ON RIEMANN ZEROS AND WEIL CONJECTURES

LUCIAN M. IONESCU

ABSTRACT. The article aims to motivate the study of the relations between the Riemann zeros, and the zeros of the Weil polynomial of a hyper-elliptic curve over finite fields, beyond the well-known formal analogy. The non-trivial distribution of the p-sectors of the Riemann spectrum recently studied by various authors, represent evidence of a yet unknown algebraic structure exhibited by the Riemann spectrum, supporting the above investigations.

This preparatory article consists essentially in a review of the topics involved, and the "maize" of relationships to be clarified subsequently. Examples are provided and further directions of investigation are suggested.

It is, if successful, a viable, possibly new approach to proving the Riemann Hypothesis, with hindsight from the proof in finite characteristic and function fields.

CONTENTS

1. Introduction

The Riemann zeros are, according to the present author, conjecturally related to the zeros of the Hasse-Weil zeta function of hyper-elliptic curves, in its rational form, as stated by the Weil Conjectures, beyond the well known formal analogy [1].

Evidence of a nontrivial structure on the Riemann spectrum, consisting of the imaginary parts of the Riemann zeros $\rho = 1/2 + it$ (assuming for now the RH), comes from their high "Graham entropy" [2], and non-uniform distribution of the p-sectors of the Riemann spectrum [3, 4, 5, 6], as well as from the well-known duality primes-zeros [7, 8, 9].

Prior hints that the relation could come via the Mobius transformation $M(z) = 1 - 1/z$ mapping the critical line on the unit circle (circular permutation of $0, \infty$,1) (and 1/2 to -1), led the author to the study of *Cramer characters* $X_p = p^{it}$ [6], reinterpreting the findings regarding their distribution [3, 4].

Now, how are the roots like $\alpha = \sqrt{q}e^{it}$ related to the unit rational circle $Q/Z = \sum Q_p/Z_p$? Thus line of thought led to the investigation of their connections with the adelic duality [5]. But another even earlier idea is: if the RH was proved in finite characteristic, part of the Weil Conjectures (Dwark,Grothendieck,Delignes), in view of the formal analogy with Weil zeros and the local-to-global principle (e.g. Minkovsky Theorem), *and* the fact that in mathematics there are no coincidences, but not yet understood connections, why not uncover the *algebraic origin* of the Riemann zeros, beyond their analytical historical origin (like the source of the Niles!), and then prove that "they are what they have to be": zeros, of the Riemann Zeta Function, as a generating function (or its fermionic analog ζ^-1/ζ, the Dirichlet series of the Mobius function).

As Prof. Connes writes in his recent essay [10]: the RH "... is, and will hopefully remain for a long time, a great motivation to uncover and explore new parts of the mathematical world.". Indeed new for the present author, but with the hope that this journey shared with some readers, will "spread the word" on its beauty and importance, not just in mathematics, but apparently towards the "Ultimate Physics Theory": Number Theory! [11, 12] (What else!? would claim Pythagoras ...).

The article is organized as a gradual review of the topics leading to the Weil Conjectures and their relation to the Riemann Zeros. The "speculations", as an *Ariadne's thread* for future research, are "sprinkled" as needed, when the "muse" cared to share a thought of inspiration; all the other e/ho-rrors and mistakes, plenty I'm sure, will copiously feed the patient reviewer (Hopefully there will be one! ... the feedback hopefully received is part of the reason for writing these notes in the first place).

2. The Weil and Euler forms of the zeta function

2.1. **The Euler form of the zeta function.** Let X_0 be an affine variety over F_p, i.e. $X(\bar{F_p}) = \lim_{r\to\infty} X(F_{p^r})$, as an inductive limit over field extensions of finite fields of characteristic p.

2.1.1. *The degree of an element via Galois correspondence.* An orbit x_0 of $x \in X(\bar{F_p})$ under the action of the Galois group $G = Gal(\bar{F_p}/F_p)$ is called a *closed point* ([36],p.4). Denote by $X_{cl} = X_0/G$ the set of closed points. For $[x] = xG \in X_{cl}$ denote by $deg([x]) = |xG|$, the size of such an orbit.

