Axiomatic Thinking

Académie Internationale de Philosophie des Sciences

Lisbon, October 11-14, 2017

—————————

Axiomatics as a functional strategy for complex proofs: the case of Riemann Hypothesis

Jean Petitot
CAMS (EHESS), Paris

2017

Abstract

My purpose is to comment some claims of André Weil (1906-1998) in his letter of March 26, 1940 to his sister Simone, in particular the following quotation: "it is essential, if mathematics is to stay as a whole, to provide a unification, which absorbs in some simple and general theories all the common substrata of the diverse branches of the science, suppressing what is not so useful and necessary, and leaving intact what is truly the specific detail of each big problem. This is the good one can achieve with axiomatics." For Weil (and Bourbaki) the main problem was to find "strategies" for finding complex proofs of "big problems". For that, the dialectic balance between general structures and specific details is crucial. I will focus on the fact that, for these creative mathematicians, the concept of structure is a *functional* concept, which has a "strategic" creative function.

The "big problem" here is *Riemann Hypothesis* (RH). Artin, Schmidt, Hasse and Weil introduced an intermediary third world between, on the one hand, Riemann original hypothesis on the non trivial zeroes of the zeta function in analytic theory of numbers, and, on the other hand, the algebraic theory of compact Riemman surfaces. The intermediary world is that of projective curves over finite fields of characteristic $p \geq 2$. RH can be translated in this context and can be proved using sophisticated tools of algebraic geometry (divisors, Riemann-Roch theorem, intersection theory, Severi-Castelnuovo inequality) coupled with the action of Frobenius maps in characteristic $p \geq 2$. Recently, Alain Connes proposed a new strategy and constructed a new topos theoretic framework à la Grothendieck were Weil's proof could be transferred by analogy back to the original RH.

Contents

1 Axiomatics, analogies, conceptual structures

My purpose is to comment some claims of André Weil (1906-1998) in his celebrated letter [22] written in prison to his sister Simone (March 26, 1940).

Let us begin with the following quotation:

> "It is hard for you to appreciate that modern mathematics has become so extensive and so complex that it is essential, *if* mathematics is to stay as a whole and not become a pile of little bits of research, to provide a unification, which absorbs in some simple and general theories all the common substrata of the diverse branches of the science, suppressing what is not so useful and necessary, and leaving intact what is truly the specific detail of each big problem. This is the good one can achieve with axiomatics (and this is no small achievement). This is what Bourbaki is up to." (p. 341)

I want to emphasize four points:

1. the *unity* of mathematics ("to stay as a whole");
2. the axiomatization of general abstract structures; but also
3. the requirement of "leaving intact what is truly the specific detail of each big problem";
4. the emphasis on "big problems".

For Weil (and Bourbaki) the dialectic balance between *general structures* and *specific details* was crucial. A "big problem" needs a conceptually *complex* proof which is a very uneven, rough, rugged *multi*-theoretical route in a sort of "Himalayan chain" whose peaks seem inaccessible. It cannot be understood without the key thesis of the *unity* of mathematics since its deductive parts are widely scattered in the global unity of the mathematical universe. It is *holistic* and it is this holistic nature I am interested in.

As was emphasized by Israel Kleiner for Wiles' proof of the Shimura-Taniyama-Weil conjecture (leading to Fermat theorem)[1]:

> "What area does the proof come from? It is unlikely one could give a satisfactory answer, for the proof *brings together many important areas – a characteristic of recent mathematics.*"

As was also emphasized by Barry Mazur:

> "The conjecture of Shimura-Taniyama-Weil is a profoundly *unifying* conjecture – its very statement hints that we may have to look to diverse mathematical fields for insights or tools that might lead to its resolution.".

[1] For a summary of the proof, see Petitot [15].

In his letter to Simone, Weil described in natural language his moves towards *Riemann Hypothesis* and he used a lot of military metaphors to emphasize the fact that finding a proof of a so highly complex conjecture is a problem of *strategy*:

> "find an opening for an attack (please excuse the metaphor)", "open a breach which would permit one to enter this fort (please excuse the straining of the metaphor)","it is necessary to inspect the available artillery and the means of tunneling under the fort (please excuse, etc.)". (...) "It will not have escaped you (to take up the military metaphor again) that there is within all of this great problems of strategy".

My purpose is not here to discuss philosophically Bourbaki's concept of structure as mere "simple and general" abstraction. It has been done by many authors (see e.g. Leo Corry's [8] "Nicolas Bourbaki: Theory of Structures"). And many authors have also criticized the very limited Bourbaki's conception of logic.

My purpose is rather to focus on the fact that, for these outstanding creative mathematicians, the concept of "structure" is a *functional* concept, which has in general a "strategic" *creative* function. Once again, the priority is "leaving intact what is truly the specific detail of each big problem". As Dieudonné always emphasized it, the "bourbakist choice" cannot be understood without references to "big problems". It concerns the context of discovery rather than the context of justification.

There is a fundamental relation between the holistic and "organic" conception of the *unity* of mathematics and the thesis that some *analogies* can be creative and lead to essential discoveries. It is a leitmotive since the 1948 Bourbaki (alias Dieudonné) *Manifesto* [2]: "L'architecture des mathématiques". The constant insistence on the "immensity" of mathematics and on its "organic" unity, the claim that "to integrate the whole of mathematics into a coherent whole" (p. 222) is not a philosophical question as for Plato, Descartes, Leibniz or "logistics", the constant critique against the reduction of mathematics to a tower of Babel juxtaposing separed "corners", all these declarations are not vanities of elitist mathematicians. They have a very precise, strictly technical function: to construct complex proofs in navigating into this holistic conceptually coherent world.

> "The "structures" are tools for the mathematician." ([2], p. 227)

"Each structure carries with it its own language" and to discover a structure in a concrete problem

> "illuminates with a new light the mathematical landscape" (Ibid. p. 227)

In [8] Leo Corry has well formulated the key point:

> "In the "Architecture" manifesto, Dieudonné also echoed Hilbert's belief in the unity of mathematics, based both on its unified methodology and in the discovery of striking analogies between apparently far-removed mathematical disciplines." ([8], p. 304)

And indeed, Dieudonné claimed that

> "Where the superficial observer sees only two, or several, quite distinct theories, lending one another "unexpected support" through the intervention of mathematical genius, the axiomatic method teaches us to look for the deep-lying reasons for such a discovery".

It is important to understand that structures are guides for *intuition* and to overcome

> "the natural difficulty of the mind to admit, in dealing with a concrete problem, that a form of intuition, which is not suggested directly by the given elements, [...] can turn out to be equally fruitful." ([2], p. 230)

So

> "more than ever does intuition dominate in the genesis of discovery" (Ibid. p. 228)

and intuition is guided by structures.

2 Progressing through a mathematical Hymalayan chain

Any proof of Riemann Hypothesis (RH) would be highly complex and unfold in the labyrinth of many different theories. As Alain Connes explains in "*An essay on Riemann Hypothesis*" ([4] p. 2) we would have (note the strategy metaphor as in Weil)

> "to navigate between the many forms of the explicit formulas [see below] and possible strategies to attack the problem, stressing the value of the elaboration of new concepts rather than 'problem solving' ."

And here "concepts" mean "structures".

In the history of RH we meet an incredible amount of deep and heterogeneous mathematics.

1. Riemann's use of complex analysis in arithmetics: ζ-function, the duality between the distribution of primes and the localization of the non trivial zeroes of $\zeta(s)$, RH.

2. The "algebraization" of Riemann's theory of complex algebraic (projective) curves (compact Riemann surfaces) by Dedekind and Weber.

3. The transfer of this algebraic framework to the arithmetics of algebraic number fields and the interpretation of integers n as "functions" on primes p. It is the archeology of the concept of spectrum (the scheme $\mathrm{Spec}(\mathbb{Z})$).

4. The move of André Weil introducing an intermediary third world (his "Rosetta stone") between arithmetics and the algebraic theory of compact Riemann surfaces, namely the world of projective curves over *finite* fields (characteristic $p \geq 2$). The translation of RH in this context and its far reaching proof using tools of algebraic geometry (divisors, Riemann-Roch theorem, intersection theory, Severi-Castelnuovo inequality) coupled with the action of Frobenius maps in characteristic $p \geq 2$.

5. The generalization of RH to higher dimensions in characteristic $p \geq 2$. The Weil's conjectures and the formal reconstruction of algebraic geometry achieved by Grothendieck: schemes, sites, toposes, etale cohomology, etc. Deligne's proof of Weil's conjectures. Alain Connes [4] emphasized the fact that, through Weil's vision, Grothendieck's culminating discoveries proceed from RH:

   "It is a quite remarkable testimony to the unity of mathematics that the origin of this discovery [topos theory] lies in the greatest problem of analysis and arithmetic." (p. 3)

6. Connes' return to the original RH in pure arithmetics by translating algebraic geometry *à la* Grothendieck (toposes, etc.) and Weil's proof in characteristic $p \geq 2$ to the world of characteristic 1, that is, the world of *tropical geometry* and *idempotent analysis*.

3 Riemann's ζ-function

3.1 The distribution of primes

The story of RH begins with the enigma of the distribution of primes. The multiplicative structure of integers (divisibility) is awful.

For $x \geq 2$, let $\pi(x)$ be the number of primes $p \leq x$. It is a *step function* increasing of 1 at every prime p (one takes $\pi(p) = \frac{1}{2}(\pi(p_-) + \pi(p_+))$ the mean value at the jump). From Legendre (1788) and the young Gauss (1792) to Hadamard (1896) and de la Vallée Poussin (1896) it has been proved the asymptotic formula called the *prime number theorem*:

$$\pi(x) \sim \frac{x}{\log(x)} \text{ for } x \to \infty \ .$$

3.2 Definitions of $\zeta(s)$

The zeta function $\zeta(s)$ encodes *arithmetic* properties of $\pi(x)$ in *analytic* structures. Its initial definition is extremely simple and led to a lot of computations at Euler time:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

which is a series – now called a Dirichlet series – absolutely convergent for integral exponents $s > 1$. Euler already proved $\zeta(2) = \pi^2/6$ (Mengoli or Basel problem, 1735) and $\zeta(4) = \pi^4/90$.

A trivial expansion and the existence of a *unique* decomposition of any integer in a product of primes show that, in the convergence domain, the sum is equal to an infinite Euler product (Euler 1748) containing a factor for each prime p (we note $\mathcal{P}$ the set of primes):

$$\zeta(s) = \prod_{p \in \mathcal{P}} \left(1 + \frac{1}{p^s} + \dots \frac{1}{p^{ks}} + \dots\right) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}} \ .$$

The *local* ζ-functions $\zeta_p(s) = \sum_{k \geq 0} \frac{1}{p^{ks}} = \frac{1}{1-\frac{1}{p^s}}$ are the ζ-functions of the local rings $\mathbb{Z}_p$ of p-adic integers (see below section 5.4).

The ζ-function is a symbolic expression associated to the distribution of primes, which is well known to have a very mysterious structure. Its fantastic strength as a tool comes from the fact that *it can be extended by analytic continuation to a meromorphic function on the entire complex plane*. It has a simple pole at $s = 1$ with residue 1.

The prime number theorem is a consequence of the fact that $\zeta(s)$ has no zeroes on the line $1 + it$. It as been improved with better approximations by many great arithmeticians.

Instead of $\pi(x)$ one can use the Tchebychev-Mangoldt function $\psi(x)$ which counts not the number of primes $p \leq x$ but the number of powers $p^k \leq x$ of p each counted with the weight $\log(p)$:

$$\psi(x) = \sum_{p,k:\ p^k \leq x} \log(p) \quad \text{(where } \psi(x) \text{ is mean-valued at the steps).}$$

Reformulated with respect to the ψ function, the prime number theorem says that $\psi(x) \sim x$.

3.3 Mellin transform, theta function and functional equation

It was discovered by Riemann in his celebrated 1859 paper [16] "*Über die Anzahl der Primzahlen unter einer gegeben Grösse*" ("On the number of prime numbers less than a given quantity"), that $\zeta(s)$ has also beautiful properties of symmetry.

This can be made explicit noting that $\zeta(s)$ is related by a *Mellin transform* (a sort of Fourier transform) to the *theta function* which has beautiful properties of *automorphy*. Automorphy means invariance of a function $f(\tau)$ defined on the Poincaré hyperbolic half complex plane $\mathcal{H}$ (complex numbers τ of positive imaginary part $\Im(\tau) > 0$) w.r.t. to a countable subgroup of the group acting on $\mathcal{H}$ by homographies (Möbius transformations) $\gamma(\tau) = \frac{a\tau+b}{c\tau+d}$.

The theta function $\Theta(\tau)$ is defined on the half plane $\mathcal{H}$ as the series

$$\Theta(\tau) = \sum_{n\in\mathbb{Z}} e^{in^2\pi\tau} = 1 + 2\sum_{n\geq 1} e^{in^2\pi\tau}$$

$\Im(\tau) > 0$ is necessary to warrant the convergence of $\sum e^{-n^2\pi\Im(\tau)}$. $\Theta(\tau)$ is what is called a *modular form* of level 2 and weight $\frac{1}{2}$. Its automorphic symmetries are:

1. symmetry under translation: $\Theta(\tau+2) = \Theta(\tau)$ (level 2, trivial since $e^{2i\pi} = 1$ implies $e^{in^2\pi(\tau+2)} = e^{in^2\pi\tau}$);
2. symmetry under inversion: $\Theta(\frac{-1}{\tau}) = \left(\frac{\tau}{i}\right)^{\frac{1}{2}}\Theta(\tau)$ (weight $\frac{1}{2}$, proof from Poisson formula).

If $f : \mathbb{R}^+ \to \mathbb{C}$ is a complex valued function defined on the positive reals, its *Mellin transform* $g(s)$ is defined by the formula:

$$g(s) = \int_{\mathbb{R}^+} f(t) t^s \frac{dt}{t} \ .$$

Let us compute the following Mellin transform:

$$\zeta^*(s) = \frac{1}{2} g\left(\frac{s}{2}\right) = \frac{1}{2}\int_0^\infty (\Theta(it) - 1)\, t^{\frac{s}{2}} \frac{dt}{t} = \sum_{n\geq 1}\int_0^\infty e^{-n^2\pi t} t^{\frac{s}{2}} \frac{dt}{t} \ .$$

In each integral, we make the change of variable $x = n^2\pi t$. The integral becomes:

$$\int_0^\infty e^{-x} x^{\frac{s}{2}-1} \left(n^2\pi\right)^{-\frac{s}{2}+1} \left(n^2\pi\right)^{-1} dx = n^{-s}\pi^{-\frac{s}{2}} \int_0^\infty e^{-x} x^{\frac{s}{2}-1} dx \ .$$

But $\int_0^\infty e^{-x} x^{\frac{s}{2}-1} dx = \Gamma\left(\frac{s}{2}\right)$ where $\Gamma(s) = \int_0^\infty e^{-x} x^{s-1} dx$ is the *gamma function*, which is the analytic meromorphic continuation of the factorial function $\Gamma(n+1) = n!$ to the entire complex plane $\mathbb{C}$. Γ satisfies the functional equation:

$$\Gamma(s+1) = s\Gamma(s)$$

and has poles at $s \in -\mathbb{N}$. The figure 1 shows its graph along the real axis.

So, we have

$$\zeta^*(s) = \zeta(s)\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}} \ .$$

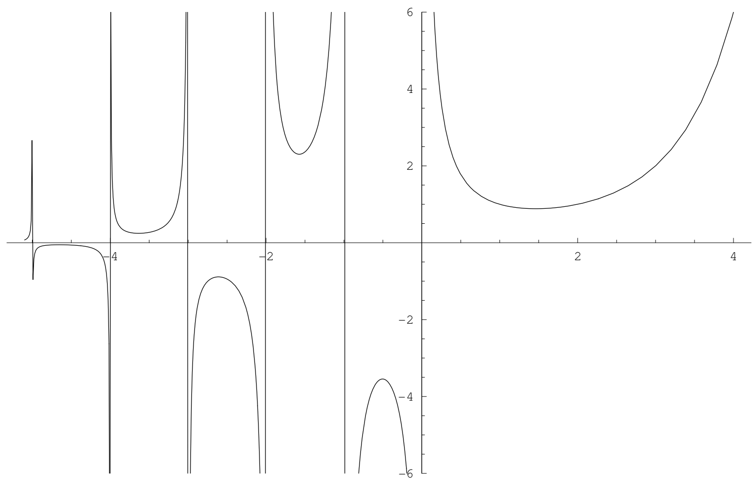

Figure 1: The Γ function on the real axis.

