INTRODUCTION TO ZETA AND L-FUNCTIONS FROM ARITHMETIC GEOMETRY AND SOME APPLICATIONS [INTRODUÇÃO ÀS FUNÇÕES L E ZETA DA GEOMETRIA ARITMÉTICA E ALGUMAS APLICAÇÕES]

MARC HINDRY (UNIVERSITÉ DENIS DIDEROT PARIS 7)

Abstract. Zeta or L-functions are modelled on the Riemann's zeta function originally defined by the series $\zeta(s) = \sum_{n\geq 1} n^{-s}$ and then extended to the whole complex plane. The zeta function has an "Euler product", a "functional equation" and though very much studied still keeps secret many of its properties, the greatest mystery being the so-called Riemann Hypothesis. Many similar (or thought to be similar) series $\sum_{n\geq 1} a_n n^{-s}$ have been introduced in arithmetic, algebraic geometry and even topology, dynamics (we won't discuss the latter). We plan basically to discuss zeta functions attached to algebraic varieties over finite fields and global fields.

The first applications of zeta functions have been the arithmetic progession theorem (Dirichlet, 1837) "*there exists one (hence infinitely) prime congruent to a modulo b, whenever a and b are coprime*" and the prime number theorem (Riemann 1859, with an incomplete proof; Hadamard and de la Vallée Poussin, 1896) "*the number of primes less than x is asymptotic to $x/\log x$*". But further applications were not restricted to the study of prime numbers, they include the study of the ring of algebraic integers, class field theory, the estimation of the size of solutions of (some) diophantine equations, etc. Moreover L-functions have provided or suggested fundamental links between algebraic varieties (motives over $\mathbb{Q}$), Galois representations, modular or automorphic forms; for example, though they do not appear explicitly in Wiles work, it seems fair to say they played an important rôle in the theory that finally led to the solution of Shimura-Taniyama-Weil conjecture and thus of Fermat's Last Theorem.

The first four lectures develop results and definitions which though all classical are perhaps not too often gathered together. The first lecture introduces Riemann's zeta function, Dirichlet L-function associated to a character, Dedekind zeta functions and describes some applications of zeta functions; the second introduces the Hasse-Weil zeta functions associated to algebraic varieties defined over a finite field, a number field or a function field as well as L-functions associated to Galois representations and modular forms; the third reviews techniques from complex analysis and estimates for zeta functions; the fourth touches the theory of special values of zeta functions, some known like the class number formula and some conjectured like the Birch and Swinnerton-Dyer formula. The fifth and final lecture is an exposition of recent work of Boris Kunyavskiĭ, Micha Tsfasman, Alexei Zykin, Amílcar Pacheco and the author around versions and analogues of the Brauer-Siegel theorem.

Prerequisite will be kept minimal whenever possible : a course in complex variable and algebraic number theory, a bit of Galois theory plus some exposure to algebraic geometry should suffice.

Mini-curso, XXI Escola de Álgebra, Brasília, julho 2010

Nota bene : Notes are given in English but the *mini-curso* will be given in Portuguese. Also these sketchy notes will be completed later and posted on my web page. [Added August 2010 : Hopefully this is done in the present version]

Nota bene : Estas notas estão escritas em inglês mas o mini-curso sera dado em português. Ela contém as idéias essenciais e seu esboço sera completado mais tarde e colocado na pagina web deste autor. [Esperamos que esteja feito nesta presente versão]

Contents

1. Lecture I : Introduction and examples

1.1. **Riemann's zeta function (and the prime number theorem).** The central object of the theory is the Riemann zeta function, defined for $\Re s > 1$ by the series

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}. \tag{1.1}$$

A fundamental property is its factorisation, known as the Euler product formula, which can be viewed as an analytic presentation of the unique factorisation theorem.

Theorem 1.1. *(Euler product formula) When $\Re s > 1$, we have :*

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} (1 - p^{-s})^{-1}. \tag{1.2}$$

This can be used to define the main branch of $\log \zeta(s)$ or compute $\frac{\zeta'}{\zeta}(s)$ and $1/\zeta(s)$ as follows

(1.3)

$$\log \zeta(s) = \sum_{m \geq 1, p} \frac{p^{-ms}}{m} \qquad \text{and} \qquad -\frac{\zeta'}{\zeta}(s) = \sum_{m \geq 1, p} (\log p) p^{-ms} = \sum_{n \geq 1} \Lambda(n) n^{-s}.$$

Here the *Mangoldt function* is implicitely defined as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \\ 0 & \text{else.} \end{cases}$$

One can also compute

$$\frac{1}{\zeta(s)} = \sum_{n=1} \mu(n) n^{-s} = \prod_{p} (1 - p^{-s}),$$

where the *Moebius function* is defined as

$$\mu(n) = \begin{cases} 1 & \text{for } n = 1 \\ (-1)^k & \text{if } n = p_1 \dots p_k \\ 0 & \text{else.} \end{cases}$$

It is easy to extend a bit this function say to $\Re s > 0$, for example via the formula

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{s-1} + 1 + s \int_1^{\infty} ([t] - t) t^{-s-1} dt, \tag{1.4}$$

which clearly displays a (simple) pole at $s = 1$ with residue 1. This formula is a special case of the following general (and easy) lemma.

Lemma 1.2. *Let a_n be a sequence of complex numbers with $a_n = O(n^c)$ for some constant c. Put $A(t) := \sum_{n \leq t} a_n$ then, for $\Re s > c + 1$:*

$$\sum_{n=1}^{\infty} a_n n^{-s} = s \int_1^{\infty} A(t) t^{-s-1} dt. \tag{1.5}$$

But actually much more is true; if you have never seen the definition of the Γ function see the beginning of lecture III.

Theorem 1.3. *(Functional Equation) The function $\zeta(s)$ extends to a function on the whole complex plane, holomorphic except for a simple pole at $s = 1$ with residue 1. Further it satisfies the following functional equation. Let $\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$ then, away from 0 and 1, the function $\xi(s)$ is bounded in any vertical strip and satisfies :*

$$\xi(s) = \xi(1-s). \tag{1.6}$$

Corollary 1.4. *The function $\zeta(s)$ does not vanish in the half-plane $\Re s > 1$; inside the half-plane $\Re s < 0$ it has only simple zeroes at even negative integers $-2, -4, -6, \ldots$. All the other zeroes are inside the critical strip $0 \leq \Re s \leq 1$.*

Proof. (Sketch) The proof relies on harmonic analysis or Fourier analysis. Denote $\hat{f}(x) := \int_{\mathbb{R}} f(x)\exp(2\pi ixy)dx$, the Fourier transform of an integrable function f. Start with the Poisson formula:

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n). \tag{1.7}$$

Define $\theta(u) := \sum_{n\in\mathbb{Z}} \exp\left(-\pi u n^2\right)$, then, applying Poisson formula to $f(x) = \exp(-\pi u x^2)$ whose Fourier transform is $\hat{f}(y) = \exp(-\pi y^2/u)/\sqrt{u}$, one gets the functional equation for the theta function (this can be interpreted as θ being a modular form of half integer weight, see section 2.5).

$$\theta(1/u) = \sqrt{u}\,\theta(u). \tag{1.8}$$

One then computes (using the change of variables $t = \pi n^2 u$) for $\Re(s) > 1$.

$$\begin{aligned}\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) &= \sum_{n\geq 1}\int_0^\infty e^{-t}t^{s/2}\pi^{-s/2}n^{-s}\frac{dt}{t}\\ &= \int_0^\infty \left\{\sum_{n\geq 1}\exp(-\pi u n^2)\right\} u^{s/2}\frac{du}{u} = \int_0^\infty \tilde{\theta}(u)\frac{u^{s/2}du}{u}\end{aligned}$$

where

$$\tilde{\theta}(u) := \sum_{n\geq 1}\exp\left(-\pi u n^2\right) = \frac{\theta(u)-1}{2}\cdot$$

Notice $\tilde{\theta}(u) = O(\exp(-\pi u)$, when u goes to infinity; plugging in (1.8) one gets

$$\tilde{\theta}\left(\frac{1}{u}\right) = \sqrt{u}\,\tilde{\theta}(u) + \frac{1}{2}\left(\sqrt{u}-1\right). \tag{1.9}$$

Since $\int_1^\infty t^{-s} = 1/(s-1)$ and using (1.9), we get

$$\begin{aligned}\xi(s) &= \int_0^1 \tilde{\theta}(u)\frac{u^{s/2}du}{u} + \int_1^\infty \tilde{\theta}(u)\frac{u^{s/2}du}{u}\\ &= \int_1^\infty \tilde{\theta}(1/u)\frac{u^{-s/2}du}{u} + \int_1^\infty \tilde{\theta}(u)\frac{u^{s/2}du}{u}\\ &= \int_1^\infty \left\{\sqrt{u}\tilde{\theta}(u) + \frac{1}{2}\left(\sqrt{u}-1\right)\right\}\frac{u^{-s/2}du}{u} + \int_1^\infty \tilde{\theta}(u)\frac{u^{s/2}du}{u}\\ &= \int_1^\infty \tilde{\theta}(u)\left\{u^{\frac{s}{2}} + u^{\frac{1-s}{2}}\right\}\frac{du}{u} + \frac{1}{s-1} - \frac{1}{s}\cdot\end{aligned} \tag{1.10}$$

The latter expression is a priori valid for $\Re(s) > 1$, but it is easy to see that, since $\tilde{\theta}(u) = O(\exp(-\pi u)$, the function is entire, it is also clearly symmetric with respect to the transformation $s \mapsto 1 - s$. Finally the function defined by the integral in the last line is bounded in every vertical strip. □

The zeroes inside the critical strip have two symmetries $s \mapsto \bar{s}$ and $s \mapsto 1 - s$ this perhaps may suggest the following.

Conjecture 1.5. *(Riemann Hypothesis) All the zeroes inside the critical strip lie on the line $\Re s = \frac{1}{2}$.*

In this direction we have the following "weak" but essential and sufficient to prove the prime number theorem!

Theorem 1.6. *(Hadamard – de la Vallée Poussin) The function $\zeta(s)$ does not vanish on the line $\Re(s) = 1$.*

Proof. Start with the trivial but useful inequality $3 + 4\cos(t) + \cos(2t) = 2(1 + \cos t)^2 \geq 0$. Using equation 1.3 we may write (for $\sigma > 1$):

$$\log \zeta(\sigma) + 4 \log |\zeta(\sigma + it)| + \log |\zeta(\sigma + 2it)| = \sum_{p,m} \frac{p^{-m\sigma}}{m} \Re(3 + 4p^{-mit} + p^{-2mit}) \geq 0.$$

Taking exponentials on both side, we obtain :

$$\zeta(\sigma)^3 |\zeta(\sigma + it)|^4 |\zeta(\sigma + i2t)| \geq 1. \tag{1.11}$$

Call h (resp. k) the order of $\zeta(s)$ at $s = \sigma + it$ (resp. at $\sigma + 2it$), then the inequality (1.11) reads, as σ tends to 1

$$1 \leq \zeta(\sigma)^3 |\zeta(\sigma + it)|^4 |\zeta(\sigma + i2t)| \sim c(\sigma - 1)^{k+4h-3}$$

with $c > 0$, hence $k + 4h - 3 \leq 0$. Since h, k are non negative integers we conclude that $h = 0$. □

Thus the non trivial zeroes lie *inside* the critical strip; one can extend the HdVP argument to show that $\zeta(\sigma + i\tau) \neq 0$ in regions like $\sigma > 1 - \frac{c_1}{\log \tau}$ and this is essentially the best know result.

Theorem 1.7. *(Prime Number Theorem) Let $\pi(x) := \#\{p \text{ prime} \mid p \leq x\}$ then*

$$\pi(x) \sim \frac{x}{\log x}. \tag{1.12}$$

Equivalently if $\psi(x) = \sum_{n \leq x} \Lambda(n)$, then $\psi(x) \sim x$.

The basic idea is to use a formula of Perron (see proposition 3.10), picking $c > 1$ and denoting $\int_{(c)}$ for the integral on the vertical line $\Re s = c$:

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \frac{1}{2\pi i} \int_{(c)} -\frac{\zeta'}{\zeta}(s) x^s ds. \tag{1.13}$$

The function inside the integral has a pole at $s = 1$ with residue x, it has no other pole in an open neighbourhood of $\Re s \geq 1$ (thanks to theorem 1.6!), thus one can move the line of integration to a contour slightly to the left of $\Re s = 1$, picking a residu x at $s = 1$ and making it plausible that the contour integral is $o(x)$ though there remains work to be done before fully proving that (see lecture III, section 3.2, for other approaches, each requiring the use of theorem 1.6).

Notice, that $|\zeta(s)| \leq \zeta(c)$ for $\Re s \geq c > 1$; using the functional equation and the fact that $\xi(s)$ is bounded in vertical strips one gets easily a bound for $\zeta(s)$ or $\xi(s)$ of the shape $O(\exp(c|s|^{1+\epsilon}))$ (away from the poles) which means that the function is *of order one* in Hadamard's terminology and thus we deduce :

Theorem 1.8. *(Hadamard product) The function $\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$ can be written as a product*

$$s(1-s)\xi(s) = e^{a+bs}\prod_{\rho}\left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}}, \tag{1.14}$$

where ρ runs over the zeroes in the critical strip.

We summarise the properties that all zeta functions $L(s)$ will (or should) enjoy:

(1) be defined by a Dirichlet series $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ (convergent in some half-plane).
(2) be equal to an Euler product $L(s) = \prod_p L_p(s)$ with $L_p(s) = 1+\sum_{m\geq 1} a_{p^m}p^{-ms}$; in fact they will be of the shape
$$L_p(s) = \prod_{j=1}^{d}(1-\alpha_{p,j}p^{-s})^{-1},$$
where d is called the *degree* of the Euler product and $|\alpha_{p,j}| \leq p^{w/2}$ with equality for almost all p and w is called the *weight* (the Riemann zeta function has degree one and weight zero).
(3) have analytic continuation to the whole complex plane with a functional equation $\Lambda(s) = \pm\Lambda(w+1-s)$ where $\Lambda(s) = Q^{-s}L_\infty(s)L(s)$ is bounded in every vertical strip; here Q is a positive real number and $L_\infty(s)$ is the product of Gamma functions $\Gamma(as+b)$.
(4) be a function of order one and therefore have Hadamard factorisation.
(5) satisfy the analogue of the Riemann hypothesis.

1.2. Dirichlet's L-functions (and the arithmetic progression theorem).

Theorem 1.9. *Let a, b be coprime integers (i.e. $\gcd(a,b) = 1$) then there exists (infinitely many) primes p congruent to a modulo b. Moreover primes are equidistributed in congruence classes in the sense that*

$$\pi(x;a,b) := \#\{p \leq x \mid p \equiv a \mod b\} \sim \frac{1}{\phi(b)}\pi(x). \tag{1.15}$$

The proof is based on the use of the following L-functions. First define *Dirichlet characters* as follows. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a homomorphism from the group of invertible elements mod N to $\mathbb{C}^*$, we extend it to a map denoted again χ from $\mathbb{Z}$ to $\mathbb{C}$ by

$$\chi(n) := \begin{cases} \chi(n \mod N) & \text{if } \gcd(n,N) = 1 \\ 0 & \text{if } \gcd(n,N) > 1. \end{cases}$$

It is convenient to introduce *primitive characters* as those who do not come from a smaller level M dividing N, i.e. for all M dividing strictly N, there is an $n \equiv 1$ mod M such that $\chi(n) \neq 0, 1$. The trivial character will be denoted χ_0.

Then define Dirichlet's L-function :

$$L(\chi, s) := \sum_{n=1}^{\infty}\chi(n)n^{-s}. \tag{1.16}$$

When χ is non trivial, the series is convergent for $\Re s > 0$ (absolutely convergent for $\Re s > 1$); it has an Euler product

$$L(\chi, s) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}. \tag{1.17}$$

When $\chi = \chi_0$ the trivial character modulo N, we get $L(\chi_0, s) = \prod_{p \mid N}(1-p^{-s})\zeta(s)$ and thus a pole at $s = 1$ but when χ is non trivial we notice that $|\sum_{n\leq x}\chi(n)| \leq N$ (because $\sum_{x<n\leq x+N}\chi(n) = 0$) hence the series $\sum \chi(n)n^{-s}$ is convergent for $\Re s > 0$ (using lemma 1.2). From the Euler product, one may infer formulas for the logarithm and logarithmic derivative :

(1.18)

$$\log L(\chi, s) = \sum_{p,m} \chi(p^m)\frac{p^{-ms}}{m} \qquad \text{and} \qquad -\frac{L'(\chi, s)}{L(\chi, s)} = \sum_{p,m} \chi(p^m)p^{-ms}\log p.$$

The function $L(\chi, s)$ has analytic continuation to the whole complex plane with a functional equation such that if χ is primitive modulo N and

$$\Lambda(\chi, s) = \left(\frac{N}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(\chi, s),$$

with $\delta = 0$ if $\chi(-1) = 1$ and $\delta = 1$ if $\chi(-1) = -1$ then

$$\Lambda(\chi, s) = w(\chi)\Lambda(\bar{\chi}, 1 - s), \tag{1.19}$$

for a complex number $w(\chi)$ with modulus 1 which can be computed as

$$w(\chi) = \frac{G(\chi)}{i^\delta\sqrt{N}},$$

where $G(\chi) = \sum_{x \mod N} \chi(x)\exp(2\pi ix/N)$ is the classical Gauss sum.