The extension $F_p(x)$ is the residue field of $O(X)_x$, the localization of the coordinate ring of X at the point x. Then $deg([x]) = [F_p(x) : F_p]$ is the degree of the extension (number of elements in the orbit, i.e. roots of the irreducible polynomial defining the extension as $F_p[X]/(f)$, adjoined to F_p).

Remark 2.1. The degree can be also described in terms of K-valued points, i.e. ([37], p.2):
(1)
$$X(K) = Hom_{Speck}(SpecK, X) = Hom_{k-alg}(k(x), K), \quad deg(x) = |Hom_{k-alg}(k(x), K)|.$$

2.1.2. *The filtration/grading of a variety via the degree function.* The relation between the number of points and sizes of Frobenius orbits is provided in the following Lemma.

Lemma 2.1. *i) If $x \in X(F_{p^r})$ and $[x] = xG \in X_{cl}$ then $deg([x]) = [X(F_{p^r}) : X(F_r])$;*
ii) ([36]*, Lemma 2.3, p.4) $N_r = |X(F_{p^r})| = \sum_{e|r} e \cdot |\{x \in X_{cl} | deg(x) = e\}|$;*
iii) ("Burnsides Lemma"?) $N_r = |X(F_{p^r})| = \sum_{[x]\in X_{cl}, deg([x])|r} deg([x])$.

Proof. i) From the discussion above;
ii) Take $K = F_{p^r}$ in Equation 1.
iii) For an orbit $[x]$ of size $e = deg([x])$ belongs entirely to the Galois extension $F_{p^r} : F_p$. Therefore the whole orbit contributes with e points to the variety X. □

Remark 2.2. This is related to the Burnsides Lemma, in the context of the orbit-stabilizer theorem for the Galois action on the variety.

X_{cl} is the quotient set of X under the action of $G =< \Phi >$, the Galois group generated by Frobenius element.

Now F_{p^r} has a natural POSet structure, and since G is isomorphic to Z, which *also* has "the same" POSet structure (divisibility), the action "fibrates" over the PPOSet structure ("functoriality"?).

I) In the algebraic closure $\bar{F_p}$ we have:
1) Stabilizers $x \in F_{p^e}$, of degree e, i.e. not in a smaller subfield, $G_x = Stab_G(x) = \Phi^e$ (e.g. $e = 1$);
2) $Fix_{\Phi^e} = F_{p^e}$ (and similarly for $X_e = X(F_{p^e})$).

3) Orbit-Stabilizers Theorem: for $x \in X$, such that $deg([x]) = |Gx| = e$, i.e. $x \in F_{p^e}$ and not in a smaller subfield, $[G : G_x] = [Z : eZ] = e$. Equivalently, its orbit is of size e (the degree).

II) Similarly for the variety $X(\bar{F_p})$ ... ??? What is the difference?

For a concrete example, see §11.

2.1.3. *Proof of the Euler form of Weil Zeta Function.* The following corolary is an easy consequence of the above Lemma [36], p.4. and of a trivial number theory argument:

Lemma 2.2. *Let $D \subset N$ be a possibly infinite subset of natural numbers. Define $N_n = \sum_{d\in D, d|n} d$ Then $\sum_{n=1}^{\infty} N_n/nt^n = \sum_{d\in D} \log \frac{1}{1-t^d}$.*

Proof 1. *We follow the proof from* [36]*, p.2, removing the X_{cl} dependency, since only $D = Im(deg)$ is used, where $deg : X_{cl} \to N$ is the degree of closed points:*

$$\sum N_n t^n/n = \sum_{n=1}^{\infty} \frac{1}{n} \sum_{d\in D, d|n} dt^n$$

$$= \sum_{n=1}^{\infty} \sum_{d\in D} t^d/n = \sum_{d\in D} \sum_{n=1}^{\infty} t^d/n$$

$$= \sum_{d\in D} \log \frac{1}{1-t^d}.$$

Remark 2.3. Filtering the divisors of n via a subset is a limitation similar to a divisor inequality in Riemann-Roch, because of FTA: $P = SpecZ$. Indeed n can be viewed as a function on $SpecZ$, and its formal logarithm is a divisor $div(n) = \sum_{p\in P} k(n) < p >$, where $n = \prod p^{k(p)}$.