$\zeta^*(s)$ (often noted $\xi(s)$) is called the *total* (or "completed") ζ-function. Due to the automorphic symmetries of the theta function it satisfies a *functional equation* (symmetry w.r.t. the critical line $\Re(s) = \frac{1}{2}$)

$$\zeta^*(s) = \zeta^*(1-s)$$

As an Euler product

$$\zeta^*(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\prod_{p\in\mathcal{P}}\frac{1}{1-\frac{1}{p^s}}$$

The factor $\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)$ corresponds to what is called the "place at infinity" ∞ of $\mathbb{Q}$ (see below section 5.7) and $\zeta^*(s)$ is a product of factors associated to all the places of $\mathbb{Q}$:

$$\zeta^*(s) = \prod_{p\in\mathcal{P}\cup\{\infty\}}\zeta_p^*(s)$$

with $\zeta_p(s) = \frac{1}{1-\frac{1}{p^s}}$ for $p \in \mathcal{P}$ and $\zeta_\infty(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)$

3.4 Zeroes of $\zeta(s)$

As $\zeta(s)$ is well defined for $\Re(s) > 1$, it is also well defined, via the functional equation of ζ^*, for $\Re(s) < 0$, and the difference between the two domains comes

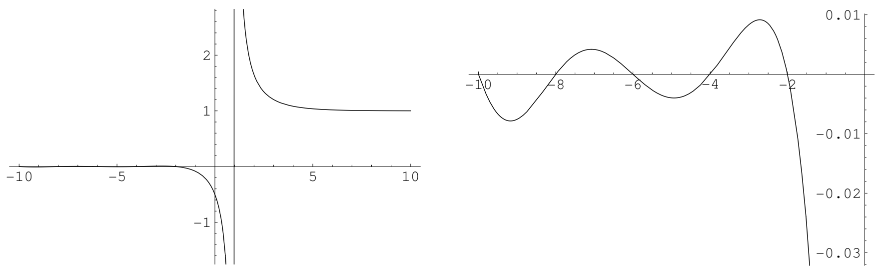

Figure 2: The graph of the zeta function along the real axis showing the pole at 1 (left). A zoom shows the trivial zeroes at even negative integers (right).

from the difference of behavior of the gamma function Γ. As ζ^* is without poles on $]1, \infty[$ (since ζ and Γ are without poles), ζ^* is also, by symmetry, without poles on $]-\infty, 0[$. So, as the $s = -2k$ are poles of $\Gamma\left(\frac{s}{2}\right)$, they must be zeroes of ζ (see figure 2). These zeroes are called "trivial zeroes".

But $\zeta(s)$ has also *non trivial* zeroes ρ, which are necessarily complex and contained in the strip $0 < \Re(s) < 1$. Due to the functional equation they are symmetric w.r.t. the critical line $\Re(s) = \frac{1}{2}$. Their distribution reflects the distribution of primes and the *localization* of these zeroes is one of the main tools for understanding the mysterious distribution of primes.

A pedagogical way for seeing the (non trivial) zeroes (J. Arias-de-Reyna) is to plot in the s plane the curves $\Re(\zeta(s)) = 0$ and $\Im(\zeta(s)) = 0$ and to look at their crossings (see figure 3).

It is traditional to write the non trivial zeroes $\rho = \frac{1}{2} + it$ with $t \in \mathbb{C}$. As they code for the irregularity of the distribution of primes, they must be irregularly distributed. But the irregularity can concern $\Re(t)$ and/or $\Im(t)$. When $\Im(t) \neq 0$ we get pairs of symmetric zeroes whose horizontal distance can fluctuate.

An enormous amount of computations from Riemann time to actual supercomputers (ZetaGrid: more than 10^{12} zeroes in 2005) via Gram, Backlund, Titchmarsh, Turing, Lehmer, Lehman, Brent, van de Lune, Wedeniwski, Odlyzko, Gourdon, and others shows that all computed zeroes lie on the critical line $\Re(s) = \frac{1}{2}$.

3.5 Riemann Hypothesis

The Riemann Hypothesis (part of 8th Hilbert problem) conjectures that *all the non trivial zeroes of $\zeta(s)$ are exactly on the critical line*, that is, are of the form $\rho = \frac{1}{2} + it$ with $t \in \mathbb{R}$ (i.e. $\Im(t) = 0$). It is an incredibly strong – still open – conjecture and an enormous part of modern mathematics has been created to solve it.

Speiser proved that RH is equivalent to the fact that all folded blue lines $\Im(\zeta(s)) = 0$ cross the critical line. One point of intersection (crossing with a red line $\Re(\zeta(s)) = 0$) is a non trivial zero and the other is called a *Gram point*.

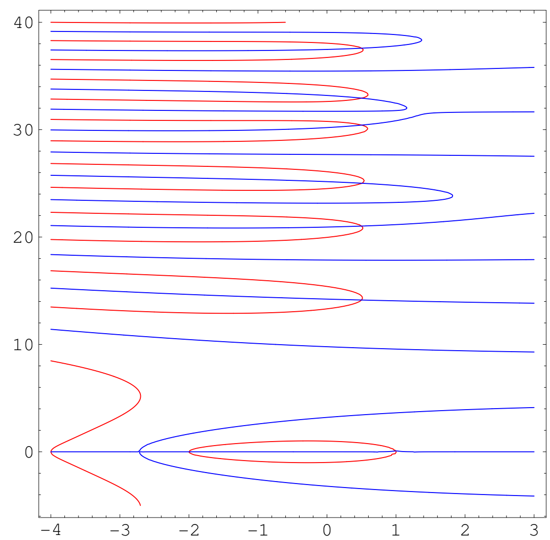

Figure 3: The null-lines of the real part (red) and the imaginary part (blue) of the zeta function.

Gram points seem to *separate* the non trivial zeroes (Gram's law), but it is not always the case. We meet actually a lot of strange configurations (see figures 4, 5).

So RH is really not evident. As noted by Pierre Cartier, the risk would be to see a pair of very close "good" zeroes bifurcate into a pair of very close symmetric "bad" zeroes.

3.6 The problem of localizing zeroes

The problem is, given the explicit definition of $\zeta(s)$, to find some informations on the *localization* of its zeroes. As was emphasized by Alain Connes, this is a wide generalization of the problem solved by Galois for polynomials (of one variable).

4 Riemann's explicit formula

One of the most "magical" results of Riemann is the *explicit and exact* formula linking explicitly and exactly the distribution of primes and the (non trivial) zeroes of $\zeta(s)$.

The idea was to factorize $\zeta(s)$ in terms of its trivial $(-2n)$ and non trivial (ρ) zeroes (all included in the left half-plane $\Re(s) < 1$) and to compare this product with the Euler product defining $\zeta(s)$ in the half-plane $\Re(s) > 1$. Riemann anticipated this possibility, which was later technically validated by Weierstrass

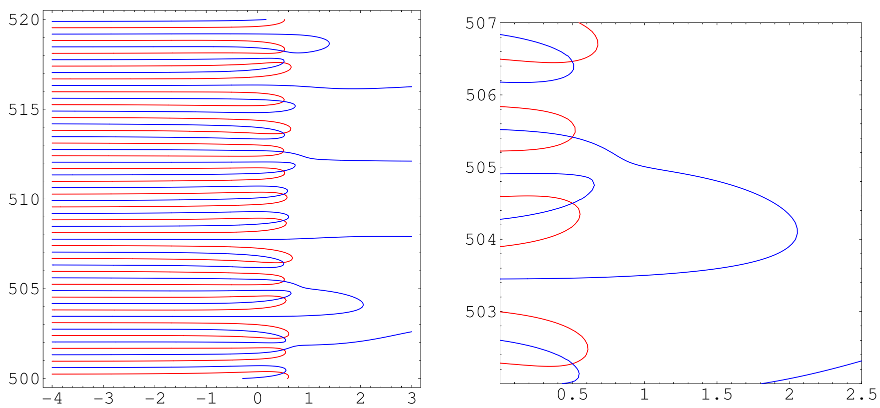

Figure 4: Configuration where a zero (crossing of folded red and blue lines) is nested. Alternating Gram→zero→Gram→zero.

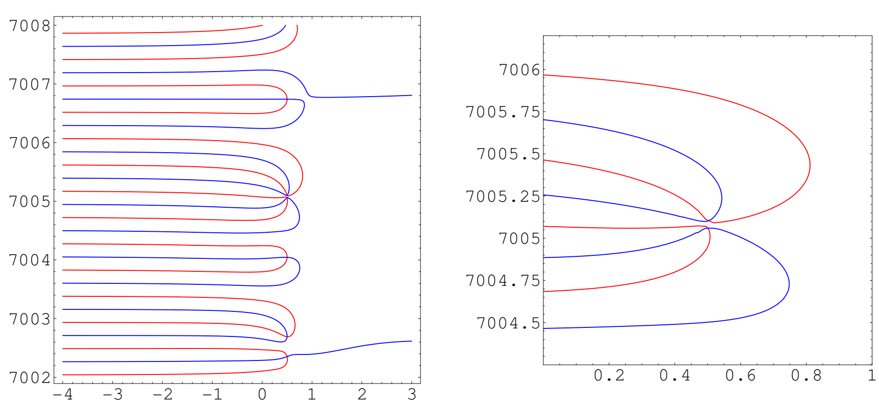

Figure 5: Lehmer's example of two extremely close consecutive zeroes *between* two Gram points. (We are at the height of the 26 830-th line)

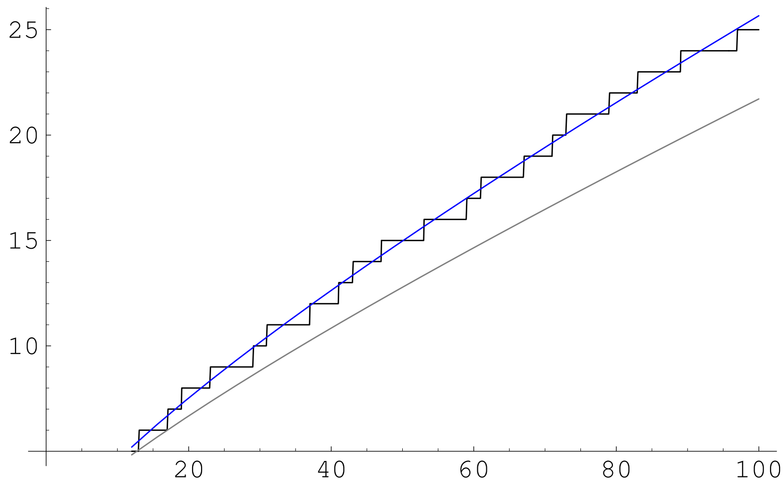

Figure 6: Two classical approximations of the distribution of primes: $\frac{x}{\log(x)}$ (in gray) and Riemann's $R(x)$ (in blue).

and Hadamard for entire functions with appropriate growth conditions. It can be shown that the entire function $(s-1)\,\zeta(s)$ satisfies these conditions and this leads to the product formula (see Paul Garrett [10]):

$$\zeta(s) = e^{a+bs} s \prod_{\rho} \left(\left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}} \right) \prod_{n \geq 1} \left(\left(1 + \frac{s}{2n}\right) e^{-\frac{s}{2n}} \right) .$$

Computations lead then to Riemann's exact explicit formula for $\pi(x)$. We have seen that, for $x \geq 2$, $\pi(x)$, the number of primes $p \leq x$, satisfies the asymptotic formula (prime number theorem) $\pi(x) \sim \frac{x}{\log(x)}$ for $x \to \infty$. A better approximation, due to Gauss (1849), is $\pi(x) \sim \mathrm{Li}(x)$ where the logarithmic integral is $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$ (for small n, $\pi(x) < \mathrm{Li}(x)$, but Littlewood proved in 1914 that the inequality reverses an infinite number of times). A still better approximation was given by a Riemann formula $R(x)$. Figure 6 shows the step function $\pi(x)$ and its two approximations $\frac{x}{\log(x)}$ (in gray) and $R(x)$ (in blue).

Let

$$f(x) = \sum_{k=1}^{k=\infty} \frac{1}{k} \pi\left(x^{\frac{1}{k}}\right) .$$

$\pi(x)$ can be retrieved from $f(x)$ by the inverse transformation (where μ is the number of prime factors of m):

$$\pi(x) = \sum_{m=1,\ m \text{ square free}}^{m=\infty} (-1)^{\mu} \frac{1}{m} f\left(x^{\frac{1}{m}}\right) \ .$$

In his 1859 paper [16], Riemann proved the following (fantastic) *explicit formula*:

$$f(x) = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}\left(x^{\rho}\right) + \int_{x}^{\infty} \frac{1}{t^2-1} \frac{dt}{t \log t} - \log 2$$

A variant of the explicit formula can be found using instead of $\pi(x)$ the Tchebychev-Mangoldt function $\psi(x)$ (see above). In this context, the formula becomes

$$\begin{aligned}\psi(x) &= \sum_{p,k:\ p^k \leq x} \log(p) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)}\right) x^s \frac{ds}{s}, \quad c > 1 \\ &= x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \log(2\pi) - \frac{1}{2} \log\left(1 - \frac{1}{x^2}\right)\end{aligned}$$

The approximation of $\pi(x)$ using Riemann's explicit formula up to the twentieth zero of $\zeta(s)$ is shown in figure 7. We see that the red curve departs from the approximation $R(x)$ and that its oscillations draw near the step function $\pi(x)$.

5 Local/global in arithmetics

Riemann's explicit formula concerns only $\zeta(s)$ and therefore only the p-adic places of $\mathbb{Q}$ (with completions $\mathbb{Q}_p$). But we know that the *structural* formulas concern $\zeta^*(s)$ with its Γ-factor and must take into account the Archimedean real place ∞ (with completion $\mathbb{R}$).

This step was accomplished by André Weil. To explain this breakthrough, let us go to the deep analogies discovered at the end of the XIXth century between arithmetics and geometry.

5.1 Dedekind-Weber analogy

One of the main idea, introduced by Dedekind and Weber in their celebrated 1882 paper [9] "*Theorie der algebraischen Funktionen einer Veränderlichen*", was to consider integers n as kinds of "polynomial functions" over the sets $\mathcal{P}$ of primes p, "functions" having a value and an order at every "point" $p \in \mathcal{P}$.

These values and orders being *local* concepts, Dedekind and Weber had to define the concept of localization in a purely *algebraic* manner. Dedekind used his concept of *ideal* he worked out to understand the "ideal numbers" introduced

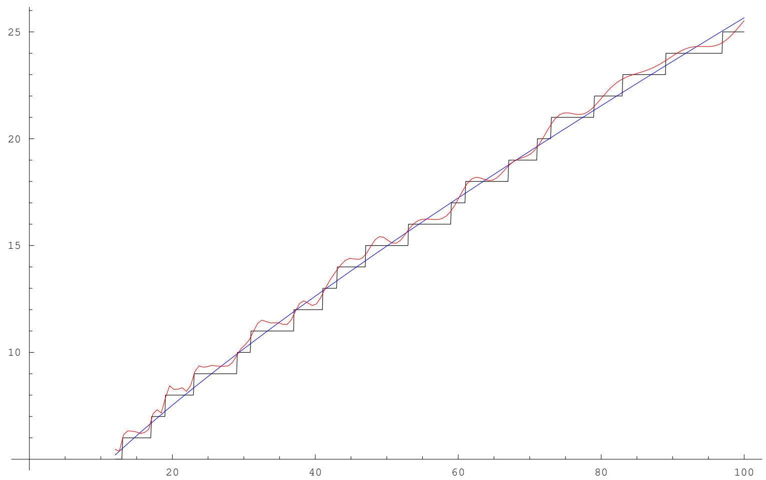

Figure 7: The approximation (red curve) of $\pi(x)$ by Riemann's explicit formula up to the twentieth zero of $\zeta(s)$.

by Kummer. If p is prime, the principal ideal $(p) = p\mathbb{Z}$ of p in $\mathbb{Z}$ is a prime (and even maximal) ideal. To localize the ring $\mathbb{Z}$ at p means to delete all the ideals $\mathfrak{a}$ that are not included into (p) and to reduce the arithmetic of $\mathbb{Z}$ to the ideals $\mathfrak{a} \subseteq (p)$.

For that, we note that if an ideal $\mathfrak{a}$ contains an invertible element then it contains 1 and is therefore trivial (improper): $\mathfrak{a} = \mathbb{Z}$. So, if we add the *inverses* of the elements of the complementary multiplicative subset S of (p), $S = \mathbb{Z} - (p)$, we "kill" all the ideals $\mathfrak{a}$ such that $\mathfrak{a} \cap S \neq \varnothing$, that is, precisely, the $\mathfrak{a} \nsubseteq (p)$. This partial quotient $\mathbb{Z}_{(p)}$ is a *local ring* ("local" means: with a *unique* maximal ideal) intermediary between $\mathbb{Z}$ and $\mathbb{Q}$ ($\mathbb{Q}$ being the localization of the prime ideal $\{0\}$).

