codes generalise.

3.1. Reed–Solomon codes. —

Definition 35. — Let $\alpha_1, \dots, \alpha_n$ be distinct elements of $\mathbb{F}_q$. Let $0 \leqslant k \leqslant n$, the code $\mathbf{RS}_k$ is defined as

$$\mathbf{RS}_k(\alpha_1, \dots, \alpha_n) \stackrel{\mathbf{def}}{=} \{(p(\alpha_1), \dots, p(\alpha_n)) \mid p \in \mathbb{F}_q[x]_{\leqslant k-1}\}.$$

It is well–known that these codes have parameters $[n, k, n-k+1]_q$ and hence reach the Singleton bound (1). However, they are constrained in the sense that the α_i's should be distinct and hence the length should be bounded by q. Thus, even if these codes have optimal parameters, it is hopeless to use them in order to construct an infinite family of codes over a fixed field $\mathbb{F}_q$ whose length goes to infinity. Here, curves enter the game. Note first that Reed–Solomon codes may be defined in a much more pedant manner as follows. Consider the projective line $\mathbb{P}^1$ and let $P_1, \ldots, P_n$ be the rational points of $\mathbb{P}^1$ with respective homogeneous coordinates $(\alpha_1 : 1), \ldots, (\alpha_n : 1)$. Then, $\mathbf{RS}_k(\alpha_1, \ldots, \alpha_n)$ may be defined as

$$\mathbf{RS}_k(\alpha_1, \ldots, \alpha_n) = \{(h(P_1), \ldots, h(P_n)) \mid h \in L((k-1)P_\infty)\}\,.$$

This leads to a natural generalisation to algebraic curves. The interest being the fact that a curve may have more rational points than the projective line and hence replacing $\mathbb{P}^1$ by an arbitrary curve may provide the opportunity of getting codes of length larger than q.

3.2. Algebraic geometry codes. — We give a minimal introduction to algebraic geometry (AG) codes. The reader interested in further references is encouraged to have a look at the surveys [**HvLP98, Duu08, CR21**] or the books [**TVN07, Sti09**]. We also refer to [**HP95, BH08**] for references on the decoding of AG codes.

Definition 36. — Let $\mathscr{X}$ be a smooth absolutely irreducible curve over $\mathbb{F}_q$. Let $\mathcal{P} = (P_1, \ldots, P_n)$ be an ordered sequence of distinct rational points of $\mathscr{X}$. Let G be a rational divisor on $\mathscr{X}$ whose support avoids the points $P_1, \ldots, P_n$. Then, the algebraic geometry code $\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G)$ is defined as

$$\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G) \overset{\mathbf{def}}{=} \{(f(P_1), \ldots, f(P_n)) \mid f \in L(G)\}.$$

Once the codes are defined, their parameters can be evaluated using the previously introduced material of algebraic geometry.

Theorem 37. — *Let $\mathscr{X}$ be a smooth absolutely irreducible curve of genus g over $\mathbb{F}_q$. let $\mathcal{P} = (P_1, \ldots, P_n)$ be a tuple of rational points of $\mathscr{X}$ and G be a rational divisor on $\mathscr{X}$ whose support avoids $P_1, \ldots, P_n$. Suppose that* $\deg G < n$. *Then, the parameters $[n, k, d]_q$ of $\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G)$ satisfy*

$$k \geqslant \deg G + 1 - g \quad \textit{with equality when } \deg G > 2g-2; \tag{6}$$

$$d \geqslant n - \deg G. \tag{7}$$

Proof. — Denote by $D_{\mathcal{P}}$ the divisor $D_{\mathcal{P}} \overset{\mathbf{def}}{=} P_1 + \cdots + P_n$. Consider the map

$$ev_{\mathcal{P}} : \left\{ \begin{array}{ccc} L(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)). \end{array} \right.$$

Its image is trivially $\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G)$. The kernel of this map is the subspace of $L(G)$ of functions f vanishing at $P_1, \ldots, P_n$. This subspace is nothing but $L(G - D_{\mathcal{P}})$. By assumption, $\deg(G - D_{\mathcal{P}}) = -(n - \deg G)$, is negative and hence, from Proposition 24 (ii), $L(G - D_{\mathcal{P}}) = \ker ev_{\mathcal{P}} = \{0\}$. Thus, $ev_{\mathcal{P}}$ is injective and

$$\dim \mathcal{C}_L(\mathscr{X}, \mathcal{P}, G) = \dim L(G) \geqslant \deg G + 1 - g,$$

with equality if $\deg G > 2g - 2$. Here, the last inequality together with the equality case are due to Riemann–Roch Theorem (Theorem 30).

For the minimum distance, let us introduce $h \in L(G) \setminus \{0\}$ such that $ev_{\mathcal{P}}(h)$ has Hamming weight d. It means that there exist distinct points $P_{i_1}, \ldots, P_{i_{n-d}}$ among $P_1, \ldots, P_n$ at which h vanishes. Consequently, $h \in L(G - P_{i_1} - \cdots - P_{i_{n-d}})$ and since $h \neq 0$, the space $L(G - P_{i_1} - \cdots - P_{i_{n-d}}) \neq \{0\}$, which, from Proposition 24 (ii) again, implies that $\deg(G - P_{i_1} - \cdots - P_{i_{n-d}}) \geqslant 0$ and hence

$$d \geqslant n - \deg G.$$

□

Let us comment this last result. It was mentioned in § 1.2 that, from Singleton bound (1), any $[n, k, d]_q$ code satisfies

$$k + d \leqslant n + 1.$$

On the other hand, Theorem 37 asserts that an $[n,k,d]_q$ AG code $\mathcal{C}_L(\mathscr{X},\mathcal{P},G)$ satisfies

$$n+1-g \leqslant k+d.$$

In summary, AG codes are in the worst case at "distance g from Singleton bound". Thus, one can expect good codes for a "not too large" genus g. On the other hand, the objective is to construct sequences of codes whose length exceeds q and more generally construct families of codes over $\mathbb{F}_q$ whose length goes to infinity. Thus, for the length to be large, we look for curves with the largest possible number of rational points.

3.3. The problem of infinite sequence of curves with many points compared to their genus.

— We expect to get sequences of curves over $\mathbb{F}_q$ whose genus grows slowly and number of rational points grows quickly. However, these two objectives are somehow in opposition: to get many rational points, we need a large genus. A well–known result due to Weil asserts that for a smooth absolutely irreducible curve $\mathscr{X}$ over $\mathbb{F}_q$,

$$\sharp\mathscr{X}(\mathbb{F}_q) \leqslant q+1+2g\sqrt{q}. \tag{8}$$

Thus, we look for a good trade off between the genus and the number of rational points. Now, we have the material to reformulate our coding theoretic problem of producing asymptotically good infinite sequences of codes in terms of the construction of sequences of algebraic curves with specific features. For this, let us consider a sequence of curves $(\mathscr{X}_s)_{s\in\mathbb{N}}$ with sequence of genera $(g_s)_{s\in\mathbb{N}}$. We suppose that the sequence $(\sharp\mathscr{X}_s(\mathbb{F}_q))_{s\in\mathbb{N}}$ goes to infinity, hence, according to Weil's bound (8), the sequence of genera should also go to infinity. Let

$$\gamma = \limsup_{s\to+\infty} \frac{\sharp\mathscr{X}_s(\mathbb{F}_q)}{g_s}\cdot \tag{9}$$

For any such curve in the sequence, we fix a rational divisor G_s and the sequence of rational points $\mathcal{P}_s=(P_1,\dots,P_{n_s})$ will be chosen as the full list of rational points, *i.e.* $n_s=\sharp\mathscr{X}_s(\mathbb{F}_q)$.

Remark 38. — One could ask whether it is possible to have a rational divisor G_s of any degree whose support avoids $P_1,\dots,P_{n_s}$ while $\{P_1,\dots,P_{n_s}\}=\mathscr{X}(\mathbb{F}_q)$? The answer is positive, such divisors G_s exist and the constraint that the support of G_s should avoid $\mathscr{X}(\mathbb{F}_q)$ is actually easy to satisfy. See [**CR21**, Rem. 15.3.8] for a detailed discussion on this specific question.

Then, the codes $\mathcal{C}_L(\mathscr{X}_s,\mathcal{P}_s,G_s)$ have parameters $[n_s,k_s,d_s]_q$ satisfying

$$\begin{array}{rcl} n_s &=& \sharp\mathscr{X}_s(\mathbb{F}_q)\\ k_s &\geqslant& \deg G_s+1-g_s\\ d_s &\geqslant& n_s-\deg G_s. \end{array}$$

Therefore, one can eliminate $\deg G_s$ and get

$$k_s+d_s \geqslant n_s+1-g_s. \tag{10}$$

Set

$$R=\limsup_{s\to+\infty}\frac{k_s}{n_s} \quad\text{and}\quad \delta=\limsup_{s\to+\infty}\frac{d_s}{n_s}\cdot$$

Then, dividing (10) by n_s and letting s go to infinity, we get

$$R+\delta \geqslant 1-\frac{1}{\gamma},$$

where γ is defined in (9). Therefore, any pair (δ,R) lying on the line of equation $R+\delta=1-\frac{1}{\gamma}$ is achievable.

Remark 39. — Even if the term $\deg G_s$ has been eliminated, this term is worth in order to chose the point in the line of equation $R+\delta=1-\frac{1}{\gamma}$ you want to target.

Exercise 40. — Prove that by choosing a relevant sequence of rational divisors (G_s) on the curves $\mathscr{X}_s$, one can reach any point of the line of equation $R+\delta=1-\frac{1}{\gamma}\cdot$

3.4. The Ihara constant $A(q)$. — Now, we would like to estimate the optimal asymptotic parameters (δ, R) that can be achieved. For that, let us introduce the *Ihara constant*:

$$A(q) \overset{\mathbf{def}}{=} \limsup_{g \to +\infty} \max_{\substack{\mathscr{X},\ \text{curve} \\ \text{of genus } g}} \frac{\sharp \mathscr{X}(\mathbb{F}_q)}{g} \cdot$$

Then, the Tsfasman–Vlăduţ–Zink (TVZ) bound asserts the existence of families of codes whose asymptotic parameters (δ, R) satisfy

$$R + \delta \geqslant 1 - \frac{1}{A(q)} \cdot$$

This opens the question of the value of $A(q)$. The remainder of these notes consists in outlining a proof of the following statement.

Theorem 41. — *For $q = p^2$ and p a prime number, we have*

$$A(q) \geqslant \sqrt{q} - 1.$$

Combining the previous result with the TVZ bound, one ca prove that for $p \geqslant 7$, and hence when q is the square of a prime and is larger than or equal to 49, the TVZ bound exceeds the Gilbert Varshamov one, proving that some families of codes from algebraic curves are better than random codes.

Let us conclude with some comments.

- Actually, the result extends to $q = p^{2m}$ for any $m \geqslant 1$ but the proof gets more complicated and involves other families of curves. Namely, the proof to follow involves modular curves, while the general case involves Shimura curves. See [**Iha81, TVZ82**].
- The TVZ bound is actually optimal. Indeed, subsequently to the publication of Tsfasman–Vlăduţ–Zink result, in [**VD83**] Drinfeld and Vlăduţ proved that for any prime power q, we always have $A(q) \leqslant \sqrt{q} + 1$.
- Another proof of Theorem 41 using a very different approach has been given by Garcia and Stichtenoth in [**GS95**].

The core of the proof of this wonderful result rests on the use of families of curves called *modular curves* which parameterise families of algebraic curves called *elliptic curves.*

4. Elliptic curves

Elliptic curves is another fascinating topic in number theory. They are also a fundamental object in cryptography but this is not the point of these notes. In this section, we start by presenting basic notions about these objects over an arbitrary field. Our objective is in particular to construct these so–called *modular curves* which will yield excellent codes. These modular curves are algebraic curves which parameterise families of elliptic curves with a specific extra structure called *level.*

Afterwards, in Section 5, we will discuss elliptic curves and modular curves over $\mathbb{C}$. This choice of discussing complex curves in such notes might seem surprising while our interest will clearly be curves over finite fields. However, a preliminary study of the complex case presents several advantages. First, it provides a much more intuitive presentation of the topics with the benefits of the possible use of analytical tools. Second, even if the analytic proofs cannot transpose in the finite field setting, they permit to compute algebraic formulas, *i.e.* polynomial equations defining modular curves. These equations turn out to be defined over $\mathbb{Z}$ and then — and this is very far from being trivial — their reduction modulo p will give the equation of a curve parameterising elliptic curves over $\mathbb{F}_p$ or $\overline{\mathbb{F}}_p$ with some level structure.