Remark 2.4. This Lemma is a "cross-section" by (degrees of) X of the classical Euler form of Riemann zeta function, based on uniqueness of factorization (The Fundamental Theorem of Arithmetic).

Corollary 2.1.

$$Z(X_0; t) = \prod_{x\in X_{cl}} \frac{1}{1 - t^{deg(x)}}.$$

Proof 2. *Apply the Lemma to the set $D = \{deg(x) | x \in X_{cl}\}$, of degrees of closed points of the variety X, and exponentiate.*

Remark 2.5. Note that the role of exponential and logarithm, are "marginal"; one can work with the generating series for the number of points $F(x) = \sum N_n t^n$ and its formal integral $G(t) = \int F(t)dt = \sum N_n t^n/n$ (see [42] for additional details). Bottom line, replace log by integration operator on (Cauchy) convolution algebra of formal power series:

$$\log \frac{1}{1-x} = \sum_{n=1}^{\infty} x^n/n.$$

As an example, consider the affine (projective) line $X = P^1$ over F_p. The "cross-section" is "trivial', since $deg([x]) = p^r$, for any $x \in F_{p^r}$ and not in a "lower" subfield F_{p^s}, with $s|r$. Then $n = \prod q^{k_q}$ defines a "cut-off" on $X = \bar{F}_p$, denoted $X_n = F_{p^n}$; the extension corresponding to incrementing the exponent k_q by 1 has degree q. $d = deg(x)|n$ implies $x \in F_{p^d}$, but not in a proper subfield. The Galois action partitions F_{p^n} into constant degree level orbits. Therefore the sum of their degrees totals p^n. Together with the point at infinity, $N_n = 1 + p^n$. The partition into orbits corresponds to the sum

$$1 + p^n = \sum_{d|n} |O_d| \cdot d.???$$

Example $n = 2$:

$$1 + p^2 = |F_p| + 2|F_{p^2} - F_p|.$$

Remark 2.6. This can be expressed in terms of the fixed points of Frobenius. Then, the roots of its characteristic polynomial should give a formula similar to the Binett's formula for the Fibonacci numbers, but for the "defect", e.g. $N_1 = 1 + p^n - a$.

2.2. **The orbit structure of X_0.** What is the orbit structure of X_0, from the Galois action etc. (cyclotomic polynomials etc.)? and why is the multiplicative function N_r a product of eigenvalues $1 - \alpha T$? How to view the Frobenius as an operator with characteristic equation the Weil polynomial? (numerator only; and NO l-adics, but possibly p-adics, because of $F_{p^r} = Hom(C_p, C_r) < - > C_{p^r}$ (how?) and $\lim C_{p^r} = Z_p$).

2.3. **Examples.** [36], p.2. Genus 0: $y^2 = 1 - x^2$. ...

Genus 1: $y^2 = 1 - x^3$ ...

2.4. **The Weil form of Zeta Function of Elliptic Curves.** In the case of elliptic curves, assuming $N_r = (1 - \alpha^r)(1 - \bar{\alpha}^r)$, which follows from the Tate-Weil proof of the Weil Conjectures for curves [40], p.32, one can easily derive the rational form of the ZF

$$Z(X_0; T) = \frac{1 - \alpha T)(1 - \bar{\alpha} T)}{(1 - T)(1 - qT)}.$$

2.5. **From Weil Form to Euler Form.** The main idea that partial fractions decompositions are involved, is exemplified.

Consider the partial fraction decomposition of the ZF of an EC:

$$\frac{1 - a_p T + pT^2}{(1 - T)(1 - pT)} = 1 + A/(1 - T) + B(1 - pT) = 1 + A \sum T^k + B \sum (pT)^k$$

$$= \sum N_n t^n/n.$$

3. The Projective Line

The projectve line $X = P^1$ has $N_n = 1 + p^n$ points over F_{p^n} (point at infinity and all other points).