$\mathbb{Z}_{(p)}$ is arithmetically much simpler than the *global* ring $\mathbb{Z}$ but more complicated than the global fraction field $\mathbb{Q}$ since it preserves the arithmetic structure inside (p). The maximal ideal of $\mathbb{Z}_{(p)}$ is $\mathfrak{m}_{(p)} = p\mathbb{Z}_{(p)}$ and the residue field is $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. In the local ring $\mathbb{Z}_{(p)}$ every ideal $\mathfrak{a}$ is equal to some power $(p)^k$ of (p). As $(p)^k \supset (p)^{k+1}$ we get a decreasing sequence – what is called a *filtration* – of ideals which exhausts the arithmetic of $\mathbb{Z}_{(p)}$. The successive quotients $\mathbb{Z}_{(p)}/p^{k+1}\mathbb{Z}_{(p)}$ correspond to the *expansion* of natural integers n in base p. Indeed, to make $p^{k+1} = 0$ is to approximate n by a sum $\sum_{i=0}^{i=k} n_i p^i$ with all $n_i \in \mathbb{F}_p$. These quotients constitute a "projective system" and their projective limit yields the ring $\mathbb{Z}_p$ of p-adic integers:

$$\mathbb{Z}_p = \varprojlim \frac{\mathbb{Z}}{p^k\mathbb{Z}} \ .$$

If $n \in \mathbb{Z}$, n is like a polynomial function on the "space" of primes p and to look at n "locally" at p is to look at n in the local ring $\mathbb{Z}_{(p)}$, while the "value" of n at p is its class in $\mathbb{F}_p$, i.e. n modulo p. This is the origin of the modern concept of *spectrum* in algebraic geometry, and in this perspective $\mathbb{Q}$ becomes the "global" field of "rational functions" on this "space".

5.2 Weil's description of Dedekind-Weber's analogy

In his letter to Simone, Weil describes very well Dedekind's analogy:

> "[Dedekind] discovered that an analogous principle permitted one to establish, by purely algebraic means, the principal results, called "elementary", of the theory of algebraic functions of one variable, which were obtained by Riemann by transcendental [analytic] means."

Since Dedekind's analogy is algebraic it can be applied to other fields than $\mathbb{C}$ according to the analogy:

Integers	$\longleftrightarrow$	Polynomials
Divisibility of integers	$\longleftrightarrow$	Divisibility of polynomials
Rational numbers	$\longleftrightarrow$	Rational functions
Algebraic numbers	$\longleftrightarrow$	Algebraic functions
Dedekind's "different" ideal	$\underset{\text{Hilbert}}{\longleftrightarrow}$	Riemann-Roch theorem
Abelian extensions	$\longleftrightarrow$	Abelian functions
Classes of ideals	$\longleftrightarrow$	Divisors

And Weil adds

> "At first glance, the analogy seems superficial. [...] But Hilbert went further in figuring out these matters."

5.3 Valuations and ultrametrics

Dedekind and Weber defined the *order* of $n \in \mathbb{N}$ at p using the decomposition of n into primes. If $n = \prod_{i=1}^{i=r} p_i^{v_i}$, v_i is called the *valuation* of n at p_i: $v_{p_i}(n)$. It is trivial to generalize the definition to $\mathbb{Z}$ and $\mathbb{Q}$. So the valuation $v_p(x)$ of $x \in \mathbb{Q}$ is the power of p in the decomposition of x in prime factors. It satisfies "good properties":

$$\begin{cases} v_p(0) = \infty \text{ by convention} \\ v_p(n) = 0 \text{ if } n \text{ is prime to } p \\ v_p(n/m) = v_p(n) - v_p(m) \\ v_p(xy) = v_p(x)v_p(y) \\ v_p(x+y) \geq \operatorname{Inf}(v_p(x), v_p(y)) \\ \mathbb{Z} = \{x \in \mathbb{Q} : v_p(x) \geq 0\} \\ (p) = p\mathbb{Z} = \{x \in \mathbb{Q} : v_p(x) \geq 1\} \\ (p)^k = \{x \in \mathbb{Q} : v_p(x) \geq k\} \end{cases}$$

The fundamental point is that $|x|_p = p^{-v_p(x)}$ is a *norm* on $\mathbb{Q}$ ($|0|_p = 0$ because by definition $v_p(0) = \infty$) defining a *non-Archimedean metric* $d_p(x, y) = |x - y|_p$ which satisfies the *ultrametric* property

$$|x + y|_p \leq \mathrm{Max}\left(|x|_p, |y|_p\right) \ .$$

This inequality is much stronger than the triangular inequality of classical metrics.

It must be emphasized that the ultrametricity property is non intuitive since the size of p^k become smaller and smaller as k increases and vanishes for $k = \infty$.

It must also be emphasized that the relative positions induced by the p-adic metric between the rationals change radically with p. As a set, $\mathbb{Q}$ remains the same, but as *metric spaces* the different p-adic $\mathbb{Q}$ are incommensurable.

5.4 p-adic numbers

The idea of expanding natural integers along the base p with a metric such that $\left|p^k\right|_p \underset{k\to\infty}{\longrightarrow} 0$ leads naturally to add a "point at infinity" to the localization $\mathbb{Z}_{(p)}$. This operation is a *completion* procedure for the metric $|\bullet|_p$ associated to the valuation v_p and is formalized by the concept of *p-adic number* introduced by Hensel.

We have seen that the successive rings $\frac{\mathbb{Z}}{p^k\mathbb{Z}}$ with the canonical projections $\frac{\mathbb{Z}}{p^k\mathbb{Z}} \to \frac{\mathbb{Z}}{p^\ell\mathbb{Z}}$ for $\ell > k$ constitute a projective system

$$\cdots \to \frac{\mathbb{Z}}{p^{k+1}\mathbb{Z}} \to \frac{\mathbb{Z}}{p^k\mathbb{Z}} \to \cdots \to \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p$$

where the arrows are the natural projections. $\mathbb{Z}_p$ is the projective limit

$$\mathbb{Z}_p = \varprojlim \frac{\mathbb{Z}}{p^k\mathbb{Z}}$$

The "profinite" object $\mathbb{Z}_p$ is a *local* ring with maximal ideal $p\mathbb{Z}_p$, residue field $\frac{\mathbb{Z}_p}{p\mathbb{Z}_p} = \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p$ and fraction field $\mathbb{Q}_p = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p\left(\frac{1}{p}\right)$. We have:

$$\begin{cases} \mathbb{Z}_p = \left\{x \in \mathbb{Q}_p : |x|_p \leq 1\right\} \\ \mathfrak{M}_p = p\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p : |x|_p < 1\right\} \\ \mathbb{Z}_p/\mathfrak{M}_p = \mathbb{F}_p \end{cases}$$

$\mathbb{Z}_p$ is the closure of $\mathbb{Z}_{(p)}$ in $\mathbb{Q}_p$. It is compact (due to Tychonoff theorem, in fact the maximal compact subring of $\mathbb{Q}_p$), totally discontinuous as limit of discrete structures, and is the completion of $\mathbb{Z}$ for the p-adic absolute value $|x|_p = p^{-v_p(x)}$.

For a polynomial $P(x) \in \mathbb{Z}[x]$, to have a root in $\mathbb{Z}_p$ is to have a root $\bmod p^n$ for every $n \geq 1$.

5.5 Hensel's geometric analogy

In Bourbaki's *Manifesto* [2], Dieudonné emphasizes Hensel's unifying analogy

> "where, in a still more astounding way, topology invades a region which had been until then the domain *par excellence* of the discrete, of the discontinuous, *viz.* the set of whole numbers." (p. 228)

As we have already noted, the geometrical lexicon of Hensel's analogy can be rigorously justified using the concept of *scheme*:

1. primes p are the (closed) points of the *spectrum* $\mathrm{Spec}(\mathbb{Z})$ of $\mathbb{Z}$,
2. the local rings $\mathbb{Z}_{(p)}$ are the fibers of the structural sheaf $\mathcal{O}$ of $\mathbb{Z}$,
3. the finite prime fields $\mathbb{F}_p$, are the residue fields at the points p,
4. integers n are global sections of $\mathcal{O}$, and
5. $\mathbb{Q}$ is the field of global sections of the sheaf of fractions of $\mathcal{O}$.

In this context, $\mathbb{Z}_p$ and $\mathbb{Q}_p$ correspond to the localization of global sections, analogous to what are called *germs* of sections in classical differential, analytic or algebraic geometry.

5.6 The local p-adic field

So, the *local* field $\mathbb{Q}_p$ is the completion of the *global* field $\mathbb{Q}$ for the valuation $v_p(x)$. $\mathbb{Z}$ is a subring of $\mathbb{Z}_p$ and $\mathbb{Q}$ is a dense subfield of $\mathbb{Q}_p$. A way of trying to understand the non-intuitive topology of $\mathbb{Z}_p$ is to consider that the ideal $p^n\mathbb{Z}_p$ is the closed ball of radius $\frac{1}{p^n}$.

We must note that the local p-adic field $\mathbb{Q}_p$ is of characteristic 0 while the residue field $\frac{\mathbb{Z}}{p\mathbb{Z}} = \frac{\mathbb{Z}_p}{p\mathbb{Z}_p} = \mathbb{F}_p$ is of characteristic p. The *lifting* of arithmetic properties from $\mathbb{F}_p$ to $\mathbb{Q}_p$ is a crucial problem.

We must note also that the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ is *not complete*. Its completion is $\mathbb{C}$ endowed with a non classical metric.

The ring of p-adic integers contains all the $(p-1)$ th roots of unity but in a sophisticated way. For instance, in $\mathbb{Z}_2$ we have

$$-1 = \sum_{k=0}^{k=\infty} 2^k$$

In general, the classical series $\frac{1}{1-p} = 1 + p + \cdots + p^n + \cdots$ is always convergent in $\mathbb{Z}_p$ and we can write $-1 = \frac{p-1}{1-p} = \sum_{n=0}^{n=\infty} (p-1)\, p^n$.

5.7 Places

On $\mathbb{Q}$ there exist not only the p-adic valuations of the "finite" primes p but also the real absolute value $|x|$, which can be interpreted as associated to an "infinite point" of $\mathrm{Spec}(\mathbb{Z})$ and is conventionally written $|x|_\infty$. To emphasize the geometrical point-like intuition, the finite primes and the infinite "point" are all called *places*. To work in arithmetics with *all* places is a necessity if we want to specify the analogy with projective (birational) algebraic geometry (Riemann surfaces) and transfer some of its results (as those of the Italian school of Severi, Castelnuovo, etc.) to arithmetics. Indeed, in projective geometry the point ∞ is on a par with the other points.

Weil emphasized strongly this point from the start. Already in his 1938 paper [21] "*Zur algebraischen Theorie des algebraischen Funktionen*", he explained that he wanted to reformulate Dedekind-Weber in a *birationally invariant* way. In his letter to Simone, he says

> "In order to reestablish the analogy [lost by the singular role of ∞ in Dedekind-Weber], it is necessary to introduce, into the theory of algebraic *numbers*, something that corresponds to the point at infinity in the theory of functions."

This is achieved by valuations, places and Hensel's p-adic numbers (plus Hasse, Artin, etc.). So, Weil strongly stressed the use of analogies as a *discovery method*:

> "*If one follows it in all of its consequences*, the theory alone permits us to reestablish the analogy at many points where it once seemed defective: it even permits us to discover in the number field simple and elementary facts which however were not yet seen."

5.8 Local and global fields

All the knowledge gathered during the extraordinary period initiated by Kummer in arithmetics and Riemann in geometry, led to the recognition of two great classes of fields, local fields and global fields.

In characteristic 0, local fields are $\mathbb{R}$, $\mathbb{C}$ and finite extensions of $\mathbb{Q}_p$. In characteristic p, local fields are the fields of Laurent series over a finite field $\mathbb{F}_{p^n}$ and their ring of integers are those of the corresponding power series. Local fields possess a discrete valuation v and are complete for the associated metric. Their ring of integers is local. Finite extensions of local fields are themselves local.

In characteristic 0, global fields are finite extensions $\mathbb{K}$ of $\mathbb{Q}$, i.e. algebraic number fields. In characteristic p, global fields are the fields of rational functions of algebraic curves over a finite field $\mathbb{F}_{p^n}$. The completions of global fields at their different places are local fields. They satisfy the *product formula*, where $\mathcal{V}$ is the set of places ν:

$$\prod_{\nu \in \mathcal{V}} |x|_\nu = 1 \text{ for every element } x.$$

We note a fundamental difference between the cases of characteristic 0 and p. In the later case, all structures are defined over a *common* base field, namely the prime field $\mathbb{F}_p$. It is not the case in characteristic 0 and *this lack of a common base* is one of the main reason of the difficulty of the arithmetic case. It has been overcome only very recently with the introduction of the paradoxical "field" $\mathbb{F}_1$ of characteristic 1 ! We will return to this breakthrough in the last part of this study.

6 The adelic context

André Weil was the first to understand that the natural context for the explicit formula and the RH was the *adelic* context, that is the embedding of the global field $\mathbb{Q}$ into the restricted product of its p-adic and real completions $\mathbb{Q}_p$ and $\mathbb{R}$. This method makes it possible to process all characteristics 0 and p simultaneously and in parallel.

6.1 Definition of adeles

If $\mathbb{K}$ is a global field, that is an algebraic number field or the field of rational functions of an algebraic curve over a finite field $\mathbb{F}_{p^n}$, it is embedded as a *discrete* subfield in its *ring* of *adeles* $\mathbb{A}_\mathbb{K}$, which is the *restricted* product of its completions $\mathbb{K}_\nu$ for its different places.

Note that, even when $\mathbb{K}$ is a dense subfield of its completions $\mathbb{K}_\nu$, it is nevertheless a discrete subfield of its ring of adeles $\mathbb{A}_\mathbb{K}$ because the topologies of the different $\mathbb{K}_\nu$ are incompatible. $\mathbb{A}_\mathbb{K}$ is topologically a locally compact ring (neither discrete nor compact, it is locally compact because it is a restricted product). It is also semi-simple (with trivial Jacobson radical) and $\mathbb{K}$ is cocompact in it.

According to a theorem of Iwasawa, this situation characterizes *conceptually* global fields and means that the *arithmetics* of $\mathbb{K}$ is correlated to the *analysis* of $\mathbb{A}_\mathbb{K}$. As says Alain Connes ([4], p.5),

> "it is the opening door to a whole world which is that of automorphic forms and representations, starting in the case of GL_1 with Tate's thesis (*Fourier analysis in number fields and Hecke's zeta-function*, 1950) and Weil's book (*Basic Number Theory*)."

The multiplicative group $\mathbb{A}_\mathbb{K}^\times$ of invertible elements of $\mathbb{A}_\mathbb{K}$ is the group (locally compact) of *ideles* of $\mathbb{K}$, and its quotient $C_\mathbb{K} = \mathbb{A}_\mathbb{K}^\times / \mathbb{K}^*$ by the multiplicative group $\mathbb{K}^*$ of $\mathbb{K}$ acting by multiplication is the group of *classes* of ideles of $\mathbb{K}$.

6.2 Adeles and subgroups of $\mathbb{Q}$

Let us emphasize the fact that the adeles of $\mathbb{Q}$ *parametrize the subgroups of* $(\mathbb{Q}, +)$.

It is well known that every finitely generated subgroup of $(\mathbb{Q}, +)$ is monogenic (reduce to the case of two generators $H = \left\langle \frac{m_1}{n_1}, \frac{m_2}{n_2} \right\rangle$, reduce to the commun denominator $n_1 n_2$, take the gcd d of the numerators $m_1 n_2$ and $m_2 n_1$, and apply Bezout to find $H = \frac{d}{n_1 n_2}\mathbb{Z}$).

But there are other subgroups of $(\mathbb{Q}, +)$. Let, $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ be the Pontryagin dual (the group of characters[2]) of the additive group $(\mathbb{Q}/\mathbb{Z}, +)$ (see below).

Theorem. Subgroups of $(\mathbb{Q}, +)$ are all of the form $H = H_a := \left\{ q \in \mathbb{Q} \mid aq \in \widehat{\mathbb{Z}} \right\}$ for $a \in \mathbb{A}_{\mathbb{Q}}^f$ a *finite* adele (i.e. an adele whose Archimedean component = 0). $\diamond$

This means that we take a finite set of p_j-adic numbers a_j and we take the rationals $q \in \mathbb{Q}$ such that $a_j q \in \mathbb{Z}_{p_j}$. But if a and a' are equivalent modulo $\widehat{\mathbb{Z}}^\times$ then $H_a \simeq H_{a'}$.

Theorem. The subgroups of $(\mathbb{Q}, +)$ are in bijection with the quotient $\mathbb{A}_{\mathbb{Q}}^f / \widehat{\mathbb{Z}}^\times$. ———— $\diamond$

6.3 Adeles and the dual of $\mathbb{Q}$: $\widehat{\mathbb{Q}} \simeq \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$

Another important property of adeles is the following.

We have already noted that $\widehat{\mathbb{Z}}$ is the Pontryagin dual (the group of characters) of the additive group $(\mathbb{Q}/\mathbb{Z}, +)$. Indeed, $\mathbb{Q}/\mathbb{Z} = \varinjlim \left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z}$ while $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ since if $n = \prod_i p_i^{\alpha_i}$ then $\mathbb{Z}/n\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ and $\varprojlim \prod = \prod \varprojlim$.

Now, the point is that the adeles (not necessarily finite) parametrize the characters of the additive group $(\mathbb{Q}, +)$ and are needed to define its Pontryagin dual $\widehat{\mathbb{Q}}$ of $\mathbb{Q}$. Indeed, it is well known that all the continuous characters of $(\mathbb{R}, +)$ are of the form

$$\chi_y : x \mapsto e^{-2\pi i y x}$$

For $(\mathbb{Q}, +)$ we still have these characters $\chi_y : r \mapsto e^{-2\pi i y r}$. They correspond to the Archimedean place ∞ of $\mathbb{Q}$ (that is to the local field $\mathbb{R}$).