Note. In this section, we assume the ground field $\mathbb{K}$ to have characteristic different from 2 and 3. Most of the material of the present section and the subsequent one are taken from the book [**Sil09**] and the lecture notes [**Mil17**].

4.1. Basic definitions. — An *elliptic curve $\mathscr{E}$* over a field $\mathbb{K}$ is a smooth projective curve of genus 1 with at least one rational point denoted by $O_{\mathscr{E}}$. From Proposition 21, the Riemann–Roch space $L(0)$ associated to the zero divisor contains only the constant functions and hence has dimension 1. Then, by Riemann–Roch Theorem, the spaces $L(2O_{\mathscr{E}})$ and $L(3O_{\mathscr{E}})$ have respective dimensions 2 and 3 (note that as soon as the divisor's degrees are positive, they are $> 2g-2$ and hence we fit in the equality case of Riemann–Roch Theorem). Denote by x, y two functions such that

$$L(2O_{\mathscr{E}}) = \mathrm{Span}_{\mathbb{K}}\{1, x\} \quad L(3O_{\mathscr{E}}) = \mathrm{Span}_{\mathbb{K}}\{1, x, y\}.$$

Note that these choices for x and y are not canonical and hence any of the following changes of variables are admissible

$$x' \leftarrow ax + b, \text{ with } a \neq 0 \qquad y' \leftarrow uy + vx + w, \text{ with } u \neq 0. \tag{11}$$

Now, consider the space $L(6O_{\mathscr{E}})$. It contains the functions

$$1, x, y, x^2, xy, x^3, y^2.$$

Moreover, again from Riemann–Roch Theorem, $L(6O_{\mathscr{E}})$ has dimension 6 and hence there is a nontrivial linear relation on these functions

$$y^2 + uxy + vy = ax^3 + bx^2 + cx + d.$$

Exercise 42. — Prove that y^2 and x^3 should be involved in this linear relation, which explains why, after a renormalisation, one can suppose the coefficient of y^2 to be 1. Deduce from this that $a \neq 0$.

Now, we perform successive changes of variables which are admissible, *i.e.* changes of variables of the form (11). A first one[7]: $y \leftarrow y + \frac{u}{2}x$ leads to an equation:

$$y^2 + v_1 y = a_1 x^3 + b_1 x^2 + c_1 x + d_1, \tag{12}$$

for some $a_1, b_1, c_1, d_1 \in \mathbb{K}$. A change $y \leftarrow y + \frac{v_1}{2}$ yields

$$y^2 = a_2 x^3 + b_2 x^2 + c_2 x + d_2. \tag{13}$$

for some $a_2, b_2, c_2, d_2 \in \mathbb{K}$. Next, a change of the form $x \leftarrow x + \frac{b_2}{3a_2}$ yields to an equation:

$$y^2 = a_3 x^3 + c_3 x + d_3, \tag{14}$$

for some $a_3, c_3, d_3 \in \mathbb{K}$. Finally, applying the change of variables $x \leftarrow a_3 x$, $y \leftarrow a_3^2 y$ and dividing both sides by a_3^4, we get an equation of the form

$$y^2 = x^3 + Ax + B, \tag{15}$$

for some $A, B \in \mathbb{K}$. Such an equation is called a *Weierstrass equation* of the curve.

Exercise 43. — Using Exercise 42, check that the last change of variables was admissible, *i.e.* that $a_3 \neq 0$.

In summary, starting from an elliptic curve $\mathscr{E}$ over $\mathbb{K}$, *i.e.* a smooth genus 1 curve with a rational point $O_{\mathscr{E}}$, we found two functions $x, y \in \mathbb{K}(\mathscr{E})$ which are both regular everywhere but at $O_{\mathscr{E}}$. These functions are related by the relation (15) and hence the function $y^2 - x^3 - Ax - B$ vanishes everywhere on $\mathscr{E}$. This leads to the following statement.

Theorem 44. — *Let $\mathscr{E}$ be an elliptic over a field $\mathbb{K}$ of characteristic different from 2 and 3,* i.e. *a smooth projective curve of genus 1 with a rational point $O_{\mathscr{E}}$, then there exist $x, y \in \mathbb{K}(\mathscr{E})$ such that the map*

$$\left\{ \begin{array}{ccc} \mathscr{E} & \dashrightarrow & \mathbb{P}^2 \\ P & \longmapsto & \left\{ \begin{array}{cc} (x(P) : y(P) : 1) & \textit{if} \quad P \neq O_{\mathscr{E}} \\ (0 : 1 : 0) & \textit{if} \quad P = O_{\mathscr{E}} \end{array} \right. \end{array} \right.$$

induces an isomorphism from $\mathscr{E}$ to the projective closure of the projective curve of equation $Y^2 = X^3 + AXZ^2 + BZ^3$.

[7] In order to keep light notation, we remove the ' in x', y' and hence write the outputs of the change of variables as the input, hence the notation $y \leftarrow y + \frac{u}{2}x$. This is not a completely rigorous notation and the reader bothered by this is encouraged to rewrite this page by replacing the x's and y's as x', x'', x''' and y', y'', y''' at the good spots.

Proof. — The fact that the image of $\mathscr{E}$ is contained in such a curve is a consequence of the previous discussion. To prove that this map is actually an isomorphism and in particular that the target curve is smooth, we refer the reader to [**Sil09**, Prop. III.3.1]. □

Remark 45. — Geometrically speaking, the sequence of changes of variables can be interpreted as follow. We started from an elliptic curve $\mathscr{E}$ and a first choice of functions x, y in $\mathbb{K}(\mathscr{E})$ lead to an isomorphism between $\mathscr{E}$ and a curve with equation (12). Then, we applied successive affine automorphisms to the plane in order to get curves of successive equations (13), (14) which are pairwise isomorphic and finish with a curve with equation (15) which is also isomorphic to $\mathscr{E}$.

Remark 46. — In the sequel, we will not only consider Weierstrass form. Actually, one can show that any curve of equation

$$y^2 = f(x)$$

where f is a squarefree polynomial of degree 3 is an elliptic curve and there is a change of variables permitting to put it in Weierstrass form.

4.2. The j–invariant.

— In what follows, it will be important to classify elliptic curves up to isomorphism. For this sake, we introduce a fundamental invariant: the *j–invariant.* Reconsider a Weierstrass equation (15)

$$y^2 = x^3 + Ax + B.$$

This equation is not unique, since once we got it, one can still apply changes of variables of the form $y \leftarrow u^3 y$, $x \leftarrow u^2 x$ and dividing both sides by u^6. This leads to another Weierstrass equation $y^2 = x^3 + A'x + B'$ where $A' = \frac{A}{u^4}$ and $B' = \frac{B}{u^6}$. Let us introduce

$$j \overset{\textbf{def}}{=} 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

This quantity is well–defined since one can prove that the denominator $4A^3 + 27B^2$ is zero if and only if the corresponding curve is singular (see [**Sil09**, Prop. III.1.4(a)(i)]). Hence, j is well–defined for any elliptic curve since, by definition, such curves are smooth. Moreover, j is left invariant by the previous change of variables and one can show that, once we obtained a Weierstrass equation, the only changes of variables preserving the Weierstrass equation structure are the aforementioned ones.

We conclude this subsection by the following statements asserting that the j–invariant characterises an elliptic curve over $\overline{\mathbb{K}}$ in a unique manner. The proof is omitted and can be found in [**Sil09**, Prop. III.1.4(b-c)].

Proposition 47. — *Two elliptic curves are isomorphic over $\overline{\mathbb{K}}$ if and only if they have the same j–invariant. Conversely, given $j_0 \in \overline{\mathbb{K}}$, there exists an elliptic curve $\mathscr{E}$ over $\mathbb{K}(j_0)$ with j–invariant j_0.*

Remark 48. — Note that two elliptic curves defined over $\mathbb{K}$ may be isomorphic over $\overline{\mathbb{K}}$ without being isomorphic over $\mathbb{K}$. For instance, suppose that -1 is not a square in $\mathbb{K}$. Then, between the curves with equation

$$y^2 = x^3 + Ax + B \quad \text{and} \quad -y^2 = x^3 + Ax + B$$

are related by the isomorphism defined over $\overline{\mathbb{K}}$ given by $(x, y) \mapsto (x, \sqrt{-1}\, y)$ but there may not exist an isomorphism defined over $\mathbb{K}$. Such curves are said to be a *twist* of each other.

Remark 49. — Starting from a j–invariant $j_0 \in \overline{\mathbb{K}}$, an explicit equation for an elliptic curve with this j–invariant is given by

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728} x - \frac{1}{j_0 - 1728} \quad \text{if} \quad j_0 \neq 0, 1728$$

and

$$y^2 + y = x^3 \ \text{ if } \ j_0 = 0 \qquad \text{and} \qquad y^2 = x^3 + x \ \text{ if } \ j = 1278.$$

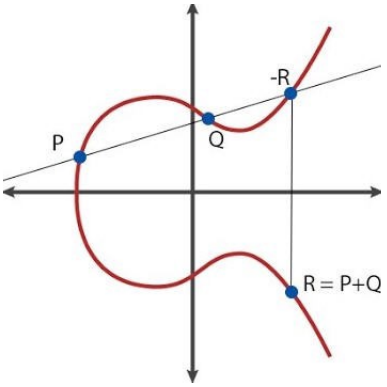

Figure 3. The addition law on an elliptic curve (Source: Cornelius Schätz blog)

4.3. The group law. — A remarkable feature of such curves is that they naturally have a group structure. Namely, given an elliptic curve $\mathscr{E}$ over $\mathbb{K}$, the set $\mathscr{E}(\mathbb{K})$ has a structure of abelian group. More generally, for any algebraic extension $\mathbb{L}$ of $\mathbb{K}$, then $\mathscr{E}(\mathbb{L})$ has an abelian group structure too. This group structure is usually represented with a so–called *chord and tangent process* as represented by Figure 3. It can be described as follows:

- Given two points $P, Q \in \mathscr{E}(\mathbb{L})$, draw the line $\mathscr{L} \subseteq \mathbb{A}^2$ (or $\mathbb{P}^2$) joining them. If $P = Q$ let $\mathscr{L}$ be the tangent line of $\mathscr{E}$ at P.
- Since the curve has degree 3, its intersection with $\mathscr{L}$ and $\mathscr{E}$ has 3 points counted with multiplicity and hence either $\mathscr{L}$ is vertical and then the third point is $R_0 = O_{\mathscr{E}}$ or denote by $R_0 = (x_{R_0}, y_{R_0})$ be the third[8] point of intersection of this line with $\mathscr{E}$.
- Let R be the point with coordinates $(x_{R_0}, -y_{R_0})$ if $R_0 \neq O_{\mathscr{E}}$ and the point $O_{\mathscr{E}}$ otherwise. This point is defined to be the *sum of P and Q*.