For a concrete example of Frobenius orbits representation of N_n take $n = 2$. Then, for $d|n = 2$, there are points with one element orbit $x \in F_p$, and 2 points orbits $x \in F_{p^2} - F_p$, with a Burnside Lemma decomposition of X_0 (the affine curve) giving:

$$N_2^* = (p^1/1) \cdot 1 + (p^2 - p^1)/2 \cdot 2 = p^2, \quad N_2 = 1 + N_2^* = 1 + p^2.$$

Each orbit $\Phi^Z(x)$ has $d = deg(x) = [F_p(x) : F_p]$ elements, where the degree d also equals the size of the Galois group Z/dZ (equivalently Φ^d fixes $F_{p^d} = F_p(x)$.

3.1. From Euler to Weil, as a path integral.

So, in general, N_n decomposes according to the POSet of divisors of n, in a "path integral partition function with propagator p", conform with the interpretation of log as an integral: $exp(\log 1/(1 - x)) = exp(\int x^k dx)$. For example, when $n = 18 = 2 \cdot 3^2$, we have :

....later...

3.2. Projective line example.

To transform the Weil form into the Euler form of the zeta function of the projective line:

$$Z_X(T) = \frac{1}{(1-T)(1-pT)},$$

consider the *logarithmic derivative of the zeta function* [44], p.27 (see Weierstrass zeta functions; conform with our observation $\log 1/(1 - x) = \int \sum x^k$):

$$G(T) = d/dT \log Z_X(T) = \frac{1}{1-T} + \frac{p}{1-pT} = \frac{1}{1-T} + \frac{1}{p^{-1}-T},$$

a "lattice form" with poles at 1 and $1/p$ (and Riemann-Weil zeros, if the Weil polynomial is non-trivial).

4. Counting Frobenius orbits and Homotopy Theory

Frobenius orbits are related to the number of irreducible polynomials $P(x)$ over F_p (see MathExchange comments [45]), since $d = |Gx| = deg(x) = [F_p(x) : F_p]$ and $F_p(x) \cong F_p[x]/(P(x))$, therefore the Galois group (generated by the Frobenius) "relates" the subfields:

$$F_p \to F_{p^d} \to F_{p^n}.$$

The skeletal category of finite extensions of of F_p (which algebraists call it the algebraic closure $\bar{F}_p$ of F_p, destroying all its "good" structure :), has a structure of a 2-category, which is equivalent (in an abstract non-sense straight forward manner) to a homotopy theory, with $G = Gal$ playing the role of the fundamental groupoid (when ignoring the base point).

Remark 4.1. A homotopy theory has an associated homology theory via abelianization. A path integral seems to emerge naturally in this context (see above comments). Now where do the periods come from? ... From the keywords: Spec $F_p[x]$, duality and Fourier Series (better: localization and Feynman Path Integral over homotopy basis; Riemann graphs and Max-Flow-Min-Cut Theorem / discrete Hodge theory).

4.1. **Example.** As a concrete example, $p = 3, n = 2$, we have the following field isomorphism

$$\phi : F_3[x]/(x^2 + 1) \to F_3[x]/(1 - x - x^2), \quad \xi = \phi(\eta) = 1 - \eta.$$

When viewing fields as Klein geometry, or representations, we transition towards the following framework: abelian category of Z-modules (discrete vector spaces), with an "irreducible connection" (voltage graphs?), and "loop group" Gal ... Duality is not canonical either (relate to Frobenius elements).

4.2. **Relation with l-adic cohomolohgy.** Pursuing the categorical picture of isomorphic finite fields (objects) corresponding to irreducible polynomials of $F_p[x]$ seems to lead to l-adic cohomology (for a "fiber"), via the etale cohomology:

$$F_{p^n} = (Hom_{Set}(Z/p^n Z, F_p), \nabla)$$

where the reduction of the structure group as the multiplicative cycle, is though of as a "connection" (see also voltage graphs). This is the "Grothendieck's way", which we will avoid, since it is on the zeta function Euler product side of the bridge connecting with the Weil form. So, what is at the other end!?

4.3. **Conclusions: Quantum Physics on a Doughnut, Prezzel etc. and Finite String Theory.** Counting finite points of the projective line, via the Frobenius partition, i.e. summing degrees of extensions, and constructing the generating function, yields the logarithmic derivative of the Weil Zeta Function (Artin-Hasse).

When there are loops quantum effects are expected: resonance (periods) and "destructive interference" occurs (defect), and "correction terms" must be included in this "partition function" (see / get inspiration from the Primon / Riemann Gas model; see also my comments from "On Zeta Functions").