The key result is the following non vanishing statement.

Theorem 1.10. *Let χ be a non trivial character, then $L(\chi, 1) \neq 0$.*

The proof will be sketched later (section 3.1, using lemma 3.3).

To deduce the Arithmetic Progression Theorem from this, we notice the easy algebraic formula, where the sum is over characters modulo N

$$\sum_\chi \bar{\chi}(a)\chi(x) = \begin{cases} \phi(N) & \text{if } x \equiv a \mod N \\ 0 & \text{else} \end{cases}$$

and proceed to write for $\Re s > 1$ and s approaching 1:

$$\begin{aligned} \sum_{p\equiv a \mod N} p^{-s} &= \frac{1}{\phi(N)}\sum_p p^{-s} + \frac{1}{\phi(N)}\sum_{\chi\neq\chi_0}\bar{\chi}(a)\sum_p \chi(p)p^{-s} \\ &= \frac{1}{\phi(N)}\log(s-1)^{-1} + \frac{1}{\phi(N)}\sum_{\chi\neq\chi_0}\bar{\chi}(a)\log L(\chi, s) + O(1). \end{aligned}$$

The non vanishing of $L(\chi, 1)$ ensures that the second term remains bounded as s goes to 1 and thus the sum on the left has to be infinite.

1.3. **Some problems from arithmetic.** We already discussed prime number distribution. Lets us now consider other type of problems where zeta and L-function may be used to advantage.

Problem 1. The classical approach to Fermat's Last Theorem led Kummer to introduce the cyclotomic fields and rings

$$K = \mathbb{Q}(\exp(2\pi i/N) \qquad \text{and} \qquad \mathcal{O}_K = \mathbb{Z}[\exp(2\pi i/N)].$$

It quickly became obvious that it was important to settle the question:

(Q1) For which value of N is the ring $\mathcal{O}_K = \mathbb{Z}[\exp(2\pi i/N)]$ a unique factorisation domain?

Later, realising the answer to the first question is too often negative, Kummer introduced the following refinement: Let $C\ell_K$ be the quotient of non zero ideals by principal ideals; this turns out to be a finite group whose cardinality is called the *class number* of K and denoted h_K.

(Q2) For which primes p, is it true that p does not divide h_K for $K = \mathbb{Z}\Big[\exp\Big(\frac{2\pi i}{p}\Big)\Big]$?

A (partial) answer can be given using zeta and L-functions.

Problem 2. Consider rings of quadratic integers if $d \neq 0, 1$ is squarefee put $K = K_d = \mathbb{Q}(\sqrt{d})$ and $\mathcal{O}_K = \mathcal{O}_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ or $\mathbb{Z}[\sqrt{d}]$ according to wether $d \equiv 1 \mod 4$ or not. One would like to know when $\mathcal{O}_d$ is a unique factorisation domain, study units, etc. [When $d < 0$ the group of units is finite; when $d > 0$, modulo ± 1 the group of units is infinite cyclic and we want to study the size of the generator $\epsilon > 1$ called the *fundamental unit*].

A (partial) answer can be given using zeta and L-functions.

Problem 3. Let us introduce a bit more of algebraic number theory. Let $K/\mathbb{Q}$ be a finite extension, every rational prime p decomposes in K as a product of prime ideals $p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$; the prime p is said to be ramified in $K/\mathbb{Q}$ if some $e_i \geq 2$ and if $f_i = [\mathcal{O}_K/\mathfrak{P}_i : \mathbb{F}_p]$ then $\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}]$. Suppose now that $K/\mathbb{Q}$ is a Galois extension with Galois group G.

Definition 1.11. The *decomposition group* of $\mathfrak{P}/p$ is the subgroup

$$D(\mathfrak{P}/p) := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

When σ is in the decomposition group one may define $\tilde{\sigma} : \mathcal{O}_K/\mathfrak{P} \to \mathcal{O}_K/\mathfrak{P}$ by the diagram

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{\sigma} & \mathcal{O}_K \\ \downarrow & & \downarrow \\ \mathcal{O}_K/\mathfrak{P} & \xrightarrow{\tilde{\sigma}} & \mathcal{O}_K/\mathfrak{P}. \end{array}$$

Definition 1.12. The kernel of the map $\sigma \to \tilde{\sigma}$ from G to $\mathrm{Gal}\,((\mathcal{O}_K/\mathfrak{P})/\mathbb{F}_p)$ is called the *inertia group* of $\mathfrak{P}/p$ and denoted $I(\mathfrak{P}/p)$.

Notice that if $\#D(\mathfrak{P}/p) = f$ and $\#I(\mathfrak{P}/p) = e$ then $\#G = [K : \mathbb{Q}] = efg$. The inertia group $I(\mathfrak{P}/p)$ is trivial unless $\mathfrak{P}/p$ is ramified. The map $\sigma \to \tilde{\sigma}$ from G to $\mathrm{Gal}\,((\mathcal{O}_K/\mathfrak{P})/\mathbb{F}_p)$ is known to be surjective and a canonical generator of the cyclic group on the right is given by the map $x \mapsto x^p$.

Definition 1.13. The Frobenius at $\mathfrak{P}$ is the element $\mathrm{Frob}_{\mathfrak{P}}$ such that for all $x \in \mathcal{O}_K$ we have

$$\mathrm{Frob}_{\mathfrak{P}}(x) \equiv x^p \mod \mathfrak{P}.$$

Notice that, in the ramified case, the Frobenius is actually a coset modulo the inertia group. Further if we pick another prime above p, say $\mathfrak{P}' = \sigma(\mathfrak{P})$ then $\mathrm{Frob}_{\mathfrak{P}'} = \sigma \,\mathrm{Frob}_{\mathfrak{P}}\, \sigma^{-1}$ thus $\mathrm{Frob}_{\mathfrak{P}}$ depends only on p up to conjugation; we will denote Frob_p this conjugacy class.

Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G, let C be a conjugacy class in G, does there exist (infinitely many) primes such that $\mathrm{Frob}_p \in C$?

The answer can be given using zeta and L-functions.

Theorem 1.14. *(Tchebotarev) Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G, let C be a conjugacy class in G, then*

$$\#\{p \leq x \mid \mathrm{Frob}_p \in C\} \sim \frac{|C|}{|G|}\pi(x). \tag{1.20}$$

Notice that this theorem is a vast generalisation of Dirichlet's theorem. Indeed if we choose $K = \mathbb{Q}(\xi)$ with $\xi = \exp(2\pi i/N)$ then $\mathcal{O}_K = \mathbb{Z}[\xi]$ and the Galois group is abelian $G = \mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^*$. The Frobenius at p is simply given by $\mathrm{Frob}_p(\xi) = \xi^p$ (for p not dividing N), thus Tchebotarev theorem in this case is equivalent to Dirichlet theorem.

Problem 4. Consider the following diophantine equations :

1. (Pell-Fermat equation) $x^2 - dy^2 = 1$ where d is a squarefree integer and $(x, y) \in \mathbb{Z}^2$.
2. (units in radical cubic field) $x^3 + dy^3 + d^2z^3 - 3dxyz = 1$ where d is a squarefree integer and $(x, y, z) \in \mathbb{Z}^3$.
3. (elliptic curves) $y^2 = x^3+ax+b$ where a, b are integers such that $4a^3+27b^2 \neq 0$ and $(x, y) \in \mathbb{Q}^2$.

Algebro-geometric consideration will reveal that in these three cases the set of solutions form a finitely generated group (of rank $r = 1$ in the first two cases and rank $r \geq 0$ in the third case); the main question is what can we say about the (minimal) size of generators of this group?

Again a (partial) answer can be given via zeta functions (wait for the last lecture though!).

A first natural generalisation of Riemann's zeta function is *Dedekind zeta function* associated to a number field K (i.e. $[K : \mathbb{Q}] = d < \infty$). Recall that the *norm* of a non zero ideal $\mathcal{I}$ of $\mathcal{O}_K$ is defined as

$$N(\mathcal{I}) := \#\mathcal{O}_K/\mathcal{I}.$$

Recall also that the embeddings of fields $\sigma : K \hookrightarrow \mathbb{C}$ can be divided into r_1 real embeddings $\sigma : K \hookrightarrow \mathbb{R}$ and r_2 *pairs* of complex embeddings $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$.

If $\alpha_1, \ldots, \alpha_d$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and $\mathrm{Tr}\,\alpha = \mathrm{Tr}^K_{\mathbb{Q}}\,\alpha$ denotes the sum of the d conjugates of α, we define the (absolute value of the) *discriminant*:

$$\Delta_K := |\det(\mathrm{Tr}(\alpha_i\alpha_j)|\,. \tag{1.21}$$

The sign of the discriminant may be an interesting issue but since we'll have no use for it, we'll neglect it. An important property is that p is ramified in $K/\mathbb{Q}$ if

and only if p divides Δ_K. This permits the following important definition of the *Dedekind zeta function* of a number field K:

$$\zeta_K(s) := \sum_{\mathcal{I}} N(\mathcal{I})^{-s}. \tag{1.22}$$

where the sum runs over non zero ideals of $\mathcal{O}_K$.

This zeta function has an Euler product (it has degree d and weight zero):

$$\zeta_K(s) := \prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1}, \tag{1.23}$$

where the product runs over non zero *prime* ideals of $\mathcal{O}_K$ (i.e. maximal ideals). This formula is an analytic version of the theorem of unique factorisation of ideals into product of prime ideals for Dedekind domains. One easily infers that

$$\log \zeta_K(s) = \sum_{\mathfrak{p},m} \frac{N(\mathfrak{p})^{-ms}}{m} \qquad \text{and} \qquad -\frac{\zeta_K'}{\zeta_K}(s) = \sum_{\mathfrak{p},m} N(\mathfrak{p})^{-ms} \log N(\mathfrak{p}).$$

Theorem 1.15. *(Hecke) The Dedekind zeta function has analytic continuation to the whole complex plane (except for a single simple pole at $s = 1$) and satisfies a functional equation. Let*

$$\xi_K(s) := \left(\frac{\sqrt{\Delta_K}}{2^{r_1}\pi^{d/2}}\right)^s \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta_K(s),$$

then

$$\xi_K(s) = \xi_K(1-s).$$

It will be convenient to introduce the following notation.

Notation 1.16. We introduce the *modified Gamma functions* as follows.

$$\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right) \qquad \text{et} \qquad \Gamma_{\mathbb{C}}(s) := (2\pi)^{-s}\Gamma\left(s\right). \tag{1.24}$$

Notice that we may rewrite the function $\xi_K(s)$ from the functional equation as :

$$\xi_K(s) := \Delta_K^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s).$$

1.4. **Analogies between number fields and function fields.** The first idea is to compare $R = \mathbb{Z}$ and $K[T]$ (with K a field); both rings are principal domains The analogy becomes more arithmetic if $K = \mathbb{F}_q$ because then quotients R/I and $K[T]/I$ are finite (for a non zero ideal).

Absolute values on $\mathbb{Z}$ are of two types : the absolute values attached to a prime ideal (or prime number) p and normalised for example by $|x|_p = p^{-\operatorname{ord}_p x}$ and the archimedean or usual absolute value $|x|_\infty = |x|$. On $K[T]$ the absolute value are apparently of two types, those associated to a prime ideal (or irreducible polynomial) P and normalised by say $|x|_P = e^{-\operatorname{ord}_P x}$, and the one given by the degree say $|x|_\infty = e^{\deg x}$; in both cases we have the *product formula*, for all non zero x in the field of fractions:

$$\prod_v |x|_v = 1. \tag{1.25}$$

For a function field, this is a restatement of the fact that the sum of multiplicities of zeroes minus the sum of multiplicities of poles of a function on a smooth complete curve is zero. For $K = \mathbb{Q}$ the formula follows from an essentially trivial verification.

But notice that, in the case $R = K[T]$, the "infinite" absolute value can be interpreted as associated to a point at infinity, introducing the projective line $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ and viewing $K[T]$ as the ring of regular functions on the affine line $\mathbb{A}^1$, then $\deg x = \log |x|_\infty$ is equal to $-\operatorname{ord}_\infty x$. We will denote M_K the set of places of K (i.e. the set of closed points of C or, if one prefers, the set of Galois conjugacy classes of points in $C(\bar{\mathbb{F}}_p)$).

When $K = \mathbb{F}_q(C)$ and $v \in M_K$, we put $q_v := q^{\deg v}$ and define :

$$\zeta_K(s) = \prod_v (1 - q_v^{-s})^{-1}.$$

Then we have the following theorem

Theorem 1.17. *(Artin, Schmidt, Weil) Let $K = \mathbb{F}_q(C)$ with a curve of genus g. The function $\zeta_K(s)$ satisfies the following.*

(1) *The function is a rational fraction in q^{-s} ie. $\zeta_K(s) = Z(C, q^{-s})$ with*

$$Z(C,T) = \frac{L(C,T)}{(1-T)(1-qT)} = \frac{\prod_{j=1}^{2g}(1-\alpha_j T)}{(1-T)(1-qT)}.$$

(2) *It satisfies the functional equation*

$$\zeta_K(1-s) = q^{(2g-2)(\frac{1}{2}-s)}\zeta_K(s).$$

(3) *(Riemann's hypothesis) $|\alpha_j| = \sqrt{q}$.*

The name "Riemann hypothesis" is coined because $\zeta_K(s) = 0$ implies $1-\alpha_j p^{-s} = 0$ and hence $\Re s = \frac{1}{2}$. Therefore $\zeta_K(s)$ has a simple pole at $s = 1$ with residue

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{h_K}{p^g(1-1/p)\log p},$$

where $h_K = L(C,1) = \prod_1^{2g}(1-\alpha_j)$ is the *class number* $\#\operatorname{Pic}^0(\mathbb{F}_p)$, the number of $\mathbb{F}_p$ points on the Jacobian of C. Notice that $h_K = p^g + O(p^{g-1/2})$ thus $1 \ll \lim_{s\to 1}(s-1)\zeta_K(s) \ll 1$.

Perhaps one of the most useful tools when studying an algebraic variety X defined over $K = \mathbb{F}_p(C)$ is the possibility of *spreading* X into a variety $\mathcal{X}$ defined over $\mathbb{F}_p$ and fibered over the *complete* curve : $\pi : \mathcal{X} \to C$ such that the generic fiber is (isomorphic to) X. When the variety is defined over $\mathbb{Q}$, one can spread it out over $\mathbb{Z}$ but the curve $\mathbb{Z}$ is not complete and one should try to add fibres at infinity, this is one of the main purposes of Arakelov theory.

2. Lecture II : The zeta functions from algebraic geometry

2.1. **The L-function associated to a Galois representation.** A central object in arithmetic or arithmetic geometry is the *absolute Galois group*

$$G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}). \tag{2.1}$$

It is natural to study this huge profinite group via its representations. Let V be a (complex) vector space of dimension n and ρ a Galois representation (all representations are assumed to be continuous):

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C}) = \mathrm{GL}(V).$$

Remark 2.1. The following observations will be applied to the Frobenius elements and the inertia subgroup (whose definition is recalled in 1.13). If $f = hgh^{-1} \in G$ then the characteristic polynomials of $\rho(f)$ and $\rho(g)$ acting on V are equal. If H is a subgroup of G, denote

$$V^H := \{v \in V \mid \forall h \in H,\ \rho(h)(v) = v\},$$

the subspace of fixed vectors. If $f \in gH$ and g centralises H (i.e. for every $h \in H$, we have $gh = hg$) then g and f leave V^H stable and the characteristic polynomials of $\rho(f)$ and $\rho(g)$ acting on V^H are equal.