Exercise 50. — (1) Prove that the intersection of $\mathscr{E}$ with a line is made of 3 points of $\mathbb{P}^2$ possibly counted with multiplicity;
(2) Prove that $R_0 \in \mathscr{E}(\mathbb{L})$;

This description is simple to understand but it is not completely obvious to prove that it provides a group structure. In particular, the associativity is far from being obvious using this description. Here we will show that this group structure can also be understood as a group law inherited from that of some quotient of the divisor group. Indeed, denote by $\mathrm{Div}_{\mathbb{K}}(\mathscr{E})$ the group of rational divisors on $\mathscr{E}$ and by $\mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})$ the subgroup of divisors of degree 0. Finally denote by $\mathrm{Princ}_{\mathbb{K}}(\mathscr{E})$ the group of principal divisors, *i.e.* of divisors of the form (f) where $f \in \mathbb{K}(\mathscr{E}) \setminus \{0\}$. From Remark 19 together with Proposition 20, $\mathrm{Princ}_{\mathbb{K}}(\mathscr{E})$ is a subgroup of $\mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})$ and the quotient is denoted

$$\mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E}) \stackrel{\mathbf{def}}{=} \mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})/\mathrm{Princ}_{\mathbb{K}}(\mathscr{E}).$$

Proposition 51. — *Let $\mathscr{E}$ be an elliptic curve over $\mathbb{K}$. Any element of $Pic^0_{\mathbb{K}}(\mathscr{E})$ has a representative of the form $P - O_{\mathscr{E}}$ where P is some rational point in $\mathscr{E}(\mathbb{K})$.*

Proof. — Let $G \in \mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})$. The divisor $G + O_{\mathscr{E}}$ has degree 1 and, from Riemann–Roch Theorem $L(G + O_{\mathscr{E}})$ has dimension 1. Thus, there exists $f \in L(G + O_{\mathscr{E}}) \setminus \{0\}$. By definition of $L(G + O_{\mathscr{E}})$, the function f satisfies

$$(f) + G + O_{\mathscr{E}} \geqslant 0.$$

The latter divisor is positive with degree 1 and hence equals some rational point P. Thus $(f)+G = P - O_{\mathscr{E}}$, which entails that G and $P - O_{\mathscr{E}}$ have the same class in $\mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E})$. □

[8] Possibly R_0 equals P or Q. This is the reason why we mentioned 3 points *counted with multiplicity*. If the intersection multiplicity of $\mathscr{L}$ with $\mathscr{E}$ at P (resp. Q) is 2 then, we set $R_0 \stackrel{\mathbf{def}}{=} P$ (resp. Q).

Theorem 52. — *Let $P, Q \in \mathscr{E}(\mathbb{K})$ and R be the sum of $P+Q$ according to the previously introduced addition law. Then, the classes of $R - O_{\mathscr{E}}$ and $(P - O_{\mathscr{E}}) + (Q - O_{\mathscr{E}})$ are the same in $Pic^0_{\mathbb{K}}(\mathbb{E})$.*

Proof. — From Exercise 50 (1), there is a point R_0 which is contained in the line $\mathscr{L}$ joining P and Q. Moreover R, R_0 are contained in a vertical line $\mathscr{L}'$, the verticality entails that, projectively speaking, R_0, R and $O_{\mathscr{E}}$ are in the projective closure of the line $\mathscr{L}'$. Let $H(X,Y,Z)$ and $H'(X,Y,Z)$ be homogeneous polynomials of degree 1 providing equations of the projective closures of $\mathscr{L}$ and $\mathscr{L}'$ respectively. The rational function $h \overset{\textbf{def}}{=} \frac{H}{H'} \in \mathbb{K}(\mathscr{E})$ has divisor

$$(h) = (P + Q + R_0) - (R_0 + R + O_{\mathscr{E}}) = (P - O_{\mathscr{E}}) + (Q - O_{\mathscr{E}}) - (R - O_{\mathscr{E}}),$$

which concludes the proof. □

As a conclusion, we have the following bijection:

$$\left\{ \begin{array}{ccc} \mathscr{E}(\mathbb{K}) & \longrightarrow & \mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E}) \\ P & \longmapsto & P - O_{\mathscr{E}} \mod \mathrm{Princ}_{\mathbb{K}}(\mathscr{E}) \end{array} \right. .$$

Via this bijection, we can equip $\mathscr{E}(\mathbb{K})$ with a group structure whose law is nothing but the previously described chord–tangent one. Therefore, $\mathscr{E}(\mathbb{K})$ equipped with the chord–tangent law has a group structure which is isomorphic to $\mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E})$.

Remark 53. — Here again, note that we discussed about the group structure of the set of rational points $\mathscr{E}(\mathbb{K})$ but actually, for any algebraic extension $\mathbb{L}/\mathbb{K}$, the set $\mathscr{E}(\mathbb{L})$ has also a group structure with $\mathscr{E}(\mathbb{L})$ as a subgroup. In particular, the whole set of geometric points $\mathscr{E}(\overline{\mathbb{K}})$ has a structure of abelian group.

4.4. Torsion and isogenies. — Once we know that elliptic curves are equipped with an abelian group structure it is of course natural to study the morphisms relating these curves. For this sake, we first need to discuss some specific subgroups of points of elliptic curves: their torsion subgroups.

4.4.1. *Torsion subgroups.* — Given an elliptic curve $\mathscr{E}$ and an integer ℓ, one is interested in the group

$$\mathscr{E}[\ell] \overset{\textbf{def}}{=} \{P \in \mathscr{E}(\overline{\mathbb{K}}) \mid \ell P = 0\},$$

where ℓP means "$P + \cdots + P$" (added ℓ times). Interestingly, this group has a natural structure of $\mathbb{Z}/\ell\mathbb{Z}$–module, and, in particular, is an $\mathbb{F}_\ell$–vector space when ℓ is prime. The next theorem asserts that this space has always dimension 2 when ℓ is prime to the characteristic. The proof of the next statement is omitted.

Theorem 54. — *Let $\mathscr{E}$ be an elliptic curve over $\mathbb{K}$. Let ℓ be an integer. If ℓ is prime to the characteristic of $\mathbb{K}$, then*

$$\mathscr{E}[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

Else, if p denotes the characteristic of $\mathbb{K}$ and $p \neq 0$, then

$$\mathscr{E}[p] \simeq \left\{ \begin{array}{cc} \textit{either} & \mathbb{Z}/p\mathbb{Z} \\ \textit{or} & 0. \end{array} \right.$$

In the former case the curve is said to be ordinary, *in the latter it is said to be* supersingular.

4.4.2. *Isogenies.* — Given two elliptic curves $\mathscr{E}, \mathscr{E}'$, an isogeny $\phi : \mathscr{E} \to \mathscr{E}'$ is a morphism between these curves sending the neutral element $O_{\mathscr{E}}$ onto $O_{\mathscr{E}'}$. Such a map is always surjective from $\mathscr{E}(\overline{\mathbb{K}})$ into $\mathscr{E}'(\overline{\mathbb{K}})$. A remarkable property is that such a map is necessarily a morphism of groups (see [**Sil09**, Thm. III.4.8]. As any morphism of curves, an isogeny $\phi : \mathscr{E} \to \mathscr{E}'$ induces a field extension $\mathbb{K}(\mathscr{E}')/\mathbb{K}(\mathscr{E})$. The *degree* of the isogeny is the degree of the field extension and the isogeny is said to be *separable* if the field extension is separable too. An isogeny of degree ℓ will usually be referred to as *an ℓ–isogeny.*

Example 55. — Taken from [**Sil09**, Ex. III.4.5]. Let $a, b \in \mathbb{K}$, $b \neq 0$ and $a^2 - 4b \neq 0$. Consider the curves with equations:

$$\begin{array}{rcl} \mathscr{E} : y^2 & = & x^3 + ax^2 + bx \\ \mathscr{E}' : y^2 & = & x^3 - 2ax^2 + (a^2 - 4b)x. \end{array}$$

The following map is a 2–isogeny:

$$\left\{ \begin{array}{ccc} \mathscr{E} & \longrightarrow & \mathscr{E}' \\ (x,y) & \longmapsto & \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right). \end{array} \right. \tag{16}$$

Exercise 56. — Check that the map (16) actually sends $\mathscr{E}$ into $\mathscr{E}'$. *Hint. Using a computer algebra software may be helpful for this exercise.*

Example 57. — Another example for isogenies of elliptic curves over a finite field $\mathbb{F}_q$ of characteristic p is the Frobenius map

$$\left\{ \begin{array}{ccc} \mathscr{E} & \longrightarrow & \mathscr{E}^{(p)} \\ (x,y) & \longmapsto & (x^p, y^p). \end{array} \right.$$

This isogeny is purely inseparable and sends the curve $\mathscr{E}$ with Weierstrass equation $y^2 = x^3 + Ax + B$ onto the curve $\mathscr{E}^{(p)}$ of equation $y^2 = x^3 + A^p x + B^p$. If $\mathscr{E}$ is defined over $\mathbb{F}_q$ (*i.e.* if $A, B \in \mathbb{F}_q$) then the Frobenius map is an endomorphism of $\mathscr{E}$.

Example 58. — For any $m > 0$ prime to the characteristic and any elliptic curve $\mathscr{E}$ over $\mathbb{K}$, the map $P \mapsto mP$ is an isogeny from $\mathscr{E}$ into itself. Its kernel is $\mathscr{E}[m]$.

A separable isogeny of degree ℓ, regarded as a group morphism $\mathscr{E}(\overline{\mathbb{K}}) \to \mathscr{E}(\overline{\mathbb{K}})$ is surjective with a finite kernel of cardinality ℓ. Its kernel is a subgroup of $\mathscr{E}[\ell]$.

Theorem 59 (**[Sil09**, Prop. III.4.12]). — *For any finite subgroup $K \subseteq \mathscr{E}(\overline{\mathbb{K}})$, there exists an elliptic curve $\mathscr{E}'$ defined over $\overline{\mathbb{K}}$ and an isogeny $\phi : \mathscr{E} \to \mathscr{E}'$ such that* $\ker \phi = K$. *The curve $\mathscr{E}'$ is sometimes denoted as $\mathscr{E}/K$.*

Remark 60. — In the previous statement, further precision can be given on the field of definition of $\mathscr{E}'$ and ϕ. The field of definition of the group K is the smallest extension $\mathbb{L}/\mathbb{K}$ such that K is globally invariant under the action of $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{L})$. The field of definition of ϕ and $\mathscr{E}'$ is that of K.

Note that the field of definition is **not** the smallest field of definition of any geometric point of K. For instance, there may be non rational m–torsion points while $\mathscr{E}[m]$ is defined over $\mathbb{K}$.

Finally, even if an isogeny $\phi : \mathscr{E} \to \mathscr{E}'$ of degree $m > 1$ is not an isomorphism in general, and hence has no inverse, it has a so–called *dual isogeny* $\hat{\phi}$ which is the unique isogeny $\hat{\phi} : \mathscr{E}' \to \mathscr{E}$ such that

$$\phi \circ \hat{\phi} : \left\{ \begin{array}{ccc} \mathscr{E} & \longrightarrow & \mathscr{E} \\ P & \longmapsto & mP \end{array} \right. \quad \text{and} \quad \hat{\phi} \circ \phi : \left\{ \begin{array}{ccc} \mathscr{E}' & \longrightarrow & \mathscr{E}' \\ Q & \longmapsto & mQ. \end{array} \right.$$

The existence and uniqueness of this map are proven in [**Sil09**, § III.6].

Example 61. — In the case of a separable isogeny $\phi : \mathscr{E} \to \mathscr{E}'$ of degree m, its kernel is a group with m elements. By Lagrange Theorem, such a finite group is of m–torsion and hence $\ker \phi \subseteq \mathscr{E}[m]$. Then $\phi(\mathscr{E}[m])$ is a finite subgroup and, from Theorem 59, there is an isogeny $\varphi : \mathscr{E}' \to \mathscr{E}'/\phi(\mathscr{E}[m])$, which is nothing but the dual isogeny of ϕ. In particular $\mathscr{E}'/\phi(\mathscr{E}[m]) \simeq \mathscr{E}/\mathscr{E}[m] \simeq \mathscr{E}$. The last isomorphism is induced by the map $P \mapsto mP$.

All the previously introduced notions: torsion, isogenies, dual isogenies will be re–discussed and better illustrated in the subsequent section about elliptic curves over $\mathbb{C}$. In this context, these notions will be much easier to visualise.

4.5. Elliptic curves over the complex numbers. — As already explained earlier, complex elliptic curves is not the topic of this lecture. It is however necessary to discuss a bit about them. In order not to spend too much time on the topic, many proofs of non trivial statements are omitted and replaced by precise references. Clearly, the summary to follow is strictly included in Chapter VI of Silverman's book [**Sil09**].

