The entanglement of structures in complex proofs

PhilMath Intersem 7. 2016

Jean Petitot
CAMS (EHESS), Paris

The axiomatic method and its use in the history of mathematics (M. Detlefsen and J-J. Szczeciniarz, orgs.) Université de Paris VII

Tuesday, June 21st

The unity of mathematics

In mathematics, the context of justification is proof. It has been deeply investigated philosophically. But the context of discovery remains mysterious and is very poorly understood.

Structural concepts in Bourbaki's sense play a crucial role in it.

I am interested in the role of such structural concepts in *complex proofs* and the only way to understand something is to look at relevant examples.

Some monthes ago (November 2015), in the *7ème Rencontres Françaises de Philosophie des Mathématiques*, I gave the example of the Wiles-Taylor proof of the Shimura-Taniyama-Weil conjecture.

Today, I will try to explain what I understand of Connes' new conceptual strategy for proving *Riemann hypothesis*.

It is Connes himself who constantly stresses the fact that we need a *conceptual* understanding of the *formulas* involved in the problem to discover good strategies of proof.

RH is a very long story entangling some of the deepest methods and results of arithmetics, analysis, and geometry.

Its conceptual content is deeply correlated to this entanglement and in particular to the *analogies* from which it is derived.

A conceptually complex proof 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 the STW conjecture:

> *"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 leads to its resolution.".*

In the same paper, Mazur adds:

> *"One of the mysteries of the Shimura-Taniyama-Weil conjecture, and its constellation of equivalent paraphrases, is that although it is indeniably a conjecture "about arithmetic", it can be phrased variously, so that: in one of its guises, one thinks of it as being also deeply "about" integral transforms in the theory of one complex variable; in another as being also "about" geometry."*

All these quotations point out that the proof unfolds in the labyrinth of many different theories.

It is exactly the same thing for Connes' strategy concerning the RH. As he explains in "*An essay on Riemann Hypothesis*" (p. 2) he tries

> *"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"."*

We will meet an incredible amount of deep and heterogeneous mathematics in Connes' "navigation".

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 Riemman surfaces: 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, topoï, etale cohomology, etc. Deligne's proof of Weil's conjectures. Alain Connes emphasized the fact that, through Weil's vision, Grothendieck's culminating discoveries proceeds 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 pure arithmetics and the original RH by translating algebraic geometry *à la* Grothendieck (topoï, 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*.

Analogies, conceptual structures, axiomatics

In his celebrated letter written in prison to his sister Simone (March 26, 1940, *Collected Papers*, vol.1, 244-255, translated by Martin Krieger, *Notices of the AMS*, 52/3 (2005) 334-341), André Weil described his move towards RH in natural language using a lot of military metaphors to emphasize the fact that finding a proof is a *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.)".*

He wrote:

> *"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. It will not have escaped you (to take up the military metaphor again) that there is within all of this great problems of strategy." (p. 341)*

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 "*Nicolas Bourbaki: Theory of Structures*" (Chapter 7 of *Modern Algebra and the Rise of Mathematical Structures*, 1996).

And many authors have criticized the very limited Bourbaki's conception of logic.

My purpose is rather to focus on the fact that, for these creative mathematicians, the concept of "structure" is a *functional* concept, which has always a "strategic" *creative* function, namely "*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".

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: "L'architecture des mathématiques" (*Les grands courant de la pensée mathématique*, F. Le Lionnais ed., Cahiers du Sud).

The constant insistance 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", are not vanities of elitist mathematicians.

They have a very precise, strictly technical function: construct complex proofs in navigating into this holistic conceptually coherent world.

> *"The "structures" are tools for the mathematician." (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" (p. 227)*

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." (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." (p. 230)*

So

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

and intuition is guided by structures.

The distribution of primes

The story of RH begins with the enigma of the distribution of primes. The multiplicative structure of integers is awfull.

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 $\pi(p) = \frac{1}{2}(\pi(p_-) + \pi(p_+))$.

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*:

$$\pi(x) \sim \frac{x}{\log(x)}$$

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 $\zeta(2) = \pi^2/6$ 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):

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

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)`

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 the complex plane*.

It has a simple pole at $s = 1$ with residue 1.

Mellin transform, theta function and functional equation

It was discovered by Riemann in his celebrated 1859 paper "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 possesses 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 $e^{-n^2\pi\Im(\tau)}$. $\Theta(\tau)$ 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 Mellin transform:

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

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 has an analytic meromorphic continuation to the entire complex plane $\mathbb{C}$ and satisfies the functional equation:

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

So, computations give

$$\zeta^*(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\left(\sum_{n\geq 1}\frac{1}{n^s}\right) = \zeta(s)\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}$$

$\zeta^*(s)$ is the *total* 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 the place at infinity ∞ of $\mathbb{Q}$ (`see below`) 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 $\zeta_\infty(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)$

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 from the difference of behavior of the gamma function Γ.

Γ has poles at $s \in -\mathbb{N}$. The figure 1 shows it on the real axis.

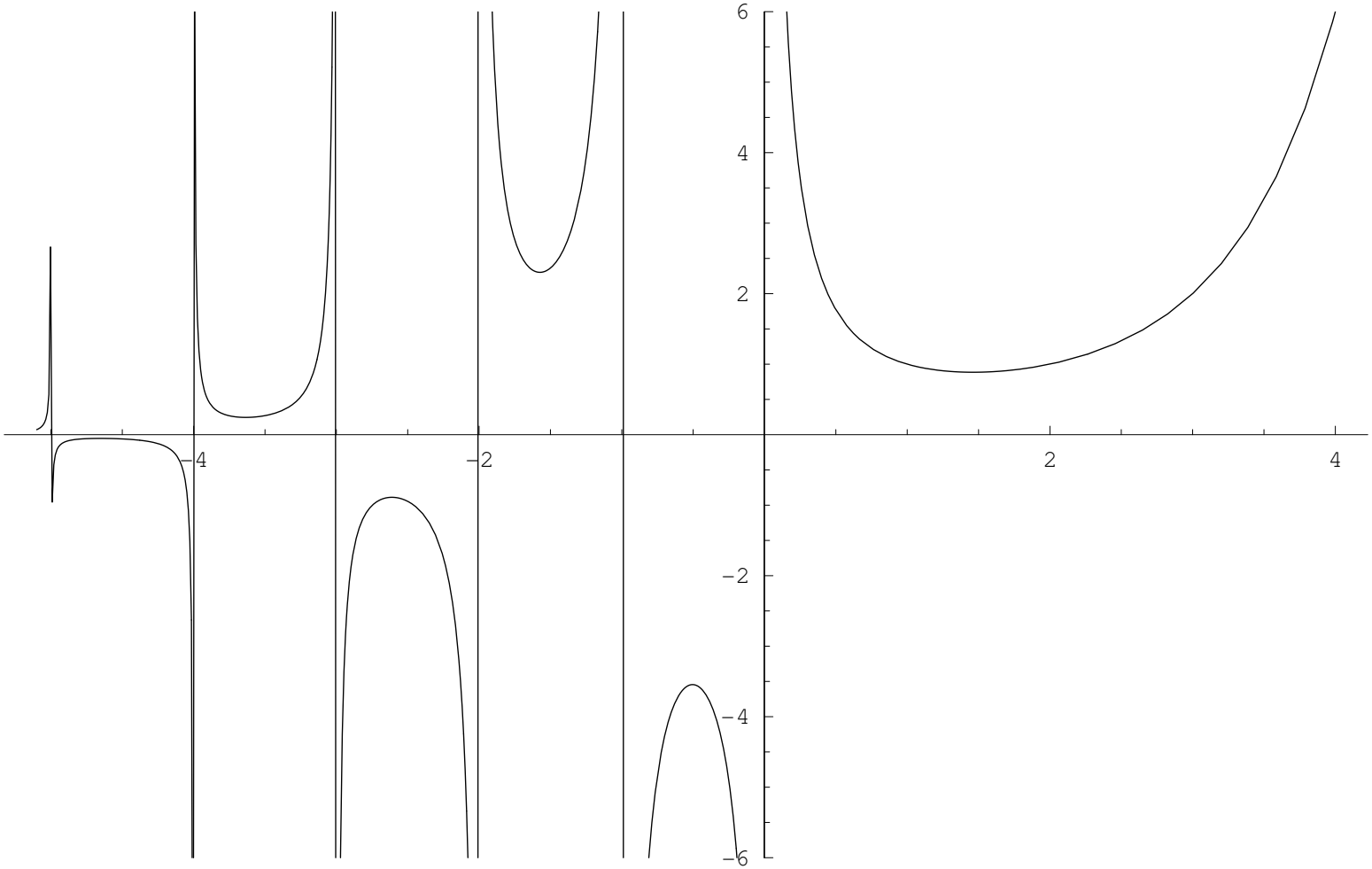
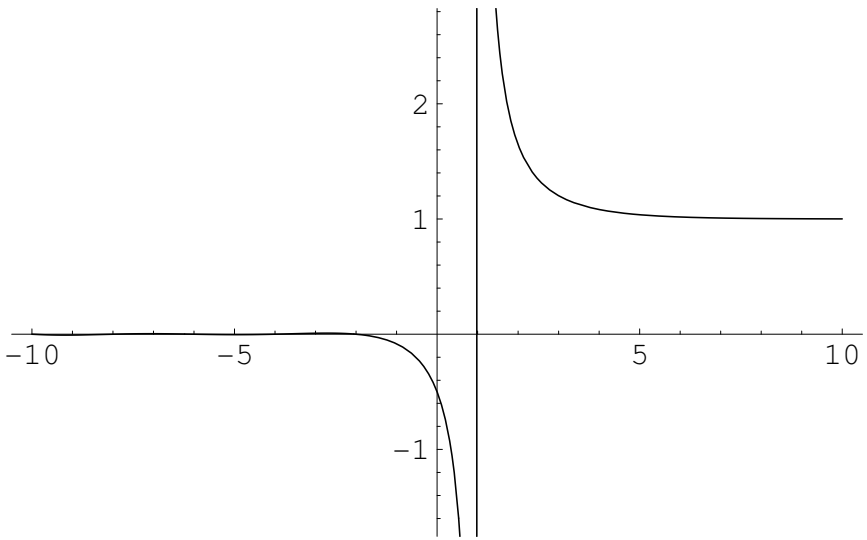


Figure: The Γ function on the real axis.