This allows the definition of Artin L-function associated to a represention ρ as :

$$L(\rho, s) = \prod_p \det\left(1 - \rho(\mathrm{Frob}_p)p^{-s} \mid V^{I_p}\right)^{-1}. \tag{2.2}$$

Denote $\chi = \chi_\rho = \mathrm{Tr}\,\rho$ the *character* of the representation; it is well known that the character determines the representation thus we may write

$$L(\chi_\rho, s) := L(\rho, s).$$

When the representation is one dimensional, it is essentially abelian (it factors via the abelian group $G/\mathrm{Ker}\,\rho$) and it is then known via Artin reciprocity law that the L-function is a generalised Dirichlet L-function (also called Hecke L-function) and satisfies analytic continuation plus functional equation. The general case is more difficult but can be attacked through Brauer's theorem.

We need to slightly extends definitions and introduce induction[1] of representations.

Definition 2.2. Let $G = \mathrm{Gal}(K/k)$ be the Galois group of an extension of number fields and let $\rho : G \to \mathrm{GL}(V)$ be a complex representation. The *Artin L-function* associated to ρ (or equivalently to its character χ_ρ) is

$$L(s, \rho) = L(s, \rho, K/k) = \prod_{\mathfrak{p}} \det\left(1 - \rho(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{p}}}\right)^{-1}, \tag{2.3}$$

(where the product runs over maximal ideals of $\mathcal{O}_k$).

The basic functoriality properties are

(1) $L(s, \rho_1 \oplus \rho_2) = L(s, \rho_1)L(s, \rho_2)$.

[1]The quickest way to define induction of finite dimensional representations of finite groups is via the tensor product of group algebras : if $H \subset G$ and $\tau : H \to \mathrm{GL}(V)$ is a representation defined over K, it corresponds to a $K[H]$-module structure on V; the representation $\mathrm{Ind}_H^G \tau$ is associated to the $K[G]$-module $W = V \otimes_{K[H]} K[G]$.

(2) If $H \subset G$ is a subgroup and $\tau : H \to \mathrm{GL}(V)$ a representation, by Galois theory $H = \mathrm{Gal}(K/K^H)$, and we have :

$$L(s, \tau, K/K^H) = L(s, \mathrm{Ind}_H^G \tau, K/k).$$

The following is a purely group theoretical statement.

Theorem 2.3. *(Brauer) Let G be a finite group and χ the character of a complex representation of G then there are subgroups H_i, one dimensional representations of H_i with characters ψ_i and integers $n_i \in \mathbb{Z}$ such that*

$$\chi = \sum_i n_i \,\mathrm{Ind}_{H_i}^G \psi_i. \tag{2.4}$$

Putting together this algebraic result and the known properties of abelian L-functions one obtains

Theorem 2.4. *Let $G = \mathrm{Gal}(K/k)$ be the Galois group of an extension of number fields and let $\rho : G \to \mathrm{GL}(V)$ be a complex representation. The Artin L-function associated to ρ extends to a meromorphic function on the complex plane and satisfies a functional equation. Let $n = \dim V$ and $c \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the complex conjugation, denote $n^+ = \dim V^+$ and $n^- = \dim V^-$, where V^+ (resp. V^-) is the eigen space corresponding to $+1$ (resp. -1) for $\rho(c)$.*

$$\Lambda(\rho, s) := N_\rho^{s/2} \Gamma_{\mathbb{R}}(s)^{n^+} \Gamma_{\mathbb{R}}(s+1)^{n^-} L(\rho, s).$$

Then

$$\Lambda(\rho, s) = w_\rho \Lambda(\check{\rho}, 1-s), \tag{2.5}$$

where $|w_\rho| = 1$ and $\check{\rho}$ is the contragredient representation[2].

Artin conjectured that $L(\rho, s)$ is entire except for a pole at $s = 1$ with order the multiplicity of the trivial representation inside ρ.

Notice that for topological reasons any continuous representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ factors through a finite group $G = \mathrm{Gal}(K/\mathbb{Q})$; there are very interesting Galois representations for which this is no longer true; the ℓ-adic representations are such examples. We'll study now the concrete example of the Tate module of an elliptic curve.

Recall (or learn) that the field of ℓ-adic numbers $\mathbb{Q}_\ell$ can be constructed as the completion of the field $\mathbb{Q}$ with respect to the absolute value $|x|_\ell := \ell^{-\,\mathrm{ord}_\ell\, x}$. The ring of integers $\mathbb{Z}_\ell = \{x \in \mathbb{Q}_\ell \mid |x|_\ell \leq 1\}$ is then the completion of $\mathbb{Z}$. Alternatively one may define $\mathbb{Z}_\ell$ as the inverse limit of the finite groups $\mathbb{Z}/\ell^n\mathbb{Z}$ (with obvious homomorphisms):

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}.$$

The field $\mathbb{Q}_\ell$ can then be viewed as the field of fractions of $\mathbb{Z}_\ell$.

To simplify the introduction we assume in the following *ad hoc* definition that the characteristic of the ground field is not 2 or 3.

Definition 2.5. An *elliptic curve* over a field K is a plane projective curve which can be defined in $\mathbb{P}^2$ by an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{2.6}$$

[2]If $\rho : G \to \mathrm{GL}(V)$ and V^* is the dual of V, then $\check{\rho} : G \to \mathrm{GL}(V^*)$ is given by $\langle \rho(g)(v), v^* \rangle = \langle v, \check{\rho}(g^{-1})(v^*) \rangle$; we have $\chi_{\check{\rho}}(g) = \chi_\rho(g^{-1}) = \bar{\chi}_\rho(g)$.

where a, b are in K and $4a^3 + 27b^2 \neq 0$ (setting $x = X/Z$ and $y = Y/Z$, one often writes the equation in the affine plane $Z \neq 0$ as $y^2 = x^3 + ax + b$). The group law is defined as follows:

(1) The origin is the point at infinity $(0 : 1 : 0)$.
(2) The inverse (or symmetrical) of $(X : Y : Z)$ is $(X : -Y, Z)$.
(3) To add two points P, Q draw the line joining them (if $P = Q$ this means draw the tangent at P to the curve) pick the third intersection point of the line with the curve, then $P + Q$ is the symmetrical point.

Remark 2.6. Changing (affine) coordinates $(x', y') = (\lambda^2 x, \lambda^3 y)$ will give a new equation $y'^2 = x'^3 + a'x' + b'$ with $(a', b') = (\lambda^4 a, \lambda^6 b)$ and $\Delta' = \lambda^{12}\Delta$. Thus if a, b are rational, after a rescaling, we may assume that a, b are integers and minimal in the sense that for all primes either p^4 does not divide a or p^6 does not divide b. We will often tacitly assume the equation is chosen to be minimal and will call the corresponding discriminant minimal. (Notice the definition should be amended to incorporate the primes 2 and 3).

Such an elliptic curve is a projective variety and an algebraic group (a group whose addition law can be expressed in terms of polynomials) and is the first example of abelian variety. Like for any algebraic group, there are natural maps such as translations, defined by $t_Q(P) = P + Q$, and multiplication by n, defined (for positive n) by $[n](P) = P + \cdots + P$.

Definition 2.7. Let X be an elliptic curve defined over K of characteristic 0 or p different from ℓ. The kernel of multiplication by ℓ^n is denoted

$$X[\ell^n] := \operatorname{Ker}\left\{[\ell^n] : X(\bar{K}) \to X(\bar{K})\right\},$$

and is isomorphic as a group to $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. The Tate module is the inverse limit

$$T_\ell(X) := \lim_{\leftarrow} X[\ell^n] \cong \left(\lim_{\leftarrow} \mathbb{Z}/\ell^n\mathbb{Z}\right)^2 \cong \mathbb{Z}_\ell^2.$$

The Galois group $G_K := \operatorname{Gal}(\bar{K}/K)$ acts on each $X[\ell^n]$ and hence on $T_\ell(X)$, providing a representation:

$$\rho_{X,\ell} : G_K \to \operatorname{GL}(T_\ell(X)) \cong \operatorname{GL}_2(\mathbb{Z}_\ell).$$

Let K be a number field. Though the representation is defined over $\mathbb{Q}_\ell$ it is known that the characteristic polynomial of $\operatorname{Frob}_\mathfrak{p}$ has rational integer coefficients which further do not depend on ℓ; in fact $\det \rho_{X,\ell}(\operatorname{Frob}_p) = p$ and $\operatorname{Tr} \rho_{X,\ell}(\operatorname{Frob}_p) = a_p = p + 1 - \#X(\mathbb{F}_p)$. This important fact makes the following definition possible, where we write V for the $\mathbb{Q}_\ell$ vector space $T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

Definition 2.8. The L-function associated to the set of representations $\rho_{X,\ell}$ is:

$$L(\rho_X, s) = \prod_{\mathfrak{p}} \det\left(1 - \rho_{X,\ell}(\operatorname{Frob}_\mathfrak{p}) N(\mathfrak{p})^{-s} \mid V^{I_\mathfrak{p}}\right)^{-1}. \tag{2.7}$$

Let us specialise a bit further to an elliptic curve X defined over $\mathbb{Q}$. The elliptic curve has good reduction modulo p whenever p does not divide the discriminant $\Delta = \Delta_X$ and then we define $a_p = a_p(X) = p + 1 - \#X(\mathbb{F}_p)$. When p divides the discriminant, the curve X modulo p has either a cusp (in which case $\dim V^I = 0$) we set $a_p = 0$ or a node with a pair of tangents (in which case $\dim V^I = 1$) which

can be defined over $\mathbb{F}_p$, in which case we set $a_p = 1$, or over a quadratic extension of $\mathbb{F}_p$, in which case we set $a_p = -1$. We have then the more explicit expression:

$$L(\rho_X, s) = \prod_{p \mid \Delta} (1 - a_p p^{-s})^{-1} \prod_{p \not\mid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}. \tag{2.8}$$

There is a finer invariant called the *conductor* of the elliptic curve (or the associated representation) which can be computed up to a factor $2^a 3^b$ by the following formula.

$$N_X = \prod_p p^{m_{X,p}},$$

where, if we define

$$n_{X,p} = \operatorname{codim}_V V^I = \begin{cases} 0 & \text{if } p \text{ does not divide } \Delta_X \\ 1 & \text{if } p \text{ divides } \Delta_X \text{ and } a_p = \pm 1 \\ 2 & \text{if } p \text{ divides } \Delta_X \text{ and } a_p = 0, \end{cases}$$

we have $m_{X,p} \geq n_{X,p}$ with equality except when p divides the discriminant, $a_p = 0$ and $p = 2$ or 3. Notice that the discriminant and conductor have the same prime factors but with different exponents.

2.2. **The zeta function of a scheme over Z.** Let R be a finitely generated ring, that is $R = \mathbb{Z}[t_1, \ldots, t_n]/I$ then for all *maximal ideal* $\mathfrak{m}$ the quotient $R/\mathfrak{m}$ is a finite field of cardinality say $N(\mathfrak{m})$; in view of the definition of the Dedekind zeta function, it is natural to introduce the *zeta function* of the ring R:

$$\zeta_R(s) = \prod_{\mathfrak{m}} \left(1 - N(\mathfrak{m})^{-s}\right)^{-1}, \tag{2.9}$$

where the product is taken over all maximal ideals of R. In view of the local definition of schemes, this definition immediately extends to schemes of finite presentation over $\mathbb{Z}$, replacing maximal ideals by *closed points*.

Definition 2.9. Let $\mathcal{X}$ be a scheme[3] of finite presentation over $\mathbb{Z}$ and denote $|\mathcal{X}|$ its set of closed points, then

$$\zeta(\mathcal{X}, s) := \prod_{x \in |\mathcal{X}|} \left(1 - N(x)^{-s}\right)^{-1}, \tag{2.10}$$

where $N(x)$ is the cardinality of the residual field at x.

If $\dim \mathcal{X} = d$, one can prove easily that the product and associated series converges for $\Re s > d$. Formally $\zeta(\mathcal{X}_1 \sqcup \mathcal{X}_2, s) = \zeta(\mathcal{X}_1, s)\zeta(\mathcal{X}_2, s)$. Thus decomposing the set of closed points according to their residual characteristic we get the Euler product decomposition where we denote $\mathcal{X}_p$ the fibre above p:

$$\zeta(\mathcal{X}, s) = \prod_p \zeta(\mathcal{X}_p, s). \tag{2.11}$$

Examples 2.10. If $\mathcal{X} = \operatorname{Spec}(\mathbb{Z})$ (resp. $\mathcal{X} = \operatorname{Spec}(\mathcal{O}_K)$), then $\zeta(\mathcal{X}, s)$ is just Riemann's zeta function (resp. Dedekind zeta function for the field K).

If $\mathcal{X} = \mathbb{A}^1_{\mathbb{Z}} = \operatorname{Spec}(\mathbb{Z}[T])$, we can identify closed points (maximal ideals) with residual characteristic p with monic irreducible polynomials in $\mathbb{F}_p[T]$, whose set

[3] A scheme can be taken as a patching of affine schemes $\operatorname{Spec}(R_i)$ and for each R_i we have $\zeta_{R_i}(s) = \zeta(\operatorname{Spec}(R_i), s)$.

we denote Irr_p; we also denote M_p the set of monic polynomials. The following computation is then straightforward :

$$\begin{aligned}\zeta(\mathbb{A}^1_{\mathbb{Z}}, s) &= \prod_p \prod_{Q\in Irr_p} (1-p^{-s\deg Q})^{-1}\\ &= \prod_p \prod_{Q\in Irr_p} \sum_{m=0}^{\infty} p^{-sm\deg Q}\\ &= \prod_p \sum_{P\in M_p} p^{-s\deg P}\\ &= \prod_p \sum_{d=0}^{\infty} p^{d-ds}\\ &= \prod_p (1-p^{1-s})^{-1}\\ &= \zeta(s-1).\end{aligned}$$

Decomposing the closed points of $\mathbb{P}^1_{\mathbb{Z}}$ as $\mathbb{A}^1_{\mathbb{Z}} \sqcup \mathbb{A}^0_{\mathbb{Z}}$ we obtain

$$\zeta(\mathbb{P}^1_{\mathbb{Z}}, s) = \zeta(s)\zeta(s-1).$$

It is clear that we should start by studying the zeta function of a variety defined over $\mathbb{F}_p$.

2.3. **The Weil zeta function of a variety over a finite field.** Let X be a smooth projective variety defined over $\mathbb{F}_p$; for a closed point x we denote $d_x = [\mathbb{F}_p(x) : \mathbb{F}_p]$. We compute

$$\log \zeta_X(s) = \sum_{x,m} \frac{N(x)^{-ms}}{m} = \sum_{x,m} \frac{p^{-d_x ms}}{m} = \sum_{n\geq 1} p^{-ns} \left(\sum_{md_x=n} \frac{1}{m} \right) \overset{\text{(say)}}{=} \sum_{n\geq 1} u_n p^{-ns}.$$

We complete the computation by observing that, for a closed point $x \in |X|$ the fact of having residual degree d_x dividing n is equivalent to corresponding to a (conjugacy class of) point in $X(\mathbb{F}_{p^n})$, thus :

$$u_n = \sum_{x\in|X|,\, d_x=\frac{n}{m}} \frac{1}{m} = \frac{1}{n} \sum_{x\in|X|,\, d_x|n} d_x = \frac{1}{n} \#X(\mathbb{F}_{p^n}).$$

We have thus shown the following.

Proposition 2.11. *Let X be a variety over $\mathbb{F}_p$, then we have the formula*

$$\zeta(X, s) = Z(X, p^{-s}), \tag{2.12}$$

where

$$Z(X, T) = \exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{p^m})}{m} T^m \right). \tag{2.13}$$

The latter formal series is known as *Weil's zeta function* attached to $X/\mathbb{F}_p$; it has been much studied and is the subject of the famous Weil conjectures (solved by Grothendieck and Deligne).