But there exists also other characters corresponding to the finite places p of $\mathbb{Q}$ (that is to the local fields $\mathbb{Q}_p$). They are of the form

$$\chi_{a_p} : r \mapsto e^{2\pi i \{a_p r\}_p}$$

where $a_p \in \mathbb{Q}_p$ is a p-adic number and where $\{a_p r\}_p$ is the *fractional* part of $a_p r$ (the part with the negative powers $\frac{1}{p^k}$ of p). One has $\{a_p r\}_p = 0$ if $a_p r \in \mathbb{Z}_p$.

[2]Recall that the characters of a group G are the morphisms of G into the group of complex numbers $z \in \mathbb{C}$ with $|z| = 1$.

Theorem. . All the characters of $\mathbb{Q}$ (that is the dual $\widehat{\mathbb{Q}}$) are of the form

$$\chi_a = e^{-2\pi i a_\infty r} \prod_p e^{2\pi i \{a_p r\}_p}$$

with $a_\infty \in \mathbb{Q}$, $a_p \in \mathbb{Q}_p$ and $a_p \in \mathbb{Z}_p$ for almost every p. ——— $\diamond$

This means that the characters of $\mathbb{Q}$ are parametrized by the adeles $a \in \mathbb{A}_\mathbb{Q}$.

Now, $\mathbb{Q} \hookrightarrow \mathbb{A}_\mathbb{Q}$, $s \longmapsto (s, \ldots s)$ (rational adeles). But if s is a rational adele, then $\chi_s = 1$.Indeed, $\chi_s = e^{2\pi i \left(-sr + \sum_p \{sr\}_p\right)}$ and, as $sr \in \mathbb{Q}$, $-sr + \sum_p \{sr\}_p$ is an *integer*. So:

Theorem. $\widehat{\mathbb{Q}} \simeq \mathbb{A}_\mathbb{Q}/\mathbb{Q}$. ——— $\diamond$

6.4 Weil's adelic explicit formula

Weil translated Riemann's explicit formula in the adelic context of the global field $\mathbb{Q}$.

He considered test functions $h(u) : C_\mathbb{Q} \to \mathbb{R}_+$ where $h(u) = h(|u|) := |u|^{\frac{1}{2}} F(|u|)$ for $F(t)$ defined on $[1, \infty)$ (i.e. F is defined on $\mathbb{R}$ but $F \equiv 0$ on $(-\infty, 1[)$. We have $h(u) = 0$ for $|u| < 1$.

For technical reasons (convergence, etc.), one must assume that F is smooth except for a finite number of "good" steps where it is mean-valued and decreases more rapidly than $\frac{1}{\sqrt{t}}$ at infinity.

Be careful that the u are classes of ideles and that their module $|u|$ is complicated, while x is a mere positive real.

Let $\widehat{h}(s) = \int h(u) |u|^s \frac{du}{u}$ be the "symbolic" Mellin transform of h, which corresponds to $\widehat{F}\left(s - \frac{1}{2}\right)$ with $\widehat{F}(s) = \int_1^\infty F(t) t^s \frac{dt}{t}$ the Mellin transform of F.

Riemann-Weil formula is (with p-adic integrals and $\int'$ meaning normalized principal value)

$$\widehat{h}(0) + \widehat{h}(1) - \sum_\rho \widehat{h}(\rho) = \sum_\nu \int'_{\mathbb{Q}_\nu^*} \frac{h\left(u^{-1}\right)}{|1-u|_\nu} \frac{du}{u}$$

For the finite places p, one finds

$$\int'_{\mathbb{Q}_\nu^*} \frac{h\left(u^{-1}\right)}{|1-u|_\nu} \frac{du}{u} = \sum_{p^k, p \text{ given}} \log(p) p^{-\frac{k}{2}} F\left(p^k\right)$$

Indeed, $h(u) = h(|u|)$ depends only on the module $|u|$ and presupposes $|u| > 1$.

So, in the in the $\int'_{\mathbb{Q}_\nu^*}$ integral, we must have $\left|u^{-1}\right| > 1$ and therefore $|u| < 1$.

But in $\mathbb{Q}_p^*$, $|u| < 1$ implies $|1 - u| = 1$ and the integral is $\int'_{\mathbb{Q}_p^*} \frac{1}{|u|^{\frac{1}{2}}} F\left(|u|^{\frac{1}{2}}\right) \frac{du}{u}$.

For the Archimedean place ∞, one finds

$$\begin{aligned}\int_{\mathbb{R}^*} \frac{h\left(u^{-1}\right)}{|1-u|} \frac{du}{u} &= \int_{\mathbb{R}^*} \frac{h(u)}{|1-u^{-1}|} \frac{du}{u} \\ &= \frac{1}{2} \int_1^{\infty} \left(\frac{h(t)}{|1-t^{-1}|} + \frac{h(t)}{|1+t^{-1}|} \right) \frac{dt}{t} \\ &= \int_1^{\infty} \frac{t^{\frac{3}{2}} F(t)}{(t^2-1)} \frac{dt}{t}\end{aligned}$$

If we convert the h formula into a F formula, we find:

$$\begin{aligned}& \widehat{F}\left(-\frac{1}{2}\right) + \widehat{F}\left(\frac{1}{2}\right) - \sum_{\rho} \widehat{F}\left(\rho - \frac{1}{2}\right) \\ = & \sum_{p^k} \log(p)\, p^{-\frac{k}{2}} F\left(p^k\right) + \int_1^{\infty} \frac{t^{\frac{3}{2}} F(t)}{(t^2-1)} \frac{dt}{t} \\ & + F(1) \left(\frac{1}{2} (\log(\pi) + \gamma) - \int_1^{\infty} \frac{1}{(t^2-1)} \frac{dt}{t} \right)\end{aligned}$$

7 The RH for elliptic curves over $\mathbb{F}_q$

One of the greatest achievements of Weil has been the *proof* of RH for the global fields in characteristic p, namely the global fields $\mathbb{K}/\mathbb{F}_q(T)$ of rational functions on an algebraic curve defined over a finite field $\mathbb{F}_q$ of characteristic p ($q = p^n$), that is finite algebraic extensions of $\mathbb{F}_q(T)$.

7.1 The "Rosetta stone"

The main difficulty was that in Dedekind-Weber's analogy between arithmetics and the theory of Riemann surfaces, the latter is "too rich" and "too far from the theory of numbers". So

> "One would be totally obstructed if there were not a bridge between the two." (p. 340)

Hence the celebrated metaphor of the "Rosetta stone":

> "my work consists in deciphering a trilingual text; of each of the three columns I have only disparate fragments; I have some ideas about each of the three languages: but I know as well there are great differences in meaning from one column to another, for which nothing has prepared me in advance. In the several years I have worked at it, I have found little pieces of the dictionary." (p. 340)

From the algebraic number theory side, one can transfer the Riemann-Dirichlet-Dedekind ζ and L-functions (Artin, Schmidt, Hasse) to the algebraic curves over $\mathbb{F}_q$. In this third world they become rational functions (quotients of *polynomials*), a fact which simplifies tremendously the situation.

7.2 The Hasse-Weil function

For the history of the ζ-function of curves over $\mathbb{F}_q$, see Peter Roquette's extremely detailed historical study [17] "*The Riemann hypothesis in characteristic p. Its origin and development*" and Pierre Cartier's 1993 survey [3] "*Des nombres premiers à la géométrie algébrique (une brève histoire de la fonction zeta)*".

1. On the *arithmetic* side (spec($\mathbb{Z}$), $\mathbb{Q}_p$, etc.), we have RH.
2. On the geometric side, we have the theory of compact Riemann surfaces (projective algebraic curves over $\mathbb{C}$).

On the *intermediary* level, at the beginning of the XX-th century Emil Artin (thesis, 1921 published in 1924, [1]) and Friedrich Karl Schmidt (1931, [18]) formulated the RH no longer for global number fields $\mathbb{K}/\mathbb{Q}$ but for global fields of functions $\mathbb{K}/\mathbb{F}_q(T)$. As Cartier says,

> "Artin-Schmidt theory is developing in parallel with that of Dirichlet-Dedekind, and seeks to mimic the already achieved results: definition by means of a Dirichlet series and Euler product, functional equation, analytic prolongation.[3]" (p. 61)

The main challenge was to interpret *geometrically* the zeta-function $\zeta_C(s)$ for algebraic curves C defined over $\mathbb{F}_q$. A key point was to understand that ζ_C was a *counting function*, counting the (finite) number $N(q^r)$ of points of C rational over the successive extensions $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$: C being defined over $\mathbb{F}_q$, all its points are with coordinates in $\overline{\mathbb{F}_q}$, and we can therefore look at its points with coordinates in intermediary extensions $\mathbb{F}_q \subset \mathbb{F}_{q^r} \subset \overline{\mathbb{F}_q}$.

The generating function of the $N(q^r)$ is by definition

$$Z_C(T) := \exp\left(\sum_{r\geq 1} N(q^r)\frac{T^r}{r}\right)$$

and the Hasse-Weil function $\zeta_C(s)$ of C is defined as

$$\zeta_C(s) := Z_C\left(q^{-s}\right) \; .$$

[3]La théorie d'Artin-Schmidt se développe donc en parallèle avec celle de Dirichlet-Dedekind, et elle s'efforce de calquer les résultats acquis : définition par série de Dirichlet et produit eulérien, équation fonctionnelle, prolongement analytique.

Note that

$$T\frac{Z_C'(T)}{Z_C(T)} = \sum_{r\geq 1} N(q^r)\, T^r \ .$$

$\zeta_C(s)$ will correspond to the two expressions of the classical Riemann's ζ-function (Dirichlet series and Euler product) if one transfers the classical concept of a *divisor* D on C (see below section 7.3) as a finite $\mathbb{Z}$-linear combination of points of C: $D = \sum_j a_j x_j$. The *degree* of D is defined as $\deg(D) = \sum_j a_j$ and D is said to be *positive* ($D \geq 0$) if all $a_j \geq 0$. Then

$$\zeta_C(s) = \sum_{D>0} \frac{1}{N(D)^s} = \prod_{P>0} \left(1 - N(D)^{-s}\right)^{-1},$$

where the D are positive divisors on $\mathbb{F}_q$-points, the P are prime positive divisors (i.e. P is not the sum of two smaller positive divisors) and the "norm" $N(D)$ is $N(D) = q^{\deg(D)}$.

The key problem is, as before, the *localization* of the zeroes of $\zeta_C(s)$. If ρ is a zero, $q^{-\rho}$ is a zero of Z_C. Conversely, if $q^{-\rho}$ is a zero and if $\rho' = \rho + k\frac{2\pi i}{\log(q)}$, then $q^{-\rho'} = q^{-\rho}$ is also a zero. So the zeroes of the Hasse-Weil function $\zeta_C(s)$ come in *arithmetic progressions*, which is a fundamentally new phenomenon.

7.3 Divisors and RR for curves

In the other direction, one try to transfer to curves over $\mathbb{F}_q$ the results of the theory of Riemann compact surfaces as curves over $\mathbb{C}$, and in particular the *Riemann-Roch theorem*.

If C is a compact Riemann surface of genus g, to deal with the distribution and the orders of zeroes and poles of meromorphic functions on C, one introduced the concept of a *divisor* D on C as a $\mathbb{Z}$-linear combination of points of C: $D = \sum_{x\in C} \operatorname{ord}_x(D)x$ with $\operatorname{ord}_x(D) \in \mathbb{Z}$ the order of D at x. All the terms vanish except a finite number of them. The *degree* of D is then defined as $\deg(D) = \sum_{x\in C} \operatorname{ord}_x(D)$. It is additive. D is said to be *positive* ($D \geq 0$) if $\operatorname{ord}_x(D) \geq 0$ at every point x.

By construction, divisors form an additive group $\operatorname{Div}(C)$, but $\operatorname{Div}(C)$ conveys very little information about the specific geometry of C. Yet, if f is a meromorphic function on C, poles of order k can be considered as zeroes of order $-k$ and the divisor $(f) = \sum_{x\in C} \operatorname{ord}_x(f)x$ is called *principal*. Due to a fundamental property of meromorphic functions on compact Riemann surfaces (a consequence of Liouville theorem), its degree vanishes: $\deg(f) = \sum_{x\in C} \operatorname{ord}_x(f) = 0$. As the meromorphic functions contitute a field $K(C)$ having the property that the order of a product is the sum of the orders, principal divisors constitute a subgroup $\operatorname{Div}_0(C)$. The quotient group $\operatorname{Pic}(C) = \operatorname{Div}(C)/\operatorname{Div}_0(C)$, that is the group of classes of divisors modulo principal divisors, is called the *Picard group* of C. It encodes a lot of information about the *specific* geometry of C

If ω and ω' are two meromorphic differential 1-forms on C, $\omega' = f\omega$ for some $f \in K(C)^* = K(C) - \{0\}$ (the set of invertible elements of $K(C)$), $\mathrm{div}(\omega') = \mathrm{div}(\omega)+(f)$ and therefore the class of $\mathrm{div}(\omega) \bmod (\mathrm{Div}_0(C))$ is *unique*: it is called the *canonical class* of C and one can show that its degree is $\deg(\omega) = 2g-2$.

For instance, if $g = 0$, C is the Riemann sphere $\widehat{\mathbb{C}}$ and the standard 1-form is $\omega = dz$ on the open subset $\mathbb{C}$. Since to have a local chart at infinity we must use the change of coordinate $\xi = \frac{1}{z}$ and since $d\xi = -\frac{dz}{z^2}$, we see that, on $\widehat{\mathbb{C}}$, ω possesses no zero and a single double pole at infinity. Hence $\deg(\omega) = -2 = 2g-2$.

For $g = 1$ (elliptic case) $\deg(\omega) = 0$ and there exist holomorphic nowhere vanishing 1-forms. As $C \simeq \mathbb{C}/\Lambda$ (Λ a lattice), one can take $\omega = dz$.

To any divisor D one can associate what is called a *linear system*, that is the set of meromorphic functions on C whose divisor (f) is greater than $-D$:

$$L(D) = \{f \in K(C)^* : (f) + D \geq 0\} \cup \{0\} \ .$$

Since a holomorphic function on C is necessarily constant (Liouville theorem), we have $L(0) = \mathbb{C}$. One of the most fundamental theorem of Riemann's theory is the theorem due to himself and his disciple Gustav Roch:

Riemann-Roch theorem. $\dim L(D) = \deg(D) + \dim L(\omega - D) - g + 1$. $\diamond$

If $\dim L(D)$ is noted $\ell(D)$, we get

$$\ell(D) - \ell(\omega - D) = \deg(D) - g + 1 \ .$$

Corollary. $\ell(\omega) = 2g - 2 + 1 - g + 1 = g$ (since $\ell(0) = 1$). ____________ $\diamond$

A very important conceptual improvement of RR is due to Pierre Cartier in the 1960s using the new tools of *sheaf theory* and *cohomology*. Let $\mathcal{O} = \mathcal{O}_C$ be the structural sheaf of rings $\mathcal{O}(U)$ of holomorphic functions on the open subsets U of C, and $\mathcal{K} = \mathcal{K}_C$ the sheaf of fields $\mathcal{K}(U)$ of meromorphic functions. To any divisor D, Cartier was able to associate a line bundle on C with a sheaf of sections $\mathcal{O}(D)$. Then he proved that the $\mathbb{C}$-vector space of global sections of $\mathcal{O}(D)$ can be identified with $L(D)$, i.e. $L(D) = H^0(C, \mathcal{O}(D))$. This *cohomological* interpretation is fundamental and allows a deep "conceptual" cohomological interpretation of RR using the fact that $\dim L(D) = \dim H^0(C, \mathcal{O}(D))$.

7.4 Divisors and RR for surfaces

For surfaces S over $\mathbb{C}$, RR is more involved. Divisors are now $\mathbb{Z}$-linear combinations no longer of points but of curves C_i. One has to use what is called the *intersection number* of two curves $C_1 \bullet C_2$ (and of divisors $D_1 \bullet D_2$). For two curves *in general position*, one defines $C_1 \bullet C_2$ in an intuitive way as the sum of the points of intersection, and one shows that, as the base field $\mathbb{C}$ is algebraically closed, this number is invariant by linear equivalence $D_1 \sim D_2$.

One shows also that for any divisors D_1 and D_2, even when $D_1 = D_2$, there exist $D_1' \sim D_1$ and $D_2' \sim D_2$ which are in general position, and one then defines $D_1 \bullet D_2$ by $D_1 \bullet D_2 = D_1' \bullet D_2'$.

The RR theorem is then

$$\sum_{j=0}^{j=2} (-1)^j \dim H^j(S, \mathcal{O}(D)) = \frac{1}{2} D \bullet (D - K_S) + \chi(S)$$

with $\chi(S) = 1 + p_a$, p_a being the “arithmetic genus”.