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



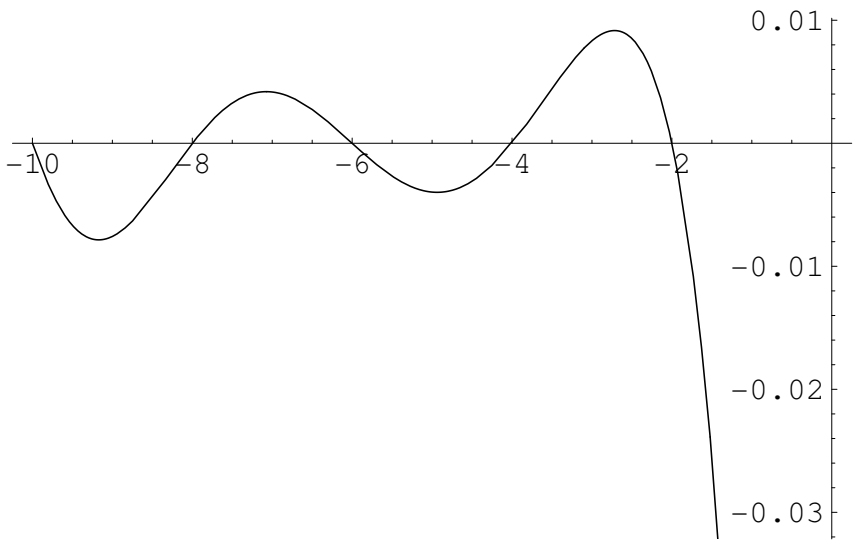


Figure: The graph of the zeta function along the real axis showing the pole at 1 (left). A zoom shows the trivial zeroes at even negative integers (right).

But $\zeta(s)$ has non trivial zeroes outside the domain $\Re(s) > 1$ where it is *explicitely defined* by the Euler product.

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).

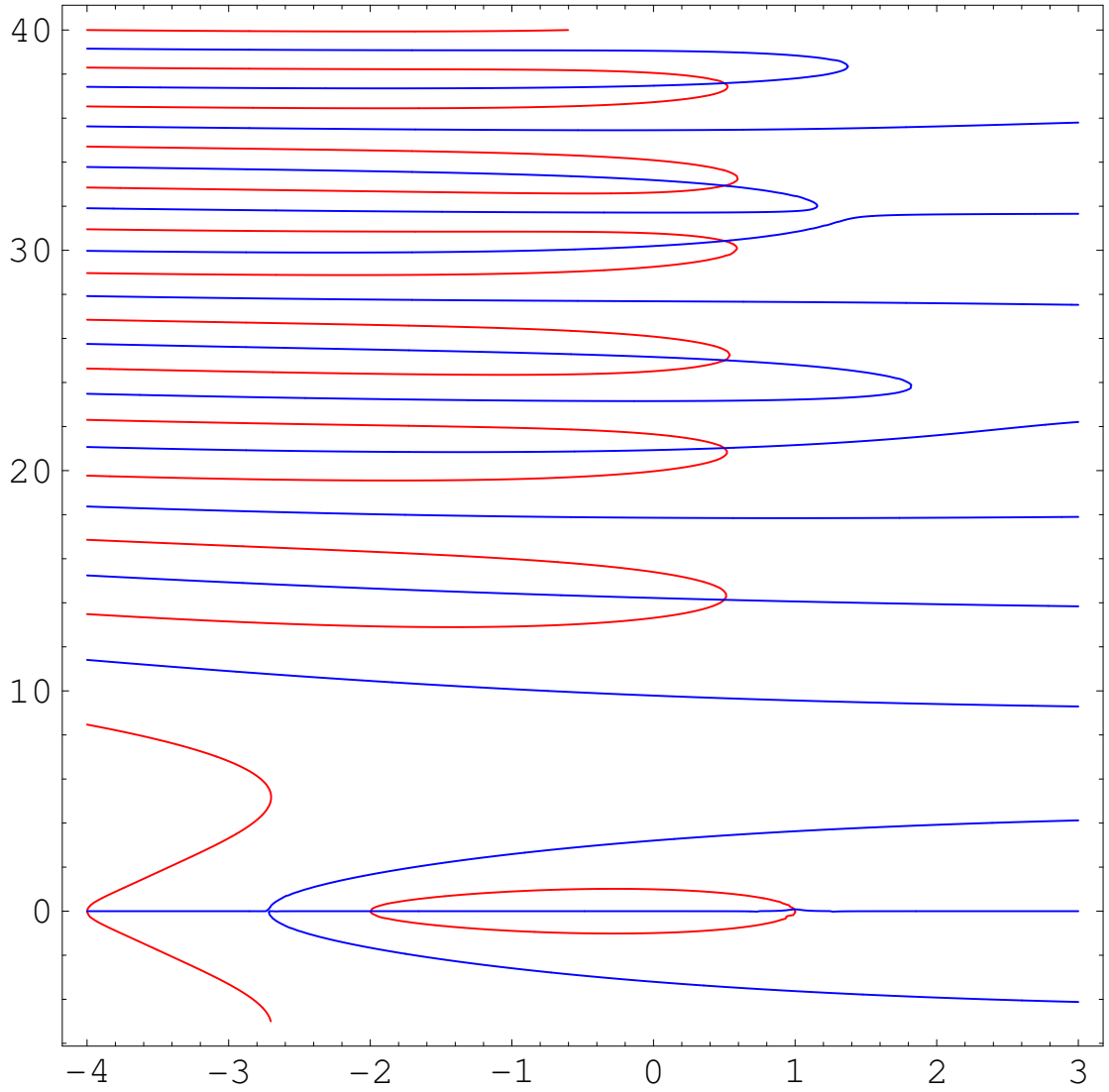


Figure: The null-lines of the real part (red) and the imaginary part (blue) of the zeta function.

It can be proved easily that all the non trivial zeroes of $\zeta(s)$ must lie inside the critical strip $0 < \Re(s) < 1$ (due to the functional equation it is sufficient to prove $\zeta(s) \neq 0$ for $\Re(s) \geq 1$, due to the Euler product expression $\zeta(s) \neq 0$ for $\Re(s) > 1$, due to the prime number theorem $\zeta(s) \neq 0$ for $\Re(s) = 1$).

Due to the functional equation they are symmetric w.r.t. the critical line $\Re(s) = \frac{1}{2}$.

It is traditional to write the non trivial zeroes $\rho = \frac{1}{2} + it$. 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.

Riemann showed that the number $N(T)$ of zeroes s.t. $0 < \Im(s) \leq T$ is of order $\frac{T}{2\pi} \log\left(\frac{T}{2\pi}\right) - \frac{T}{2\pi}$ and it is known that there exist an infinity of zeroes on the critical line and that the zeroes "concentrate" in a precise sense on the critical line.

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 $\Re(s) = \frac{1}{2}$.

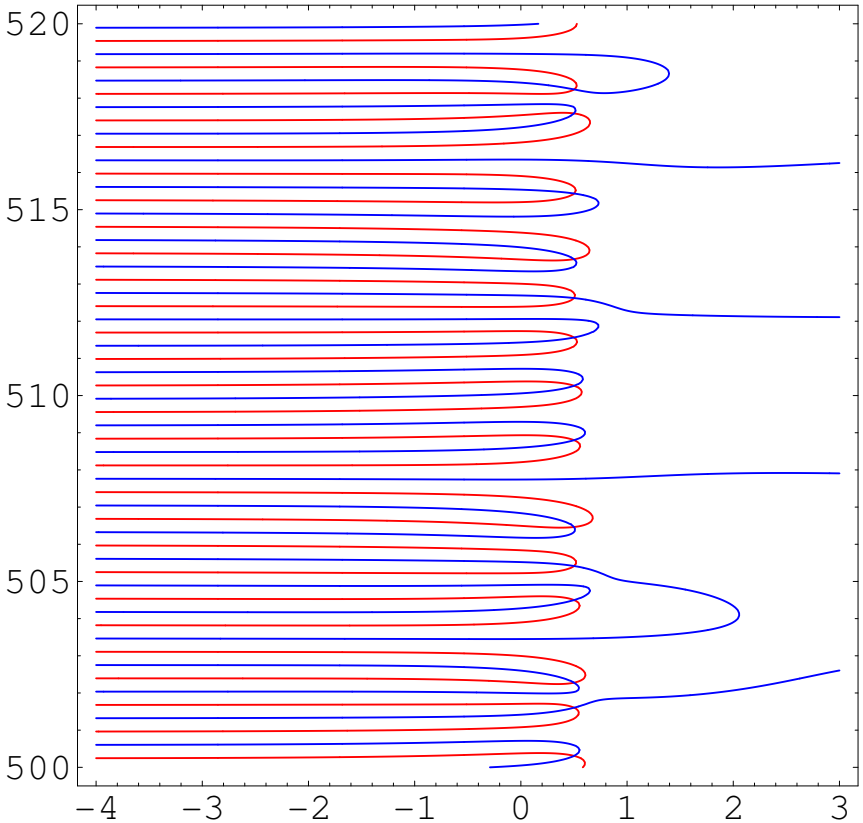
Riemann hypothesis

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.