Example 2.12. Let us compute the (easy) example of $X = \mathbb{P}^n$. In this case $\#X(\mathbb{F}_{p^m}) = \frac{p^{m(n+1)}-1}{p^m-1} = p^{mn} + p^{m(n-1)} + \cdots + p^m + 1$, thus

$$\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{p^m})}{m} T^m = \sum_{j=0}^{n} \sum_{m=1}^{\infty} \frac{p^{mj}}{m} T^m = -\sum_{j=0}^{n} \log(1-p^j T),$$

thus:

$$Z(\mathbb{P}^n, T) = \frac{1}{(1-T)(1-pT)\dots(1-p^{n-1}T)(1-p^nT)}. \tag{2.14}$$

Notice that a simple verification will reveal that :

$$Z(\mathbb{P}^n, T) = (-1)^{n+1} p^{\frac{n(n+1)}{2}} T^{n+1} Z\left(\mathbb{P}^n, \frac{1}{p^n T}\right).$$

The pattern is actually quite general :

Theorem 2.13. *(Weil's conjectures) Let X be a smooth projective variety over $\mathbb{F}_p$ of dimension n.*

1. *(Rationality) There are polynomial $P_j(X,T) = \prod_{i=1}^{b_j}(1-\alpha_{j,i}T) \in \mathbb{Z}[T]$ for $j = 0, \dots, 2n$ such that*

$$Z(X,T) = \frac{P_1(X,T)\dots P_{2n-1}(X,T)}{P_0(X,T)\dots P_{2n}(X,T)} = \prod_{j=0}^{2n} P_j(X,T)^{(-1)^{j+1}}. \tag{2.15}$$

   Further $b_0 = b_{2n} = 1$ and $P_0(X,T) = 1-T$ and $P_{2n}(X,T) = 1-p^nT$.
2. *(Functional equation) Let $\chi(X) = \sum_{j=0}^{2n}(-1)^j b_j$ be the Euler-Poincaré characteristic then*

$$Z(X,T) = \pm p^{\frac{n\chi(X)}{2}} T^{\chi(X)} Z\left(X, \frac{1}{p^n T}\right). \tag{2.16}$$

3. *(Riemann hypothesis) The algebraic integers $\alpha_{j,i}$ satisfy $|\alpha_{j,i}| = p^{j/2}$.*
4. *The numbers $b_j = b_j(X)$ satisfy continuity in smooth families and in particular if X is the reduction modulo a prime ideal of a variety Y defined over a number field K, then the $b_j(X)$ are equal to the Betti numbers of the complex variety $Y \otimes_K \mathbb{C}$.*

Example. Let X be an elliptic curve over $\mathbb{F}_p$. We have $b_0 = b_2 = 1$, $b_1 = 2$ and $P_0(T) = 1-T$, $P_2(T) = 1-pT$ and $P_1(T) = 1 - aT + pT^2$. There is an algebraic integer α with $\alpha\bar{\alpha} = p$ such that

$$Z(X,T) = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)}.$$

This is equivalent to Hasse's theorem which says that

$$\#X(\mathbb{F}_{p^m}) = p + 1 - \alpha^m - \bar{\alpha}^m.$$

The proof of this theorem is way beyond the scope of these notes. Suffices to quote the existence of a cohomology theory[4], which we'll denote $H^j(X)$ which is functorial, hence the Frobenius "$x \mapsto x^p$" induced a map $f = f_j : H^j(X) \to H^j(X)$, and is such that the following Lefschetz trace formula holds:

[4]For the expert we are writing $H^j(X) = H^j_{\text{ét}}(X \times \bar{\mathbb{F}}_p, \mathbb{Q}_\ell)$, the ℓ-adic étale cohomology.

(2.17)

$$\#X(\mathbb{F}_{p^m}) = \#\{x \text{ fixed by Frobenius power } m\} = \sum_{j=0}^{2n}(-1)^j \operatorname{Tr}(f^m \mid H^j(X)).$$

A formal computation, based on the elementary formula

$$\exp\left(\sum_{m=1}^{\infty} \operatorname{Tr}(f^m \mid V)\frac{T^m}{m}\right) = \det(1 - fT \mid V)^{-1},$$

then gives

$$Z(X,T) = \prod_{j=0}^{2n} \det\left(1 - fT \mid H^j(X)\right)^{(-1)^{j+1}}, \tag{2.18}$$

and we just have to define $P_j(X,T) = \det(1 - fT \mid H^j(X))$ to obtain the first part. The functional equation follows formally from the Poincaré duality: a canonical non degenerate pairing

$$H^j(X) \times H^{2n-j}(X) \longrightarrow H^{2n}(X) = \mathbb{Q}_\ell, \tag{2.19}$$

such that $\langle f_j x, f_{2n-j} y\rangle = p^n \langle x, y\rangle$. Indeed an elementary argument shows that the existence of such a pairing implies

$$\det(1 - f_j T \mid H^j(X)) = (-1)^{B_j} \frac{p^{nB_j} T^{B_j}}{\det(f_j \mid H^j(X))} \det\left(1 - \frac{f_{2n-j}}{p^n T} \mid H^{2n-j}(X)\right).$$

The Riemann Hypothesis lies deeper; again the name comes from the easy conclusion that it implies that zeroes (resp. poles) of $\zeta_X(s)$ lies on vertical lines $\Re s = m + \frac{1}{2}$, with $0 \le m \le \dim X - 1$ (resp. on vertical lines $\Re s = m$, with $0 \le m \le \dim X$).

2.4. **The Hasse-Weil L-functions.** Let X be again a smooth projective variety of dimension n defined over $\mathbb{Q}$. When $M = H^i(X)$ one uses the Hodge decomposition:

$$H^i(X(\mathbb{C}), \mathbb{C}) = \oplus_{p+q=i} H^{p,q},$$

together with the "Frobenius at infinity", i.e. the map F_∞ induced by the complex conjugation on $X(\mathbb{C})$ to define numbers:

$$h^{p,q} = \dim_{\mathbb{C}} H^{p,q} \qquad \text{and} \qquad h^{p,\pm} = \dim_{\mathbb{C}} H^{p,\pm} \tag{2.20}$$

where $H^{p,\pm} := \{c \in H^{p,p} \mid F_\infty(c) = \pm(-1)^p c\}$. We can finally define the Gamma factor as

(2.21)

$$L_\infty(M,s) := \begin{cases} \displaystyle\prod_{p<q, p+q=i} \Gamma_{\mathbb{C}}(s-p)^{h^{p,q}} & \text{if } i \text{ is odd} \\ \displaystyle\prod_{p<q, p+q=i} \Gamma_{\mathbb{C}}(s-p)^{h^{p,q}} \Gamma_{\mathbb{R}}(s - \frac{i}{2})^{h^{\frac{i}{2},+}} \Gamma_{\mathbb{R}}(s+1-\frac{i}{2})^{h^{\frac{i}{2},-}} & \text{if } i \text{ is even.} \end{cases}$$

When X is smooth modulo p, it is clear (or should be ...) what the correct Euler factor for the L and zeta function of X must be. For a model $\mathcal{X}$ of X over $\mathbb{Z}$

we have $\zeta_{\mathcal{X}}(s) = \prod_p \zeta_{\mathcal{X}_p}(s)$; to ease notation we write X_p for the reduction modulo p; we have $\zeta_{\mathcal{X}_p}(s) = Z(X_p, p^{-s})$ and from the Weil conjecture we know that

$$Z(X_p, p^{-s}) = \prod_{j=0}^{2n} \det(1 - \mathrm{Frob}_p\, p^{-s} \mid H^j(X_p))^{(-1)^{j+1}}$$
$$= \prod_{j=0}^{2n} \det(1 - \mathrm{Frob}_p\, p^{-s} \mid H^j(X))^{(-1)^{j+1}},$$

the last equality being a property of continuity (or smooth base change) of the cohomology.

We thus naturally define

$$\zeta_p(X, s) := \zeta(X_p, p^{-s}) \qquad \text{and} \qquad L_p(H^j(X), s) := \det(1 - \mathrm{Frob}_p\, p^{-s} \mid H^j(X))^{-1}.$$

The cohomological interpretation is needed to provide the correct factor at the "bad primes", namely

$$L_p(H^j(X), s) := \det(1 - \mathrm{Frob}_p\, p^{-s} \mid H^j(X)^{I_p})^{-1}.$$

Definition 2.14. Let X be a smooth projective variety of dimension n defined over $\mathbb{Q}$; the Hasse-Weil zeta and L-functions are defined by:

$$L(H^j(X), s) := \prod_p L_p(H^j(X), s) := \prod_p \det(1 - \mathrm{Frob}_p\, p^{-s} \mid H^j(X)^{I_p})^{-1}, \tag{2.22}$$

and

$$\zeta(X, s) = \prod_{j=0}^{2n} L(H^j(X), s)^{(-1)^j}. \tag{2.23}$$

One may now state the following conjecture (known in many interesting cases but widely open).

Conjecture 2.15. *Let X be a smooth projective variety defined over $\mathbb{Q}$. The function $L(H^j(X), s) = \prod_p L_p(H^j(X), s)$ extends analytically to the complex plane except, when j is even, for a pole at $s = 1 + j/2$. Further there exists an integer N, the conductor of the Galois representation on $H^j(X)$, such that if we define:*

$$\Lambda(H^j(X), s) := N^{s/2} L_\infty(H^j(X), s) L(H^j(X), s), \tag{2.24}$$

then we have the functional equation

$$\Lambda(H^j(X), s) = \pm \Lambda(H^j(X), j + 1 - s) \tag{2.25}$$

For example, if X is an elliptic curve defined over $\mathbb{Q}$, we write $L(X, s)$ instead of $L(H^1(X), s)$; then we have

$$\Lambda(X, s) = N_X^{s/2} \Gamma_{\mathbb{C}}(s) L(X, s) \qquad \text{and} \qquad \Lambda(X, s) = \pm \Lambda(X, 2 - s),$$

and the conjecture is in this case a theorem thanks to the work of Wiles et al. Notice that the Hasse-Weil zeta function can be written

$$\zeta_X(s) = \frac{\zeta(s)\zeta(s-1)}{L(X, s)}.$$

Remark 2.16. All this can be formulated, mutadis mutandis, over function fields, replacing the number field K by $\mathbb{F}_q(C)$ and prime ideals by places of the function field. For example, if X is a (smooth projective) variety over $K = \mathbb{F}_q(C)$, the L-functions associated can be defined as

$$L(H^j(X), s) = \prod_v \det(1 - \mathrm{Frob}_v\, q_v^{-s} \mid H^j(X)^{I_v})^{-1},$$

where $q_v = q^{\deg v}$. The theory is far more advanced over function fields than over number fields; for example analytic continuation and functional equation are known, in fact Grothendieck theory shows that the L-function is actually a rational fraction in q^{-s} and the functional equation reads $L(H^j(X), j+1-s) = \pm q^{d_j(s-\frac{j+1}{2})} L(H^j(X), s)$, where d_j is an integer which can be interpreted as the degree of a conductor. Finally the (analogue of) Riemann hypothesis is a theorem in the function field case : the zeroes of $L(H^j(X), s)$ all have real part equal to $\frac{j+1}{2}$; via Deligne-Grothendieck this is equivalent to the statement that the numerator has the form $\prod_j (1 - \beta_j q^{-s})$ with $|\beta_j| = q^{\frac{j+1}{2}}$.

2.5. The L-function associated to a modular form.

Definition 2.17. Poincaré's half-plane $\mathcal{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$; its "compactification" $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

The group $\mathrm{GL}_2^+(\mathbb{R})$ of matrices 2×2 with positive determinant or $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$ via $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \mapsto (az+b)/(cz+d)$. The groups $\mathrm{GL}_2^+(\mathbb{Q})$ and $\mathrm{SL}(2,\mathbb{Z})$ act on $\mathcal{H}^*$. The latter action is discrete thus one may form the quotients $Y := \mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}$ and $X := \mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}^*$, which are Riemann surfaces. In fact, $Y \cong \mathbb{A}^1(\mathbb{C})$ and $X \cong \mathbb{P}^1(\mathbb{C})$.

Among subgroups of finite index in $\mathrm{SL}(2,\mathbb{Z})$ the most important are

Definition 2.18. A subgroup $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ is a *congruence subgroup* if it contains $\Gamma(N)$ for some N, where

$$\Gamma(N) := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid A \equiv I \mod N \right\}.$$

We denote $Y(N) := \Gamma(N)\backslash\mathcal{H}$ and $X(N) := \Gamma(N)\backslash\mathcal{H}^*$.

Apart from $\Gamma(N)$ itself, other examples include :

(1) The congruence subgroup

$$\Gamma_1(N) := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

We denote $Y_1(N) := \Gamma_1(N)\backslash\mathcal{H}$ and $X_1(N) := \Gamma_1(N)\backslash\mathcal{H}^*$;

(2) The congruence subgroup

$$\Gamma_0(N) := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid c \equiv 0 \mod N \right\}.$$

We denote $Y_0(N) := \Gamma_0(N)\backslash\mathcal{H}$ et $X_0(N) := \Gamma_0(N)\backslash\mathcal{H}^*$.

The subgroup $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ and $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$, via the map $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N$.

One knows $Y_0(N)$ (resp. $Y_1(N)$, $Y(N)$) are algebraic affine curves whereas $X_0(N)$ (resp. $X_1(N)$, $X(N)$) are projective algebraic curves. Further, $X_0(N)$ and $X_1(N)$ are defined over $\mathbb{Q}$, whereas $X(N)$ is defined over $\mathbb{Q}(\exp(2\pi i/N))$.

Definition 2.19. Let Γ be a congruence subgroup. A *modular form* of weight k with respect to Γ, is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that :

(1) For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $z \in \mathcal{H}$, we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z); \tag{2.26}$$

(2) The function f is holomorphic on $\mathcal{H}^*$, i.e. for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$, the limit of $f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-k}$, when $\Im z$ goes to infinity, exists. If this limit is zero f is said to be *parabolic*.

Write $M_k(\Gamma)$ for the space of modular forms for Γ with weight k and $S_k(\Gamma)$ for the subspace of parabolic forms.

Any congruence subgroup Γ contains some $T_h := \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$, with h non zero minimal : for example, $T_1 \in \Gamma_1(N)$. Hence if $f \in M_k(\Gamma)$ then $f(z+h) = f(z)$, so we can write the Fourier expansion :

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q_h^n\,, \qquad \text{where} \qquad q_h := \exp\left(\frac{2\pi i z}{h}\right). \tag{2.27}$$

If f is holomorphic on $\mathcal{H}^*$ then $a_n = 0$ for $n < 0$, while vanishing at ∞ reads $a_n = 0$ for $n \leq 0$ (nota bene : the full condition for f to be a modular form is holomorphy at all points in $\mathbb{P}^1(\mathbb{Q}) = \mathcal{H}^* \setminus \mathcal{H}$).

Remark 2.20. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^+$, then $\delta := ad - bc > 0$ and, if we put $\gamma' = \delta^{-1/2}\gamma$, we'll have $\gamma' \in \mathrm{SL}_2(\mathbb{R})$ and $\gamma' \cdot z = \gamma \cdot z$. If f is modular with weight k for γ', we'll have

$$f\left(\frac{az+b}{cz+d}\right) = \delta^{k/2}(cz+d)^k f(z). \tag{2.28}$$

Definition 2.21. Let $f \in S_k(\Gamma_0(N))$ and $f(z) = \sum_{n=1}^{\infty} a_n \exp(2\pi i n z) = \sum_{n=1}^{\infty} a_n q^n$ its Fourier expansion. The *Dirichlet series* associated to f is :

$$L(s,f) := \sum_{n=1}^{\infty} a_n n^{-s}. \tag{2.29}$$

Notice the relation :

$$\Gamma_{\mathbb{C}}(s)L(f,s) = (2\pi)^{-s}\Gamma(s)L(f,s) = \int_0^{\infty} f(it)t^{s-1}dt. \tag{2.30}$$

Definition 2.22. Let $f = \sum_n a_n(f)q^n \in M_k(\Gamma_0(N))$. The *Hecke operators* are defined as follows.

(1) if p does not divide N, the operator $f \mapsto T_p f$ is defined by :

$$a_n(T_p f) := a_{np}(f) + p^{k-1} a_{n/p}(f),$$

where, by convention, $a_{n/p} = 0$ if p does not divide n.

(2) If p divides N, the operator $f \mapsto U_p f$ is defined by :

$$a_n(U_p f) := a_{np}(f).$$

Theorem 2.23. (Hecke, see [DiSh08]) *The Hecke operators commute. If $f = \sum_n a_n(f) q^n \in S_k(\Gamma_0(N))$ is an eigenvector for each operator, i.e $T_p f = \lambda_p f$, $U_p f = \lambda_p f$, then $a_p(f) = \lambda_p a_1(f)$, if further f is normalised by the condition $a_1(f) = 1$, the L-function $L(s, f)$ factorises into an Euler product of the shape :*

(2.31)

$$L(s,f) = \sum_{n=1}^{\infty} a_n(f) n^{-s} = \prod_{p \mid N} (1 - a_p(f) p^{-s})^{-1} \prod_{p \not| N} (1 - a_p(f) p^{-s} + p^{k-1-2s})^{-1}.$$

Proof. (partial sketch) The commutation follows from a direct computation. We do now computations for p not dividing N, leaving the (easier) computation for p dividing N to the reader. Suppose that $T_p(f) = \lambda_p f$ then we have $\lambda_p a_n(f) = a_{np}(f) + p^{k-1} a_{n/p}(f)$ hence $a_p(f) = \lambda_p(f) a_1(f)$ and, if $a_1(f) = 1$ (which we now suppose) then $a_p(f) = \lambda_p(f)$. When p is coprime with n we infer $a_{np} = a_n a_p$ and more generally $a_{np^r} = a_n a_{p^r}$ from which an Euler product decomposition follows. Finally the recurrence relations $\lambda_p a_{p^r} = a_p a_{p^r} = a_{p^{r+1}} + p^{k-1} a_{p^{r-1}}$ are equivalent to the formula $\sum_r a_{p^r} T^r = (1 - a_p T + p^{k-1} T^2)^{-1}$.