What is called *Serre duality* says that

$$\dim H^2(S, \mathcal{O}(D)) = \dim H^0(S, \mathcal{O}(K_S - D)) \ .$$

Now, $\dim H^0$ and $\dim H^2$ are ≥ 0 while $-\dim H^1$ is ≤ 0, so one gets the RR *inequality* :

$$\ell(D) + \ell(K_S - D) \geq \frac{1}{2} D \bullet (D - K_S) + \chi(S) \ .$$

7.5 RR for curves over $\mathbb{F}_q$

From Artin to Weil, the theory of compact Riemann surfaces has been transferred to the intermediary case of the curves C over $\mathbb{F}_q$. In particular, Schmidt and Hasse transferred the Riemann-Roch theorem. A fundamental consequence was that $Z_C(T)$ not only satisfies a *functional equation* but is alsoa *rational function* of T.

For instance, let us consider the simplest case $\mathbb{K} = \mathbb{F}_q(T)$ (analogous to the simplest number field $\mathbb{Q}$). Each unitary polynomial $P(T) = T^m + a_1 T^{m-1} + \ldots + a_m$ of degree m gives a contribution $(q^m)^{-s}$ to the additive (Dirichlet) formulation of $Z_{\mathbb{K}}(T)$ since the norm $q^{\deg(P)}$ of its ideal is q^m. But there are q^m such polynomials since the m coefficients a_j belong to $\mathbb{F}_q$ which is of cardinal q. So

$$\begin{cases} \zeta_{\mathbb{K}}(s) = \sum_{m=0}^{m=\infty} q^m (q^m)^{-s} = \frac{1}{1-q^{1-s}} \\ Z_C(T) = \frac{1}{1-qT}. \end{cases}$$

Hence, as $Z_C(T)$ is a rational function of T, it has a *finite* number of zeroes $t_1, \ldots, t_M$ and therefore, the zeroes of $\zeta_C(s)$ are organized in a *finite number of arithmetic progressions* $\rho_j + k\frac{2\pi i}{\log(q)}$ with $q^{-\rho_j} = t_j$. *This is a fundamental difference with the arithmetic case, which makes the proof of RH much easier.*

7.6 The Frobenius morphism

In the $\mathbb{F}_q$ case, a completely original phenomenon appears. Indeed, a fundamental property of any finite field $\mathbb{F}_q$ is that $x^q = x$ for every element x. So, one can consider the *automorphism* φ_q of $\overline{\mathbb{F}_q}$, $\varphi_q : x \mapsto x^q$ (it is an automorphism) and retrieve $\mathbb{F}_q$ as the field of *fixed points* of φ_q. φ_q is called the *Frobenius* morphism.

For a curve $C/\mathbb{F}_q$, the Frobenius φ_q acts, for every r, on the set of points $C(\mathbb{F}_{q^r})$ with coordinates in $\mathbb{F}_{q^r}$, and the number $N_r = N(q^r)$ of points of C

rational over $\mathbb{F}_{q^r}$ is *the number of fixed points* of the Frobenius φ_{q^r}. So, the generating counting function $Z_C(T)$ counts fixed points and has to do with the world of *trace formulas* counting fixed points of maps. In particular, $N_1 = C(\mathbb{F}_q) = \#\varphi_q^{\text{Fix}} = \left|Ker\left(\varphi_q - Id\right)\right|$. It is like a "norm".

7.7 RH for elliptic curves (Schmidt and Hasse)

Schmidt (see [18]) was the first to add the point at infinity (as for projective curves and compact Riemann surfaces) and to understand that, in the case of $\mathbb{K}/\mathbb{F}_q(T)$, the functional equation of ζ_C was correlated to the duality between divisors D and $D-K$ in Riemann's theory. As Cartier [3] says

> "we meet here one of the first manifestation of the trend towards a geometrization in the study of the ζ function.[4]" (p. 69)

Schmidt proved that

$$Z_C(T) = \frac{L(T)}{(1-T)(1-qT)}$$

with $L(T)$ a polynomial of degree $2g$. The fact that Z_C is a *rational* function corresponds to the fact that Riemann's ζ function is a meromorphic function.

For instance, if we come back to the simple case of $\mathbb{K} = \mathbb{F}_q(T)$ and look at its projective extension $\mathbb{P}$ of genus $g=0$ by adding the point ∞, we must add this point to the q^m other points and, using the fact that $\exp\left(\sum_{m\geq 1}\frac{T^m}{m}\right) = \frac{1}{(1-T)}$, we get

$$\begin{cases} Z_{\mathbb{P}}(T) & = \exp\left(\sum_{m\geq 1}(q^m+1)\frac{T^m}{m}\right) \\ & = \left(\exp\left(\sum_{m\geq 1} q^m \frac{T^m}{m}\right)\right)\left(\exp\left(\sum_{m\geq 1}\frac{T^m}{m}\right)\right) \\ & = \frac{1}{(1-T))(1-qT)} \\ & \\ \zeta_{\mathbb{P}}(s) & = \frac{1}{(1-q^{-s})(1-q^{1-s})} \end{cases}$$

with $L(T) = 1$ a polynomial of degree 0.

Schmidt showed moreover that $L(T)$ is, in fact, the *characteristic polynomial* of the Frobenius φ_q, i.e. the "norm" (the determinant) of $Id - T\varphi_q$. So

$$Z_C(T) = \frac{\det\left(Id - T\varphi_q\right)}{(1-T)(1-qT)}$$

and $Z_C(T)$ satisfies the *functional equation*

[4] "On voit se manifester ici l'une des premières apparitions de la tendance à la géométrisation dans l'étude de la fonction ζ."

$$Z_C\left(\frac{1}{qT}\right)=q^{1-g}T^{2-2g}Z_C(T)$$

while for ζ_C the symmetric functional equation is

$$q^{(g-1)s}\zeta_C(s)=q^{(g-1)(1-s)}\zeta_C(1-s)$$

$T\to\frac{1}{qT}$ corresponding to the symmetry $s\to 1-s$.

Then, in three fundamental papers of 1936 "*Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II, III*" [11], Hasse proved RH for *elliptic curves*. As $g=1$, $L(T)$ is a polynomial of degree 2. And as C is elliptic, it has a *group* structure (C is isomorphic to its Jacobian $J(C)$), which is used as a crucial feature in the proof. Indeed, one can consider the *group* endomorphisms $\psi : C\to C$ and their graphs Ψ in $C\times C$, what Hasse called *correspondences*.

For $g=1$, $Z_C(T)$ satisfies the functional equation

$$Z_C\left(\frac{1}{qT}\right)=Z_C(T)$$

and ζ_C the symmetric functional equation

$$\zeta_C(s)=\zeta_C(1-s)$$

as Riemann's arithmetic ζ.

Then, Hasse proved that, due to the functional equation, $L(T)$ is the polynomial $L(T)=1-c_1T+qT^2$ with

$$L(1)=1-c_1+q=N_1=|C(\mathbb{F}_q)|\ .$$

So

$$L(T)=(1-\omega T)(1-\overline{\omega}T)$$

with $\omega\overline{\omega}=q$ and $\omega+\overline{\omega}=c_1$ the *inverses* of the zeroes since

$$L(T)=\omega\overline{\omega}\left(T-\frac{1}{\omega}\right)\left(T-\frac{1}{\overline{\omega}}\right)\ .$$

As $|\omega|=|\overline{\omega}|$, we have $|\omega|=\sqrt{q}$. But, since $\zeta_C(s)=Z_C(q^{-s})$, the zeroes of $\zeta_C(s)$ correspond to $q^{-s_j}=(\omega_j)^{-1}$. So we must have

$$\left|q^{-s_j}\right|=|q|^{-\Re(s_j)}=q^{-\Re(s_j)}=\frac{1}{|\omega_j|}=\frac{1}{\sqrt{q}}=q^{-\frac{1}{2}}$$

and $\Re(s) = \frac{1}{2}$. *Hence, the RH for elliptic curves over* $\mathbb{F}_q$.

We can rewrite RH in a way easier to generalize. One has $|C(\mathbb{F}_q)| - q - 1 = -c_1$ with $c_1 = \omega + \overline{\omega} = 2\Re(\omega)$. But $\omega = \sqrt{q}e^{i\alpha}$ and therefore $\Re(\omega) = \sqrt{q}\cos(\alpha)$. So $c_1 = 2\sqrt{q}\cos(\alpha)$ and RH is equivalent to

$$||C(\mathbb{F}_q)| - q - 1| \leq 2q^{\frac{1}{2}} \ .$$

8 Weil's "conceptual" proof of RH

To tackle the case $g > 1$, Weil had to take into account that C is no longer isomorphic to its Jacobian. For a description of Weil's proof, see e.g. James Milne's paper [14] "*The Riemann Hypothesis over finite fields from Weil to the present day*" (2015). See also Marc Hindry [12].

Weil worked over $\overline{\mathbb{F}_q}$ (to have a good intersection theory) and in the *square* $S = \overline{C} \times \overline{C}$ of the curve C extended to $\overline{\mathbb{F}_q}$. He used the graph Φ_q of the Frobenius φ_q on $\overline{\mathbb{F}_q}$, which is a divisor of the surface $S = \overline{C} \times \overline{C}$. As the $\mathbb{F}_q$-points of C, i.e. $C(\mathbb{F}_q)$, are the *fixed* points of φ_q, their number is the intersection number: $\Phi_q \bullet \Delta$ where Δ is the *diagonal* of $S = \overline{C} \times \overline{C}$.

Then Weil transferred to this $\overline{C}$ Hurwitz trace formula (1887), which says that, for a Riemann surface $\overline{C}$ and a divisor Φ in $S = \overline{C} \times \overline{C}$ associated to a map $\varphi : \overline{C} \to \overline{C}$, one has:

$$\begin{aligned} \Phi \bullet \Delta &= \operatorname{Tr}\left(\varphi \mid H_0\left(\overline{C}, \mathbb{Q}\right)\right) - \operatorname{Tr}\left(\varphi \mid H_1\left(\overline{C}, \mathbb{Q}\right)\right) \\ &\quad + \operatorname{Tr}\left(\varphi \mid H_2\left(\overline{C}, \mathbb{Q}\right)\right) \ . \end{aligned}$$

Here this formula implies that:

$$\begin{aligned} \Phi_q \bullet \Delta &= \Phi_q \bullet \xi_1 - \operatorname{Tr}\left(\varphi_q \mid H_1\left(\overline{C}\right)\right) + \Phi_q \bullet \xi_2 \\ &= 1 - \operatorname{Tr}\left(\varphi_q \mid H_1\left(\overline{C}\right)\right) + q \end{aligned}$$

with $\xi_1 = e_1 \times \overline{C}$ and $\xi_2 = \overline{C} \times e_2$ (e_j points of $\overline{C}$).

If one considers the symmetric quadratic intersection form $s(D, D') = D \bullet D'$, one notes that $\xi_1 \bullet \xi_1 = \xi_2 \bullet \xi_2 = 0$ (the ξ_j are isotropic) and $\xi_1 \bullet \xi_2 = 1$ (it is exactly the reverse of orthonormality).

The key point is that, in this geometric context, RH for curves over $\mathbb{F}_q$ is equivalent to the *negativity condition* $D \bullet D \leq 0$ for all divisors D of degree $= 0$. And this is equivalent to the *Castelnuovo-Severi inequality* for *every* divisor D :

$$D \bullet D \leq 2(D \bullet \xi_1)(D \bullet \xi_2) \ .$$

Indeed, let

$$\operatorname{def}(D) = 2(D \bullet \xi_1)(D \bullet \xi_2) - D \bullet D = 2d_1d_2 - D \bullet D \geq 0$$

be what Severi called the "defect" of the divisor D. Writing def $(mD + nD') \geq 0$ for all m, n, we find

$$|D \bullet D' - d_1 d_2' - d_1' d_2| \leq (\mathrm{def}\,(D)\,\mathrm{def}\,(D'))^{\frac{1}{2}} \ .$$

If we apply this to the Frobenius divisor Φ_q when $\overline{C}$ has genus g, and use the fact that $d_1 = \Phi_q \bullet \xi_1 = 1$ and $d_2 = \Phi_q \bullet \xi_2 = q$, we can compute def $(\Phi_q) = 2gq$ and def $(\Delta) = 2g$. So we get

$$|\Phi_q \bullet \Delta - q - 1| \leq 2gq^{\frac{1}{2}} \ .$$

But, as $\Phi_q \bullet \Delta = \left|\overline{C}\,(\mathbb{F}_q)\right|$, one has

$$\left|\left|\overline{C}\,(\mathbb{F}_q)\right| - q - 1\right| \leq 2gq^{\frac{1}{2}}$$

which proves RH for genus g.

It is to prove Castelnuovo-Severi inequality that RR enters the stage with the inequality

$$\ell(D) - \ell(K_S - D) \geq \frac{1}{2} D \bullet (D - K_S) + \chi\,(S) \ .$$

Indeed, let us suppose $D \bullet D > 0$.

1. One then uses RR to show that after some rescaling $D \rightsquigarrow nD$ we must have $\ell(nD) > 1$. So one can suppose $\ell(D) > 1$.

2. Now it can be shown that if $\ell(D) > 1$, then D is linearly equivalent to $D' > 0$. One can therefore suppose $D > 0$.

3. Then one shows that this implies the positivity $(D \bullet \xi_1) + (D \bullet \xi_2) > 0$. So $D \bullet \xi_1$ and $D \bullet \xi_2$ cannot vanish at the same time (D cannot be orthogonal to both the ξ_j).

4. One then applies Castelnuovo-Severi lemma saying that if, for every D s.t. $D \bullet D > 0$, $D \bullet \xi_1$ and $D \bullet \xi_2$ cannot vanish at the same time then for any divisor D

$$D \bullet D \leq 2\,(D \bullet \xi_1)\,(D \bullet \xi_2) \ .$$

9 Connes' strategy : "a universal object for the localization of L functions"

9.1 Come back to arithmetics

To summarize: Weil introduced an intermediate world, the world of curves over finite fields $\mathbb{F}_q$. He reformulated the RH in this new framework and used tools inspired by algebraic geometry and cohomology over $\mathbb{C}$ to prove it.

It is well known that the generalization of this result to *higher dimensions* led to his celebrated conjectures and that the strategy for proving them has been at the origin of the monumental programme of Grothendieck (schemes, sites, toposes, etale cohomology). But after Deligne's proof of Weil's conjectures in 1973 the original RH remained unbroken.

Some years ago, Alain Connes proposed a new strategy consisting in constructing a new *geometric* framework for arithmetics where Weil's proof could be transferred by analogy.

His fundamental discovery is that a strategy could consist in working in the world of "*tropical algebraic geometry in characteristic* 1", and apply it to the non-commutative space of the classes of adeles. In his 2014 Lectures at the Collège de France he said that he was looking since 18 years for a geometric interpretation of adeles and ideles in terms of algebraic geometry *à la* Grothendieck. And in his essay [4] he explains:

> "It is highly desirable to find a geometric framework for the Riemann zeta function itself, in which the Hasse-Weil formula, the geometric interpretation of the explicit formulas, the Frobenius correspondences, the divisors, principal divisors, Riemann-Roch problem on the curve and the square of the curve all make sense. (p.8)"

The reader will find some details of this program in his extraordinary paper [7] (2016) with Caterina Consani "*Geometry of the scaling site*".[5]

9.2 The Hasse-Weil function in characteristic 1: Soulé's work

The first move towards an interpretation of Riemann's original $\zeta(s)$ in terms of a $\zeta_C(s)$ for an "untraceable" curve-like object C defined over an "untraceable" new "prime field" $\mathbb{F}$ was achieved by Christophe Soulé.

We have seen that for curves C over finite fields $\mathbb{F}_q$, the Hasse-Weil zeta function $\zeta_C(s)$ counts the (finite) number $N(q^r)$ of points of C rational over the successive extensions $\mathbb{F}_{q^r}$. Yet, the generating function of the $N(q^r)$

$$Z_C(T) := \exp\left(\sum_{r\geq 1} N(q^r)\frac{T^r}{r}\right)$$

(remind that $\zeta_C(s) := Z_C(q^{-s})$) can be defined for a lot of functions $N(q^r)$ which do not derive from a curve.

A natural question is therefore to know if it is possible to retrieve Riemann's original $\zeta(s)$ as a *limit case* of Hasse-Weil function $Z_N(q^{-s})$ for a well defined N. But what type of limit case? For curves over $\mathbb{F}_{q=p^k}$, that is global fields

[5] For previous elements, see Connes, Consani, Marcolli [5].

$K(C)/\mathbb{F}_q(t)$, the base field $\mathbb{F}_p$ is a *common* underlying structure to all localizations. For the global field $\mathbb{Q}$, there is no evident equivalent and this lack of a common base raises Hymalayan difficulties.