We meet a lot of strange configurations.

For instance in figure 4 we show a configuration where a zero at the crossing of two folded lines (one red and the other blue) is *nested* inside a large folded blue line yielding another zero when crossing the upper folded red line.



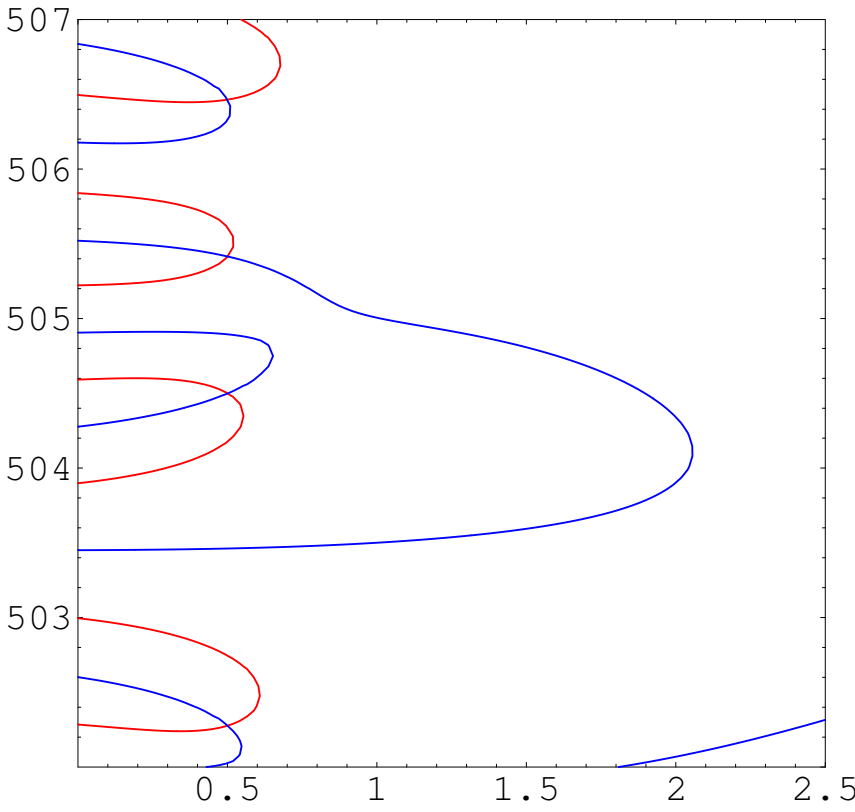


Figure: Configuration where a zero (crossing of folded red and blue lines) is nested.

Speiser proved that RH is equivalent to the fact that all folded blue lines cross the critical line (there is always a single non trivial zero on such a folded blue line).

When it is the case, one point is a zero and the other is called a *Gram point* that is a point where a blue line ($\zeta(s)$ real) crosses the critical line with $\zeta(s) \neq 0$.

Gram points seem to *separate* the non trivial zeroes (Gram's law), but it is not exactly the case.

There are situations where a zero and a Gram point are extremely close and in the reverse order and these "bad" situations increase continuously (Lehmer).

The figure 5 shows Lehmer's example with two extremely close zeroes between two Gram points (we note that we are at the height of the 26 830th line).

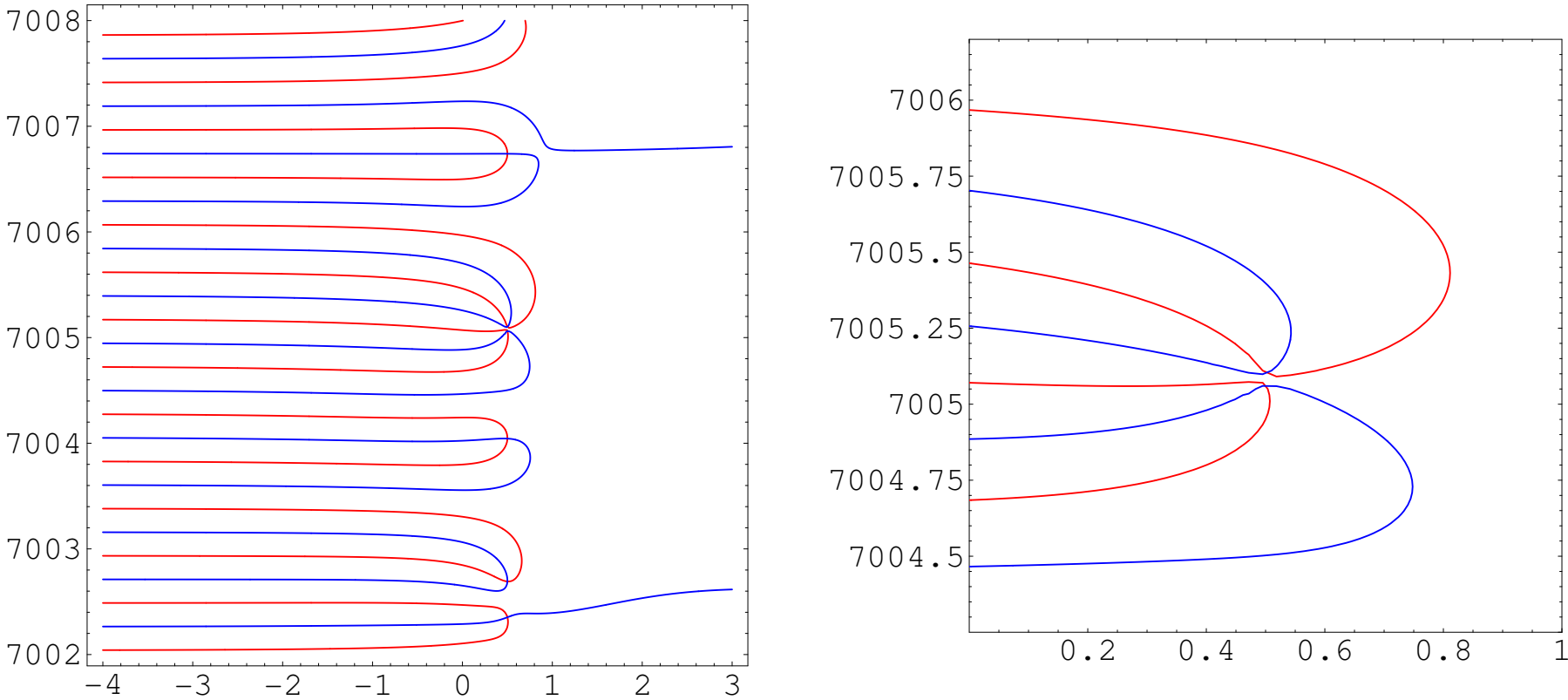


Figure: Lehmer's example of two extremely close zeroes of the zeta function.

It seems that there exists always a zero between two Gram points (Rosser's law). But it is not the case.

Figure 6 shows the first counterexample (we note that we are at the height of the 55 998 101th line).