4.5.1. *Lattices and the Weierstrass $\wp$ function.* — In the complex setting, an elliptic curve is isomorphic to a complex torus. Namely, a lattice of $\mathbb{C}$ is a discrete subgroup Λ with compact quotient and it is well–known that such a group is of the form

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

where ω_1, ω_2 are linearly independent over $\mathbb{R}$. The relation between a torus $\mathbb{C}/\Lambda$ and an elliptic curve is far from being obvious and the key for connecting these two objects is Weierstrass $\wp_\Lambda$ function defined as

$$\wp_\Lambda(z) \overset{\mathbf{def}}{=} \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

This is a meromorphic function with pole locus Λ which is Λ–periodic, *i.e.* for any $z \in \mathbb{C} \setminus \Lambda$ and $\omega \in \Lambda$, $\wp(z+\omega) = \wp(z)$. The proof of convergence of the series is left to the reader.

Note that, since $\wp$ is Λ–periodic, it passes to the quotient and induces a meromorphic function on the torus $\mathbb{C}/\Lambda$. The function $\wp$ is fundamental in the sense that actually, any Λ–periodic meromorphic function can be expressed as a rational function in $\wp$ and its derivative $\wp'$ as explained by the following statement.

Theorem 62. — *There exist complex numbers g_2, g_3, which depend on Λ such that*

$$\forall z \in \mathbb{C} \setminus \Lambda, \qquad \wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 + g_2\wp_\Lambda(z) + g_3.$$

Proof. — The series

$$\wp(z) - \frac{1}{z^2} = \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

is even and vanishes at 0. Hence, in the neighbourhood of 0, its Taylor series expansion depends only on z^2. Thus, we deduce that $\wp_\Lambda$ has a Laurent series expansion at 0 of the form

$$\wp_\Lambda(z) = \frac{1}{z^2} + O(z^2),$$

and

$$\wp'_\Lambda(z) = -\frac{2}{z^3} + O(z).$$

Therefore, in a neighbourhood of 0, $\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 = O(\frac{1}{z^2})$ and there is a constant $g_2 \in \mathbb{C}$ such that

$$\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 - g_2\wp_\Lambda(z) = O(1). \tag{17}$$

The function $\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 - g_2\wp_\Lambda(z)$ is Λ–periodic, meromorphic on $\mathbb{C}$ with pole locus contained in Λ. From (17), it has no pole at 0 and, by Λ–periodicity has no pole at all and hence is holomorphic on $\mathbb{C}$. Since it continuous and Λ–periodic on $\mathbb{C}$, it is bounded, and by Liouville's theorem, it should be constant. Therefore, there exists $g_3 \in \mathbb{C}$ such that $\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 + g_2\wp_\Lambda(z) + g_3$. □

Exercise 63. — Prove that a Λ–periodic holomorphic function is bounded on $\mathbb{C}$.

A finer analysis of the series permits to estimate g_2, g_3 in terms of Λ and to prove that the equation $y^2 = 4x^3 + g_2x + g_3$ is that of a smooth curve, and hence of an elliptic curve. With this theorem at hand, we deduce the existence of a map from the torus $\mathbb{C}/\Lambda$ into the elliptic curve $\mathscr{E}$ of equation $y^2 = 4x^3 + g_2x + g_3$:

$$\Psi_\Lambda : \left\{ \begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & \mathscr{E} \\ z & \longmapsto & (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1). \end{array} \right. \tag{18}$$

Note that this map is well–defined everywhere, since at 0 which is a pole of order 2 of $\wp_\Lambda$ and of order 3 of $\wp'_\Lambda$ one can renormalise as $(z^3\wp_{\Lambda(z)} : z^3\wp'_\Lambda(z) : z^3)$ and evaluate at 0, which yields the point $O_{\mathscr{E}} = (0:1:0)$. The following statement gathers several nontrivial and fundamental results on complex tori: it states a one-to-one correspondence between elliptic curves and complex tori when regarded as complex varieties **but also as groups**.

Theorem 64. — *The map Ψ_Λ defined in* (18) *is a biholomorphic isomorphism between $\mathbb{C}/\Lambda$ and the elliptic curve $\mathscr{E}$ of equation $y^2 = 4x^3 + g_2x + g_3$. Moreover, it also induces a group isomorphism from $\mathbb{C}/\Lambda$*

equipped with the addition law inherited from that of $\mathbb{C}$ into $\mathscr{E}(\mathbb{C})$ equipped with its group law introduced in § 4.3. Conversely, given any elliptic curve $\mathscr{E}_0$ over $\mathbb{C}$, there exists a lattice $\Lambda_0 \subset \mathbb{C}$ such that $\mathscr{E}_0$ is isomorphic to $\mathbb{C}/\Lambda_0$ via the map Ψ_{Λ_0}.

Proof. — See [**Sil09**, Prop. VI.3.6] for the group isomorphism. For the construction of a lattice from an elliptic curve, see [**Sil09**, § VI.1]. □

4.5.2. *Torsion, isogenies.* — An interest of the complex setting is that the previous results on torsion and isogenies are pretty easy to understand when regarding elliptic curves as complex tori.

Let us start with the torsion. From Theorem 54, for m prime to the characteristic, the m–torsion of an elliptic curve is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. In the complex setting, consider a torus $\mathbb{C}/\Lambda$. Then, the torsion points correspond to points $z \in \mathbb{C}$ such that $mz \in \Lambda$ and hence they correspond to the points of the lattice $\frac{1}{m}\Lambda \supset \Lambda$. Then, the torsion subgroup of $\mathbb{C}/\Lambda$ is isomorphic to $\frac{1}{m}\Lambda/\Lambda$. Since Λ is of the form $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ for some $\mathbb{R}$–independent elements $\omega_1, \omega_2 \in \mathbb{C}$, we deduce that

$$(\mathbb{C}/\Lambda)[m] \simeq \left(\frac{1}{m}\Lambda\right)/\Lambda = \frac{\mathbb{Z}\frac{\omega_1}{m} \oplus \mathbb{Z}\frac{\omega_2}{m}}{\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2} \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

Now consider isogenies. When considering complex tori, isogenies are holomorphic maps $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. It turns out that such maps lift to $\mathbb{C}$ and have a very particular structure.

Theorem 65. — *Let $\Lambda, \Lambda' \subset \mathbb{C}$ be two lattices and $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be a holomorphic map 0 sending onto 0. Then f lifts to a holomorphic map $f_0 : \mathbb{C} \to \mathbb{C}$ such that*

$$\forall z \in \mathbb{C}, \quad f_0(z) \mod \Lambda' = f(z \mod \Lambda).$$

Moreover, f_0 is a similitude, i.e. *there exists $a \in \mathbb{C}$ such that*

$$\forall z \in \mathbb{C}, \ f_0(z) = az.$$

Proof. — See [**Sil09**, Thm. VI.4.1]. □

With this statement at hand, we deduce that an isogeny $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is induced by a map $z \mapsto az$ with $a\Lambda \subseteq \Lambda'$.

Example 66. — For instance, consider the lattices

$$\Lambda = \mathbb{Z} \oplus \mathbb{Z}2i \quad \text{and} \quad \Lambda' = 2\mathbb{Z} \oplus \mathbb{Z}2i$$

then we easily see that the map $z \mapsto 2z$ induces an isogeny $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$.

From a similitude $z \mapsto az$ such that $a\Lambda \subset \Lambda'$, the degree of the corresponding isogeny is given by $\sharp(\Lambda'/a\Lambda)$. In the previous example, the isogeny has degree 2.

Finally, let ℓ be a prime integer, and suppose that we have a degree–ℓ isogeny $\phi_1 : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. This entails the existence of $a \in \mathbb{C}$ such that $\sharp(\Lambda'/a\Lambda) = \ell$. From the structure theorem of finitely generated modules over principal ideal rings, we deduce the existence of $\omega_1, \omega_2 \in \mathbb{C}$ such that

$$\Lambda = \mathbb{Z}\frac{\ell\omega_1}{a} \oplus \frac{\omega_2}{a}, \quad \Lambda' = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

and ϕ_1 is induced from the similitude $z \mapsto az$.

Exercise 67. — Prove the last assertion.

Now consider the map $z \mapsto \frac{\ell}{a}z$. It induces an isogeny $\phi_2 : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ of degree ℓ. Moreover the composition of the two isogenies :

$$\phi_2 \circ \phi_1 : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda''$$

is defined by $z \mod \Lambda \mapsto \ell z \mod \Lambda$ and hence is nothing but the multiplication by ℓ in $\mathbb{C}/\Lambda$. Therefore, ϕ_2 is nothing but the dual isogeny map $\hat{\phi}_1$ of ϕ_1.

4.6. Automorphisms.

— Now, we have a nice description of morphisms of complex elliptic curves. Moreover, an endomorphism of an elliptic curve, or equivalently of a complex torus $\mathbb{C}/\Lambda$, is induced by a similitude $z \mapsto az$ such that $a\Lambda \subset \Lambda$.

One will also be interested in the sequel by automorphisms of an elliptic curve, which correspond to similitudes $z \mapsto az$ such that $a\Lambda = \Lambda$. One can prove that such an a satisfies $|a| = 1$.

Remark 68. — Clearly for any integer N and any lattice Λ we have $N\Lambda \subset \Lambda$ and the map $z \mapsto Nz$ induces an endomorphism of $\mathbb{C}/\Lambda$ which is the multiplication by N map. In addition, if there exists $a \in \mathbb{C}\backslash\mathbb{Z}$ such that $a\Lambda \subset \Lambda$, then the corresponding elliptic curve is said to be *with complex multiplication*.

An elementary automorphism for any complex torus is $z \mapsto -z$. Back to the map Ψ_Λ in (18) and using the fact that $\wp_\Lambda$ and $\wp'_\Lambda$ are respectively even and odd, we deduce that this map corresponds on the elliptic curve to the symmetry with respect to the x–axis:

$$(x, y) \longmapsto (x, -y).$$

Furthermore, some sporadic elliptic curves have nontrivial automophisms coming from $z \mapsto az$ with $|a| = 1$ and $a \notin \{\pm 1\}$.

Theorem 69. — *Let $\mathbb{C}/\Lambda$ be a complex torus with an automorphism $z \mapsto az$ with $|a| = 1$ and $a \notin \{\pm 1\}$. Equivalently, the lattice Λ satisfies $\Lambda = a\Lambda$. Then, Λ is the image by a similitude of one of these two lattices:*

$$\mathbb{Z} \oplus \mathbb{Z}i \quad \text{or} \quad \mathbb{Z} \oplus \mathbb{Z}\rho,$$

where $\rho = e^{\frac{i\pi}{3}}$.