In [19] Christophe Soulé worked out the fine and deep idea of looking at $Z_N(q^{-s})$ for $q \to 1$. More precisely, as $Z_N(T)$ has a pole of order $N(1)$ at $q = 1$, he looked at limits

$$\zeta_N(s) = \lim_{q \to 1} Z_N\left(q^{-s}\right)(q-1)^{N(1)} \ .$$

The question becomes then to know if there exists a counting function N yielding

$$\zeta_N(s) = \zeta^*(s) = \zeta(s)\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}$$

Now, such a "function" N *does* exist. If one takes the logarithms, one gets

$$\log \zeta_N(s) = \log \zeta^*(s) = \lim_{q \to 1}\left(\sum_{r \geq 1} N(q^r)\frac{q^{-sr}}{r} + N(1)\log(q-1)\right)$$

and Connes and Consani have shown in [6] that the logarithmic derivative is given by the formula

$$\frac{\zeta_N'(s)}{\zeta_N(s)} = \frac{\zeta^{*\prime}(s)}{\zeta^*(s)} = -\int_1^\infty N(u)\,u^{-s}\frac{du}{u}$$

where N is the well-defined *distribution*

$$N(u) = u + 1 - \frac{d}{du}\left(\sum_\rho \frac{u^{\rho+1}}{\rho+1}\right)$$

the ρ being the non trivial zeroes of $\zeta(s)$. $N(u)$ is the derivative in the distribution sense of the increasing *step* function $J(u)$ on $[1, \infty)$ diverging to $-\infty$ at 1 (see figure 8).

$$J(u) = \frac{u^2}{2} + u - \left(\sum_\rho \frac{u^{\rho+1}}{\rho+1}\right)$$

9.3 Semi-rings and semi-fields of characteristic 1

The second move in implementing Connes' strategy is to find what can mean an algebraic geometry in characteristic $q = 1$.[6] The (revolutionary) first idea is to change the basic algebraic structures and shift from rings and fields to *semi-rings* and *semi-fields*, that is, to algebraic structures $\left(A, \mathring{+}, \mathring{\times}\right)$ where $\mathring{+}, \mathring{\times}$

[6]For an overview of the various approaches towards $\mathbb{F}_1$-geometry, see, e.g., López Peña–Lorscheid [13].

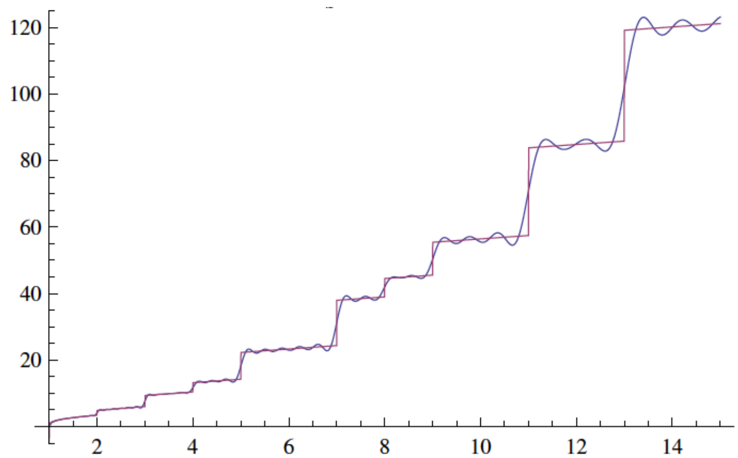

Figure 8: The integral of Soulé's distribution.

are only *monoid* laws (i.e. associative, with neutral element, $\mathring{+}$ commutative, $\mathring{\times}$ distributive). In particular, one can look at $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$ using the sup $\vee$ as new addition $\mathring{+}$ and the $+$ or the $\times$ as new multiplication $\mathring{\times}$.

For instance $\mathbb{Z}_{\max} = \{-\infty\} \cup \mathbb{Z}$ with $\mathring{+} = \vee$ and $\mathring{\times} = +$ is a semi-field with $-\infty$ as the neutral element of $\mathring{+} = \vee$ since $x \vee -\infty = x$, and with 0 as the neutral element of $\mathring{\times} = +$ since $x + 0 = x$. $\mathbb{Z}_{\max}$ is a semi-field $\mathbb{K}$ whose $\mathbb{K}^{\mathring{\times}}$ is infinite cyclic (there exists no field with this property). It is essential to note that $\mathbb{Z}_{\max}$ is a semi-field with *natural Frobenius endomorphisms*. Indeed, if $n \in \mathbb{N}^{\times}$, $\varphi_n : x \mapsto x^n = nx$ ($\mathring{\times} = +$ is the natural addition and therefore exponentiation is the natural multiplication) is an endomorphism of $\mathbb{Z}_{\max}$ since $n\,(x \vee y) = nx \vee ny$ and $n\,(x + y) = nx + ny$. Through the φ_n, the *multiplication* $\times$ can be taken into account in $\mathbb{Z}_{\max}$.

Idem for $\mathbb{R}_{\max}$. More generally, if H is any abelian ordered group, $H_{\max} = \{-\infty\} \cup H$ with $\mathring{+} = \vee$ ($-\infty$ is the neutral element) and $\mathring{\times} = +$ is a semi-field.

Another semi-field is $\mathbb{R}^{+}_{\max} = \mathbb{R}^{+}$ with $\mathring{+} = \vee$ (0 is the neutral element since all x are > 0) and $\mathring{\times} = \times$ (1 remains the neutral element). It is the *exponential* transform of $\mathbb{R}_{\max}$.

In these semi-algebras, the "addition" $\mathring{+}$ is *idempotent* since $x \mathring{+} x = x \vee x = x$ and it is for this reason that one says they are of *characteristic* 1.

The basic structure in characteristic 1 is the Boolean semi-field $\mathbb{B} = \{0, 1\}$ with $\vee$ and $\times$, and hence $1 \vee 1 = 1$. $\mathbb{R}^{+}_{\max}$ is an extension of $\mathbb{B}$ (there don't exist *finite* extensions of $\mathbb{B}$). Its Galois group is

$$\mathrm{Gal}\left(\mathbb{R}^{+}_{\max}\right) := \mathrm{Aut}_{\mathbb{B}}\left(\mathbb{R}^{+}_{\max}\right) = \mathbb{R}^{*}_{+}\ ,$$

and the $\lambda \in \mathbb{R}^{*}_{+}$ act as *Frobenius maps* $\varphi_\lambda : x \mapsto x^\lambda$. One has actually $(x \vee y)^\lambda =$

$x^\lambda \vee y^\lambda$ since $x, y \geq 0$ and $\lambda > 0$, and of course $(xy)^\lambda = x^\lambda y^\lambda$. So one gets a *Frobenius flow* (a multiplicative 1-parameter group) φ_λ on $\mathbb{R}^+_{\max}$.

Now, one can extend the classification of finite fields (the $\mathbb{F}_{p^n}$) to finite semi-fields. A simple but remarkable result is that $\mathbb{B}$ is the only finite semi-field which is not a field.

Theorem. If $\mathbb{K}$ is a finite semi-field, then either $\mathbb{K}$ is a field (a $\mathbb{F}_{p^n}$) or $\mathbb{K} = \mathbb{B}$. $\diamond$

Indeed, let $x \neq 0$ in $\mathbb{K}$. As $\mathbb{K}^\times$ is finite, $x^n = 1$ for an n. Let $b = 1 + x + \ldots x^{n-1} = 1 + a$. We have $xb = b$. If $b = 0$, then $b = 0 = 1 + a$, $a = -1$ and the semi-group $+$ is a group and $\mathbb{K}$ is a field. If $b \neq 0$, then $x = bb^{-1} = 1$ and $\mathbb{K} = \mathbb{B}$.

So one can use the Boolean semi-field $\mathbb{B}$ as a foundation for a new world of algebraic structures, try to do algebraic geometry in characteristic 1, that is, over a putative "non-existent" field $\mathbb{F}_1$, and look at the possibility of transferring Weil's proof of RH to this new framework. In this new world *we can still use* Frobenius endomorphisms as in the case of curves over a finite field.

We have already emphasized that for curves over $\mathbb{F}_{q=p^n}$, that is, global fields $K(C)/\mathbb{F}_q(t)$, the base field $\mathbb{F}_p$ is a common underlying structure to all localizations, while it is not the case for the global field $\mathbb{Q}$ and its algebraic extensions. A great advance is the idea that $\mathbb{B}$ can overcome this lack.

Remark. The world of semi-rings and semi-fields in characteristic 1 is intimately correlated to what is called *tropical geometry*, *idempotent analysis*, and what Victor Maslov called "*dequantization*". The idea is to take $+$ as the "multiplication" and conjugate it with scaling $x \mapsto x^\varepsilon$ where ε is a scale which $\to 0$ as $\hbar \to 0$ in the semiclassical approximations of quantum mechanics. Now, it is well known that

$$\lim_{\varepsilon \to 0} \left(x^{\frac{1}{\varepsilon}} + y^{\frac{1}{\varepsilon}} \right)^\varepsilon = x \vee y$$

A great advantage of this framework for optimization problems is that *Legendre* transforms become simply *Fourier* transforms. Its origin is to be found in the technique of *Newton polygons* introduced by Newton to localize the zeroes of polynomials.

9.4 The arithmetic topos $\mathfrak{A} = \left(\widehat{\mathbb{N}^\times}, \mathbb{Z}_{\max}\right)$

The third move of Connes' strategy was to find the "untraceable" geometric arithmetic-like object $\mathfrak{A}$ enabling to interpret $\zeta(s)$ as a $\zeta_\mathfrak{A}(s)$. The jump is fantastic. Connes and Consani used the topos conception of algebraic geometry developed by Grothendieck and considered a topos adapted by construction to characteristic 1.

Connes' challenge was to find

> "the bridge between noncommutative geometry and topos points of view." (p.21)

His construction is quite astonishing. He succeeded in *identifying*

1. the natural action of the multiplicative group $\mathbb{R}_+^\times$ of classes of ideles on the noncommutative space $\mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q} / \widehat{\mathbb{Z}}^\times$,
2. the natural action of the Frobenius maps φ_λ, $\lambda \in \mathbb{R}_+^\times$ on the points of the "arithmetic topos" $\mathfrak{A}$ over $\mathbb{R}_+^{\max}$

Such an identification paves the way for a translation of the *arithmetic* universe of RH into a *geometric* new universe, this translation being far more powerful than the analogy of Dedekind-Weber-Weil.

The starting point is incredibly simple, "d'une simplicité biblique". Connes and Consani identify $\mathbb{N}^\times$ to the small category with a single object $*$ and morphisms $n \in \mathbb{N}^\times$ with composition $n \circ m$ given by the multiplication nm. We can schematize this identification as $(* \circlearrowleft N^\times)$. Then they look at the category $\widehat{\mathbb{N}^\times}$ of presheaves on $\mathbb{N}^\times$, that is the category of contravariant functors $(\mathbb{N}^\times)^{op} \to \mathfrak{Set}$, that is the category of sets endowed with a $\mathbb{N}^\times$-action.

If $\mathbb{N}^\times$ is endowed with the trivial Grothendieck topology, presheaves become sheaves and $\widehat{\mathbb{N}^\times}$ becomes a *topos* over the site $\mathbb{N}^\times$. Now, $\mathbb{Z}_{\max} = (\{-\infty\} \cup \mathbb{Z}, \vee, +)$ is a semi-ring in this topos since $\mathbb{N}^\times$ acts on $\mathbb{Z}_{\max}$ through the Frobenius maps φ_n. Connes takes it as the *structural sheaf* of the topos $\widehat{\mathbb{N}^\times}$ and calls $\mathfrak{A} = \left(\widehat{\mathbb{N}^\times}, \mathbb{Z}_{\max}\right)$ the *arithmetic site* (or topos). It is a *geometric* object "defined over" $\mathbb{B}$, "geometric" in the topos sense but of an arithmetic essence.[7]

The key idea is then to develop the new *analogy*:

$$\begin{array}{c}\text{arithmetic site } \mathfrak{A} = \left(\widehat{\mathbb{N}^\times}, \mathbb{Z}_{\max}\right) \\ \text{over the finite semi-field } \mathbb{B} \text{ of characteristic } 1 \\ \Updownarrow \\ \text{algebraic curve } C \\ \text{over the finite field } \mathbb{F}_q \text{ of characteristic } p\end{array}$$

10 The steps of the strategy

10.1 The points of the topos $\mathfrak{A}$

The first remarkable fact is that *the points of the topos $\mathfrak{A}$ correspond, up to isomorphism, to the additive subgroups H of $\mathbb{Q}$*. But we have seen in section 6.2 that the subgroups of $(\mathbb{Q}, +)$ are parametrized by (finite) adeles. So, through the subgroups of $(\mathbb{Q}, +)$, we can build a bridge between the arithmetic world of adeles and a geometric universe in the sense of Grothendieck's topos. This new bridge opens up a vast array of new methods, new tactics and new strategies for demonstrating HR in the arithmetic case.

[7] As was emphasized by a reviewer, "$\mathbb{Z}_{\max}$, when viewed just as a semi-field, is not sufficiently deep" because "multiplication of numbers is not part of the structure of $\mathbb{Z}_{\max}$ as a semi-field. By employing the arithmetic site, multiplication is put back in. The true object to consider is then $\mathbb{Z}_{\max}$ regarded as a sheaf over the arithmetic site."

Recall that a point of a topos $\mathcal{T}$ is a geometric morphism $p : \mathfrak{Set} \to \mathcal{T}$, that is a pair of adjoint functors $p^* \dashv p_*$ with p^* preserving finite limits (as p^* is a left adjoint, it is left exact and preserves general colimits) :

$$\mathcal{T} \quad \begin{array}{c} \xrightarrow{p^*} \\ \xleftarrow[p_*]{} \end{array} \quad \mathfrak{Set}$$

This means that $\text{Hom}_{\mathfrak{Set}} (p^* (F), S) \simeq \text{Hom}_{\mathcal{T}} (F, p_* (S))$, for $F \in \mathcal{T}$ and $S \in \mathfrak{Set}$. The image $p^* (F)$ is the stalk of the topos $\mathcal{T}$ at the point p.

In our case, an element F of $\widehat{\mathbb{N}^\times}$ is simply a set $X = F(*)$ endowed with an action θ_n of $\mathbb{N}^\times$ and a point $(p^*, p_*) : \widehat{\mathbb{N}^\times} \to \mathfrak{Set}$ associates functorially to each (X, θ) a set $p^* ((X, \theta))$ such that $\text{Hom}_{\mathfrak{Set}} (p^* ((X, \theta)), S) \simeq \text{Hom}_{\widehat{\mathbb{N}^\times}} ((X, \theta), p_* (S))$.

Let $Y : \mathbb{N}^\times \to \widehat{\mathbb{N}^\times}$ be the Yoneda functor $* \mapsto Y_* : (\mathbb{N}^\times)^{op} \to \mathfrak{Set}$ defined by $Y_* (*) = \mathbb{N}^\times$ and $Y_* (n) =$ multiplication by n (noted $\times n$) in $\mathbb{N}^\times$. To $p^* : \widehat{\mathbb{N}^\times} \to \mathfrak{Set}$ one associates the covariant functor $\mathfrak{p} : \mathbb{N}^\times \to \mathfrak{Set}$

$$\mathfrak{p} = p^* \circ Y : \mathbb{N}^\times \xrightarrow{Y} \widehat{\mathbb{N}^\times} \xrightarrow{p^*} \mathfrak{Set}$$

More informally we can say that $\mathfrak{p}$ associates first $\left(\mathbb{N}^\times \circlearrowleft \times N^\times\right)$ to $(* \circlearrowleft N^\times)$ and then $\left(X \circlearrowleft \times N^\times\right) = p^* \left(\mathbb{N}^\times \circlearrowleft \times N^\times\right)$ to $\left(\mathbb{N}^\times \circlearrowleft \times N^\times\right)$. A special case $\mathfrak{I}$ is when $p^* \left(\mathbb{N}^\times \circlearrowleft \times N^\times\right) = \left(\mathbb{N}^\times \circlearrowleft \times N^\times\right)$ is the identity.

Then Connes and Consani show that, since p^* is a *geometric* morphism, $\mathfrak{p}$ is *flat*. This means :

1. $X = \mathfrak{p} (*) \neq \varnothing$,
2. Every pair of elements $x, x' \in X$ are the images of some element $z \in X$ through two morphisms $\mathfrak{p} (k)$ and $\mathfrak{p} (k')$, $k, k' \in \mathbb{N}^\times$ (i.e. x, x' are always in some orbit of the $\mathbb{N}^\times$-action),
3. If $\mathfrak{p} (k) (x) = \mathfrak{p} (k) (x')$, then $k = k'$ (i.e. the $\mathbb{N}^\times$-action is free).

So that, beyond the given action of the multiplicative *monoid* $(\mathbb{N}^\times, \times)$ on X, there is in fact an action of the *ring* $(\mathbb{N}^\times, \times, +)$. If one defines H_+ as X endowed with the (well defined) commutative and associative addition $x + x' := \mathfrak{p} (k + k') (z)$ for a z such that $\mathfrak{p} (k) (z) = x$ and $\mathfrak{p} (k') (z) = x'$, one can transfer to X the construction of the ring $\mathbb{Z}$ from the multiplicative monoid $\mathbb{N}^\times$.

Moreover, one can show that the $\mathbb{N}^\times$-action is *simplifiable*, which means that for every pair $x, x' \in X$ there exists a $z \in X$ such that either $x + z = x'$ or $x' + z = x$ and so either $x - x'$ or $x' - x$ can be well defined.