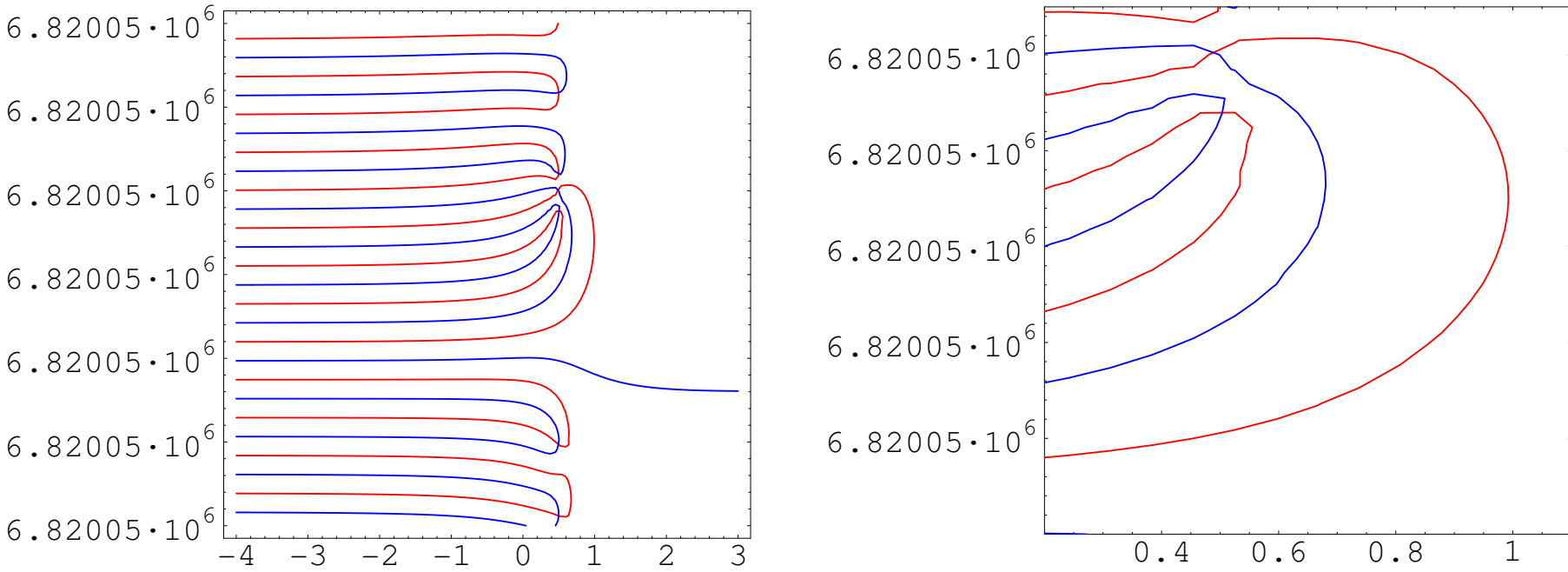


Figure: The first counterexample to Rosser's law.

So RH is really not evident.

As noted 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.

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, it is a great generalization of the problem solved by Galois for polynomials (of one variable).

If we consider a polynomial $P(x) = a_n x^n + \ldots + a_1 x + a_0$, the coefficients a_j give the symmetric functions of the roots and the problem of solving the equation $P(x) = 0$ is to go far beyond this raw information and find the localization of the zeroes.

Riemann's explicit formula

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

We have seen that, for $x \geq 2$, $\pi(x)$, the number of primes $p \leq x$ satisfies the asymptotic formula (prime number theorem) $\pi(x) \sim \frac{x}{\log(x)}$.

A better approximation, due to Gauss (1849), is $\pi(x) \sim \mathrm{Li}(x)$ where the logarithmic integral is $\mathrm{Li}(x) = \int_2^x \frac{dx}{\log(x)}$ (for small n, $\pi(x) < \mathrm{Li}(x)$, but Littelwood proved in 1914 that the inequality reverses an infinite number of times).

A still better approximation is given by the Riemann formula $R(x)$, where $\mu(n)$ is the Möbius function $\mu(n) = (-1)^r$ if n is a product of r distinct primes and 0 otherwise:

$$\pi(x) \sim R(x) = \left(\sum_{n \geq 1} \frac{\mu(n)}{n} \operatorname{Li}\left(x^{\frac{1}{n}}\right) \right) + \frac{1}{\pi} \arctan\left(\frac{\pi}{\log(x)}\right)$$

Figure 7 shows the step function $\pi(x)$ and its two approximations $\frac{x}{\log(x)}$ (in gray) and $R(x)$ (in blue).

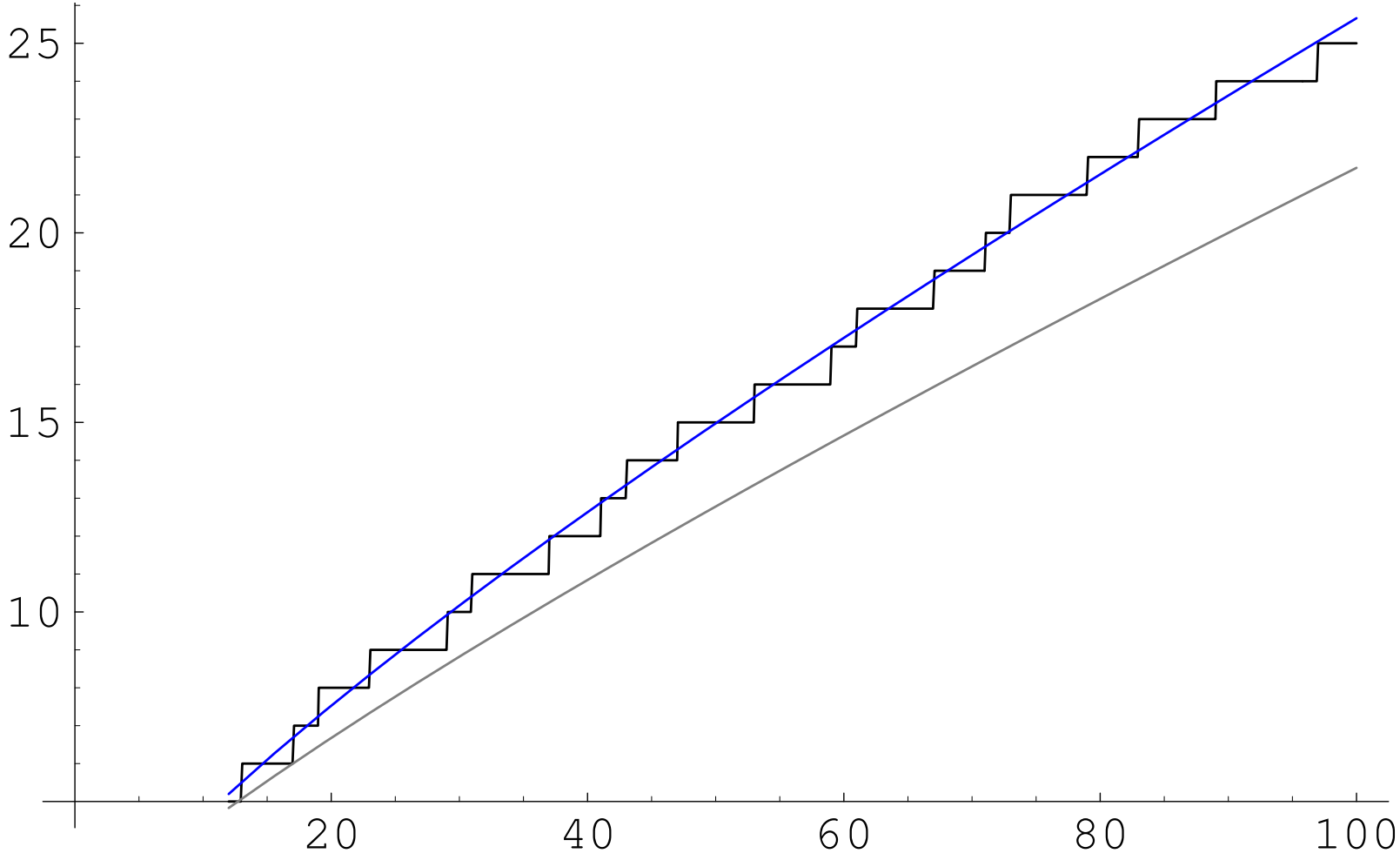


Figure: Two classical approximations of the distribution of primes.

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

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 an inverse transformation):

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

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

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

The approximation of $\pi(x)$ using Riemann's explicit formula up to the twentieth zero of $\zeta(s)$ is shown in figure 8.

We see that the red curve departs from the approximation $R(x)$ and that its oscillations draw near $\pi(x)$.