Proof. — Let Λ be a lattice such that $a\Lambda = \Lambda$ and $\nu \in \Lambda \setminus \{0\}$ be a vector of minimal modulus. Since we look for Λ up to a similitude, one can assume that $\nu = 1$ and that for all $\omega \in \Lambda \setminus \{0\}$, $|\omega| \geqslant 1$. Assuming that $1 \in \Lambda$, then, by assumption on Λ, we deduce that a, a^2 are elements of Λ too. Since $a \notin \mathbb{R}$, its minimal polynomial over $\mathbb{R}$ is

$$\begin{aligned}(x-a)(x-\bar{a}) &= x^2 + 2\mathrm{Re}(a)x + |a|^2 \\ &= x^2 + 2\mathrm{Re}(a)x + 1,\end{aligned}$$

where $\mathrm{Re}(a)$ denotes the real part of a. Consequently,

$$a^2 + 1 = -2\mathrm{Re}(a)a.$$

Note that $|a| = 1$ and $a \notin \mathbb{R}$ entails $-1 < \mathrm{Re}(a) < 1$. If $2\mathrm{Re}(a) \notin \mathbb{Z}$, then there is $\varepsilon \in \{-1, 0, 1\}$ such that

$$a^2 + \varepsilon a + 1 = \gamma a$$

for some $0 < \gamma < 1$. Since the left–hand side is a $\mathbb{Z}$–linear combination of elements of Λ, then $\gamma a \in \Lambda$ which contradicts the assumption that any nonzero $\omega \in \Lambda$ satisfies $|\omega| \geqslant 1$. Therefore $\mathrm{Re}(a) \in \{-\frac{1}{2}, 0, \frac{1}{2}\}$. Case $\mathrm{Re}(a) = 0$ provides the case $\Lambda = \mathbb{Z} \oplus \mathbb{Z}i$ and the two other cases provide the same lattice, namely $\mathbb{Z} \oplus \mathbb{Z}\rho$. □

The corresponding elliptic curves can be proved to have respective equations:

$$\begin{array}{lllllll} y^2 &=& x^3 + x & \text{for} & \Lambda &=& \mathbb{Z} \oplus \mathbb{Z}i \quad (j\text{–invariant } 1728) \\ y^2 &=& x^3 + 1 & \text{for} & \Lambda &=& \mathbb{Z} \oplus \mathbb{Z}\rho \quad (j\text{–invariant } 0). \end{array} \tag{19}$$

The corresponding automorphisms being respectively

$$\begin{array}{lll} (x, y) & \longmapsto & (-x, iy) \\ (x, y) & \longmapsto & (\rho x, -y). \end{array}$$

Note that these automorphisms have respective orders 4 and 6 which are the multiplicative orders of i and ρ. Finally, note that for any field containing fourth and sixth roots of 1, the curves with equations (19) have a nontrivial automorphism group. Moreover, one can prove that they are the only curves with non trivial automorphism groups [**Sil09**, Thm. III.10.1] and that their automorphism groups have respective cardinalities 4 and 6.

5. Modular curves

5.1. The Poincaré upper half plane. — The objective is to classify elliptic curves over $\mathbb{C}$ up to isomorphism. As explained in § 4.5, this reduces to classify lattices up to similitudes whose definition is recalled there.

Definition 70 **(Similitudes of $\mathbb{C}$).** — A *similitude* of $\mathbb{C}$ is a map of the form $z \mapsto az$ for some $a \in \mathbb{C}^\times$.

Besides the action of the group of similitudes on the set of lattices of $\mathbb{C}$, lattices are described by a basis which is not unique. This requires to introduce another group action on the possible bases. Namely, given a lattice

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2,$$

the basis (ω_1, ω_2) is not unique and any other basis (μ_1, μ_2) is deduced from (ω_1, ω_2) by

$$\begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix} = M \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, \quad \text{for some } M \in \mathbf{GL}_2(\mathbb{Z}).$$

Up to swapping the entries of the basis, one can always assume that the bases we consider have the same orientation, *i.e.* that $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$ (resp. $\mathrm{Im}(\frac{\mu_1}{\mu_2}) > 0$), where $\mathrm{Im}(\cdot)$ denotes the imaginary part of a complex number. If the bases are chosen under this constraint, then the transition matrix M always has a positive determinant and hence is in $\mathbf{SL}_2(\mathbb{Z})$. Therefore, the set of lattices of $\mathbb{C}$ is in one-to-one correspondence with the classes of pairs $(\omega_1, \omega_2) \in \mathbb{C}^2$ with $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$ modulo the action of $\mathbf{SL}_2(\mathbb{Z})$. Next, we need to consider the action of similitudes. Starting from $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$ and applying the similitude $z \mapsto \frac{1}{\omega_2} z$, we get a similar lattice:

$$\mathbb{Z} \oplus \mathbb{Z}\tau$$

with $\tau = \frac{\omega_1}{\omega_2}$ and hence $\mathrm{Im}(\tau) > 0$. Let

$$\mathbb{H} \stackrel{\mathbf{def}}{=} \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\},$$

be the *Poincaré upper half plane.* Then any lattice up to similitude can be associated to an element $\tau \in \mathbb{H}$ and the action of $\mathbf{SL}_2(\mathbb{Z})$ on bases of lattices induces the following action on $\mathbb{H}$. Starting from

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}),$$

M acts on bases as:

$$M \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{pmatrix}.$$

Therefore since $\tau = \frac{\omega_1}{\omega_2}$, we naturally define the action of $\mathbf{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by

$$M \cdot \tau \stackrel{\mathbf{def}}{=} \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d}. \tag{20}$$

In summary, according to the discussion of § 4.5, we have the following correspondence:

Elliptic curves up to isomorphism	⟷	Complex tori up to biholomorphic isomorphisms	⟷	Lattices of $\mathbb{C}$ up to similitudes	⟷	Points of $\mathbb{H}$ modulo the action (20) of $\mathbf{SL}_2(\mathbb{Z})$

Moreover, fundamental domains for the action of $\mathbf{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ are represented in Figure 4, which is a famous picture that you can find in so many books of geometry or number theory.

5.2. The curve $X_0(1)$. — So, to parameterise the set of elliptic curves up to isomorphism, we can consider the quotient $\mathbf{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. It is proved in [**Mil17**, Prop. 2.21] that this quotient is a complex variety isomorphic to $\mathbb{A}^1$, *i.e.* to the complex affine line. This is not surprising, Theorem 65 entails that complex elliptic curves up to ismomorphisms are in one-to-one correspondence with $\mathbb{C}$ via the map $\mathscr{E} \mapsto j(\mathscr{E})$, where $j(\mathscr{E})$ denotes the j–invariant of $\mathscr{E}$.

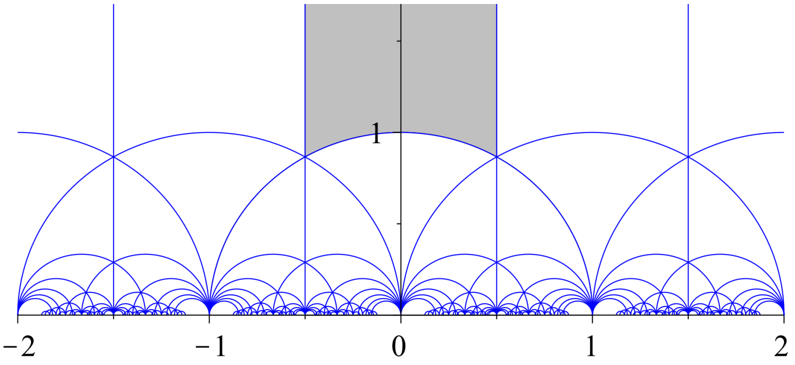

FIGURE 4. Fundamental domain for the action of $\mathbf{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ (Source: Wikipedia)

Next, for convenience and in order to apply results on algebraic curves introduced in § 2, it will be useful to have some projective closure of this parameterising curve. In the complex setting, this is nothing but a compactification and the affine line can be compactified with one point. However, for a reason which will appear to be more natural in the sequel, the compactification will be made via a somehow more complicated construction.

The idea is to join to $\mathbb{H}$ all the elements of $\mathbb{Q}$ which lie on the boundary of $\mathbb{H}$ together with a point at infinity. Namely, we define

$$\mathbb{H}^* \stackrel{\mathbf{def}}{=} \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

Next let us see how the action of $\mathbf{SL}_2(\mathbb{Z})$ extends to $\mathbb{P}^1(\mathbb{Q})$.

Proposition 71. — *Consider the following action of $\mathbf{SL}_2(\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Q})$:*

$$\forall M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}),\ (u:v) \in \mathbb{P}^1(\mathbb{Q}), \quad M \cdot (u:v) = (au+bv : cu+dv).$$

This action is transitive, i.e. *for any $(u:v), (u':v') \in \mathbb{P}^1(\mathbb{Q})$, there exists $M \in \mathbf{SL}_2(\mathbb{Z})$ such that $M \cdot (u:v) = (u':v')$.*

Proof. — First, let us prove that the orbit of $(0:1)$ equals the whole $\mathbb{P}^1(\mathbb{Q})$. Note first that

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot (0:1) = (-1:0) = (1:0).$$

Hence $(1:0)$ is in the orbit of $(0:1)$. Next, consider any other point $(s:t) \in \mathbb{P}^1(\mathbb{Q}) \setminus \{(1:0)\}$, *i.e.* such that $t \neq 0$. After multiplying the coordinates by a common denominator, one can suppose that $s, t \in \mathbb{Z}$ and after possibly dividing by their greatest common denominator, one can suppose s, t are prime to each other. By Bézout's Theorem, there exist $u, v \in \mathbb{Z}$ such that $su + tv = 1$ and then

$$\begin{pmatrix} t & u \\ -s & v \end{pmatrix} \cdot (0:1) = (u:v) \quad \text{and} \quad \begin{pmatrix} t & u \\ -s & v \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}).$$

Therefore, any element of $\mathbb{P}^1(\mathbb{Q})$ is in the orbit of $(0:1)$. Finally, given two elements $(u:v), (u':v') \in \mathbb{P}^1(\mathbb{Q})$ there exist M, M' such that $(u:v) = M \cdot (0:1)$ and $(u':v') = M' \cdot (0:1)$ and $(u':v') = M'M^{-1}(u:v)$. □

Therefore, the quotient $\mathbf{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$ is nothing but the compactification of $\mathbf{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ by adjoining a single point. This quotient is usually denoted as $X_0(1)$ and is nothing but the Riemann sphere $\mathbb{P}^1(\mathbb{C})$.

In terms of functions on $X_0(1)$, there exists a holomorphic function $j : \mathbb{H} \to \mathbb{C}$ which is invariant under the action of $\mathbf{SL}_2(\mathbb{Z})$ and such that the induced map $\mathbf{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ is bijective. This map realises an isomorphism between $X_0(1)$ and $\mathbb{P}^1(\mathbb{C})$. It can be "made explicit" as follows. From $\tau \in \mathbb{H}$ construct the lattice $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$. Then using the Weierstrass $\wp_{\Lambda_\tau}$ function, compute an equation of the elliptic curve corresponding to $\mathbb{C}/\Lambda_\tau$. Then, $j(\tau)$ is nothing but the j–invariant of this latter elliptic curve.

5.3. The curve $X_0(\ell)$. — Once we have a curve parameterising elliptic curves up to isomorphisms, we are still a bit far from our objective since we look for a family of curves whose sequence of genera goes to infinity, while we only got $\mathbb{P}^1$ which has genus 0. To get curves with a higher genus, we need to enhance the structure and the idea is not only to classify elliptic curves up to isomorphism but to classify for a fixed integer ℓ, the ℓ–isogenies $\mathscr{E} \to \mathscr{E}'$ up to isomorphism. In the sequel we are only interested in the case where ℓ is prime (but many of the results to follow extend to an arbitrary degree of isogeny).

Remark 72. — Note that, here, by "up to ismomorphism" we mean that two isogenies $\phi_1 : \mathscr{E}_1 \to \mathscr{E}_1'$ and $\phi_2 : \mathscr{E}_2 \to \mathscr{E}_2'$ will be said to be *isomorphic* if there exist two isomorphisms $\eta : \mathscr{E}_1 \to \mathscr{E}_2$ and $\nu : \mathscr{E}_1' \to \mathscr{E}_2'$ such that the following diagram commutes.

$$\begin{tikzcd}
\mathscr{E}_1 \arrow[r, "\phi_1"] \arrow[d, "\eta"'] & \mathscr{E}_2 \arrow[d, "\nu"] \\
\mathscr{E}_1' \arrow[r, "\phi_2"] & \mathscr{E}_2'
\end{tikzcd}$$

From Theorem 59, an ℓ–isogeny $\mathscr{E} \to \mathscr{E}'$ corresponds to a pair $(\mathscr{E}, C)$ where $C \subseteq \mathscr{E}[\ell]$ is a subgroup of cardinality ℓ. Then, in the complex setting, it reduces to classify pairs of lattices Λ, Λ' such that $\Lambda \subseteq \Lambda'$ and $\sharp(\Lambda'/\Lambda) = \ell$. The structure theorem for finitely generated modules over a principal ideal ring asserts that there exists a basis ω_1, ω_2 of Λ such that

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \quad \text{and} \quad \Lambda' = \mathbb{Z}\frac{\omega_1}{\ell} \oplus \mathbb{Z}\omega_2.$$

With the above description, one sees easily that $\mathscr{E}[\ell] = (\frac{1}{\ell}\Lambda)/\Lambda \simeq \mathbb{F}_\ell \oplus \mathbb{F}_\ell$ and Λ'/Λ identifies to an $\mathbb{F}_\ell$–subspace of dimension 1 of $\mathscr{E}[\ell]$, namely the subspace spanned by the class of $\frac{\omega_1}{\ell}$. Since we wish to classify elliptic curves $\mathscr{E}$ with a given ℓ–torsion subgroup C, we need to classify changes of basis preserving this subgroup. Observe that the action of $\mathbf{SL}_2(\mathbb{Z})$ on bases of Λ induces a natural action of $\mathbf{SL}_2(\mathbb{F}_\ell)$ on $\mathscr{E}[\ell] = (\frac{1}{\ell}\Lambda)/\Lambda$. The elements of $\mathbf{SL}_2(\mathbb{F}_\ell)$ that fix the class of $\frac{\omega_1}{\ell}$ are the upper triangular matrices. This motivates the definition of the *congruence subgroup* $\Gamma_0(\ell) \subset \mathbf{SL}_2(\mathbb{Z})$ defined as

$$\Gamma_0(\ell) \stackrel{\mathbf{def}}{=} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod \ell \right\}.$$

Namely, this is the group of elements of $\mathbf{SL}_2(\mathbb{Z})$ which induce an automorphism of $\mathscr{E}[\ell]$ fixing C.