□

When $k = 2$, this L-function looks like the L-function associated to an elliptic curve. Let us check that, under a further condition, $L(f, s)$ satisfies the functional equation expected for an elliptic curve. Notice the matrix $W_N := \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$ (which does not belong to $\mathrm{SL}(2, \mathbb{Z})$ but to $\mathrm{GL}_2^+(\mathbb{Q})$) normalises the subgroup $\Gamma_0(N)$, since

$$W_N \begin{pmatrix} a & b \\ c & d \end{pmatrix} W_N^{-1} = \begin{pmatrix} d & -c/N \\ -bN & a \end{pmatrix}.$$

Therefore W_N acts on $M_k(\Gamma_0(N))$ (resp. $S_k(\Gamma_0(N))$), and since $W_N^2 = -NId$, it acts as an involution and the spaces $M_2(\Gamma_0(N))$ (resp. $S_2(\Gamma_0(N))$) decompose into the sum of two eigenspaces such that :

$$f\left(-\frac{1}{Nz}\right) = f(W_N \cdot z) = \pm N^{k/2} z^k f(z) \tag{2.32}$$

Theorem 2.24. (Hecke) *Let $\epsilon = \pm 1$ and $f(\tau) = \sum_{n \geq 1} a_n \exp(2\pi i n \tau)$ a parabolic modular form for $\Gamma_0(N)$ of weight k such that*

$$f\left(-\frac{1}{N\tau}\right) = \epsilon N^{k/2} \tau^k f(\tau). \tag{2.33}$$

Put $\Lambda(s, f) := N^{s/2} (2\pi)^{-s} \Gamma(s) L(s, f)$, where $L(s, f) := \sum_{n=1}^{\infty} a_n n^{-s}$. The function $\Lambda(s, f)$ has analytic continuation to $\mathbb{C}$ and satisfies a functional equation

$$\Lambda(s, f) = i^k \epsilon \Lambda(k - s, f). \tag{2.34}$$

Further, $\Lambda(s, f)$ is bounded in every vertical strip.

Proof. Notice that for $\tau = it$ (with $t \in \mathbb{R}_+$) the equation (2.33) reads

$$f\left(\frac{i}{Nt}\right) = (i)^k \epsilon N^{k/2} t^k f(it).$$

The analogy with equation (1.8) used to prove the functional equation of the Riemann zeta function is now evident. We may compute, invoking (2.30) and using a change of variable $t \mapsto 1/Nt$:

$$\begin{aligned}
\Lambda(s,f) &= N^{s/2} \int_0^\infty f(it) t^{s-1} dt \\
&= N^{s/2} \int_0^{\frac{1}{\sqrt{N}}} f(it) t^{s-1} dt + N^{s/2} \int_{\frac{1}{\sqrt{N}}}^\infty f(it) t^{s-1} dt \\
&= N^{-s/2} \int_{\frac{1}{\sqrt{N}}}^\infty f(i/Nt) t^{-s-1} dt + N^{s/2} \int_{\frac{1}{\sqrt{N}}}^\infty f(it) t^{s-1} dt \\
&= i^k \epsilon N^{\frac{1}{2}(k-s)} \int_{\frac{1}{\sqrt{N}}}^\infty f(it) t^{k-1-s} dt + N^{s/2} \int_{\frac{1}{\sqrt{N}}}^\infty f(it) t^{s-1} dt \\
&= \int_{\frac{1}{\sqrt{N}}}^\infty f(it) \left[i^k \epsilon N^{\frac{1}{2}(k-s)} t^{k-s} dt + N^{s/2} t^s \right] \frac{dt}{t}.
\end{aligned} \tag{2.35}$$

The latter expression defines an entire function (one needs the elementary fact that $|a_n| = O(n^c)$, and hence $|f(it)| = O(\exp(-2\pi t))$ as t goes to infinity). The $(i^k\epsilon)$-symmetry when s is replaced by $k-s$ is now obvious, as the property of being bounded in any vertical strip. □

We close this chapter stressing the marvelous result of Wiles which identifies L-functions associated to Galois representations (the Tate module), Hasse-Weil L-function of elliptic curves over $\mathbb{Q}$ and L-functions of weight two modular forms with rational coefficients. More precisely, if X is an elliptic curve defined over $\mathbb{Q}$, with conductor $N = N_X$ and $L(X,s) = \sum_{n\geq 1} a_n n^{-s}$ is its Hasse-Weil function as defined in (2.8), then Wiles theorem asserts that the function $f(z) := \sum_{n\geq 1} a_n \exp(2\pi i n z)$ is a modular form with respect to the group $\Gamma_0(N)$; in fact this result gives a correspondence between (isogeny classses of) elliptic curves of conductor N defined over $\mathbb{Q}$ and parabolic modular forms with respect to $\Gamma_0(N)$ which are eigen forms for all Hecke operators, have rational Fourier coefficients and do not come from modular forms with respect to some $\Gamma_0(M)$ with M strictly dividing N. This actually can be viewed as one instance of the very general program of Langlands, part of which says that Hasse-Weil functions should all be "automorphic".

3. Lecture III : Some techniques and estimates from complex analysis

3.1. **Classical lemmas.** We begin with the Stirling formula for the Gamma function.

The Gamma function. It is first defined for $\Re s > 0$ by the integral

$$\Gamma(s) := \int_0^\infty e^{-t} t^s \frac{dt}{t}. \tag{3.1}$$

Integration par part yields the formula $s\Gamma(s) = \Gamma(s+1)$ and hence analytic continuation to $\mathbb{C}$ with simple poles at non positive integers $0, -1, -2, -3, \ldots$.

Lemma 3.1. *(Stirling formula) When s stays away from negative reals, we have:*

$$\log \Gamma(s) = \left(s - \frac{1}{2}\right) \log s - s + \frac{1}{2} \log(2\pi) + O\left(\frac{1}{|s|}\right).$$

The following corollary of Stirling's formula will be useful: away from poles and uniformly in any vertical strip we have, as $|\tau|$ tends to infinity:

$$|\Gamma(\sigma + i\tau)| \sim c(\sigma) \exp(-\frac{\pi}{2}|\tau|)|\tau|^{\sigma - \frac{1}{2}}. \tag{3.2}$$

Dirichlet series.

Lemma 3.2. *Suppose that the series $L(s) = \sum_{n=1}^\infty a_n n^{-s}$ converges for $s = s_0$, then it converges uniformly in domains of the shape $\{s \in \mathbb{C} \mid \Re s \geq c > \Re s_0\}$ or $\{s \in \mathbb{C} \mid |s - s_0| \leq C\Re(s - s_0)\}$. Consequently any Dirichlet series $L(s)$ has an abscissa of convergence σ_c such it diverges for $\Re s < \sigma_c$ and converges on the half-plane $\Re s > \sigma_c$ to a holomorphic function.*

Lemma 3.3. *(Landau) Suppose $a_n \geq 0$ and that the series $L(s) = \sum_{n=1}^\infty a_n n^{-s}$ converges for $\Re s > \sigma_0$ and the function has analytic continuation to a neighbourhood of σ_0, then the abscissa of convergence is strictly smaller than σ_0.*

Application. We can now give the promised proof of the non vanishing $L(\chi, 1) \neq 0$ (theorem 1.10) which is used in the proof of the arithmetic progression theorem (theorem 1.9). In fact the key is Landau's lemma plus the observation that, if $K = \mathbb{Q}(\exp(2\pi i/N))$ then we have the factorisation

$$\zeta_K(s) = \zeta(s) \prod_{\chi \neq \chi_0} L(\chi, s), \tag{3.3}$$

where the product is over primitive non trivial characters modulo N. Now if some $L(\chi, 1) = 0$, the product on the right is an entire function, thus, by Landau's lemma, the Dirichlet series defining $\zeta_K(s)$ would be convergent for all s, but this is clearly false.

Holomorphic functions

Lemma 3.4. *(Cauchy's formula) Let $f(s)$ be holomorphic inside the circle $\mathcal{C}$ of center z and radius R, then*

$$\left|\frac{f^{(n)}(z)}{n!}\right| = \left|\frac{1}{2\pi i} \int_{\mathcal{C}} \frac{f(s)}{(s-z)^{n+1}} dz\right| \leq \max_{|s-z|=R} |f(s)|/R^n.$$

This can be viewed as stating that a bound valid for f remains essentially valid for its derivatives.

Lemma 3.5. *(Phragmén-Lindelöf) Let $f(s)$ be holomorphic in a strip $a \leq \Re(s) \leq b$ with reasonable growth (i.e. for example $|f(s)| \ll \exp(|s|^c)$).*

1. *Suppose $\sup_{t\in\mathbb{R}} (|f(a+it)|, |f(b+it)|) = M$ then $|f(s)| \leq M$ in the whole strip.*
2. *Suppose $|f(a+it)| \leq M_a(1+|t|)^\alpha$ and $|f(b+it)| \leq M_b(1+|t|)^\beta$ then $|f(\sigma+it)| \leq M_\sigma(1+|t|)^{v(\sigma)}$, where $M_\sigma = M_a^{u(\sigma)} M_b^{1-u(\sigma)}$, $v(\sigma) = \alpha u(\sigma) + \beta(1-u(\sigma))$ and u is the affine function with values $u(a) = 1$ and $u(b) = 0$.*

Lemma 3.6. *(Borel-Carathéodory) Let $f(s)$ be holomorphic for $|s| \leq R$; assume $\max_{|s|=R} \Re f(s) = A$ then, for $0 < r < R$ we have*

$$\max_{|s|\leq r} |f(s)| \leq \frac{2Ar}{R-r} + \frac{R+r}{R-r}|f(0)|.$$

Lemma 3.7. *(Hadamard's three circles lemma) Let $f(s)$ be holomorphic in an annulus $R_1 \leq |s| \leq R_2$ then the function $M(r) := \sup_{|s|=r} |f(s)|$ is log convex in $\log r$, that is*

$$\log M(r) \leq \frac{\log(R_2/r)}{\log(R_2/R_1)} \log M(R_1) + \frac{\log(r/R_1)}{\log(R_2/R_1)} \log M(R_2).$$

Lemma 3.8. *(Jensen's formula) Let f be holomorphic in a disk $D(0,R)$ with no zero at $s = 0$ or on the circle $|s| = R$, denote $z_1, \ldots, z_n$ its zeroes and $n(r) := \#\{|z| < r \mid f(z) = 0\}$, then :*

$$\frac{1}{2\pi} \int_0^{2\pi} \log \left| f(Re^{i\theta} \right| d\theta - \log |f(0| = \log \frac{R^n}{|z_1| \ldots |z_n|} = \int_0^R n(r) \frac{dr}{r}.$$

We recall the notation $\int_{(c)} f(s)ds = i \int_{-\infty}^{+\infty} f(c+it)dt$.

Lemma 3.9. *(Perron's integral)*

$$\frac{1}{2\pi i} \int_{(c)} \frac{y^s ds}{s(s+1)\ldots(s+h)} = \begin{cases} \frac{1}{h!}\left(1 - \frac{1}{y}\right)^h & \text{if } y \geq 1 \\ 0 & \text{else.} \end{cases} \tag{3.4}$$

This follows by moving the line of integration to the left (resp. to the right) if $y \geq 1$ (resp. if $y < 1$) picking up residues at $s = -k$ equal to $\frac{1}{h!}\binom{h}{k}(-1)^k x^{-k}$ (resp. no residue).

Proposition 3.10. *(Perron's Formula) Let $L(s) = \sum_{n=1}^\infty a_n n^{-s}$ be absolutely convergent for $\Re s = c$ then*

$$\frac{1}{2\pi i} \int_{(c)} \frac{L(s)x^{s+h} ds}{s(s+1)\ldots(s+h)} = \frac{1}{h!} \sum_{n\leq x} a_n (x-n)^h. \tag{3.5}$$

(For $h = 0$ one has to slightly modify the formulas so that when $y = 1$ (or $x = n$) one gets a contribution $1/2$ instead of 1).

3.2. **Tauberian theorems.** We give two examples of so-called tauberian theorems, each one leading to a proof of the prime number theorem. It is relatively easy to show that if $\sum_{n\leq x} a_n = \lambda x + o(x)$ then $\lim_{\sigma\to 1}(\sigma-1)\sum_n a_n n^{-\sigma} = \lambda$, this type of summation results are called *abelian theorems*; the converse is not always true and typically theorems asserting (under additional hypothesis) the reciprocal are called *tauberian theorems.*

Theorem 3.11. *(Ikehara) Let $Z(s) = \sum_{n\geq 1} a_n n^{-s}$ be a Dirichlet series convergent for $\Re s > 1$ with $a_n \geq 0$; suppose that $Z(s) - \frac{\lambda}{s-1}$ extends to a holomorphic function on $\Re s \geq 1$ then we have:*

$$\sum_{n\leq x} a_n = \lambda x + o(x). \tag{3.6}$$

Notice that the theorem applied to $Z(s) = -\zeta'(s)/\zeta(s)$ gives

$$\psi(x) := \sum_{n\leq x} \Lambda(n) \sim x,$$

and thus immediately implies the prime number theorem, once we have Hadamard – de la Vallée Poussin result (theorem 1.6).

The next result, due to Newmann, has a similar but distinct flavour.

Theorem 3.12. *Let $h(t)$ be a bounded locally integrable function then the integral*

$$F(s) = \int_0^{+\infty} h(u)e^{-su}du$$

is convergent and holomorphic on the half-plane $\Re(s) > 0$. Suppose this function has analytic continuation to an open neighbourhood of $\Re(s) \geq 0$, then the integral for $s = 0$ converges and

$$F(0) = \int_0^{+\infty} h(u)du.$$

Denote $\theta(t) := \sum_{p\leq x} \log p$. We may apply the latter theorem to the function

$$\begin{aligned} F(s) &= \int_1^{+\infty} \frac{\theta(t)-t}{t^{s+2}}dt \\ &= \int_0^{+\infty} \frac{\theta(e^u)-e^u}{e^{u(s+2)}}e^u du = \int_0^{+\infty} \left[\theta(e^u)e^{-u} - 1\right] e^{-us}du. \end{aligned}$$

Indeed the function $h(u) := \theta(e^u)e^{-u} - 1$ is piecewise continuous. Checking holomorphic continuation we'll conclude that the integral

$$F(0) = \int_0^{+\infty} (\theta(e^u)e^{-u} - 1)du = \int_1^{+\infty} \frac{\theta(t)-t}{t^2}dt$$

is convergent. It is then elementary to conclude $\theta(x) \sim x$ which is a form of the prime number theorem.

To check analytic continuation, apply the following transformations to $F(s)$ (for $\Re(s) > 0$) :

$$\begin{aligned} F(s) &= \int_1^{+\infty} \frac{\theta(t) - t}{t^{s+2}} dt \\ &= \sum_{n=1}^{\infty} \int_n^{n+1} \theta(t) t^{-s-2} dt - \int_1^{+\infty} t^{-s-1} dt \\ &= \sum_{n=1}^{\infty} \theta(n) \frac{n^{-s-1} - (n+1)^{-s-1}}{s+1} - \frac{1}{s} \\ &= \frac{1}{s+1} \sum_{n=1}^{\infty} n^{-s-1} \left(\theta(n) - \theta(n-1)\right) - \frac{1}{s} \\ &= \frac{1}{s+1} \sum_{p} p^{-s-1} \log(p) - \frac{1}{s}. \end{aligned}$$

On the other hand

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p,m\geq 1} \log(p) p^{-ms} = \sum_{p} \log(p) p^{-s} + \sum_{p,m\geq 2} \log(p) p^{-ms}.$$

The second term is holomorphic for $\Re(s) > 1/2$, hence $\sum_p \log(p) p^{-s} = -\frac{\zeta'(s)}{\zeta(s)} +$ holomorphic function on $\Re(s) > 1/2$, and finally

$$F(s) = -\frac{\zeta'(s+1)}{(s+1)\zeta(s+1)} - \frac{1}{s} + \text{ holomorphic function on } \Re(s) > -1/2.$$

Using Hadamard – de la Vallée Poussin result (theorem 1.6) we may conclude.