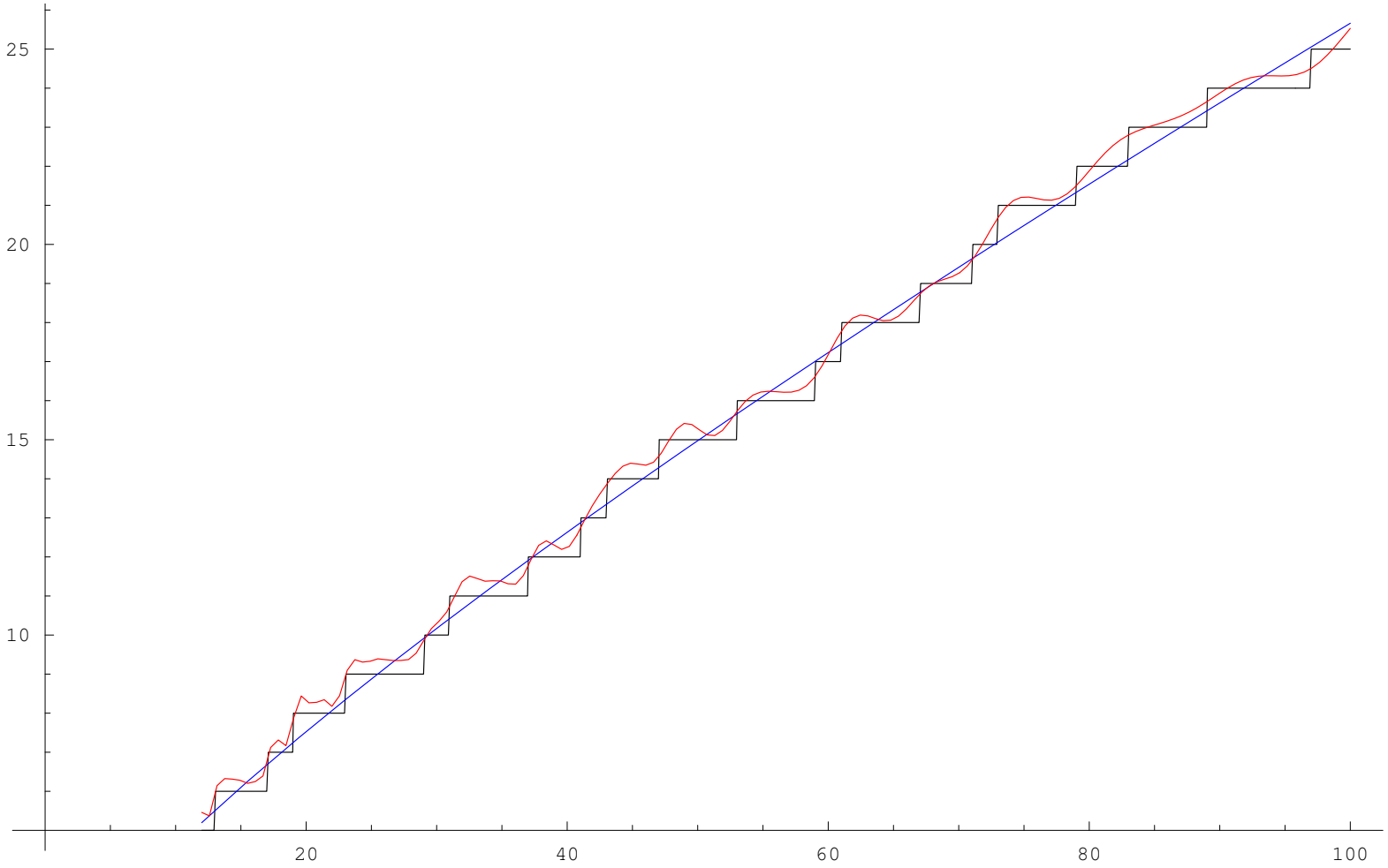


Figure: The approximation (red curve) of $\pi(x)$ by Riemann's explicit formula up to the twentieth zero of $\zeta(s)$.

A simpler explicit formula can be found using instead of $\pi(x)$ 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 $\psi(x) \sim x$.

In this context, Riemann explicit 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 van Mangoldt 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 Weil.

Weil's explicit formula

André Weil interpreted and generalized Riemann's explicit formula in an incredibly deep manner.

First he considered the formula in the context of *distribution theory*, where discontinuous fonctions such as $\psi(x) = \sum_{p,k:\ p^k \leq x} \log(p)$ can be interpreted using sums of Dirac distributions $D_p = \sum_{\ p^k} \log(p)\delta\left(u - p^k\right)$.

Indeed, $\psi(x) = \left\langle D, \chi_{[0,x]}(u) \right\rangle$ where $\chi_{[0,x]}$ is the characteristic function of $[0, x]$).

D_p is associated to the p-factor of ζ, that is to the p-adic place of $\mathbb{Q}$, and there must be also a D_∞ corresponding to the Archimedean real place ∞.

The formula becomes then a duality between D applied to "correct" functions $g(u)$ on $\mathbb{R}_+$ and the sum of the values of Mellin transform $\widehat{g}(s) = \int_0^\infty g(u)\, u^s \frac{ds}{s}$ on the poles 0 and 1 and the zeroes ρ of $\zeta^*(s)$:

$$\widehat{g}(0) + \widehat{g}(1) - \sum_\rho \widehat{g}(\rho) = \sum_\nu W_\nu(g)$$

where the W_ν are distributions associated to the different places p, ∞ of $\mathbb{Q}$. The W_p have their support on the p^k and W_∞ is a smooth function with a singularity at 1.

The admissible functions g must satisfy some strong conditions to make the formulas and integrals well defined.

If g is a "test" function (i.e. smooth with compact support) there is no problem.

But one needs more general functions, which are smooth excepted at "good" step discontinuities at isolated points u_0, where $g(u_0) = \frac{1}{2}\left(g\left(u_0^-\right) + g\left(u_0^+\right)\right)$ and with growth conditions which warrant that $\widehat{g}(s)$ is analytic in an open strip $\Re(s) \in]-\varepsilon, 1+\varepsilon[$ containing all the poles and zeroes of ζ^*.

Then, a lot of elementary computations show that:

For finite places,

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\widehat{g}\,(s)\,ds=\sum_{p,k\geq 1}\log(p)g\left(p^k\right),\quad 1<c<1+\varepsilon.$$

Using the fact that the Mellin transform of $\chi_{[0,x]}$ is $\int_0^x u^{s-1}ds=\frac{x^s}{s}$, this formula has for particular case the previous formula

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

For the Archimedean place ∞ (that is the Γ-factor of ζ^*), one gets a component of the form

$$\begin{aligned}
\text{term}_\infty &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(-\frac{\Gamma'(s)}{\Gamma(s)}\right)\widehat{g}(s)\,ds, \quad 1<c<1+\varepsilon \\
&= \frac{1}{2}\left(\log(\pi)+\gamma\right)g(1)+\int_1^\infty g(u)\frac{du}{u} \\
&\quad +\int_1^\infty \frac{\left(g(u)-g(1)\right)}{u^2-1}\frac{du}{u}.
\end{aligned}$$

Let $g^*(u) = \frac{1}{u} g\left(\frac{1}{u}\right)$ be the function whose Mellin transform is the symmetric $\widehat{g^*}(s) = \widehat{g}(1-s)$ of $\widehat{g}(s)$ w.r.t. the critical line:

$$\begin{aligned}
\widehat{g^*}(s) &= \int_0^\infty g^*(u)\, u^s \frac{du}{u} = \int_0^\infty \frac{1}{u} g\left(\frac{1}{u}\right) u^s \frac{du}{u} \\
&= -\int_\infty^0 v g(v)\, v^{1-s} \frac{dv}{v^2}, \quad v = \frac{1}{u} \\
&= \int_0^\infty g(v)\, v^{1-s} \frac{dv}{v} = \widehat{g}(1-s)
\end{aligned}$$

Then Weil's explicit formula obtains with $W_\nu(g)$ constructed from components as above for g and g^*.

For $\widehat{g}(s) = \frac{x^s - 1}{s}$ and $g(u) = \chi_{[0,x]}(u) - \chi_{[0,1]}(u) = \chi_{[1,x]}(u)$ (with the rule $\chi_{[1,x]} = -\chi_{[x,1]}$ if $x < 1$), one retrieves the Mangoldt formula.

Indeed $\widehat{g}(0) = \log(x)$, $\widehat{g}(1) = x - 1$, and $\widehat{g}(\rho) = \frac{x^\rho - 1}{\rho}$.

So the LHS is

$$\widehat{g}(0) + \widehat{g}(1) - \sum_\rho \widehat{g}(\rho) = \log(x) + x - 1 - \sum_\rho \frac{x^\rho}{\rho} + \sum_\rho \frac{1}{\rho}$$

while the RHS is

$$\Sigma = \sum_{p^k \leq x} \log(p) + \frac{1}{2}(\log(\pi) + \gamma) + \int_1^\infty g(u) \frac{du}{u} + \int_1^\infty \frac{(g(u) - g(1))}{u^2 - 1} \frac{du}{u}$$

with

$$\begin{aligned}
\Sigma &= \sum_{p^k \leq x} \log(p) + \frac{1}{2}(\log(\pi) + \gamma) + \int_1^\infty g(u) \frac{du}{u} + \int_1^\infty \frac{(g(u) - g(1))}{u^2 - 1} \frac{du}{u} \\
&= \sum_{p^k \leq x} \log(p) + \frac{1}{2}(\log(\pi) + \gamma) + \int_1^x \frac{du}{u} + \int_1^x \frac{1}{(u^2 - 1)} \frac{du}{u} \\
&= \sum_{p^k \leq x} \log(p) + \frac{1}{2}(\log(\pi) + \gamma) + \log(x) + \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right)
\end{aligned}$$

since

$$
\begin{aligned}
\frac{1}{2}\left(\log\left(1-\frac{1}{u^2}\right)\right)' &= \frac{1}{2}\left(\log\left(\frac{u^2-1}{u^2}\right)\right)' \\
&= \frac{1}{2}\left(\log\left(u+1\right)+\log\left(u-1\right)-2\log\left(u\right)\right)' \\
&= \frac{1}{2}\left(\frac{1}{u+1}+\frac{1}{u-1}-\frac{2}{u}\right) \\
&= \frac{1}{u\left(u^2-1\right)}
\end{aligned}
$$

So LHS = RHS means

$$\sum_{p^k \leq x} \log(p) + \frac{1}{2}(\log(\pi) + \gamma) + \log(x) + \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right)$$
$$= \log(x) + x - 1 - \sum_{\rho} \frac{x^\rho}{\rho} + \sum_{\rho} \frac{1}{\rho}$$

that is

$$\sum_{p^k \leq x} \log(p)$$
$$= x - 1 - \sum_{\rho} \frac{x^\rho}{\rho} + \sum_{\rho} \frac{1}{\rho} - \frac{1}{2}(\log(\pi) + \gamma) - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right)$$

Van Mangoldt formula

$$\sum_{p,k:\ p^k \leq x} \log(p) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \log(2\pi) - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right)$$

is therefore equivalent to

$$-1 + \sum_{\rho} \frac{1}{\rho} - \frac{1}{2}\left(\log\left(\pi\right) + \gamma\right) = -\log(2\pi)$$

that is

$$\sum_{\rho} \frac{1}{\rho} = 1 + \log\left(\frac{1}{2\sqrt{\pi}}\right) + \frac{\gamma}{2}$$

which can be proved.