Exercise 73. — Prove that the canonical map

$$\mathbf{SL}_2(\mathbb{Z}) \longrightarrow \mathbf{SL}_2(\mathbb{F}_\ell)$$

given by the reduction of the coefficients modulo ℓ is surjective. To do it:

(a) Prove that an element of $\mathbf{SL}_2(\mathbb{F}_\ell)$ has a lift $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in Z$ such that a, b are nonzero and prime to each other.

(b) Prove that for such a lift, c, d can be replaced by c', d' such that $c \equiv c' \mod \ell$ and $d \equiv d' \mod \ell$ so that $\det \begin{pmatrix} a & b \\ c' & d' \end{pmatrix} = 1$.

Therefore, the set of ℓ–isogenies between elliptic curves up to isomorphism is in one-to-one correspondence with the complex variety

$$\Gamma_0(\ell)\backslash\mathbb{H}.$$

This variety has a compactification

$$X_0(\ell) \stackrel{\mathbf{def}}{=} \Gamma_0(\ell)\backslash\mathbb{H}^*.$$

This is a compact Riemann surface and it can be proved that such an object is actually algebraic, *i.e.* is biholomorphic with a smooth complex projective curve. This structure of algebraic curve is discussed further.

The next statement gives a crucial information, namely the genus of $X_0(\ell)$.

Theorem 74. — *For a prime number $\ell > 3$, the genus g_ℓ of $X_0(\ell)$ equals*

$$g_\ell = \begin{cases} \frac{\ell-1}{12} - 1 & \text{if} \quad \ell \equiv 1 \quad \mod [12] \\ \frac{\ell-5}{12} & \text{if} \quad \ell \equiv 5 \quad \mod [12] \\ \frac{\ell-7}{12} & \text{if} \quad \ell \equiv 7 \quad \mod [12] \\ \frac{\ell+1}{12} & \text{if} \quad \ell \equiv 11 \quad \mod [12]. \end{cases}$$

We first need two technical lemmas.

Lemma 75. — *Let ℓ be a prime integer. Let $\Lambda \subseteq \mathbb{C}$ be a lattice and Λ_1, Λ_2 be two distinct lattices both containing Λ and $\sharp(\Lambda_1/\Lambda) = \sharp(\Lambda_2/\Lambda) = \ell$. Suppose that $a\Lambda_1 = \Lambda_2$ for some $a \in \mathbb{C}$. Then $|a| = 1$ and $a\Lambda = \Lambda$. Equivalently, given an elliptic curve $\mathscr{E}$ over $\mathbb{C}$ and two distinct subgroups C_1, C_2 of cardinality ℓ of $\mathscr{E}[\ell]$. If the curves $\mathscr{E}/C_1$ and $\mathscr{E}/C_2$ are isomorphic, then there is an automorphism of $\mathscr{E}$ sending C_1 onto C_2.*

Remark 76. — Note that if $\mathscr{E}$ has such an automorphism, then it should be one of the two curves mentioned in Theorem 69.

Proof of Lemma 75. — **Step 1. An adapted basis.** We claim that there exists $\omega_1, \omega_2 \in \mathbb{C}$ such that

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \quad \text{and} \quad \Lambda_1 = \mathbb{Z}\frac{\omega_1}{\ell} \oplus \mathbb{Z}\omega_2 \quad \text{and} \quad \Lambda_2 = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\frac{\omega_2}{\ell}\cdot \tag{21}$$

The existence of ω_1, ω_2 can be obtained as follows. First, the structure theorem for finitely generated modules over principal ideal rings asserts the existence of a basis η_1, η_2 such that

$$\Lambda = \mathbb{Z}\eta_1 \oplus \mathbb{Z}\eta_2 \quad \text{and} \quad \Lambda_1 = \mathbb{Z}\frac{\eta_1}{\ell} \oplus \mathbb{Z}\eta_2.$$

Next, we claim that

$$\Lambda_2 = \mathbb{Z}\eta_1 \oplus \mathbb{Z}\frac{u\eta_1 + \eta_2}{\ell},$$

for some $u \in \{0, \ldots, \ell-1\}$. Indeed, consider $\left(\frac{1}{\ell}\Lambda\right)/\Lambda$, which isomorphic to $\mathbb{F}_\ell \times \mathbb{F}_\ell$. In this quotient, Λ_1/Λ and Λ_2/Λ are identified to two $\mathbb{F}_\ell$–subspaces of dimension 1 in direct sum. The subspace Λ_1/Λ is spanned by the class of $\frac{\eta_1}{\ell}$ and the fact that Λ_1/Λ and Λ_2/Λ are in direct sum in $\left(\frac{1}{\ell}\Lambda\right)/\Lambda$ entails that Λ_2/Λ should be spanned by the class of $\frac{u\eta_1+\eta_2}{\ell}$ for some $u \in \mathbb{F}_\ell$. This implies that there exists $u \in \{0, \ldots, \ell-1\}$ such that $\frac{u\eta_1+\eta_2}{\ell} \in \Lambda_2$ and hence

$$\mathbb{Z}\eta_1 \oplus \mathbb{Z}\frac{u\eta_1 + \eta_2}{\ell} \subseteq \Lambda_2.$$

Then, since $\sharp(\Lambda_2/\Lambda) = \ell$, we can deduce that the above inclusion is actually an equality. Finally, define ω_1, ω_2 as

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \overset{\mathbf{def}}{=} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix}.$$

Note that the above change of variables is given by a matrix in $\mathbf{SL}_2(\mathbb{Z})$ and provides a basis for Λ which satisfies (21).

Step 2. The modulus of a. A classical notion in lattice theory is that of the *determinant* or *volume* of the lattice. It can be defined as follows. Consider $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ and regard $\mathbb{C}$ as a 2–dimensional $\mathbb{R}$–vector space with canonical basis $(1, i)$. Since any basis of Λ can be deduced from (ω_1, ω_2) by applying a matrix in $\mathbf{GL}_2(\mathbb{Z})$, *i.e.* a matrix with determinant ± 1, the quantity $|\det(\omega_1, \omega_2)|$ is the same for any basis of Λ. Hence we denote this quantity $|\det \Lambda|$. From (21), we have

$$\det \Lambda_1 = \frac{1}{\ell} \det \Lambda = \det \Lambda_2. \tag{22}$$

Moreover, the multiplication by a map $z \mapsto az$ regarded as an $\mathbb{R}$–linear endomorphism of $\mathbb{C}$ has determinant $|a|^2$. Indeed, writing $a = a_0 + DA_1$, the map is represented in the basis $(1, i)$ by the matrix

$$\begin{pmatrix} a_0 & -a_1 \\ a_1 & a_0 \end{pmatrix},$$

whose determinant is $a_0^2 + a_1^2 = |a|^2$. Next, the assumption $\Lambda_2 = a\Lambda_1$ together with (22) give

$$\det \Lambda_1 = \det \Lambda_2 = |a|^2 \det \Lambda_1,$$

which yields $|a|^2 = 1$.

Step 3. We aim to prove that $a\Lambda = \Lambda$. Suppose it does not. Since $\Lambda \subseteq \Lambda_1$, $\Lambda \subseteq \Lambda_2$ and $a\Lambda \subseteq a\Lambda_1 = \Lambda_2$, then $\Lambda + a\Lambda \subseteq \Lambda_2$. Recall that $\sharp\Lambda_2/\Lambda = \ell$ and ℓ is prime. Then, since we assumed that $\Lambda \subsetneq \Lambda + a\Lambda$, we get $\Lambda + a\Lambda = \Lambda_2$. Similarly, one deduces that $a^{-1}\Lambda + \Lambda = \Lambda_1$. Next, from (21), we see that $\Lambda_1 + \Lambda_2 = \frac{1}{\ell}\Lambda$ and hence

$$a^{-1}\Lambda + \Lambda + a\Lambda = \frac{1}{\ell}\Lambda.$$

By induction,

$$a^{-s}\Lambda + \cdots + a^{-1}\Lambda + \Lambda + a\Lambda + \cdots + a^{s}\Lambda = \frac{1}{\ell^s}\Lambda.$$

Therefore, for any $s \geqslant 0$, there exists a finite sequence $(\mu_i^s)_{i=-s}^{s}$ of elements of Λ such that

$$\sum_{i=-s}^{s} a^i \mu_i^s = \frac{1}{\ell^s}\omega_1.$$

Then, for any $N \geqslant 0$,

$$\begin{aligned} \sum_{s=0}^{N}\sum_{i=-s}^{s} a^i \mu_i^s &= \sum_{s=0}^{N} \frac{1}{\ell^s}\omega_1, \\ \sum_{i=-N}^{N} a^i \nu_i &= \sum_{s=0}^{N} \frac{1}{\ell^s}\omega_1, \end{aligned}$$

where the ν_i's are in Λ. When N goes to infinity, the right hand side is a convergent series. Thus, so does the left hand side and hence, its general term should go to 0. From the previous step, we know that $|a| = 1$ and since the ν_i's are in Λ which is discrete, then $\nu_i = 0$ for any sufficiently large i. Therefore, the sequence of partial sums of the left–hand side is stationary while that of the right–hand side is note. This is a contradiction. Therefore $a\Lambda = \Lambda$. □

Lemma 77. — *Let $\mathscr{E}_i \overset{\textbf{def}}{=} \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}i)$ and consider its automorphism group G_i induced by the multiplications by $\{\pm 1, \pm i\}$ in $\mathbb{C}$. Then, any $P \in \mathscr{E}_i(\mathbb{C})$ which has a non trivial stabiliser under the action of G_i is in $\mathscr{E}[2]$.*

Similarly, let $\mathscr{E}_\rho \overset{\textbf{def}}{=} \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\rho)$, where $\rho = e^{\frac{i\pi}{3}}$ with its automorphism group G_ρ induced by the multiplications by $\{\pm 1, \pm\rho, \pm\rho^2\}$, then any $P \in \mathscr{E}_\rho(\mathbb{C})$ with a non trivial stabiliser under the action of G_ρ is in $\mathscr{E}[6]$.

Proof. — In the case $\mathscr{E}_i$, denote by $\Lambda_i \overset{\textbf{def}}{=} \mathbb{Z} \oplus \mathbb{Z}i$. Since G_i is cyclic of order 4, its only nontrivial subgroups are $\{\pm 1\}$ and G_i itself. A point $P \in \mathscr{E}_i(\mathbb{C})$ stabilised by $\{\pm 1\}$ corresponds to $z \in \mathbb{C}$ such that $z \equiv -z \mod \Lambda_i$. That is to say $2z \in \Lambda_i$ and hence $P \in \mathscr{E}_i[2]$. Similarly if P is stabilised by all G_i it is *a fortiori* stabilised by $\{\pm 1\}$ and hence should be in $\mathscr{E}_i[2]$.