3.3. **Estimates for zeta functions.** We now use the previous theory to give estimates for zeta functions. Let us axiomatise the properties we will use (we think of M as being $H^w(X)$ for some smooth projective variety): there is a weight $w = w(M)$, a "Betti number" $b = b(M)$, "Hodge numbers" h_i, h_i', a conductor $N = N(M)$.

(1) (Euler product) We have $L(M, s) = \prod_p L_p(M, s)$ with

$$L_p(M, s) = \prod_{j=1}^{b(M)} (1 - \alpha_{p,j} p^{-s})^{-1},$$

such that $|\alpha_{p,j}| \leq p^{w/2}$ with equality whenever p does not divide $N = N(M)$. Therefore the Euler product is absolutely convergent for $\Re s > 1 + w/2$.

(2) (Functional equation) Define the "*completed*" L-function as:

$$\Lambda(M, s) = N^{s/2} \prod_i \Gamma_{\mathbb{R}}(s + a_i)^{h_i} \Gamma_{\mathbb{C}}(s + b_i)^{h_i'} L(M, s),$$

then $\Lambda(M, s) = \pm\Lambda(M, w + 1 - s)$.

We will also study some consequences of the (generalised) Riemann Hypothesis which states that the zeroes of $\Lambda(M, s)$ are located on the line $\Re s = (w + 1)/2$.

Lemma 3.13. *Let $\sigma > 1 + w/2$ then*
(3.7)
$$|L(M,\sigma+it)| \le \zeta(\sigma - w/2)^{b(M)} \quad \text{and} \quad |\log L(M,\sigma+it)| \le b(M)\log\zeta(\sigma-w/2).$$

Proof. We simply use the inequality $|1-z|^{-1} \le (1-|z|)^{-1}$ (when $|z|<1$) to write

$$|L(M,\sigma+it)| = \prod_p \prod_{j=1}^{b(M)} |1-\alpha_{p,j}p^{-s}|^{-1} \le \prod_p (1-p^{\frac{w}{2}-\sigma})^{-b(M)} = \zeta(\sigma-\frac{w}{2})^{b(M)}.$$

The second inequality is proven in the same fashion. □

Using the functional equation and Phragmén–Lindelöf, one gets

Corollary 3.14. *(Convexity bound) Define $H = \sum_i h_i + 2\sum_i h'_i$ then*

$$|L(M,\sigma+it)| \ll \left(N(1+|t|)^H\right)^{\psi(\sigma)+\epsilon} \tag{3.8}$$

where ψ is a convex function such that

$$\psi(\sigma) = \begin{cases} 0 & \text{when } \sigma \ge 1+\frac{w}{2} \\ \frac{w+1}{2} - \sigma & \text{when } \sigma \le \frac{w}{2}. \end{cases}$$

Proof. Indeed from the functional equation we get that

$$L(M,s) = N^{\frac{w+1}{2}-s}\frac{L_\infty(M,w+1-s)}{L_\infty(M,s)}L(M,w+1-s).$$

Now Stirling formula (3.2) implies that, as t goes to infinity,

$$\frac{L_\infty(M,w+1-\sigma-it)}{L_\infty(M,\sigma+it)} \sim C|t|^{H(\frac{w+1}{2}-\sigma)}.$$

This gives the formula for $\psi(\sigma)$ outside the critical strip; the convexity of $\psi(\sigma)$ is a restatement of Phragmén–Lindelöf estimate. □

Notice that when $\sigma \in [\frac{w}{2}, 1+\frac{w}{2}]$ then $\min\{0, \frac{w+1}{2}-\sigma\} \le \psi(\sigma) \le \frac{1}{2}(1+\frac{w}{2}-\sigma)$ so that for example

$$L\left(\frac{w+1}{2}+it\right) \ll (N(1+|t|)^H)^{\frac{1}{4}+\epsilon} \qquad \text{and} \qquad L\left(\frac{w+1}{2}\right) \ll N^{\frac{1}{4}+\epsilon}.$$

If we allow the generalised Riemann hypothesis then using Borel-Carathéodory and the three circles lemma one can show

Corollary 3.15. *Assume further the L function satisfies the generalised Riemann hypothesis then we may choose $\psi(\sigma) = \min\{0, \frac{w+1}{2}-\sigma\}$ and in particular*

$$L\left(\frac{w+1}{2}+it\right) \ll (N(1+|t|)^H)^{\epsilon} \qquad \text{and} \qquad L\left(\frac{w+1}{2}\right) \ll N^{\epsilon}. \tag{3.9}$$

Proof. Assuming the Riemann Hypothesis, the function $g(s) = \log L(M,s)$ is holomorphic on $\Re s > \frac{w+1}{2}$ and $\Re g(s) = \log|L(M,s)| \ll \log(N(1+|t|^H)$. Using Borel-Carathéodory lemma we obtain a bound of the shape $|g(\frac{w+1}{2}+\eta+it)| \ll \eta^{-1}\log(N(1+|t|^H)$. Applying Hadamard's three circles lemma to the circles of center σ_1+it (where σ_1 is chosen very large) and radii $\sigma_1 - \frac{w}{2} - 1 - \eta$, $\sigma_1 - \sigma$ and $\sigma_1 - \frac{w+1}{2} - \eta$, we will obtain a bound $|g(\frac{w+1}{2}+2\eta+it)| \ll \eta^{-1}\left(\log(N(1+|t|^H)\right)^{1-\eta}$ from which it follows that $L(M,s)$ is $O\left((N(1+|t|^H))^\epsilon\right)$ when $\Re s \ge \frac{w+1}{2}$. □

Applying Cauchy's bounds, one gets similar estimates for the derivatives, i.e. for example $\frac{1}{r!}L^{(r)}\left(\frac{w+1}{2}\right) \ll_{r,\epsilon} N^{\epsilon}$. As explained in the last lecture, it would be very interesting to show a similar *lower bound* for the first non vanishing derivative, i.e. if we let r be the order of vanishing of $L(s)$ at $s = \frac{w+1}{2}$ then does there exist a lower bound of the shape:

$$\frac{1}{r!}L^{(r)}\left(\frac{w+1}{2}\right) \gg N^{-\epsilon}\,?$$

This question is intimately connected with the distribution of zeroes near $s = \frac{w+1}{2}$ as one can see for example on the Hadamard factorisation.

$$L(M,s) = e^{As+B}\prod_{\rho}\left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}}.$$

In fact, if such an estimate is true, it implies, via Jensen formula (lemma 3.8) applied to $f(s) = L^*(\frac{w+1}{2}+s) := L(\frac{w+1}{2}+s)s^{-r}$ with a small radius η, that, if we denote $n(r)$ the number of zeroes in the disk of center $\frac{w+1}{2}$ and radius r, we have $\int_0^{\eta} n(r)\frac{dr}{r} = o(\log N)$. In particular this would imply that ρ_0 the zero closest to $\frac{w+1}{2}$ (but different) satisfies $|\rho_0 - \frac{w+1}{2}| \gg N^{-\epsilon}$.

4. Lecture IV : Special values of zeta functions

Convention 4.1. By convention we will call the "special value" at $s = k$ (in practice k will be an integer or half an integer) of a meromorphic function $L(s)$ the leading term of its Taylor expansion; that is if L has a zero of order r at $s = k$ (resp. a pole of order $-r$) we define:

$$L^*(k) := \lim_{s\to k}(s-k)^{-r}L(s).$$

There is a wealth of fascinating formulas, the oldest being

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \text{more generally} \quad \pi^{-2n}\zeta(2n) \in \mathbb{Q}^*.$$

In general the special value will have the shape:

$$\zeta^*(M,k) = (\text{rational number}) \times (\text{period}) \times (\text{regulator}).$$

In the previous example the period is π^{2n} and the regulator is trivial (i.e. equal to 1). The interest of "special values" was noted explicitely by Hecke whom we quote : "*the precise knowledge of the behaviour of an analytic function in the neighbourhood of its singular points is a source of number-theoretic theorems*".

We will mainly be concerned by the size of *regulators*; the idea is simple : suppose $L \cong \mathbb{Z}^n$ is a lattice in $E = \mathbb{R}^n$, then, in order to give bounds for a set of generators of L it suffices to have two estimates:

(1) An upper bound for the covolume $\mathrm{vol}(E/L)$;
(2) A lower bound for the norm of the smallest non zero vector in L.

Indeed one of Minkowski' s theorem in geometry of numbers states that there is a basis $e_1, \dots, e_n$ of L such that

$$\prod_{i=1}^{n} |e_i| \le c_n \,\mathrm{vol}(E/L)$$

(Notice that for *any* basis we have $\mathrm{vol}(E/L) \le \prod_{i=1}^n |e_i|$.)

The two examples of lattices of interest will be the following.

Lattice of units of a number field. Let F be a number field with r_1 real embeddings $\sigma_1, \dots, \sigma_{r_1}$ and r_2 pairs of complex embeddings $\{\tau_j, \bar{\tau}_j\}$ (for $1 \le j \le r_2$). Define the logarithmic map

$$LOG : \mathcal{O}_F^* \to \mathbb{R}^{r_1+r_2},$$

by $LOG(x) = (\log|\sigma_1(x)|, \dots, \log|\sigma_{r_1}(x)|, 2\log|\tau_1(x)|, \dots, 2\log|\tau_{r_2}(x)|)$. Then the kernel is given by the roots of unity and the image is a discrete subgroup contained in the hyperplane H with equation $x_1 + \cdots + x_{r_1} + y_1 + \cdots + y_{r_2} = 0$. In fact $L := LOG(\mathcal{O}_F^*)$ is a lattice in H which means that the rank of $\mathcal{O}_F^*$ is $r := r_1 + r_2 - 1$ (the fact that the rank is at most $r_1 + r_2 - 1$ is clear, the equality is a theorem due to Dirichlet). The regulator is the covolume of this lattice which can be computed by the explicit formula, where $\epsilon_1, \dots, \epsilon_r$ is basis of $\mathcal{O}_F^*/$ roots of unity :

$$R_F = |\det(\delta_i \log|\sigma_i(\epsilon_j)|)| \tag{4.1}$$

where σ_i runs among all pairwise non conjugate embeddings minus one[5] and $\delta_i = 1$ (resp. $= 2$) for σ_i real (resp. for σ_i complex).

The question of bounding the size of generators of the group of units is thus tantamount to bounding R_F.

Mordell-Weil Lattice. Let A be an elliptic curve (or more generally an abelian variety) defined over $K = \mathbb{Q}$ (or more generally over a global field K). The Mordell-Weil theorem states that $A(K)$ is a finitely generated group. Further there is a canonical height (also called Néron-Tate height[6]) $\hat{h} : A(K) \to \mathbb{R}$, which provides an intrinsic notion of *size* of a rational point and satisfies the following properties :

(1) It is a counting function, which means that the set $\{x \in A(K) \mid \hat{h}(x) \leq C\}$ is finite for any C.
(2) It is a positive definite quadratic function, which means that

$$\langle x, y \rangle := \frac{1}{2}(\hat{h}(x+y) - \hat{h}(x) - \hat{h}(y))$$

is bilinear and the induced quadratic map $\hat{h}_{\mathbb{R}} : A(K) \otimes \mathbb{R} \to \mathbb{R}$ is positive in the usual sense.

One can give a quick construction of the Néron-Tate height as follows.

Define first the (logarithmic) "naïve height" of a point $P \in \mathbb{P}^n(K)$ with projective coordinates $P = (x_0, \ldots, x_n)$ by the formula

$$h(P) := \sum_{v \in M_K} \log \max |x_i|_v \,. \tag{4.2}$$

Notice that the definition is independent of the choice of projective coordinates, thanks to the product formula (1.25). Choosing an embedding $\phi : A \hookrightarrow \mathbb{P}^n$ we obtain a height $h := h_\phi : A(K) \to \mathbb{R}$ defined by $h_\phi(P) := h(\phi(P))$. The Néron-Tate height is then equal to the limit :

$$\hat{h}(P) = \hat{h}_\phi(P) = \lim_m \frac{h(2^m P)}{4^m}. \tag{4.3}$$

Definition 4.2. Let $P_1, \ldots, P_r$ denote a $\mathbb{Z}$-basis of $A(K)/A(K)_{\text{tor}}$, the Néron-Tate *regulator* is the determinant :

$$\mathrm{Reg}(A/K) := \det\left(\langle P_i, P_j \rangle\right)_{1 \leq i,j \leq r} . \tag{4.4}$$

The regulator is the square of the covolume of the lattice $A(K)/A(K)_{\text{tor}}$ in $A(K) \otimes \mathbb{R}$. The question of bounding the size of generators of the Mordell-Weil group $A(K)$ is thus tantamount to bounding $\mathrm{Reg}(A/K)$.

---

[5]The definition seems to depend on the omitted embedding but the formula $\sum_{i=1}^{r_1} \log|\sigma_i(\epsilon)| + 2\sum_{j=1}^{r_2} \log|\tau_j(\epsilon)| = 0$ is true for all unit ϵ and shows that the absolute value of the determinant does not depend on this choice.

[6]To be precise, the canonical height is in the general case a bilinear form $(\cdot,\cdot) : A(K) \times A^\vee(K) \to \mathbb{R}$ where $A^\vee$ denotes the dual abelian variety; one then needs a polarisation $\lambda : A \to A^\vee$ (or alternatively an embedding $A \hookrightarrow \mathbb{P}^n$) to define the height $\hat{h}_\lambda(x) = -\frac{1}{2}(x, \lambda(x))$. Since we'll deal essentially with the example of elliptic curves this subtlety disappears.

4.1. **The residue of Dedekind zeta function.** The first deep theorem about special values we will mention is:

Theorem 4.3. *The special value of the Dedekind zeta function at $s = 1$ is:*

$$\zeta_F^*(1) = \lim_{s\to 1}(s-1)\zeta_F(s) = \frac{h_F R_F}{\sqrt{\Delta_F}} \cdot \frac{2^{r_1}(2\pi)^{r_2}}{w_F}. \tag{4.5}$$

Via the functional equation, this translates into the following slightly more elegant formula : the function $\zeta_F(s)$ has a zero of order $r_1 + r_2 - 1$, the rank of the group of units, and :

$$\zeta_F^*(0) := \lim_{s\to 0} s^{-r_1-r_2+1}\zeta_F(s) = -\frac{h_F R_F}{w_F}.$$

Here all quantities have been defined except w_F which is the number of roots of unity inside F^*; it can be viewed as the cardinality of $\mathcal{O}^*_{F,\text{torsion}}$.

4.2. **Class number formulas.** Let χ denote a non trivial Dirichlet character. It is possible to give a finite expression for the series $L(\chi, 1) := \sum_{n\geq 1} \frac{\chi(n)}{n}$ using the following elementary formula. Put $\ell(\theta) := \sum_{n\geq 1} \exp(in\theta)n^{-1}$. Then, for $\theta \in]0, 2\pi[$, we have

$$\ell(\theta) = -\log(2\sin(\theta/2)) + i\left(\frac{\pi}{2} - \frac{\theta}{2}\right).$$

For a primitive character $\chi \neq \chi_0$ one may deduce

$$L(\chi,1) = \begin{cases} \pi i \frac{G(\chi)}{N^2} \sum_{a=1}^N \bar{\chi}(a)a & \text{if } \chi(-1) = -1 \\ -\frac{G(\chi)}{N} \sum_{a=1}^N \bar{\chi}(a)\log|1-\exp(2\pi a/N)| & \text{if } \chi(-1) = +1. \end{cases} \tag{4.6}$$

On the other hand, when $K = \mathbb{Q}(\exp(2\pi i/N)$, we have

$$\zeta_K(s) = \zeta(s)\prod_{\chi} L(\chi, s),$$

where the product is over non trivial primitive Dirichlet characters modulo N. We may deduce the first form of the class number formula :

$$\frac{2^{r_1}(2\pi)^{r_2}}{w}\frac{hR}{\sqrt{\Delta}} = \prod_{\chi\neq\chi_0} L(\chi, 1). \tag{4.7}$$

Let us specialise a bit to $N = p$ a prime number. By writing the corresponding formulas for $K = \mathbb{Q}(\exp(2\pi i/p)$ and $K^+ := K \cap \mathbb{R} = \mathbb{Q}(\cos(2\pi i/p))$ we then obtain formulas

$$h_K = w_K \frac{R_{K^+}}{R_K} \prod_{\text{odd}\,\chi}\left(-\frac{1}{2}B_\chi\right) \tag{4.8}$$

where we set $B_\chi = \frac{1}{p}\sum_{a=1}^p \chi(a)a$ and recall that $w_K = 2p$ is the number of roots of unity in K.