This implies that H_+ is the *positive* part of an *abelian additive totally ordered group* (H, H_+), the $\mathbb{N}^\times$-action being

$$\mathfrak{p} (k) (x) = \underbrace{x + \ldots + x}_{k \text{ times}} = kx$$

(H, H_+) is an increasing union of subgroups isomorphic to $(\mathbb{Z}, \mathbb{Z}_+)$ and is isomorphic to an additive subgroup of $(\mathbb{Q}, \mathbb{Q}_+)$. Indeed if $x \in X$, there exists an injection $j_x : H \hookrightarrow \mathbb{Q}$ given by $j_x(x) = 1$ and $j_x(x') := \frac{k'}{k}$ deduced from every $z \in X$ such that $\mathfrak{p}(k)(z) = x$ and $\mathfrak{p}(k')(z) = x'$ ($\frac{k'}{k}$ is well defined).

Theorem. The category of points of the arithmetic topos $\widehat{\mathbb{N}^\times}$ is canonically equivalent to the category whose objects are the totally ordered groups (H, H_+) isomorphic to non trivial subgroups of $(\mathbb{Q}, \mathbb{Q}_+)$ and morphisms are order preserving injections. ——— $\diamond$

In particular, the subgroups of $\mathbb{Q}$: $H_p = \left\{ \frac{n}{p^k} \mid n \in \mathbb{Z}, k \in \mathbb{N} \right\}$ for p prime, are *special* points of $\widehat{\mathbb{N}^\times}$. And as the primes p are the (closed) points of the scheme $\mathrm{Spec}(\mathbb{Z})$, one gets a *canonical interpretation* of $\mathrm{Spec}(\mathbb{Z})$ into the arithmetic topos $\mathfrak{A}$.

But we have already seen that the non trivial subgroups of $(\mathbb{Q}, \mathbb{Q}_+)$ are classified by the quotient of finite adeles $\mathbb{A}_{\mathbb{Q}}^f / \widehat{\mathbb{Z}}^\times$. In fact:

Theorem. The isomorphism classes of points of the arithmetic topos $\mathfrak{A}$ are canonically isomorphic to the noncommutative space $\mathbb{Q}_+^\times \backslash \mathbb{A}_{\mathbb{Q}}^f / \widehat{\mathbb{Z}}^\times$ where $\mathbb{Q}_+^\times$ acts by multiplication. ——— $\diamond$

Let $\mathfrak{p}_H$ be the point of $\widehat{\mathbb{N}^\times}$ represented by the subgroup H and let $H_{\max}$ be the semi-field $H_{\max} = \{-\infty\} \cup H$ with $\mathring{+} = \vee$ ($-\infty$ is the neutral element) and $\mathring{\times} = +$.

Theorem. $H_{\max}$ is the stalk of the structural sheaf $\mathbb{Z}_{\max}$ at the point $\mathfrak{p}_H$. $\diamond$

The special case $\mathfrak{I}$ corresponds to $\mathfrak{p}_{\mathbb{Z}}$ for which $H_{\max} = \mathbb{Z}_{\max}$.

10.2 Extension of scalars

In Connes' analogy, the arithmetic topos corresponds to a curve C over a finite field $\mathbb{F}_q$. We have seen that Weil's proof of RH uses intersection theory and RR in the square $\overline{C} \times \overline{C}$.

So, to keep on with the analogy, one has to define the square $\overline{\mathfrak{A}} \times \overline{\mathfrak{A}}$ and use the Frobenius maps to "count the points". It is a very difficult and highly technical stuff. The aim is to construct an analogy where $\overline{C}$, holomorphic and meromorphic functions on $\overline{C}$, as well as their zeros and poles, can have natural equivalents.

The starting idea is rather subtle. Connes adds a *scaling flow* to the arithmetic topos. The underlying site of the scaled topos $\overline{\mathfrak{A}}$ is constructed using the semi-direct product $[0, \infty) \rtimes \mathbb{N}^\times$ to modify the natural category structure of open subsets of the half-line $[0, \infty)$.

The category $\mathfrak{C}$ is the category with objects the *open intervals* Ω of $[0, \infty)$ (the $[0, a)$ and $\varnothing$ are included, $\varnothing$ is an initial object) and with morphisms $n : \Omega \to \Omega'$ the $n \in \mathbb{N}^\times$ such that $n\Omega \subset \Omega'$ (i.e. n acts as a scaling). So we have a topological space $[0, \infty)$ with a $\mathbb{N}^\times$-scaling. The category $\mathfrak{C}$ has fiber products. One considers then the Grothendieck topology J on $\mathfrak{C}$ defined by the covering of open intervals Ω by families of open intervals $\{\Omega_j\}$ and the sheaves over the site $(\mathfrak{C}, J)$, that is sheaves over $[0, \infty)$ which are $\mathbb{N}^{\times}$-equivariant. Connes takes for $\overline{\mathfrak{A}}$ this category $\mathfrak{Sh}(\mathfrak{C}, J)$ of sheaves:

$$\overline{\mathfrak{A}} = \mathfrak{Sh}(\mathfrak{C}, J) \ .$$

10.3 The structural sheaf

Connes insists on the "enormous gain" due to the fact that the scaled arithmetic topos $\overline{\mathfrak{A}}$ has a *structural sheaf* $\mathcal{O}$ which is *a semi-ring object*.

The key definition is the following. It opens the world of *tropical geometry* in this new context. If $\Omega \subset [0, \infty)$ is an open interval, $\mathcal{O}(\Omega)$ is the semi-ring of functions $f : \Omega \to \mathbb{R}_{\max}$

1. with values $f(\lambda)$ in $\mathbb{R}_{\max} = \{-\infty\} \cup (\mathbb{R}, +)$,
2. continuous,
3. piecewise affine,
4. *convex*
5. with *integral* slopes $f' \in \mathbb{Z}$ except at points where f' presents a discontinuity (an angular point).

As for the morphisms (scaling) $n : \Omega \to \Omega'$, Connes defines $\mathcal{O}\left(\Omega \xrightarrow{n} \Omega'\right)$ by $f(\lambda) \mapsto f(n\lambda)$. It is a coherent definition since $f'(n\lambda) = nf'(\lambda)$ and if $f' \in \mathbb{Z}$ then $nf' \in \mathbb{Z}$. $\mathcal{O}$ is a semi-ring in $\overline{\mathfrak{A}}$ and a semi-algebra over $\mathbb{R}_{\max}$.

The deep analogy with algebraic curves in the classical Riemann's theory is the following:

$\overline{\mathfrak{A}}$	$\overline{C}$
f piecewise affine	f analytic
$-f$	$\frac{1}{f}$
f convex	f holomorphic
linear point λ : $f'(\lambda_-) = f'(\lambda_+)$	f holomorphic invertible at z
angular point λ with $f'(\lambda_-) < f'(\lambda_+)$	zero of f
angular point λ with $f'(\lambda_-) > f'(\lambda_+)$	pole of f

We see that once the universe of admissible f has been delimited by their continuity and their affine structure, the convexity constraint allows to distinguish between "holomorphic" f with only "zeros" (convex angular points) and "meromorphic" f that can also have "poles" (concave angular points). But the essential constraint is that the slopes must be *integers*. This can be weakened by extension.

10.4 Points of $\mathfrak{A}$ and $\overline{\mathfrak{A}}$ over $\mathbb{R}_+^{\max}$

When one extends the scalars to $\mathbb{R}_+^{\max}$, one adds a lot of new points, namely all the subgroups of rank 1 of $\mathbb{R}$. They are the subgroups of the form λH_a with a $\lambda \in \mathbb{R}$ scaling an additive subgroup H_a of $\mathbb{Q}$. Remember (see above section 6.2) that the H_a are parametrized by the *finite* adeles a.

It can be shown that – just as one has $C\left(\overline{\mathbb{F}_q}\right) = \overline{C}\left(\overline{\mathbb{F}_q}\right)$ in the case of curves over $\mathbb{F}_q$ – one has here $\overline{\mathfrak{A}}\left(\mathbb{R}_+^{\max}\right) = \mathfrak{A}\left(\mathbb{R}_+^{\max}\right)$. The action of the Frobenius maps φ_λ, $\lambda \in \mathbb{R}_+^\times$ on these points correspond to the action of the classes of ideles modulo $\widehat{\mathbb{Z}}^\times$ i.e. $\mathbb{R}_+^\times$.

The basic analogy is now

$C/\mathbb{F}_q$	$\mathfrak{A}/\mathbb{B}$
structural sheaf $\mathcal{O}_C$	structural sheaf $\mathcal{O} = \mathbb{Z}_{\max}$
extension $\overline{C}/\overline{\mathbb{F}_q}$	extension $\overline{\mathfrak{A}}/\mathbb{R}_+^{\max} = \left([0,\infty) \rtimes \mathbb{N}^\times, \mathcal{O}\right)$
	$\mathcal{O} = \left\{ \begin{array}{c} \text{continuous,} \\ \text{piecewise affine,} \\ \text{convex} \\ \text{with integral slopes} \end{array} \right\}$ functions $f : \Omega \to \mathbb{R}_{\max}$
	$\mathcal{K}$ = non necessarily convex functions
$\overline{C}\left(\overline{\mathbb{F}_q}\right) = C\left(\overline{\mathbb{F}_q}\right)$	$\overline{\mathfrak{A}}\left(\mathbb{R}_+^{\max}\right) = \mathfrak{A}\left(\mathbb{R}_+^{\max}\right)$

Theorem. The isomorphism classes of points of the scaled arithmetic topos $\overline{\mathfrak{A}}\left(\mathbb{R}_+^{\max}\right) = \mathfrak{A}\left(\mathbb{R}_+^{\max}\right)$ are canonically isomorphic to the noncommutative space $\mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q} / \widehat{\mathbb{Z}}^\times$, where $\mathbb{Q}^\times$ acts by multiplication. ______________ $\diamond$

So it becomes possible to do algebraic geometry on the adeles' classes.

It is important to note that the points of the initial arithmetic topos $\mathfrak{A}$ correspond to *abstract* groups isomorphic to the H_a defined by finite adeles a. Now, we add to a an Archimedean component $\lambda \in \mathbb{R}$ (a scaling) and look at λH_a no longer as an abstract subgroup but as a *well defined subgroup* of $\mathbb{R}$. All the points λH_a of $\overline{\mathfrak{A}}$ lie over the point H_a of $\mathfrak{A}$.

Theorem. If $\mathfrak{p}_H$ is the point of $\overline{\mathfrak{A}}$ defined by the rank 1 subgroup H of $\mathbb{R}$, the stalk of the structural sheaf $\mathcal{O}$ at $\mathfrak{p}_H$ is the semi-ring $\mathcal{R}_H$ of germs at $\lambda = 1$ (the identity scaling) of functions f which are (1) $\mathbb{R}_{\max}$ -valued, (2) continuous, (3) piecewise affine, (4) convex, (5) with slopes *belonging to H*. ______ $\diamond$

Let $x = f(1) \in \mathbb{R}_{\max}$ and $h_- = f'(1_-) \in H$ and $h_+ = f'(1_+) \in H$. As f is convex, $h_- \leq h_+$. If $h_- = h_+$, f is regular (linear) at 1 and if $h_- < h_+$, f is singular at 1 (angular point). $\mathcal{R}_H$ is the semi-ring of triplets (x, h_-, h_+) with

$$\begin{aligned}
(x, h_-, h_+) \vee \left(x', h'_-, h'_+\right) &= \left\{ \begin{array}{c} (x, h_-, h_+) \text{ if } x > x' \\ \left(x', h'_-, h'_+\right) \text{ if } x < x' \\ \left(x, h_- \wedge h'_-, h_+ \vee h'_+\right) \text{ if } x = x' \end{array} \right. \\
(x, h_-, h_+) + \left(x', h'_-, h'_+\right) &= \left(x + x', h_- + h'_-, h_+ + h'_+\right)
\end{aligned}$$

Then one defines the *order* of f as $\operatorname{ord}(f) = h_+ - h$. As f is *convex*, $\operatorname{ord}(f) \geq 0$. If $\operatorname{ord}(f) = 0$ then f is linear.

For a rescaling μ, the action of Frobenius φ_μ on $\mathcal{O}$ is given by

$$\varphi_\mu : \mathcal{R}_H \to \mathcal{R}_{\mu H}, (x, h_-, h_+) \mapsto (x, \mu h_-, \mu h_+)$$

10.5 The RR strategy

In the framework of the scaled arithmetic topos, one can transfer to the square $\overline{\mathfrak{A}} \times \overline{\mathfrak{A}}$ Weil's RR strategy for trying to prove RH.

The "graphs" of the *Frobenius scaling flow* φ_λ define a flow of Frobenius scaling "correspondences" Φ_λ on $\overline{\mathfrak{A}} \times \overline{\mathfrak{A}}$ ($\lambda \in \mathbb{R}_+^\times$) and one has $\Phi_\lambda \circ \Phi_{\lambda'} = \Phi_{\lambda\lambda'}$ up to some technicalities when $\lambda\lambda' \in \mathbb{Q}$ while $\lambda, \lambda' \notin \mathbb{Q}$.

11 The "elliptic" case of periodic points

11.1 An analogy with $\mathbb{F}_p$ elliptic curves

In $\overline{\mathfrak{A}}$, all the points λH_p with $H_p = \left\{ \frac{n}{p^k} \mid n \in \mathbb{Z}, k \in \mathbb{N} \right\}$ lie over the point H_p of $\mathfrak{A}$. They are parametrized by $\mathbb{R}_+^* / p^{\mathbb{Z}}$ and constitute in some sense a "circle" C_p over p which is a periodic orbit of the Frobenius scaling flow φ_λ.

Remark. When one makes the link of this toposic approach of arithmetics with the explicit formulas, one finds that the "length" of C_p must be $\log p$. It has been a long while since Selberg noted the deep analogy of Riemann's explicit formula with his own "trace formula" concerning the eigenvalues of the Laplacian of hyperbolic compact surfaces (Riemann surfaces of genus ≥ 2). It is the log of the length of the closed geodesics (i.e. the periodic orbits of the geodesic flow) which is involved.

Connes and Consani have recently proved RR in that simple case, which as they say, is "encouraging". More precisely they have shown that the algebraic geometry of *elliptic curves* over $\mathbb{F}_p$ can be completely transfered to the C_p.

The analogy is with the 1959 theory of John Tate (see *A review of non-Archimedean elliptic functions* [20] and the correspondence with Serre).

The classical theory of elliptic curves E_τ as quotients $\mathbb{C}/\Lambda$ of $\mathbb{C}$ by a lattice $\Lambda = \langle 1, \tau \rangle$ with $\Im(\tau) > 0$ (i.e. $\tau \in \mathcal{H}$, the hyperbolic Poincaré half-plane) cannot be extended to the p-adic context. To overcome this difficulty, Tate remarked that, since functions f over E_τ are doubly periodic functions $f(z)$ over $\mathbb{C}$ with periods 1 and τ (elliptic functions), one can "absorb" the period 1 in the change of variables $z \mapsto u = e^{2\pi i z}$.

This is a Fourier transform transforming the cylinder $(\mathbb{C}/\mathbb{Z}, +, 0, \times, 1)$ into $(\mathbb{C}^*, \times, 1, \exp, 1)$. Then $f(z)$ becomes a function $f(u)$ on $\mathbb{C}^*$ with period τ. Applying again a Fourier transform, namely $q = e^{2\pi i \tau}$ ($|q| < 1$ since $\Im(\tau) > 0$), $f(z)$ becomes q-periodic and hence a function on $\mathbb{C}^*/q^{\mathbb{Z}}$. Indeed,

$$\text{if } z \mapsto z + \tau, \text{then } e^{2\pi i z} \mapsto e^{2\pi i (z+\tau)} = e^{2\pi i z} e^{2\pi i \tau} = q e^{2\pi i z}$$

So E_τ can be identified with $\mathbb{C}^*/q^{\mathbb{Z}}$, $q = e^{2\pi i\tau}$, and Tate reformulated the whole theory of elliptic curves in that new context and showed how it can be transfered to the p-adic case. The reason of the transfer is that (p. 2)

> "these Fourier expansions, suitably normalized, yield "universal" identities among power series with rational integral coefficients."

11.2 The periodic orbit $C_p \simeq \mathbb{R}_+^*/p^{\mathbb{Z}}$ of the Frobenius scaling flow

The analogy is then between Tate's $\mathbb{C}^*/q^{\mathbb{Z}}$ and Connes' $\mathbb{R}_+^\times/p^{\mathbb{Z}}$.

The $\mathbb{R}_{\max}$-valued functions f are now *multiplicatively p-periodic* functions $f(\lambda)$ defined on the scales $\lambda \in \mathbb{R}_+^\times$, i.e. on $\mathbb{R}_+^\times/p^{\mathbb{Z}}$. So, the f are periodically scale invariant and can be considered as defined on $[1, p]$. Remember that the algebraic operations are $\mathring{+} = \vee$ and $\mathring{\times} = +$.

$\mathcal{O}(C_p) = \mathcal{O}_p$ is the sheaf ot germs of p-periodic functions $f(\lambda)$ which are (1) $\mathbb{R}_{\max}$ -valued, (2) continuous, (3) piecewise affine ($f(\lambda) = h\lambda + a$), (4) convex, (5) with slopes $f'(\lambda) = h$ in H_p at all points λ. (As $f'(\lambda) \in H_p$ is the same as $\lambda f'(\lambda) \in \lambda H_p$ the condition (5) is invariant.) They are the equivalent of holomorphic functions in Tate's case.