Consider now the case of $\mathscr{E}_\rho$. Denote by $\Lambda_\rho \overset{\textbf{def}}{=} \mathbb{Z} \oplus \mathbb{Z}\rho$. Since G_ρ is cyclic of order 6, its only possible nontrivial subgroups are $\{\pm 1\}$, $\{1, \rho^2, \rho^4\}$ and G_ρ itself. Let us consider points which are stabilised by one of these groups.

Let $P \in \mathscr{E}_\rho(\mathbb{C})$ stabilised by $\{\pm 1\}$, then the very same reasoning as for $\mathscr{E}_i$ yields $P \in \mathscr{E}_\rho[2]$.

Let $P \in \mathscr{E}_\rho(\mathbb{C})$ stabilised by $\{1, \rho^2, \rho^4\}$. This corresponds to $z \in \mathbb{C}$ satisfying $\rho^2 z \equiv z \mod \Lambda_\rho$. Writing $z = a + b\rho^2$ for some $a, b \in \mathbb{R}$ and using the relation $1 + \rho^2 + \rho^4 = 0$, we get

$$a + \rho^2 b \equiv -b + \rho^2(a - b) \mod \Lambda_\rho.$$

This entails that

$$\left\{ \begin{aligned} -b &= a + \mu \\ a - b &= b + \nu, \end{aligned} \right.$$

where $\mu, \nu \in \mathbb{Z}$. By elimination, we deduce that $3a \in \mathbb{Z}$ and $3b \in \mathbb{Z}$, that is to say $z \in \frac{1}{3}\Lambda_\rho$ and hence $P \in \mathscr{E}_\rho[3]$.

Finally, the previous discussion entails that a point stabilised by the whole G_ρ should be in $\mathscr{E}_\rho[2] \cap \mathscr{E}_\rho[3]$, and hence is nothing but $O_{\mathscr{E}_\rho}$. □

Proof of Theorem 74. — The idea is to consider the projection map $\pi : X_0(\ell) \to X_0(1)$, which sends a class of isomorphisms of isogenies $\phi : \mathscr{E} \to \mathscr{E}'$ onto the isomorphism class of $\mathscr{E}$. This map is algebraic (this will appear more naturally in § 5.4). The objective is to apply Riemann Hurwitz formula (Theorem 31) to π in order to compute the genus of $X_0(\ell)$.

Step 1. The degree of π. The degree of π is the generic number of pre-images of a point of $X_0(1)$. Such a point corresponds to a curve $\mathscr{E}$ up to isomorphism and its pre-image is the set of isomorphism classes of ℓ–isogenies $\mathscr{E} \to \mathscr{E}'$ or equivalently, the ismomorphism classes of pairs $(\mathscr{E}, C)$ where C is a subgroup of cardinality ℓ of $\mathscr{E}[\ell]$. From Lemma 75, if $\mathscr{E}$ has no nontrivial automorphism, then two distinct subgroups C_1, C_2 provide non isomorphic pairs $(\mathscr{E}, C_1), (\mathscr{E}, C_2)$. Thus, in this situation, the number of pre-images of $\mathscr{E}$ by π corresponds to the number of subgroups of cardinality ℓ in $\mathscr{E}[\ell]$. Since ℓ is prime, then from Theorem 54, $\mathscr{E}[\ell] \simeq \mathbb{F}_\ell \times \mathbb{F}_\ell$ and hence is a vector space of dimension 2 over $\mathbb{F}_\ell$. Next, a subgroup of cardinality ℓ of $\mathscr{E}[\ell]$ is nothing but a subspace of dimension 1 and the number of subspaces of dimension 1 (*i.e.* of lines) of $\mathbb{F}_\ell \times \mathbb{F}_\ell$ equals $\sharp\mathbb{P}^1(\mathbb{F}_\ell) = \ell + 1$. Thus,

$$\deg \pi = \ell + 1.$$

Now, the map is ramified at the points corresponding to curves with nontrivial automorphisms and possibly the point at inifinity. From Theorem 69, the curves with nontrivial automorphisms correspond to the tori $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}i)$ and $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\rho)$, where $\rho = e^{\frac{i\pi}{3}}$. For these tori, we need to understand the action of the automorphisms on the ℓ–torsion.

Step 2. Ramification at $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}i)$. The curve is equipped with a nontrivial automorphism η of order 4, which corresponds to the multiplication by i in $\mathbb{C}$. This automorphism acts on the ℓ–torsion and, from [**Sil09**, Thm. III.4.8], such an automorphism is a group automorphism and hence its action on $\mathscr{E}[\ell]$ regarded as an $\mathbb{F}_\ell$–vector space is $\mathbb{F}_\ell$–linear. We denote by η_ℓ, the automorphism η restricted to $\mathscr{E}[\ell]$. From Lemma 77, since $\ell > 3$ any point in $\mathscr{E}[\ell] \setminus \{O_{\mathscr{E}}\}$ has has an orbit of cardinality 4 under η_ℓ. Therefore, η_ℓ has order 4 and two situations may occur. Either $\ell \equiv 1 \mod 4$, then $\mathbb{F}_\ell$ contains fourth roots of 1 and η_ℓ regarded as an $\mathbb{F}_\ell$–automorphism of $\mathbb{F}_\ell \times \mathbb{F}_\ell$ is diagonalisable as

$$\begin{pmatrix} \iota & 0 \\ 0 & -\iota \end{pmatrix},$$

where ι denotes a primitive fourth root of 1. In this situation, η_ℓ acts on the lines of $\mathbb{F}_\ell \times \mathbb{F}_\ell$ by fixing the two lines corresponding to the eigenspaces of η_ℓ and any other line has an orbit of cardinality 2, indeed $\eta_\ell^2 = -\mathrm{Id}$, which leaves any line invariant. Two lines of $\mathscr{E}[\ell]$ in a same orbit under η_ℓ correspond to a same point in $X_0(\ell)$. This point is a ramification point with ramification index 2. Therefore, if $\ell \equiv 1 \mod 4$, then there are 2 unramified points in the pre-image of the isomorphism class of $\mathscr{E}$ by π and $\frac{\ell-1}{2}$ ramified points with ramification index 2.

Otherwise $\ell \equiv 3 \mod 4$. In this situation η_ℓ has no eigenspace in $\mathscr{E}[\ell]$ and the orbit of any line has cardinality 2. Thus, there are $\frac{\ell+1}{2}$ points above $\mathscr{E}$ which are all ramified with ramification index 2.

Step 3. Ramification at $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\rho)$. Here we have an automorphism η of order 6 and denote again by η_ℓ its restriction to $\mathscr{E}[\ell]$. Here again, from Lemma 77, we know that η_ℓ has also order 6. In this situation, if $\ell \equiv 1 \mod 3$, then $\mathbb{F}_\ell$ contains sixth roots of unity and η_ℓ is diagonalisable. Therefore, the two eigenspaces of η_ℓ are left invariant and any other $\mathbb{F}_\ell$–line of $\mathscr{E}[\ell]$ has an orbit of cardinality 3. Indeed, here again $\rho^3 = -\mathrm{Id}$ and hence leaves any line globally invariant. In such a situation, the pre-image of $\mathscr{E}$ consists in 2 unramified points corresponding to the two eigenspaces of η_ℓ in $\mathscr{E}[\ell]$ and $\frac{\ell-1}{3}$ points with ramification index 3.

If $\ell \equiv 2 \mod 3$, then any line of $\mathscr{E}[\ell]$ has an orbit of cardinality 3 under the action of η_ℓ and hence the pre-image of $\mathscr{E}$ by π consists in $\frac{\ell+1}{3}$ points, all with ramification index 3.

Step 4. Ramification at infinity. The point at infinity of $X_0(1)$ is the quotient of $\mathbb{P}^1(\mathbb{Q})$ under the action of $\mathbf{SL}_2(\mathbb{Z})$, which, from Proposition 71, consists in a single orbit. We wish to estimate the number of orbits in $\mathbb{P}^1(\mathbb{Q})$ under the action of $\Gamma_0(\ell)$. We claim that their number is 2, namely, the orbit of $(0:1)$ and that of $(1:0)$. Indeed,

$$\Gamma_0(\ell)\cdot(0:1) = \{(b:d)\in\mathbb{P}^1(\mathbb{Q}) \text{ with } \gcd(b,d)=1 \text{ and } d \text{ prime to } \ell\}$$

and

$$\Gamma_0(\ell)\cdot(1:0) = \{(a:c)\in\mathbb{P}^1(\mathbb{Q}) \text{ with } \gcd(a,c)=1 \text{ and } \ell \text{ dividing } c\}.$$

One easily sees that the two orbits form a partition of $\mathbb{P}^1(\mathbb{Q})$. This entails that the pre-image of the point at infinity of $X_0(1)$ consists in two points P, Q whose ramification indexes satisfy $e_P + e_Q = \ell + 1$.

Final step. Computation of the genus. Denote by g_ℓ the genus of $X_0(\ell)$ and by $g_1 = 0$ that of $X_0(1)$. Riemann–Hurwitz formula asserts that

$$2g_\ell - 2 = (2g_1 - 2)(\ell+1) + \nu_i + \nu_\rho + \nu_\infty,$$

where ν_i, ν_ρ and ν_∞ are the respective contributions of the ramifications above $\mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}i)$, $\mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}\rho)$ and the point at infinity. We get

$$\nu_2 = \begin{cases} \frac{\ell-1}{2} & \text{if} \quad \ell\equiv 1 \mod 4 \\ \frac{\ell+1}{2} & \text{if} \quad \ell \equiv 3 \mod 4\end{cases}, \quad \nu_3 = \begin{cases} 2\frac{\ell-1}{3} & \text{if} \quad \ell\equiv 1 \mod 3 \\ 2\frac{\ell+1}{3} & \text{if} \quad \ell \equiv 2 \mod 3\end{cases} \quad \text{and} \quad \nu_\infty = \ell - 1.$$

An easy but cumbersome calculation treating separately the four cases $\ell \equiv 1, 5, 7, 11 \mod 12$ yields the expected result. □

5.4. The modular equation. — To conclude this section, we give a statement whose proof is omitted but which may help the reader to be convinced that $X_0(\ell)$ has a structure of algebraic curve. We refer the reader to [**Mil17**, Thm. 6.1] for a proof.

Theorem 78. — *There exists an irreducible polynomial $\Phi_\ell \in \mathbb{Z}[x,y]$ such that for any pair $\mathscr{E}, \mathscr{E}'$ of elliptic curves related with a degree ℓ isogeny $\mathscr{E}\to\mathscr{E}'$, then $\Phi_\ell(j(\mathscr{E}), j(\mathscr{E}')) = 0$.*

Remark 79. — A database of the polynomials Φ_ℓ for small values of ℓ is available on Andrew Sutherland's webpage: `https://math.mit.edu/∼drew/ClassicalModPolys.html`

Let us give some comments about this statement. First, note that the projective closure of the complex curve of equation $\Phi_\ell(x,y) = 0$ is a "singular model" for $X_0(\ell)$. Indeed, any point of $X_0(\ell)$ corresponds to an isomorphism class of ℓ–isogeny $\mathscr{E}\to\mathscr{E}'$. This yields a rational map

$$\begin{cases} X_0(\ell) & \longrightarrow & \mathbb{P}^2(\mathbb{C}) \\ (\mathscr{E}\to\mathscr{E}') & \longmapsto & (j(\mathscr{E}) : j(\mathscr{E}') : 1). \end{cases}$$

The image of this map is contained into the curve with equation $\Phi_\ell(x,y)=0$. However, this latter curve is full of singularities and hence is not isomorphic to $X_0(\ell)$. Nevertheless, (and this is far from being obvious) this permits to deduce that $X_0(\ell)$ is itself defined over $\mathbb{Q}$ and hence, its reduction modulo p makes sense.