Remark. As ρ and $1-\rho$ are zeroes,

$$2\sum_{\rho}\frac{1}{\rho}=\sum_{\rho}\frac{1}{\rho}+\sum_{\rho}\frac{1}{1-\rho}=\sum_{\rho}\frac{1}{\rho\left(1-\rho\right)}=2+\log\left(\frac{1}{4\pi}\right)+\gamma$$

As RH $\iff$ $1-\rho=\overline{\rho}$, we see that

$$\text{RH}\iff\sum_{\rho}\frac{1}{|\rho|^2}=2+\log\left(\frac{1}{4\pi}\right)+\gamma$$

More generally, RH is equivalent to the *positivity condition* for "test" functions:

$$\sum_{\rho} \widehat{g}(\rho)\,\overline{\widehat{g}\left(\overline{1-\rho}\right)} \geq 0 \quad \forall g \text{ smooth with compact support}$$

Indeed, if RH is true, then $\overline{1-\rho} = \rho$ and $\sum_{\rho} \widehat{g}(\rho)\,\overline{\widehat{g}(\rho)} = \sum_{\rho} \left|\widehat{g}(\rho)\right|^2 \geq 0$.

Conversely, if $\rho_0 \neq \overline{1-\rho_0}$ is a "bad" zero, on can construct a g violating the positivity condition.

Local/global in arithmetics

One of the main idea, introduced by Dedekind and Weber in their celebrated 1882 paper "Theorie der algebraischen Funktionen einer Verandlichen" (*J. Reine Angew. Math*, 92 (1882) 181-290), was to consider integers n as kinds of "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.

It is the origin of the modern concept of *spectrum* in algebraic geometry.

Then $\mathbb{Q}$ becomes the "global" field of "rational functions" on this "space".

If p is prime, the ideal $(p) = p\mathbb{Z}$ of p in $\mathbb{Z}$ is a prime (and even maximal) ideal. To localize $\mathbb{Z}$ 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* (that is with a *unique* maximal ideal) intermediary between $\mathbb{Z}$ and $\mathbb{Q}$ ($\mathbb{Q}$ is the localization of the prime ideal $\{0\}$).

$\mathbb{Z}_{(p)}$ is arithmetically much simpler than the *global* ring $\mathbb{Z}$ but more complex than the global fraction field $\mathbb{Q}$ since it preserves all the arithmetic inside (p).

The maximal ideal of $\mathbb{Z}_{(p)}$ is $\mathfrak{m}_{(p)} = p\mathbb{Z}_{(p)}$ and the residue field is $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

If $n \in \mathbb{Z}$, to look at n "locally" at p is to look at n in $\mathbb{Z}_{(p)}$.

The "value" of n at p is its class in $\mathbb{F}_p$, i.e. $n \bmod p$ and the local structure of n at p can be read in $\mathbb{Z}_{(p)}$.

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 $n_i \in \mathbb{F}_p$.

Weil's description of Dedekind'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 $\mathbb{C}$.

integers	$\longleftrightarrow$	polynomials
divisibility of integers	$\longleftrightarrow$	divisibility of polynomials
rationals	$\longleftrightarrow$	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."*

Valuations and ultrametricity

Dedekind and Weber defined the *order* of $n \in \mathbb{N}$ at p using the decomposition of n into primes.

Let $n = \prod_{i=1}^{i=r} p_i^{v_i}$. v_i is 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:

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

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 *metric* $d_p(x, y) = |x - y|_p$ and that, due to the last inequality, it satisfies the *ultrametric* property

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

which is *non-Archimedean* and 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.

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* (Hensel).

The successive rings $\frac{\mathbb{Z}}{p^k\mathbb{Z}}$ with the canonical projections $\frac{\mathbb{Z}}{p^k\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{p^\ell\mathbb{Z}}$ for $\ell > k$ constitute a projective system

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

where the arrows are the natural projections.

Let $\mathbb{Z}_p$ be 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 $\mathbb{Q}_p = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p\left(\frac{1}{p}\right)$.

$\mathbb{Z}_p$ 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 $\mathrm{mod}\, p^n$ for every $n \geq 1$.

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

The local p-adic field

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 $\frac{1}{p^n}$.

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 $(p-1)\,\mathrm{th}$ 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
$-1 = \frac{p-1}{1-p} = \sum_{n=0}^{n=\infty} (p-1)\, p^n$.

Hensel's geometric analogy

In Bourbaki's *Manifesto*, Dieudonné emphasizes Hensel's unifying analogy (with those of Hilbert spaces and Haar measure):

> *"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 rigourously justified using the concept of *scheme*:

primes p are the points of the *spectrum* of $\mathbb{Z}$,

the finite prime fields $\mathbb{F}_p$ are the fibers of the structural sheaf $\mathcal{O}$ of $\mathbb{Z}$,

integers n are global sections of $\mathcal{O}$,

and $\mathbb{Q}$ 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, analog to what are called *germs* of sections in classical geometry.

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 an "infinite" prime and is conventionally written $|x|_\infty$.

To emphasize the geometrical intuition of a "point", the "finite" and "infinite" primes are also called *places*.

To work in arithmetics with *all* places is a necessity if we want to continue 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 "*Zur algebraischen Theorie des algebraischen Funktionen*" (*Journal de Crelle*, 179 (1938) 129-138) he explains that he wants 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."*

It 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."*

Local and global fields

All the knowledge gathered during the extraordinay 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 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:

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

To summarize, 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 $\mathbb{R}$.

These local fields are the completions of $\mathbb{Q}$ at its finite (non Archimedean, ultrametric) and infinite (Archimedean) *places*.

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 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 (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 $\mathbb{K}$.

Adeles and subgroups of $\mathbb{Q}$

For the following, it is essential to 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 $(\mathbb{Q}, +)$.

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 $= 0$).

Here, $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ is the Pontryagin dual (the group of characters) of the additive group $(\mathbb{Q}/\mathbb{Z}, +)$ (see below).

This means that we take a finite set of p_j-adic numbers a_j and we take the rationals $q \in \mathbb{Q}$ s.t. $a_j q \in \mathbb{Z}_{p_j}$. 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 $\mathbb{A}_{\mathbb{Q}}^f / \widehat{\mathbb{Z}}^\times$.

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 parametrize the *characters* of the additive group $(\mathbb{Q}, +)$ and are needed to define its Pontryagin dual $\widehat{\mathbb{Q}}$.

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 exist 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 $a_p r \in \mathbb{Z}_p$.

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

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

Now, $\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}$, $s \longmapsto (s, \dots s)$ (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*.

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

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:

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

The RH for curves over $\mathbb{F}_q$ (Weil)

One of the greatest achievements of Weil has been the proof of RH for 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 $\mathbb{F}_q(T)$.

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 *polynomials*, which simplifies tremendously the situation.

The Hasse-Weil function

For the history of the ζ-function of curves over $\mathbb{F}_q$, see Cartier's 1993 paper "*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).

On the arithmetic side (spec($\mathbb{Z}$), $\mathbb{Q}_p$, $\mathbb{A}_{\mathbb{Q}}$, etc.), we have RH.

On the geometric side, we have the theory of compact Riemann surfaces (projective algebraic curves on $\mathbb{C}$).

On the intermediary level, at the beginning of the XXth century Emil Artin (thesis, 1921 published in 1924) and Friedrich Karl Schmidt (1931) 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,

> *"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." (p. 61)*

The main challenge was to interpret *geometrically* the zeta-function $\zeta_C(s)$ for algebraic curves C defined over $\mathbb{F}_q$.

It took a long time 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 is defined over $\mathbb{F}_q$, all its points are with coordinates in $\overline{\mathbb{F}_q}$, and we can look at its points with coordinates in intermediate 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

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

Note that $T\frac{Z_C'(T)}{Z_C(T)} = \sum_{r\geq 1} N(q^r)\,T^r$. The Hasse-Weil function $\zeta_C(s)$ of C is defined as

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

It corresponds to the two expressions of the classical Riemann's ζ-function (Dirichlet series and Euler product) if one introduces the concept of a *divisor* D on C as a finite $\mathbb{Z}$-linear combination of points of C: $D = \sum_j a_j x$.

The *degree* of D is $\deg(D) = \sum_j a_j$.

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

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*.

Divisors and classical Riemann-Roch (curves)

On the other direction, one try to transfer to curves over $\mathbb{F}_q$ the results of the theory of Riemann compact surfaces, 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 introduces the concept of a *divisor* D on C as a $\mathbb{Z}$-linear combination of points of C:

$D = \sum_{x \in C} \mathrm{ord}_x(D)x$ with $\mathrm{ord}_x(D) \in \mathbb{Z}$ the order of D at x.

All the terms vanish except a finite number of them.