Notice that $r_1(K) = 0$, $r_2(K) = [K : \mathbb{Q}]/2 = (p-1)/2$ whereas $r_1(K^+) = [K^+ : \mathbb{Q}] = (p-1)/2$ and $r_2(K^+) = 0$ thus $\mathcal{O}_K^*$ and $\mathcal{O}_{K^+}^*$ have the same rank and the latter is a subgroup of finite index in the former. One can finally identify the quotient $\frac{R_{K^+}}{R_K}$ with the class number of K^+ and obtain the following class number formula.

Theorem 4.4. *Let $K = \mathbb{Q}(\exp(2\pi i/p))$ and $K^+ := K \cap \mathbb{R} = \mathbb{Q}(\cos(2\pi i/p))$ and let h_p and h_p^+ be their respective class number then*

1. *One may factor $h_p = h_p^+ h_p^-$ where h_p^- is an integer.*
2. *One has the formula*

$$h_p^- = w_K \prod_{\text{odd } \chi} \left(-\frac{1}{2} B_\chi\right). \tag{4.9}$$

One may in fact prove similar class number formulas for any abelian extensions of $\mathbb{Q}$. For a quadratic field K with discriminant Δ the corresponding basic formula is

$$\mathrm{Res}(\zeta_K, 1) = \begin{cases} \frac{2\pi h_K}{w_K \sqrt{\Delta}} & \text{if } K \text{ imaginary} \\ \frac{2 h_K \log \epsilon}{\sqrt{\Delta}} & \text{if } K \text{ real,} \end{cases} \tag{4.10}$$

where ϵ is the fundamental unit. On the other hand if $K = \mathbb{Q}(\sqrt{D})$ we have a decomposition $\zeta_K(s) = \zeta(s) L(\chi_D, s)$ and hence

$$\mathrm{Res}(\zeta_K, 1) = L(\chi_D, 1), \tag{4.11}$$

where the character χ_D can be described as follows. Any prime number p is either decomposed or inert or ramified in $K/\mathbb{Q}$, which means that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_1$ or $\mathfrak{p}$ or $\mathfrak{p}^2$; if we denote $\mathcal{D}$, $\mathcal{I}$, $\mathcal{R}$ the set of decomposed, inert or ramified primes we have

$$\begin{aligned} \zeta_K(s) &= \prod_{p \in \mathcal{D}} (1 - p^{-s})^{-2} \prod_{p \in \mathcal{I}} (1 - p^{-2s})^{-1} \prod_{p \in \mathcal{R}} (1 - p^{-s})^{-1} \\ &= \zeta(s) \prod_{p \in \mathcal{D}} (1 - p^{-s})^{-1} \prod_{p \in \mathcal{I}} (1 + p^{-s})^{-1} = \zeta(s) \prod_p (1 - \chi_D(p) p^{-s})^{-1}. \end{aligned} \tag{4.12}$$

Thus for $p \neq 2$ we have $\chi_D(p) = \left(\frac{D}{p}\right)$ (the Legendre symbol); the fact that the function χ_D thus defined is a Dirichlet character is essentially equivalent to the quadratic reciprocity law, the ancestor of Artin reciprocity law.

These formulas are basic for theoretical study and explicit computations of class numbers.

4.3. **The Birch and Swinnerton-Dyer conjecture.** There are many results and conjectures about special values of Hasse-Weil zeta and L-functions, let us mention there are general conjectures by Lichtenbaum, Deligne, Beilinson and Bloch-Kato. I'll only discuss here the mother of them all : the Birch and Swinnerton-Dyer conjecture.

We first need to define more quantities; we'll do it for elliptic curves over $K = \mathbb{Q}$ or $\mathbb{F}_p(C)$ though it would not be much more difficult to do it for abelian varieties over global fields. Let $R := \mathrm{Spec}(\mathbb{Z})$ or C, we have a so-called *Néron model* $\mathcal{A} \to R$ with neutral section $e : R \to \mathcal{A}$.

1. We already introduced the Néron-Tate regulator which we denote $\mathrm{Reg}(A/K)$.
2. The *Tate-Shafarevich group* is defined as a measure of a local-global cohomological obstruction (where v runs over all places of K):

$$Ш(A/K) := \ker \left\{ H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), A_K) \to \prod_v H^1(\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v), A_{K_v}) \right\}.$$

(3) The *Tamagawa numbers* is the product $\mathcal{T}(A/K) = \prod_v c_v(A/K)$ where the quantity $c_v(A/K)$ is the number of components defined over the residual field of the special fiber above v of the Néron model of A/K.
(4) (When $K = \mathbb{Q}$) The *period* is $\Omega_A = \int_{A(\mathbb{R})} \omega$ where ω is the Néron differential.
(5) The *height* $h(A/K)$ is the Faltings height in the case of number fields and simply $\deg e^*\Omega^1_{\mathcal{A}/C}$ in the function field case; we also introduce the *exponential height* as $H(A/K) = \exp(h(A/K))$ in the number field case and $H(A/K) = p^{h(A/K)}$ in the function field case.

For convenience define

$$\mathcal{W}(A/K) := \begin{cases} \Omega_{A/K} & \text{in the number field case} \\ H(A/K)^{-1}p^{d(1-g)} & \text{in the function field case,} \end{cases}$$

then we may formulate

Conjecture 4.5 (The Birch & Swinnerton-Dyer conjecture)**.** *The following statements holds true.*

(1) *The L-function $L(A/K, s)$ is analytic at $s = 1$ and*

$$\operatorname{rank} A(K) = \operatorname{ord}_{s=1} L(A/K, s).$$

(2) *The group $Ш(A/K)$ is finite.*
(3) *The special value at $s = 1$ is given by*

(4.13)
$$L^*(A/K, 1) = \lim_{s\to 1} \frac{L(A/K, s)}{(s-1)^r} = \frac{\#Ш(A/K) \cdot \operatorname{Reg}(A/K)}{\#A(K)_{\text{tor}} \cdot \#A^\vee(K)_{\text{tor}}} \cdot \mathcal{T}(A/K) \cdot \mathcal{W}(A/K).$$

The conjecture can be viewed as a sophisticated version of the local global principle. One collects local informations (for elliptic curves this involves only the number of points modulo p) and builds with them a global object (the L-function), using analytical continuation beyond the half-plane of convergence, one hopes to gather important global information encoded in the L-function such as the rank of the Mordell-Weil group, the Néron-Tate regulator. Notice that for example the BSD conjecture asserts that:

(1) The Mordell-Weil group is finite if and only if $L(A/K, 1) \neq 0$.
(2) (Parity conjecture) Let $r = \operatorname{rank} A(K)$ then the sign of the functional equation is $(-1)^r$.

Both of these corollaries have been checked on thousands of examples and it is known, for modular elliptic curves, that if $L(A/K, 1) \neq 0$ (resp. if $L(A/K, 1) = 0$ and $L'(A/K, 1) \neq 0$) then $r = 0$ (resp. $r = 1$).

This marvelous conjecture is far from settled; the Tate-Shafarevich group is not even known to be finite in general and analytic continuation until $s = 1$ of the L-function is only known for elliptic curves over $\mathbb{Q}$ (Wiles) and modular or CM abelian varieties (Shimura). Over $\mathbb{Q}$ if the order of the zero of $L(A/\mathbb{Q}, s)$ is ≤ 1, the first two items are true and the third is true up to a rational number which, in a finite number of cases has been computed to be 1!

The situation is better over function fields where we know that $\operatorname{rank} A(K) \leq \operatorname{ord}_{s=1} L(A/K, s)$, and finiteness of some ℓ-primary component of $Ш(A/K)$ is equivalent to the equality $\operatorname{rank} A(K) = \operatorname{ord}_{s=1} L(A/K, s)$. Further, when true, these

equivalent statement imply the full conjecture; thus there is a large supply of abelian varieties over function fields for which the full BSD conjecture is settled.

5. Lecture V : Brauer-Siegel type theorems (and conjectures)

5.1. **Brauer-Siegel theorem for number fields.**

Theorem 5.1 (Brauer-Siegel Theorem)**.** *Suppose that F varies over a family of number fields of fixed degree over $\mathbb{Q}$. Denote by Δ_F the absolute value of the discriminant of $F/\mathbb{Q}$ and suppose that Δ_F tends to infinity, then :*

$$\log(h_F \cdot R_F) \sim \log\left(\Delta_F^{1/2}\right), \tag{5.1}$$

where h_F denotes the class number of F and R_F the regulator of the group of units of F.

Applications.

(1) For imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$ the theorem yields
$$D^{\frac{1}{2}-\epsilon} \ll h_{-D} \ll D^{\frac{1}{2}+\epsilon},$$
displaying in an explicit way that the class number goes to infinity quite rapidly.

(2) For real quadratic fields $K = \mathbb{Q}(\sqrt{D})$ the theorem yields
$$D^{\frac{1}{2}-\epsilon} \ll h_D \log \epsilon_D \ll D^{\frac{1}{2}+\epsilon},$$
displaying in an explicit way that at least one of the two quantities (the class number and the size of the fundamental unit) goes to infinity quite rapidly. It also provides a bound
$$\log \epsilon_D \ll D^{\frac{1}{2}+\epsilon}, \tag{5.2}$$
which is best possible for the D's with say bounded h_D (conjectured to be infinitely many).

(3) For any degree d, it is possible to construct sequences of fields F of degree d with small regulator hence large class number, say $h_F \gg \Delta_F^{\frac{1}{2}-\epsilon}$. For example take $F = \mathbb{Q}(\alpha)$ with α a root of $P(T) = \prod_{j=1}^{d}(T - ja) + b$ (for well chosen a, b).

(4) In general we get bounds for both the regulator and class number
$$h_F \ll \Delta_F^{\frac{1}{2}+\epsilon} \qquad \text{and} \qquad R_F \ll \Delta_F^{\frac{1}{2}+\epsilon}.$$

The proof of the Brauer-Siegel starts with the formula for the residue of $\zeta_F(s)$ and essentially boils down to show that $\Delta_F^{-\epsilon} \ll \zeta_F^*(1) \ll \Delta_F^{\epsilon}$ for fields of fixed degree $[F : \mathbb{Q}] = d$. The upper bound is relatively easy and follows from an integral representation similar to (1.10) of the shape:

$$\xi_F(s) = \frac{\lambda_F}{s(s-1)} + f_F(s),$$

where $\lambda_F = \xi_F^*(1)$ is the residue of $\xi_F(s)$ at $s = 1$ and $f_F(s)$ is such that for real s we have $f_F(s) \geq 0$ and even $\gg \Delta_F^{s/2}$. Picking $\sigma > 1$ we obtain

$$\lambda_F \leq \sigma(\sigma - 1)\xi_F(\sigma).$$

Elementary estimates give $\zeta_F(\sigma) \leq \zeta(\sigma)^d \leq \left(1 + \frac{1}{\sigma-1}\right)^d$ and thus choosing $\sigma = 1 + 1/\log \Delta_F$ we'll get a bound of the shape $\lambda_F \ll \Delta_F^{\frac{1}{2}}(\log \Delta_F)^d$, hence $\zeta_F^*(1) = (2\pi)^{r_2}\Delta_F^{-\frac{1}{2}}\lambda_F \ll (\log \Delta_F)^d$.

The lower bound is much harder. Granting the Riemann hypothesis or more modestly granting the non existence of Siegel zeroes, i.e. zero of $\zeta_F(s)$ located on a segment $[1-\frac{c}{\log\Delta},1[$ we can give a quick proof. Indeed selecting a point $0<\sigma<1$ where $\zeta_F(\sigma)<0$ (or equivalently $\xi_F(\sigma)<0$) we get

$$\lambda_F > \sigma(1-\sigma)f_F(\sigma) \gg \sigma(1-\sigma)\Delta_F^{\frac{1-\sigma}{2}}.$$

Thus if we are allowed to choose $\sigma = 1-1/\log\Delta_F$ we get the required estimate. In fact this proof requires non existence of zeroes of the zeta function on the segment $[1-c_\epsilon\Delta^{-\epsilon},1]$; this is exactly what Siegel proved for quadratic fields (and was extended by Brauer to all number fields, using theorem 2.3) with, unfortunately, ineffective (not computable) constants c_ϵ; we give below a sketch of proof of Siegel's result.

One can ask what happens if we relax the conditions and allow say $[K:\mathbb{Q}]$ to go to infinity; the question has been thoroughly explored by Tsfasman and Vlăduţ. To describe one of their main results we need a bit of notation.

Definition 5.2. For a number field K and $q=p^m$ we denote $\Phi_q(K)$ the number of places of K with norm equal to q. For a sequence of number fields K_i we define the limits (when they exist):

$$\Phi_q := \lim_i \frac{\Phi_q(K_i)}{\log\sqrt{\Delta_{K_i}}}; \quad \Phi_{\mathbb{R}} := \lim_i \frac{r_1(K_i)}{\log\sqrt{\Delta_{K_i}}} \quad \text{and} \quad \Phi_{\mathbb{C}} := \lim_i \frac{r_2(K_i)}{\log\sqrt{\Delta_{K_i}}}.$$

We call *asymptotically exact* a family for which these limits all exists (this can always be achieved by extracting a subsequence).

In the following a sequence K_i of fields is *almost normal* if each K_i is contained or contains a normal field K_i' with $[K_i':K_i]$ or $[K_i:K_i']$ bounded (the definition given in [TsVl02] is actually more general) .

Theorem 5.3. *(Tsfasman – Vlăduţ) Let K_i be an asymptotically exact family of number fields and assume that either all $K_i/\mathbb{Q}$ are almost normal or that GRH holds, then*

$$\lim_i \frac{\log\left(h_{K_i}R_{K_i}\right)}{\log\sqrt{\Delta_{K_i}}} = 1 + \sum_q \Phi_q \log\left(\frac{q}{q-1}\right) - \Phi_{\mathbb{R}}\log 2 - \Phi_{\mathbb{C}}\log 2\pi. \tag{5.3}$$

Remark 5.4. If $[K:\mathbb{Q}]$ is bounded or even if $[K:\mathbb{Q}]/\log\Delta_K$ goes to zero, we see easily that $\Phi_q = \Phi_{\mathbb{R}} = \Phi_{\mathbb{C}} = 0$ and we recover the original Brauer-Siegel theorem, but there exists many interesting families of fields for which the limit in theorem 5.3 is not equal to 1.

5.1.1. *Appendix: Siegel's theorem according to Goldfeld.* The proof of Brauer–Siegel theorem without using GRH is complicated. We give here Golfeld's proof [Go74] in the (essential) case of quadratic fields. It is based on the relatively elementary (see below) fact that for a quadratic (real) character of conductor D, we have the bounds $D^{-1/2} \ll |L(1,\chi)| \ll \log D$; to obtain a better lower bound is more delicate and is the true content of Siegel's theorem.

Theorem 5.5. *For all $\epsilon > 0$ there exists $C(\epsilon) > 0$ such that for all real characters of conductor D we have*

$$L(1,\chi) \gg \frac{C(\epsilon)}{D^{\epsilon}}. \tag{5.4}$$

As mentionned before, the proof requires the following two lemmas.

Lemma 5.6. *Let χ be a Dirichlet character of modulus D then*

$$|L(1,\chi)| \ll \log D.$$

Proof. We split the converging series at Y :

$$L(1,\chi) = \sum_{m\le Y} \frac{\chi(m)}{m} + \sum_{m>Y} \frac{\chi(m)}{m}.$$

The first sum is bounded by $\sum_{m\le Y} \frac{1}{m} \le \log Y + c_1$; for the second sum we introduce $M_\chi := \max |\sum_{A<m<B} \chi(m)|$; clearly $M_\chi \le D$. Abel's summation then gives:

$$\left|\sum_{m>Y} \frac{\chi(m)}{m}\right| \le \sum_{m\ge Y} \left|\sum_{n\le m} \chi(n)\right| (m^{-1} - (m+1)^{-1}) \ll M_\chi Y^{-1}$$

The choice $Y = M_\chi$ provides $L(1,\chi) \ll \log M_\chi \le \log D$. □

Lemma 5.7. *Let χ be a quadratic Dirichlet character of modulus D then*

$$|L(1,\chi)| \gg D^{-1/2}.$$

Proof. Indeed if χ corresponds to an imaginary quadratic field K (in particular Δ_K is equal to D up to a small factor) then we have

$$L(\chi,1) = \mathrm{Res}_{s=1}\zeta_K(s) = \frac{2\pi h_K}{w\sqrt{\Delta_K}} \gg D^{-1/2},$$

whereas if χ corresponds to a real quadratic field K then we have

$$L(\chi,1) = \mathrm{Res}_{s=1}\zeta_K(s) = \frac{2h_K \log\epsilon}{\sqrt{\Delta_K}} \gg D^{-1/2}.$$

□

Proof. (sketch of proof of theorem 5.5) Introduce the product of zeta functions:

$$f(s) := \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2).$$

The crucial property is that the Dirichlet coefficients of $f(s) = \sum a_n n^{-s}$ are positive[7]; indeed the Euler factor is

$$f_p(s) = \frac{1}{(1-p^{-s})(1-\chi_1(p)p^{-s})(1-\chi_2(p)p^{-s})(1-\chi_1\chi_2(p)p^{-s})}$$

and thus

$$\log f_p(s) = \sum_{m\ge 1} (1+\chi_1(p^m))(1+\chi_2(p^m))\frac{p^{-ms}}{m}.$$

We denote $\lambda := L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2)$ the residue of $f(s)$ at $s=1$.