An interesting fact is that, since $\Phi_\ell \in \mathbb{Z}[x,y]$, for any pair of ℓ–isogenous curves $\mathscr{E}\to\mathscr{E}'$ over $\mathbb{F}_p$ we have $\Phi_\ell(j(\mathscr{E}), j(\mathscr{E}')) \equiv 0 \mod p$. Moreover, if ℓ and p are prime to each other, it is known that the polynomial Φ_ℓ is irreducible modulo p (see for instance [**Mor90**, Thm. 5.9]). Thus, the curve over $\mathbb{F}_p$ of equation $\Phi_\ell(x,y) = 0$ turns out to be a singular model of a smooth curve over $\mathbb{F}_p$, that we will also denote by $X_0(\ell)$ such that $X_0(\ell)(\overline{\mathbb{F}}_p)$ parameterises ℓ–isogenies $\mathscr{E}\to\mathscr{E}'$ over $\overline{\mathbb{F}}_p$ up to isomorphism. These curves over $\mathbb{F}_p$ will be the objects of interest in order to prove the main theorem of this course, namely Theorem 41.

Finally, the reader interested in a rigorous study of the reductions of modular curves cannot avoid the language of schemes. For such a development, we refer the reader to the article of Celgene and Rapoport [**DR73**] or the book of Katz and Mazur [**KM85**].

6. Proof of the main Theorem

Now, we almost have the material to prove Theorem 41. We have our family of curves $X_0(\ell)$ for ℓ a prime integer distinct from the characteristic p.

6.1. Genus of modular curves over finite fields. — Let us briefly discuss the genus of the curve. The discussion to follow is far from being trivial. Thus, the reader is encouraged first to directly admit the conclusion. Namely that the genus of a modular curve over a finite field is that of its complex counterpart. Let us briefly sketch the reasons why this holds.

It is known (see for instance in [**Mor90**, Thm. 5.9]) that, the curve $X_0(\ell)$ has a smooth projective model described by equation with coefficients in $\mathbb{Z}$ and whose reduction modulo p is smooth too.

Next, as already mentioned in Remark 29, two different notions of genus are associated to a curve, the *arithmetic* genus p_a and the *geometric* one g. The genus introduced by Definition 25 in § 2.7 is the geometric one. The arithmetic genus, which can be defined for instance from the Hilbert function of the variety [**Har77**, Ch. IV], is always larger than or equal to the geometric one and they coincide if and only if the curve is smooth.

Next, Grauert Theorem [**Har77**, Cor. III.12.9] permits to assert that the reduction modulo p of the aforementioned model $X_0(\ell)$ has the same arithmetic genus as the complex curve itself. Moreover, since this model and its reduction are smooth, they also have the same geometric genus. Therefore, the genus of the curve $X_0(\ell)$ over $\mathbb{F}_p$ is the same as that of its complex counterpart and hence is given by Theorem 74.

6.2. The locus of supersingular curves. — There remains to get an estimate of the number of rational points of such curves. For this we will focus on $\mathbb{F}_{p^2}$–points since their number can be bounded from below using the two following statements.

Proposition 80. — *Let $\mathscr{E}$ be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$, then $\mathscr{E}$ is defined over $\mathbb{F}_{p^2}$.*

Proof. — By definition, a supersingular curve $\mathscr{E}$ satisfies $\mathscr{E}[p] = \{0\}$. Therefore, the multiplication by p map $[p] : E \to E$ is totally inseparable.

Consider now the Frobenius map

$$\phi : \left\{ \begin{array}{ccc} \mathscr{E} & \longrightarrow & \mathscr{E}^{(p)} \\ (x,y) & \longmapsto & (x^p, y^p). \end{array} \right.$$

It is a degree p isogeny, hence it has a dual isogeny $\hat{\phi}$ such that $\hat{\phi} \circ \phi = [p]$. Since $[p]$ is totally inseparable, $\hat{\phi}$ should be inseparable either and hence, so should be the Frobenius map

$$\hat{\phi} : \left\{ \begin{array}{ccc} \mathscr{E}^{(p)} & \longrightarrow & \mathscr{E}^{(p^2)} \\ (x,y) & \longmapsto & (x^p, y^p). \end{array} \right.$$

Thus, $\mathscr{E}^{(p^2)} = \mathscr{E}$ and hence $\mathscr{E}$ is defined over $\mathbb{F}_{p^2}$. □

Theorem 81. — *The number of $\overline{\mathbb{F}}_p$–isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ equals*

$$\left\lfloor \frac{p}{12} \right\rfloor + \left\{ \begin{array}{cccccc} 0 & \textit{if} & p & \equiv & 1 & \bmod 12 \\ 1 & \textit{if} & p & \equiv & 5 & \bmod 12 \\ 1 & \textit{if} & p & \equiv & 7 & \bmod 12 \\ 2 & \textit{if} & p & \equiv & 11 & \bmod 12. \end{array} \right.$$

Proof. — See [**Sil09**, Thm. V.4.1]. □

6.3. Proof of the main theorem. — With these two last statements at hand we can finally provide the proof of Theorem 41. We restrict the proof to the case $p \geqslant 5$. Note that Tsfasman–Vlăduţ–Zink theorem remains true when $p = 2, 3$ but the coding theoretic interest is rather limited.

Proof of Theorem 41. — Consider the sequence of curves $X_0(\ell)$ for $\ell \equiv 11 \mod 12$. From Theorem 74 it has genus $g_\ell = \frac{\ell+1}{12}$. From Theorem 81, the curve $X_0(1)$ has at least $\frac{p-1}{12}$ $\mathbb{F}_{p^2}$–rational points corresponding to isomorphism classes of supersingular elliptic curves. Such an elliptic curve with no nontrivial automorphism has $\ell + 1$ pre-images in $X_0(\ell)$ which also correspond to supersingular elliptic curves and hence are $\mathbb{F}_{p^2}$–rational points. Depending on the class of p modulo 12 the curves with j–invariant 0 and 1728 may be supersingular. More precisely, from [**Sil09**, Ex. V.4.4 & V.4.5],

- for $p \equiv 1 \mod 12$, both curves are ordinary (*i.e.* non supersingular) and then any supersingular curve has no nontrivial automorphism and hence has $\ell + 1$ pre-images in $X_0(\ell)(\mathbb{F}_{p^2})$. Therefore, from Theorem 81,
$$\sharp X_0(\ell)(\mathbb{F}_{p^2}) \geqslant (\ell+1)\frac{p-1}{12}\cdot$$
- for $p \equiv 5 \mod 12$, the curve with $j = 0$ is supersingular and the one with $j = 1728$ is ordinary. Therefore, there are $\frac{p-5}{12} + 1$ supersingular curves and all of them but one have $\ell + 1$ distinct pre-images. The remaining curve is the one with $j = 0$ and an automorphism group of order 6. Its treatment is very similar to the proof of Theorem 74. Consider the action of the automorphism of order 6 on the ℓ–torsion. From Lemma 77, this induces an automorphism η or order 6 of $\mathscr{E}[\ell] \simeq \mathbb{F}_\ell^2$. Since $\ell \equiv 11 \mod 12$, then $\ell \equiv 2 \mod 3$ and hence $\mathbb{F}_\ell$ does not contains the sixth roots of unity. Thus, η is not diagonalisable and hence cannot fix a line. Consequently, one proves that the orbit of any line is the union of 3 distinct lines ($\eta^3 = -\mathrm{Id}$, which fixes the lines). Therefore, the curve with j–invariant 0 has $\frac{\ell+1}{3}$ pre-images and Consequently, using Theorem 81:
$$\sharp X_0(\ell)(\mathbb{F}_{p^2}) \geqslant (\ell+1)\frac{p-5}{12} + \frac{\ell+1}{3} = (\ell+1)\frac{p-1}{12}\cdot$$
- for $p \equiv 7 \mod 12$, the curve with $j = 0$ is ordinary and the one with $j = 1728$ is supersingular. A similar reasoning yields
$$\sharp X_0(\ell)(\mathbb{F}_{p^2}) \geqslant (\ell+1)\frac{p-7}{12} + \frac{\ell+1}{2} = (\ell+1)\frac{p-1}{12}\cdot$$
- for $p \equiv 11 \mod 12$, both curves are supersingular and we get:
$$\sharp X_0(\ell)(\mathbb{F}_{p^2}) \geqslant (\ell+1)\frac{p-11}{12} + \frac{\ell+1}{2} + \frac{\ell+1}{3} = (\ell+1)\frac{p-1}{12}\cdot$$

In summary, we always have a lower bound $(\ell+1)\frac{p-1}{12}$ on the number of rational points. Then
$$\frac{\sharp X_0(\ell)(\mathbb{F}_{p^2})}{g_\ell} \geqslant \frac{\frac{p-1}{12}(\ell+1)}{\left(\frac{\ell+1}{12}\right)} = p-1.$$

Thus, over $\mathbb{F}_q$ for $q = p^2$, we identified a family of curves whose number of $\mathbb{F}_q$–rational points goes to infinity and whose ratio, number of $\mathbb{F}_q$–points divided by the genus goes to $\sqrt{q} - 1$. Which turns out to be optimal. □

References

[BH08] Peter Beelen and Tom Høholdt. The decoding of algebraic geometry codes. In *Advances in algebraic geometry codes*, volume 5 of *Ser. Coding Theory Cryptol.*, pages 49–98. World Sci. Publ., Hackensack, NJ, 2008.

[Cou16] Alain Couvreur. Introduction to coding theory, 2016. Personal lecture notes.

[CR21] Alain Couvreur and Hugues Randriambololona. Algebraic geometry codes and some applications. In W. Cary Huffman, Jon-Lark Kim, and Patrick Solé, editors, *Concise Encyclopedia of Coding Theory.* Chapman and Hall/CRC, 2021.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., Vol. 349, pages 143–316. Springer, Berlin, 1973.

[Duu08] Iwan M. Duursma. Algebraic geometry codes: general theory. In *Advances in algebraic geometry codes*, volume 5 of *Ser. Coding Theory Cryptol.*, pages 1–48. World Sci. Publ., Hackensack, NJ, 2008.

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

[Gop81] Valerii D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6):1289–1290, 1981. In Russian.

[GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Inventiones Mathematicae*, 121:211–222, 1995.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[HP95] Tom Høholdt and Ruud Pellikaan. On the decoding of algebraic–geometric codes. *IEEE Trans. Inform. Theory*, 41(6):1589–1614, Nov 1995.

[HvLP98] Tom Høholdt, Jacobus Hendricus van Lint, and Ruud Pellikaan. Algebraic geometry of codes. In *Handbook of coding theory, Vol. I, II*, pages 871–961. North-Holland, Amsterdam, 1998.

[Iha81] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28:721–724, 1981.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[Lor96] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[Mar88] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problemy Peredachi Informatsii*, 24(1):51–60, 1988.

[Mil17] James S. Milne. Modular functions and modular forms (v1.31), 2017. Available at `www.jmilne.org/math/`.

[Mor90] Carlos J. Moreno. *Algebraic curves over finite fields.* Cambridge tracts in mathematics. Cambridge University Press, Cambridge, 1990.

[Sha94] Igor R. Shafarevich. *Basic algebraic geometry. 1.* Springer-Verlag, Berlin, second edition, 1994.

[Sil09] Joseph Silverman. *The arithmetic of elliptic curves*, volume 106. Springer-Verlag New York, second edition, 2009.

[Ste99] Serguei A. Stepanov. *Codes on algebraic curves.* Kluwer Academic/Plenum Publishers, New York, 1999.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[TVN07] Michael A. Tsfasman, Serge Vlăduţ, and Dmitry Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2007.

[TVZ82] Michael A. Tsfasman, Serge G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

[VD83] Sergei G. Vlăduţ and Vladimir G. Drinfeld. Number of points of an algebraic curve. *Funct. Anal. Appl.*, 17:53–54, 1983.

[VM84] S. G. Vlăduţ and Yu. I. Manin. Linear codes and modular curves. In *Current problems in mathematics, Vol. 25*, Itogi Nauki i Tekhniki, pages 209–257. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984.

[Wal00] Judy L. Walker. *Codes and curves*, volume 7 of *Student Mathematical Library.* American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2000. IAS/Park City Mathematical Subseries.

Alain Couvreur, Inria, France • *E-mail :* `alain.couvreur@inria.fr`