The *degree* of D is then defined as $\deg(D) = \sum_{x \in C} \mathrm{ord}_x(D)$. It is additive.

D is said to be *positive* ($D \geq 0$) if $\mathrm{ord}_x(D) \geq 0$ at every point x.

If f is a meromorphic function on C, poles of order k can be considered as zeroes of order $-k$ and the divisor $(f) = \sum_{x \in C} \mathrm{ord}_x(f)x$ is called *principal* and its degree vanishes: $\deg(f) = \sum_{x \in C} \mathrm{ord}_x(f) = 0$.

By construction, divisors form an additive group $\mathrm{Div}(C)$ and, 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 $\mathrm{Div}_0(C)$.

The quotient group $\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Div}_0(C)$, that is the group of classes of divisors modulo principal divisors, is called the *Picard group* of C.

If ω and ω' are two meromorphic differential 1-forms on C, $\omega' = f\omega$ for some $f \in K(C)^*$ (the set of invertible elements of $K(C)$), $\mathrm{div}(\omega') = \mathrm{div}(\omega) + (f)$ and therefore the class of $\mathrm{div}(\omega)$ $\mathrm{mod}\,(\mathrm{Div}_0(C))$ 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 exists 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 S whose divisor (f) is greater than $-D$:

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

Since a holomorphic function on S is necessarilly constant (Liouville), 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.
$\dim L(D) = \deg(D) + \dim L(\omega - D) - g + 1$.

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 $\ell(0) = 1$).

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.

Let $\mathcal{U} = \{U_i\}$ be an open covering of C and D a divisor.

We take a family $f_i \in \mathcal{K}(U_i)$ whose zeroes and poles give exactly the points of D with their orders and we glue them on the intersections $U_i \cap U_j$ using $f_{ij} \in \mathcal{O}(U_i \cap U_j)^*$ (non vanishing holomorphic functions).

The $\{f_i, f_{ij}\}$ define a global section of the quotient sheaf $\mathcal{K}^*/\mathcal{O}^*$, and this section corresponds exactly to D.

Now, the f_{ij} can be used to define a line bundle on C with a sheaf of sections $\mathcal{O}(D)$ and Cartier has shown 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 $\dim L(D) = \dim H^0(C, \mathcal{O}(D))$.

Divisors and classical Riemann-Roch (surfaces)

For surfaces S, 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.

One shows that, as the base field is algebraically closed, this number is invariant by linear equivalence.

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.

One then defines $D_1 \bullet D_2 = D_1' \bullet D_2'$.

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* :

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

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

From Artin to Weil, the theory of compact Riemann surfaces has been transfered to the intermediate case of the curves $C/\mathbb{F}_q$. Schmidt and Hasse transfered the RR theorem.

A fundamental consequence was that $Z_C(T)$ not only satisfies a *functional equation* but is a *rational function* of T.

For instance, let us consider the simplest case $\mathbb{K} = \mathbb{F}_q(T)$ (coresponding 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 of its ideal is q^m.

But there are q^m such polynomials since the m coefficients a_j belong to $\mathbb{F}_q$. 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 easier.

The Frobenius

But in the $\mathbb{F}_q$ case, a completely original phenomenon appears.

A fundamental property of any finite field $\mathbb{F}_q$ is that $x^q = x$ for every 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, $N_1 = C(\mathbb{F}_q) = \#\varphi_q^{\mathrm{Fix}} = \left|Ker\left(\varphi_q - Id\right)\right|$. It is like a "norm".

RH for elliptic curves (Schmidt and Hasse)

Schmidt was the first to add the point at infinity (projective curves) 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 says

> *"on voit se manifester ici l'une des premières apparitions de la tendance à la géométrisation dans l'étude de la fonction ζ." (p. 69)*

Schmidt proved that

$$Z_C(T) = \frac{L(T)}{(1-T)(1-qT)} \text{ with } L(T) \text{ a polynomial of degree } 2g$$

He showed also 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

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

For ζ_C the symmetric functional equation is

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

Then, in three fundamental papers of 1936, 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*.

Hasse proved that, due to the functional equation, $L(T)$ is the polynomial $L(T) = 1 - c_1 T + qT^2$ 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.

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

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

and $\Re(s) = \frac{1}{2}$.

Hence, the RH.

Let us rewrite RH.

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

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

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.

He worked on $\overline{\mathbb{F}_q}$ (to have a good intersection theory) and in the *square* $S = \overline{C} \times \overline{C}$ of the curve C extended to $\overline{\mathbb{F}_q}$.

For a description of Weil's proof, see e.g. James Milne's paper "*The Riemann Hypothesis over finite fields from Weil to the present day*" (2015).

Let Φ_q be the graph of the Frobenius φ_q on $\overline{\mathbb{F}_q}$. It is a divisor of the surface S.

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 $S = \overline{C} \times \overline{C}$.

But one can apply 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:

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

Here the trace formula becomes

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

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

One considers the symmetric quadratic intersection form $s(D, D') = D \bullet D'$. We note 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 D of degree $= 0$.

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

$$\mathrm{def}\,(D) = 2\,(D \bullet \xi_1)\,(D \bullet \xi_2) - D \bullet D = 2d_1 d_2 - D \bullet D \geq 0$$

be what Severi called the "defect" of the divisor D.

Writing $\mathrm{def}\,(mD + nD') \geq 0$ for all m, n, we find

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

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 compute $\mathrm{def}\,(\Phi_q) = 2gq$ and $\mathrm{def}\,(\Delta) = 2g$. 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 is the generalization for genus g of RH (see above).

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 D

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

Remark. To the Hasse-Weil function $\zeta_C(s)$ is associated an *explicit formula* as in the arithmetic case.

The RHS is an intersection number $D \bullet \Delta$ between the diagonal Δ of $\overline{C} \times \overline{C}$ and a certain divisor $D = \sum_k a_k \Phi^k$ which is an integral linear combination of powers of Φ.

The terms $\widehat{h}(0) + \widehat{h}(1)$ of the LHS $\widehat{h}(0) + \widehat{h}(1) - \sum_\rho \widehat{h}(\rho)$ correspond to the $D \bullet \xi_j$ with $\xi_1 = e_1 \times \overline{C}$ and $\xi_2 = \overline{C} \times e_2$ (e_j points of $\overline{C}$).

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

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, topoï, 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 transfered by analogy.

The fundamental discovery is that for finding a strategy, one needs to work in the world of "*tropical algebraic geometry in characteristic* 1", and apply it to the noncommutative 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.

In his essay 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)"*

I will try to summarize now Connes' last two years Lectures.

Ingredients : semi-fields and characteristic 1

There are some key ingredients needed for implementing the strategy.

The main 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 $\mathring{+}, \mathring{\times}$ are *monoid* laws (i.e. associative, with neutral element, $\mathring{+}$ commutative, $\mathring{\times}$ distributive).

In particular, one can look at $\mathbb{Z}$ and $\mathbb{Q}$ using the sup $\vee$ as new addition $\mathring{+}$ and the $+$ or the $\times$ as new multiplication $\mathring{\times}$.

We will need in the following:

$\mathbb{Z}_{\max} = \{-\infty\} \cup \mathbb{Z}$ with $\mathring{+} = \vee$ ($-\infty$ is the neutral element since $x \vee -\infty = x$) and $\mathring{\times} = +$ (with neutral element 0).

$\mathbb{Z}_{\max}$ 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 there are *natural Frobenius maps* on $\mathbb{Z}_{\max}$. Indeed, if $n \in \mathbb{N}^{\times}$, $\varphi_n : x \mapsto x^{\circ n} = nx$ is an *endomorphism* of $\mathbb{Z}_{\max}$ (of course, $n(x \vee y) = nx \vee ny$ and $n(x + y) = nx + ny$).

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.

$\mathbb{R}^+_{\max} = \mathbb{R}^+$ 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, addition is idempotent $x \mathring{+} x = x \vee x = x$ and 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 $\times$, with $1 \vee 1 = 1$.

$\mathbb{R}^+_{\mathsf{max}}$ is an extension of $\mathbb{B}$ (there don't exist *finite* extensions of $\mathbb{B}$). Its Galois group is

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

and the $\lambda \in \mathbb{R}^*_+$ act as *Frobenius maps* $x \mapsto x^\lambda$.

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) on $\mathbb{R}^+_{\max}$.

Now, one can extend the classification of finite fields (the $\mathbb{F}_{p^n}$) to finite semi-fields. The result is remarkable.

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

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 the base 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 transfering Weil's proof of RH to this new framework.

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 V.P. 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 $\longrightarrow 0$ as $\hbar \longrightarrow 0$ in the semiclassical approximations of quantum mechanics.

Now, it is well known that

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

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.

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

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 $\mathbb{F}_{q^r}$.

The generating function of the $N(q^r)$ is
$Z_C(T) := \exp\left(\sum_{r\geq 1} N(q^r)\frac{T^r}{r}\right)$ and $\zeta_C(s) := Z_C(q^{-s})$.

But such Z_C are defined for every function $N(q^r)$, even if $N(q^r)$ does not derive from a curve.

An interesting question is therefore to know if it is possible to retrieve Riemann's original $\zeta(s)$ as a *limit case* of a 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 $K(C)/\mathbb{F}_q(t)$, 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.