[7]The "true" reason for this is that if the characters χ_i correspond to quadratic fields K_i then, up to finitely many Euler factors, the function $f(s)$ is the Dedekind zeta function of the field K_1K_2.

The following claim is easy but its innocent and trivial proof is responsible for the ineffectivity in Siegel's theorem.

Lemma 5.8. *For all $\epsilon > 0$, there exists χ_1 mod D_1 and $\beta \in]1-\epsilon, 1[$ such that for any χ_2 we have $f(\beta) \leq 0$.*

Indeed if there are no Siegel zeroes, any $\beta \in]1-\epsilon, 1[$ will do; otherwise let $\beta \in]1-\epsilon, 1[$ be a zero for some χ_1.

By shifting in the following positive integral the line of integration from $\sigma = 2$ to $\sigma = -\beta$ we get, using Perron's formula

$$1 \ll \frac{1}{4!}\sum_{n\leq x} a_n n^{-\beta}(1-\frac{n}{x})^4 = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} f(s+\beta)\frac{x^s}{s(s+1)(s+2)(s+3)(s+4)}ds$$
$$= \lambda\frac{x^{1-\beta}}{(1-\beta)(2-\beta)(3-\beta)(4-\beta)(5-\beta)} + \frac{f(\beta)}{4!} + O\left(\frac{(D_1D_2)^{1+\epsilon}}{x^\beta(1-\beta)}\right).$$

Here the upper bound for $\int_{(-\beta)} f(s+\beta)\frac{x^s}{s(s+1)(s+2)(s+3)(s+4)}ds$ relies on the functional equation and Phragmén-Lindelöf as in section 3.3.

Since by lemma 1 we have $f(\beta) \leq 0$ we infer that $1 \ll \lambda\frac{x^{1-\beta}}{1-\beta}$ if $(D_1D_2)^{2+\epsilon} \ll x$ because $\lambda \gg \frac{1}{D_1D_2}$. Consequently, since $\lambda \ll L(1,\chi_1)\log(D_1D_2)\log D_1$ we get upon picking $x = c(D_1D_2)^{2+\epsilon} = c'D_2^{2+\epsilon}$:

$$L(1,\chi_2) > cD_2^{-(2+\epsilon)(1-\beta)}(\log D_2)^{-1},$$

which gives what we want provided (say) $(2+\epsilon)(1-\beta) < \epsilon/2$ and D_2 is large enough. □

5.2. **Brauer-Siegel theorem for abelian varieties.** A look at the residue formula for the Dedekind zeta function and the Birch and Swinnerton formula suggests the following correspondence:

$$\begin{array}{ccc} \zeta_F(s) & \leftrightarrow & L(A/K,s) \\ h_F & \leftrightarrow & |Ш(A/K)| \\ R_F & \leftrightarrow & \mathrm{Reg}(A/K) \\ \mathcal{O}^*_{F,\mathrm{torsion}} & \leftrightarrow & (A(K)\times A^\vee)(K)_{\mathrm{torsion}} \\ \sqrt{\Delta_F} & \leftrightarrow & \Omega_A \text{ or } H(A/K), \end{array}$$

and, being a bit more audacious:

Conjecture 5.9. *(Analogue of Brauer-Siegel theorem for abelian varieties) Consider the family of abelian varieties A of fixed dimension d, defined either over a fixed number field K or over the function field K of a smooth, projective, geometrically connected algebraic curve $\mathcal{C}$ defined over the finite field $\mathbb{F}_q$ with $q := p^n$ elements. Denote by $H(A/K)$ its exponential height and suppose that it tends to infinity, then :*

$$\log(\#Ш(A/K)\cdot\mathrm{Reg}(A/K)) \sim \log H(A/K), \tag{5.5}$$

where $\#Ш(A/K)$*, resp.* $\mathrm{Reg}(A/K)$*, denotes the order of the Tate-Shafarevich group, resp. the Néron-Tate regulator of* A/K*.*

If true this conjecture implies the following remarks.

(1) It provides an upper bound $\mathrm{Reg}(A/K) \ll H(A/K)^{1+\epsilon}$ and thus a bound for the size of generators of the Mordell-Weil group.
(2) Similarly, since the regulator cannot be too small, it implies a bound for the size of the Tate-Shafarevich group, namely $\#Ш(A/K) \ll H(A/K)^{1+\epsilon}$.
(3) When $r = 0$ (or equivalently under the BSD conjecture when $L(A/K, 1) \neq 0$) we get a lower bound $\#Ш(A/K) \gg H(A/K)^{1-\epsilon}$.

Just like in the number field case, it is interesting to look at the "orthogonal case" when one fixes the abelian variety and makes the field K grow in towers. There is the following result[8] over function fields.

Theorem 5.10. *(Tsfasman-Kunyavskiĭ* [KuTs08]*; Zykin* [Zy09]*) Let* A_0 *be an elliptic curve defined over* $\mathbb{F}_p$ *and let* $K_i = \mathbb{F}_p(C_i)$ *be a tower of fields with the genus of* C_i *going to infinity. then*

$$\lim_i \frac{\log_p(\#Ш(A_0/K)\,\mathrm{Reg}(A/K))}{g(C_i)} = 1 - \sum_{m=1} \beta_m \log_p \frac{|A_0(\mathbb{F}_{p^m})|}{p^m}. \tag{5.6}$$

where β_m *is defined as the limit (assumed to exist – which is always possible after extracting a subsequence) of* $|C_i(\mathbb{F}_{p^m})|/g(C_i)$*.*

Notice that finiteness of the Tate-Shafarevich group is, in the case of a constant abelian variety, a theorem due to Milne.

The situation over number fields is still very conjectural (we formulate here everything over $\mathbb{Q}$ but there is no difficulty in extending at least the statements to arbitrary abelian variety and number field) :

Theorem 5.11. *(H–*[Hi07]*) Assuming BSD conjectures for elliptic curves* $A/\mathbb{Q}$ *and the generalised Riemann hypothesis for* $L(A/\mathbb{Q}, s)$ *then*

$$\limsup \frac{\log\left(\#Ш(A/\mathbb{Q}) \cdot \mathrm{Reg}(A/\mathbb{Q})\right)}{\log H(A/\mathbb{Q})} \leq 1.$$

Assuming further an analytic estimates of the type $L^*(A/\mathbb{Q}, 1)| \gg H(A/\mathbb{Q})^{-\epsilon}$ *then* $\log\left(\#Ш(A/\mathbb{Q}) \cdot \mathrm{Reg}(A/\mathbb{Q})\right) \sim \log H(A/\mathbb{Q})$*.*

The situation over function fields is better.

Theorem 5.12. *(H–Pacheco* [HiPa10]*) Consider the family of elliptic curves over a function field* $K = \mathbb{F}_q(C)$*. Assume finiteness of some* ℓ*-primary component of* $Ш(A/K)$ *(or equivalently that the order of the zero of* $L(A/K, s)$ *at* $s = 1$ *is the expected one) then*

$$-5 \leq \liminf \frac{\log\left(\#Ш(A/K)\cdot\mathrm{Reg}(A/K)\right)}{\log H(A/K)} \leq \limsup \frac{\log\left(\#Ш(A/K)\cdot\mathrm{Reg}(A/K)\right)}{\log H(A/K)} \leq 1.$$

Assuming further an analytic estimates of the type $L^*(A/K, 1)| \gg H(A/K)^{-\epsilon}$ *then* $\log\left(\#Ш(A/K) \cdot \mathrm{Reg}(A/K)\right) \sim \log H(A/K)$*.*

Granting the BSD conjecture, the proof requires the following three estimates :

[8]Tsfasman indicated to me there is a gap in the paper [KuTs08] hence, though the result is most probably true, the proof should be regarded as incomplete at the present time.

(1) Show that $1 \leq \#A(K) \times A^\vee(K)_{\mathrm{tor}} \ll H(A)^\epsilon$.
(2) Show that $1 \leq \mathcal{T}(A/K)_{\mathrm{tor}} \ll H(A)^\epsilon$.
(3) Show that $H(A)^{-\epsilon} \ll L^*(A/K, s) \ll H(A)^\epsilon$.

Each is somewhat delicate but the lower bound in the third is the most difficult and a general argument is still missing. Nevertheless for some families the conjecture may be fully proven :

Theorem 5.13. *(H–Pacheco* [HiPa10]*) Consider the family of elliptic curves E_d over the function field $K = \mathbb{F}_p(t) = \mathbb{F}_p(\mathbb{P}^1)$ defined by their Weierstrass equation:*

$$y^2 + xy = x^3 - t^d.$$

The Tate-Shafarevich group of E_d/K is finite and, as d goes to infinity, we have:

$$\log\left(\#Ш(E_d/K) \cdot \mathrm{Reg}(E_d/K)\right) \sim \log H(E_d/K) \sim \frac{d}{6}\log q.$$

This family was studied by Ulmer who showed that is contains curves with very large rank.

6. Commented bibliography

We give here indications about where and what to read to go further than this brief and sketchy introduction.

Lecture I. Among excellent general references on analytic number theory I'll recommend [Da80, IwKo04, Te95]. For algebraic number theory, including an introduction to Artin and Dedekind zeta functions read [La70].

Lecture II. A concise introduction to Weil conjectures may be found in [Ha83] (appendix C.); for the construction of an adequate cohomology a comprehensive reference is [Mi80], the presentation of Hasse-Weil zeta functions is inspired by [Se70, Se65], for a nice introduction to elliptic curves see [Sil86], for modular forms see [DiSh08]; the theory of automorphic representation has its roots in [Ta50], see [Bu97] for a friendly introduction.

Lecture III. The classical complex variable lemmas, Tauberian theorems and analytic estimates may be found in [Da80, IwKo04, Te95]. To see the use of tauberian theorems in the context of Hasse-Weil L-functions, read for example [HiPa05, HiPaWa05].

Lecture IV. For a description of many formulas (some conjectural) describing special values of zeta and L-functions see [RaScSc88, Be85, BlKa90, De79, GrZa86, Li83, Wa82], the BSD formula over function fields was formulated in [Ta66], for related conjectures see also [Ta65],

Lecture V. The classical Brauer-Siegel theorem is proven in [Br47, Sie35]; a later and simpler proof appeared in [Go74]; for further study see [St74, Ts01, TsVl02]. The various analogues for elliptic curves and abelian varieties are studied in [Hi07, HiPa10, KuTs08, Zy09], the example is studied in [Ul02]. For the lower bound conjecture and its link with small zeroes [IwLuSa00].

References

[Be85] A. Beilinson, *Higher regulators and values of L-functions* J. Soviet Math. **30**, 2036–2070, 1985.

[BlKa90] S. Bloch, K. Kato, *L-Functions and Tamagawa Numbers of Motives*, *in* The Grothendieck Festschrift, Vol. 1 (P. Cartier et al. eds.), Birkhäuser, 1990.

[Br47] R. Brauer. *On zeta-functions of algebraic number fields*, Amer. J. Math. **69**, 243–250, 1947.

[Bu97] D. Bump, *Automorphic forms and representations*, Cambridge University Press, 1997.

[Da80] H. Davenport, *Mutiplicative Number Theory*, GTM 74, Springer, 1980.

[De79] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*. Symp. Pure Math. A.M.S. 33, 313–346, 1979.

[DiSh08] F. Diamond, J. Shurman, *Introduction to modular forms*, GTM 228, Springer, 2008.

[Go74] D. Golfeld, *A simple proof of Siegel's theorem*, Proc. Nat. Acad Sci. US 71, 1974, page 1055.

[GrZa86] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*, Inventiones Mat. **84**, 225–320, 1986.

[Ha83] R. Hartshone, *Algebraic geometry*, GTM 52, Springer-Verlag, 1983.

[Hi07] M. Hindry, *Why is it difficult to compute the Mordell-Weil group?*, In Diophantine Geometry Proceedings (éd. Zannier), Scuola Norm. Pisa 2007, 197–219.

[HiPa05] M. Hindry, A. Pacheco, *Sur le rang des jacobiennes sur un corps de fonctions*. Bull. Soc. Math. France **133**, 275–295, 2005.

[HiPaWa05] M. Hindry, A. Pacheco, R. Wazir, *Fibrations et conjecture de Tate*, J. Number Th. **112**, 345–368, 2005.

[HiPa10] M. Hindry, A. Pacheco, *Analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic*. Preprint, 2010.

[IwKo04] H. Iwaniec, E. Kowalski, *Analytic number theory.* Colloquium Publications. American Mathematical Society 53, 2004.

[IwLuSa00] H. Iwaniec, W. Luo, P. Sarnak, *Low lying zeroes of families of L-functions*. Publ. Math. I.H.É.S. **91**, 55–131, 2000.

[KuTs08] B. Kunyavskiĭ, M. Tsfasman, *Brauer-Siegel theorem for elliptic surfaces*, Int. Math. Res. Not. IMRN **8** , 9 pp, 2008.

[La70] S. Lang, *Algebraic number theory*, Addison-Wesley, 1970.

[Li83] S. Lichtenbaum, *Zeta functions of varieties over finite fields at $s = 1$*. Arithmetic and geometry, Vol. I, 173–194, Progr. Math., 35, Birkhäuser, 1983.

[Mi80] J. S. Milne, *Étale cohomology*, Princeton University Press, 1980.

[RaScSc88] M. Rapoport, N. Schappacher, P. Schneider, *Beilinson's conjectures and Special Values of L-Functions*, Perspectives in Mathematics, Academic Press, 1988.

[Se70] J-P. Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou 1969/70, exposé 19.

[Se65] J-P. Serre, *Zeta and L-functions*, in Arithmetic Algebraic Geometry (ed. Schilling), 8292, New York: Harper and Row, 1965.

[Sie35] C. L. Siegel. *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. **1**, 83–86, 1935.

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*. GTM 106, Springer-Verlag, 1986.

[St74] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Inv. Math. **23**, 135–152, 1974.

[Ta50] J. Tate, *Fourier Analysis in Number fields and Hexke's Zeta-Functions*, Ph.D Princeton 1950 [reproduced in *Algebraic Number Theory*, éd. Cassels, Frölich, Academic Press, 1967].

[Ta65] J. Tate, *Algebraic cycles and poles of zeta functions*, in Arithmetic Algebraic Geometry (ed. Schilling), 93110, New York: Harper and Row, 1965.

[Ta66] J. Tate, *On the Birch and Swinnerton-Dyer conjecture and a geometric analog*, Sém. Bourbaki exp. **306**, 1965/66.

[Te95] G. Tenenbaum, *Introduction à la théorie analytique et probabilistique des nombres*, *Cours Spécialisés*. Société Mathématique de France, Paris, seconde édition, 1995.

[Ts01] M. Tsfasman, *Asymptotic properties of global fields.* Mullen, Gary L. (ed.) et al., Finite fields with applications to coding theory, cryptography and related areas. Proceedings of the 6th international conference on finite fields and applications, Oaxaca, México, May 2001.

[TsVl02] M. Tsfasman, S. Vlăduţ, *Infinite global fields and the generalized Brauer-Siegel theorem.* Mosc. Math. J. **2**, 329–402, 2002.

[Ul02] D. Ulmer, *Elliptic curves with high rank over function fields*, Annals of Math. **155**, 295–315, 2002.

[Wa82] L. C. Washington, *Introduction to cyclotomic fields*, GTM Springer, 1982 .

[Zy09] A. Zykin, *On the Brauer-Siegel theorem for families of elliptic surfaces over finite fields* (in Russian), Mat. Zametki, **86**, 148-150. English translation: Math. Notes 86, 140–142, 2009.

Université Denis Diderot Paris VII, Institut de Mathématiques de Jussieu, U.F.R. Mathématiques, case 7012, 175 rue de Chevaleret, 75013 Paris, France

E-mail address: hindry@math.jussieu.fr