$\mathcal{O}(C_p)^\times = \mathcal{O}_p^\times$ is the sheaf of invertible elements of $\mathcal{O}_p$ that is of the f whose germs are *linear* at every point, and therefore differentiable of class C^1. It is evident that there cannot exist *non constant global sections* of $\mathcal{O}_p^\times$ since we would have a f p-periodic, C^1, and everywhere convex, which is impossible.

$\mathcal{K}(C_p) = \mathcal{K}_p$ is the sheaf of germs of functions $f(\lambda)$ which are (1) $\mathbb{R}_{\max}$ -valued, (2) continuous, (3) piecewise affine, (4) *non necessarilly convex*, (5) with slopes $f'(\lambda)$ in H_p at all points λ. $\mathcal{K}_p$ has a lot of global sections (the equivalent of elliptic functions in Tate's case).

11.3 Divisors

As in the classical case, *Cartier divisors* are global sections of the quotient sheaf $\mathcal{K}_p/\mathcal{O}_p^\times$. As in the classical case, they are finite formal sums D of points $\mathfrak{p}_\lambda$, that is of rank 1 subgroups λH_p of $\mathbb{R}$. The fundamental difference is that the *order* $D(\mathfrak{p}_\lambda)$ of D at $\mathfrak{p}_\lambda$ belongs now to $\lambda H_p \subset \mathbb{R}$ and no longer to $\mathbb{Z}$. So, if $D = \sum_{j=1}^{j=n} D(\mathfrak{p}_{\lambda_i})\mathfrak{p}_{\lambda_i}$, $\deg(D) = \sum_{j=1}^{j=n} D(\mathfrak{p}_{\lambda_i}) \in \mathbb{R}$ is a *real* number.

Now let f be continuous, piecewise affine, with multiplicative period p, and with slopes in H_p. If one decomposes f in its affine parts on a fondamental domain $\lambda_0 < \lambda_1 < \cdots < \lambda_n = p\lambda_0$ and remember that $\mathrm{ord}(f)$ at $\mathfrak{p}_\lambda$ is $\lambda\left(h\left(\lambda^+\right) - h\left(\lambda^-\right)\right)$, one sees that, as in the classical case, the degree of the principal divisor (f) vanishes: $\deg((f)) = 0$.

There is another number that can be associated to a divisor. If $p > 2$, $H_p/(p-1)H_p \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Then, for $H = \lambda H_p$, consider the map

$$\chi : H \to \mathbb{Z}/(p-1)\mathbb{Z}, \mu \mapsto \frac{\mu}{\lambda} \in H_p$$

$\frac{\mu}{\lambda}$ being seen as an element of $H_p/(p-1)H_p \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. The map χ can be extended to divisors by linearity and one shows that $\chi((f)) = 0$ for principal divisors. So, one can consider the map $(\deg, \chi)$ from divisors to $\mathbb{R} \times \mathbb{Z}/(p-1)\mathbb{Z}$. The principal divisors constitute the kernel of $(\deg, \chi)$.

11.4 The Frobenius scaling flow in the "elliptic" case

Remember that for a rescaling μ, the action of the Frobenius φ_μ on the structural sheaf $\mathcal{O}$ is given by

$$\varphi_\mu : \mathcal{R}_H \to \mathcal{R}_{\mu H}, (x, h_-, h_+) \mapsto (x, \mu h_-, \mu h_+)$$

On the functions $f(\lambda)$, the natural action is

$$\varphi_\mu(f)(\lambda) := \mu f\left(\mu^{-1}\lambda\right)$$

Indeed, in the multiplicative semi-field $\mathbb{R}_+^{\max}$, φ_μ acts as $\varphi_\mu : x \to x^\mu$. In the additive semi-field $\mathbb{R}_{\max}$ (which is the log of $\mathbb{R}_+^{\max}$), φ_μ acts therefore as $\varphi_\mu : x \to \mu x$.

Now, f is valued in $\mathbb{R}_{\max}$ and piecewise affine: $f(\lambda) = h\lambda + a$, and the φ_μ act on the a. So we must have

$$\varphi_\mu(f)(\lambda) = h\lambda + \mu a = \mu\left(h\mu^{-1}\lambda + a\right) = \mu f\left(\mu^{-1}\lambda\right)$$

The φ_μ act also on divisors.

1. If $D = \sum_j (H_j, h_j \in H_j)$, then $\varphi_\mu(D) = \sum_j (\mu H_j, \mu h_j \in \mu H_j)$,
2. $\deg\left(\varphi_\mu(D)\right) = \mu \deg(D)$,
3. $\chi\left(\varphi_\mu(D)\right) = \mu\chi(D)$.

11.5 "Elliptic" functions and "theta" functions

In the classical case, it is well known that *elliptic* functions on the elliptic curve $E_\tau = \mathbb{C}/\Lambda$ can be expressed using *theta* functions. Due to Liouville theorem, an *entire* elliptic function on E_τ is necessarilly constant.

So if we want to get non constant functions we have two possibilities:

1. to keep the periodicity, weaken the property of being entire, and accept meromorphic functions;
2. to weaken the periodicity and keep the property of being entire.

The first possibility leads to elliptic functions and the second to theta functions.

Tate reformulated the Θ-functions when the elliptic curve E_τ is written as $\mathbb{C}^*/q^{\mathbb{Z}}$ with $q = e^{2\pi i\tau}$. Tate's formula is

$$\begin{aligned}\Theta(w) &= \sum_{\mathbb{Z}} (-1)^n q^{\frac{n(n-1)}{2}} w^n \\ &= (1-w) \prod_{m=1}^{m=\infty} (1-q^m)(1-q^m w)\left(1-q^m w^{-1}\right)\end{aligned}$$

and $\Theta(w)$ satisfies the functional equation

$$-w\Theta(qw) = \Theta(w)$$

As in Tate's case, Connes defined a theta function $\Theta(\lambda)$ on the whole $\mathbb{R}_+^\times$,

1. which is no longer p-periodic (i.e. "elliptic"),
2. but which is globally (1) continuous, (2) piecewise affine, (3) convex (i.e. globally "holomorphic"),
3. and which satisfies a functional equation.

Tate's term $(1-w)\prod_{m=1}^{m=\infty}(1-q^m w) = \prod_{m=0}^{m=\infty}(1-q^m w)$ is translated into $\Theta_+(\lambda)$ $\lambda \in (0,\infty)$

$$\Theta_+(\lambda) := \sum_{m=0}^{m=\infty} (0 \vee (1-p^m\lambda))$$

and Tate's term $\prod_{m=1}^{m=\infty}\left(1-q^m w^{-1}\right)$ is translated into

$$\Theta_-(\lambda) := \sum_{m=1}^{m=\infty} \left(0 \vee \left(p^{-m}\lambda - 1\right)\right)$$

The term $\prod_{m=1}^{m=\infty}(1-q^m)$ can be skipped.

Then, one shows the functional equation

$$\begin{cases} \Theta_+(p\lambda) = \Theta_+(\lambda) - (0 \vee (1-\lambda)), \\ \Theta_-(p\lambda) = \Theta_+(\lambda) + (0 \vee (\lambda-1)), \text{ and therefore} \\ \Theta(p\lambda) = \Theta(\lambda) + \lambda - 1 \text{ since } (0 \vee x) - (0 \vee (-x)) = x \end{cases}$$

Connes and Consani then proved the equivalent of the classical reconstruction of all elliptic functions from theta functions. From the basic theta function $\Theta(\lambda)$, they define a whole family of theta functions $\Theta_{h,\mu}$ parametrized by $(h,\mu) \in H_p^+ \times \mathbb{R}_+^\times$, that is by a positive slope and a rescaling. These functions $\Theta_{h,\mu}$ are associated with the Frobenius scaling flow

$$\Theta_{h,\mu}(\lambda) := \mu\Theta\left(\mu^{-1}h\lambda\right)$$

(the role of μ and μ^{-1} is to warrant that the slopes remain in H_p).

Their divisors are

$$\delta(h,\mu) := \left(\text{point } \mu h^{-1}H_p,\ \text{order } \mu\right)$$

(one checks that $\mu \in \mu h^{-1}H_p$ since $\mu = \mu h^{-1}h$ and $h \in H_p$). Let $D = D_+ - D_-$ be a divisor with $D_+ = \sum_i \delta(h_i, \mu_i)$ and $D_- = \sum_j \delta\left(h'_j, \mu'_j\right)$ and suppose that $\deg(D) = 0$.

Theorem. If $\chi(D) = 0$ (that is if $h \in H_p$ satisfies $(p-1)h = \sum_i h_i - \sum_j h'_j$), then the function

$$f(\lambda) := \sum_i \Theta_{h_i,\mu_i}(\lambda) - \sum_j \Theta_{h'_j,\mu'_j}(\lambda) - h\lambda$$

is a global section of $\mathcal{K}_p$ with divisor $(f) = D$. Moreover all "elliptic" functions can be recovered through such a canonical decomposition. ______________◇

11.6 p-adic norm, filtration and dimension

As the slopes of the f are in $H_p = \left\{\frac{n}{p^k} \mid n \in \mathbb{Z}, k \in \mathbb{N}\right\}$ we can look at them "p-adically" that is by filtering them through the p^k.

Let $h(\lambda) \in H_p$ be the slope of f at λ. Connes defines the appropriate p-adic norm $\|f\|_p$ of f as

$$\|f\|_p := \max_{\lambda \in \mathbb{R}_+^\times} \left\{\frac{|h(\lambda)|_p}{\lambda}\right\}$$

with $|\bullet|_p$ the p-adic norm normalized by $|p|_p = \frac{1}{p}$. As $h(p\lambda) = \frac{1}{p}h(\lambda)$, this definition is appropriate since, $\frac{|h(\lambda)|_p}{\lambda}$ is *invariant* by the scaling periodicity $\lambda \mapsto p\lambda$:

$$\frac{|h(p\lambda)|_p}{p\lambda} = \frac{p\,|h(\lambda)|_p}{p\lambda} = \frac{|h(\lambda)|_p}{\lambda}$$

The ultrametricity of this p-adic norm is compatible with the algebraic operations $\overset{\circ}{+} = \vee$ and $\overset{\circ}{\times} = +$ on functions.

One has also $\|p^a f\|_p = p^{-a}\|f\|_p$ and $\|f\|_p \leq 1$ iff the restriction $f\mid_{[1,p]}$ has *integral* slopes.

11.7 The $H^0(D)$ and their dimension

As in the classical case, if D is a divisor one can consider the space $H^0(D)$ (or $L(D)$) of the f such that $D + (f) \geq 0$.

$$H^0(D) := \{f \in \mathcal{K}_p \mid D + (f) \geq 0\}$$

which is a $\mathbb{R}_{\max}$-module (i.e. stable by $\vee$).

The challenge becomes to prove the Riemann-Roch theorem. But for that, one must at first define the *dimensions* of the spaces $H^0(D)$ (they are the $\ell(D) = \dim_{\mathbb{C}}(L(D))$ in the classical case). This is not trivial at all since they are $\mathbb{R}_{\max}$-modules.

To define $\dim\left(H^0(D)\right)$, Connes *filters* the $H^0(D)$ using the p-adic norm, that is the filtration of $H^0(D)$ by the

$$H^0(D)^{p^n} = \left\{f \in H^0(D) \text{ s.t. } \|f\|_p \leq p^n\right\}$$

and proposes the formula

$$\dim\left(H^0(D)\right) := \lim_{n\to\infty} p^{-n} \dim_{top}\left(H^0(D)^{p^n}\right)$$

where, for a topological space X, $\dim_{top}(X)$ is the smallest k such that for every sufficiently fine open covering $\mathcal{U} = \{U_i\}$of X, every point x of X belongs to at most $k+1$ open sets U_i.

11.8 RR theorem

RR theorem. If $D \in \operatorname{Div}(C_p)$ is a positive divisor, then $\dim\left(H^0(D)\right) = \deg(D)$. If D is *any* divisor, then

$$\dim\left(H^0(D)\right) - \dim\left(H^0(-D)\right) = \deg(D)$$

(remember that these numbers are real numbers and not integers). $H^0(-D)$ corresponds to Serre's duality between $H^0(D)$ and $H^0(K-D)$ in the classical case. ◇

11.9 The rest of the story

Connes' programme is now (2017) to develop the *intersection theory* in the square $\overline{\mathfrak{A}} \times \overline{\mathfrak{A}}$ of the scaled arithmetic topos, to prove RR for this "surface" and show that for divisors D on $\overline{\mathfrak{A}} \times \overline{\mathfrak{A}}$ one has the inequality

$$\dim\left(H^0(D)\right) + \dim\left(H^0(-D)\right) \geq \frac{1}{2} D \bullet D$$

which would be the analog of the classical formula over $S = \overline{C} \times \overline{C}$ for curves:

$$\ell(D) + \ell(K_S - D) \geq \frac{1}{2} D \bullet (D - K_S) + \chi(S)$$

References

[1] Artin, E., 1921. "Quadratische Körper im Gebiete der höheren Kongruenzen I, II" , *Math.Zeitschr.*, 19 (1924) 153- 246. See *Collected Papers*, Addison-Wesley, Reading, MA, 1965.

[2] Bourbaki, N. (alias J. Dieudonné) 1948. Manifesto: "L'architecture des mathématiques", *Les grands courants de la pensée mathématique*, F. Le Lionnais ed., Cahiers du Sud, 1948.

[3] Cartier, P., 1993. "Des nombres premiers à la géométrie algébrique (une brève histoire de la fonction zeta)", *Cahiers du Séminaire d'Histoire des mathématiques* (2ème série), tome 3 (1993) 51-77.

[4] Connes, A., 2015. "An essay on the Riemann Hypothesis", *Open Problems in Mathematics*, (J.F. Nash, M.Th. Rassias, eds), Springer, 225-257..

[5] Connes, A., Consani, C., Marcolli, M., 2007. "The Weil proof and the geometry of the adeles class space", *Algebra, Arithmetic, and Geometry*, (Y. Tschinkel, Y. Zarhin, eds.), Springer, 2009.

[6] Connes, A., Consani, C., 2009. "Schemes over $\mathbb{F}_1$ and zeta functions", https://arxiv.org/pdf/0903.2024.pdf

[7] Connes, A., Consani, C., 2016. "Geometry of the scaling site", https://arxiv.org/abs/1603.03191.

[8] Corry, L., 1996. "Nicolas Bourbaki: Theory of Structures", *Modern Algebra and the Rise of Mathematical Structures*, (Chapter 7), Birkhäuser, 1996.

[9] Dedekind, R., Weber, H., 1882. "Theorie der algebraischen Funktionen einer Veränderlichen", *Journal für die reine und angewandte Mathematik*, 92 (1882) 181-290, Berlin.

[10] Garrett, P., 2012. "Riemann-Hadamard product for $\zeta(s)$", http://www-users.math.umn.edu/ garrett/m/ number_theory/ riemann_hadamard_product.pdf

[11] Hasse, H., 1936. "Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II, III", *J. Reine Angew. Math.*, 175 (1936) 55-62, 69-88, 193-208.

[12] Hindry, M., 2012. "La preuve par André Weil de l'hypothèse de Riemann pour une courbe sur un corps fini", http://www.math.polytechnique.fr/xups/xups12-02.pdf

[13] López Peña, J., Lorscheid, O., 2009. "Mapping $\mathbb{F}_1$-land. An overview of geometries over the field with one element"', https://arxiv.org/abs/0909.0069

[14] Milne, J., 2015. "The Riemann Hypothesis over finite fields from Weil to the present day", *The Legacy of Bernhard Riemann after One Hundred and Fifty Years* (L. Ji, F. Oort, S-T Yau eds), Advanced Lectures in Mathematics 35, International Press, 2015, 487-565.

[15] Petitot, J., 1993. "The unity of mathematics as a method of discovery: Wiles' example", http://jeanpetitot.com/ArticlesPDF/STW_Wiles.pdf

[16] Riemann, B., 1859. "Über die Anzahl der Primzahlen unter einer gegeben Grösse", *Monatsberichte der Königlichen Preußischen Akademie der Wissenschaften zu Berlin*. Aus dem Jahre 1859. S. 671-680. ("On the number of prime numbers less than a given quantity").

[17] Roquette, P., 2003. *The Riemann hypothesis in characteristic p, its origin and development*, 1,
https://www.mathi.uni-heidelberg.de/ roquette/rv.pdf

[18] Schmidt, F. K., 1931. "Analytische Zahlentheorie in Körpern der Charakteristik p, *Math. Zeitschr.*, 33 (1931) 1-32.

[19] Soulé, C., 2004. "Les variétés sur le corps à un élément, *Mosc. Math. J.*, 4 (2004), 1, 217-244.

[20] Tate, J., 1993. "A review of non-Archimedean elliptic functions", *Elliptic curves, modular forms, and FermatÕs last theorem*, Int. Press, Cambridge, MA, 1995, 162-184.

[21] Weil, A., 1938. "Zur algebraischen Theorie des algebraischen Funktionen", *Journal de Crelle*, 179 (1938) 129-138.

[22] Weil, A., 1940, Letter to his sister Simone (March 26, 1940), *Collected Papers*, vol.1, 244-255. Translated by M. Krieger, *Notices of the AMS*, 52/3 (2005) 334-341.