Christophe Soulé had the fine idea to look at polynomials $Z_N\left(q^{-s}\right)$ for $q \longrightarrow 1$.

More precisely, as $Z_N\left(T\right)$ has a pole of order $N\left(1\right)$ at $q = 1$, he looked at limits

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

The question is then to know if there exists a counting function N giving

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

Such a "function" N *does* exist.

If one takes the logarithms, one gets

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

Connes and Consani have shown 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*

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

$N(u)$ is the derivative in the distribution sense of the increasing *step* function $J(u)$ on $[1, \infty)$ diverging to $-\infty$ at 1 (see figure).

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

See figure 9

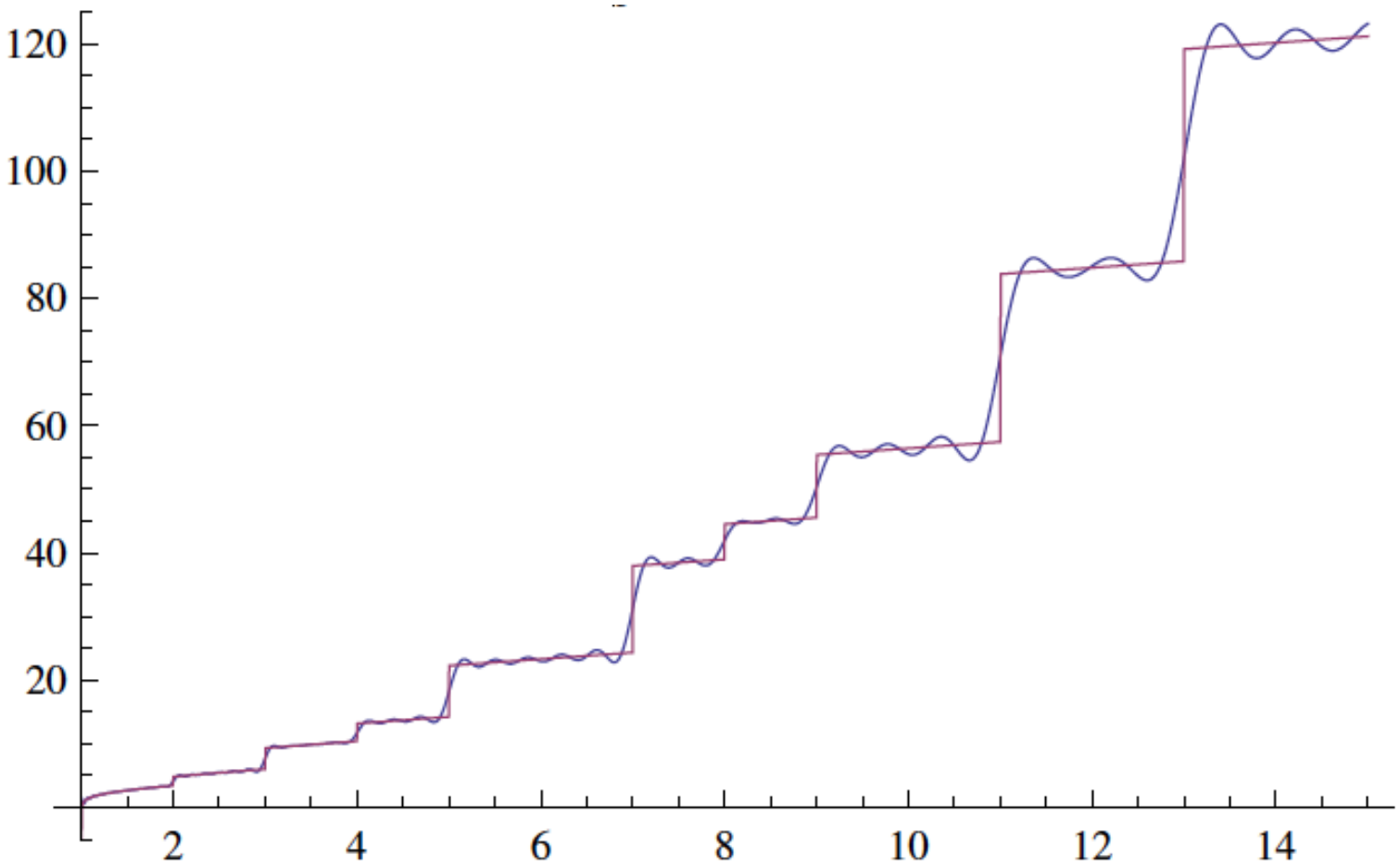


Figure: The integral of Soulé's distributrion

The arithmetic topos $\mathfrak{A}$

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

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 $\mathbb{R}_+^{\max}$

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.

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.

As the category is trivial, $\widehat{\mathbb{N}^\times}$ is a *topos* on the site $\mathbb{N}^\times$ endowed with the trivial Grothendieck topology. Now, $\mathbb{Z}_{\max}$ 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" $\mathbb{B}$.

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

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

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* $\mathbb{Q}$.

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) :

$$\mathcal{T} \quad \underset{p_*}{\overset{p^*}{\rightleftarrows}} \quad \mathfrak{Set}$$

This means that $\mathrm{Hom}_{\mathfrak{Set}}\left(p^{*}\left(F\right),S\right)\simeq\mathrm{Hom}_{\mathcal{T}}\left(F,p_{*}\left(S\right)\right)$, for $F\in\mathcal{T}$ and $S\in\mathfrak{Set}$.

$p^{*}\left(F\right)$ is the stalk of the topos $\mathcal{T}$ at the point p.

(See e.g. Mac Lane and Moerdijk and the Web site *nLab*.)

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 $p^*((X, \theta))$ s.t. $\mathrm{Hom}_{\mathfrak{Set}}(p^*((X, \theta)), S) \simeq \mathrm{Hom}_{\widehat{\mathbb{N}^{\times}}}((X, \theta), p_*(S))$.

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 in $\mathbb{N}^{\times}$.

To $p^* : \widehat{\mathbb{N}^{\times}} \to \mathfrak{Set}$ one associates the covariant functor $\mathfrak{p} : \mathbb{N}^{\times} \to \mathfrak{Set}$

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

and shows 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).

This means that beyond the given action of the multiplicative monoid $(\mathbb{N}^{\times}, \times)$ on X, there is in fact an action of the ring $(\mathbb{N}^{\times}, \times, +)$.

So, if one defines H_{+} as X endowed with the (well defined) commutative and associative addition $x + x' := \mathfrak{p}\left(k + k'\right)(z)$ for a z s.t. $\mathfrak{p}\left(k\right)(z) = x$ and $\mathfrak{p}\left(k'\right)(z) = x'$, 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 $z \in X$ s.t. 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 $z \in X$ s.t. $\mathfrak{p}(k)(z) = x$ 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.

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 $\widehat{\mathbb{N}^\times}$.

As the primes p are the 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.

Let $\mathfrak{p}_H$ be the point of $\widehat{\mathbb{N}^\times}$ represented by the subgroup H and let $H_{\max}$ be (see above) 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 $\mathfrak{p}_H$.

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".

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 $[0, \infty) \rtimes \mathbb{N}^{\times}$.

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 $n \in \mathbb{N}^{\times}$ s.t. $n\Omega \subset \Omega'$ (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.

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

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. with integral slopes $f' \in \mathbb{Z}$ except at points where f' presents a discontinuity (angular point),
5. convex.

As for the morphisms (scaling) $n : \Omega \to \Omega'$, one 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

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) that the H_a are parametrized by the finite adeles a.

It can be shown that – 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. $\mathbb{R}_+^\times$.

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.

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 (1) continuous, (2) $\mathbb{R}_{\max}$ -valued, (3) piecewise affine, (4) convex, (5) with slopes in H.

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

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

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

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

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

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 $\lambda, \lambda' \notin \mathbb{Q}$.

The "elliptic" case of periodic points

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* 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,

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

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."*

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 $f(\lambda)$ (1) continuous, (2) piecewise affine ($f(\lambda) = h\lambda + a$), (3) convex, (4) 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 (4) 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 f whose germs are *linear* at every point, i.e. C^1.

It is evident that there cannot exist *non constant global sections* of $\mathcal{O}_p^\times$ since we would have 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 $f(\lambda)$ (1) continuous, (2) piecewise affine, (3) *non necessarilly convex*, (4) 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).

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: $\deg\left((f)\right) = 0$.

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 $H_p / (p-1) H_p \leftrightarrow \mathbb{Z} / (p-1) \mathbb{Z}$.

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 $(\deg, \chi)$.

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. $\chi\left(\varphi_\mu(D)\right) = \mu\chi(D)$.

“Elliptic” functions and “theta” functions

In the classical case, it is well known that *elliptic* functions on the elliptic curve $E_\tau = C/\Lambda$ 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

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

(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.

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 $\mathring{+} = \vee$ and $\mathring{\times} = +$ on functions.

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

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 s.t. $D + (f) \geq 0$.

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

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 s.t. 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.

RR theorem

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

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

(remember that these numbers are real numbers and not integers).

$H^0\left(-D\right)$ corresponds to Serre's duality between $H^0\left(D\right)$ and $H^0\left(K - D\right)$ in the classical case.

The rest of the story

Connes' programme is now 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:

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

The analogy is

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