Why this is String Theory? A: primes dual to fundamental frequencies and fine structure constant, Euler beta integrals / Jacobi sums as Veneziano amplitudes etc. etc.

5. Localization and partial fraction decomposition: adelic picture

So, how numerator and denominator of the Weil form of the zeta function, contribute to the "adelic series" representation of the zeta function (partition function), in terms of degrees?

$$Q/Z = \sum Q_p/Z_p, \quad 1/6 = 1/2 - 1/3 = ...(\textit{adelic representation}).$$

Similar of polynomials?

$$Q[x]/Z[x] = \sum Q_p[x]/Z_p$$

and "localization" of $Z[x]$ polynomials at p (splitting).

Note: localization is a mode general tool / concept then the usual duality via Fourier transform (that's why partial fraction decomposition and Fourier series are directly related).

5.1. **An example.**

As a motivating example, recall how to compute the Fourier coefficients of a periodic arithmetic function, using partial fractions decomposition ([43], Example 7.1).

The period 3 arithmetic function $a(n) : 1, 5, 2, 1, 5, 2, ...$ has its generating function the series $F(z) = 1 + 5z + 2z^2 + z^3 + ...$ (algebra of functions, dual to convolution algebra of power series), which is rational (like Weil's zeta function):

$$F(z) = (1 + 5z + z^2) \sum_k z^{3k} = \frac{1 + 5z + z^2}{1 - z^3}.$$

Its partial fractions decomposition:

$$F(z) = \frac{A_0}{1 - z} + \frac{A_1}{1 - \rho z} + \frac{A_2}{1 - \rho^2 z}, \quad \rho = e^{2\pi i/3},$$

has coefficients A_i the Fourier series coefficients of a. Indeed, representing the fractions back as geometric series (convolution algebra inverses):

$$F(z) = \sum_n (A_0 + A_1\rho^n + A_2\rho^{2n} z^n$$

gives its coefficients represented as Fourier series coefficients:

$$\sum_{k=0,1,2} A_k \rho^k = a(n) = \sum_{k=0,1,2} \hat{a}(k)\rho^k.$$

In this example, the constants A_i satisfy the system:

$$3A_0 = 1 + 5 + 2, \ 3A_1 = 1 + 5\rho^2 + 2\rho^4, \ 3A_2 = 1 + 5\rho + 2\rho^2,$$

which yield $A_0 = 8/3, A_1 = -(4 + 3\rho)/3, A_2 = (-1 + 3\rho)/3$. Thus the finite Fourier series of a is:

$$a(n) = \frac{8}{3} + (-\frac{4}{3} - \rho)\rho^n + (-\frac{1}{3} + \rho)\rho^{2n}.$$

5.2. **Generating functions, Localization and Calculus.** The other "good example" is obtaining the closed form for the Fibonacci numbers [43], 1.1.

here the arithmetic function f_k is the solution of a recursive equation, or equivalently the solution of a finite differences equation.

The general framework is Calculus in a convolution algebra via $DF = F \star \mu$ finite differences, and $\sum a = a \star 1$ the corresponding integral (FTC is $\mu \star 1 = \delta$).

The paradigm is: 1) convert (duality) the arithmetic function $f \in Hom(N, C)$ into a generating function $F(z)$ (convolution algebra); 2) the recursive equation implies a polynomial equation for $F(z)$, which when solved yields a rational function for $F(z)$ (Weil!?); 3) Decompose it into partial fractions, i.e. represent it as an *adele*; 4) the (simple) pole part correspond to geometric series (integrals); 5) sum up and compare with the original generating function.

In our example, we have:

$$f_0 = 0, f_1 = 1, \ and \ f_{k+2} = f_{k+1} + f_k, \ for \ k \geq 0.$$

$$F(z) = \sum f_k z^k, \ Rec. \ Eq. \ \Rightarrow \ \frac{1}{z^2}(F(z) - z) = \frac{1}{z}F(z) + F(z)$$

$$F(z) = \frac{z}{1 - z - z^2} = \frac{1/\sqrt{5}}{1 - \alpha z} + \frac{1/\sqrt{5}}{1 - \bar{\alpha} z}, \ \alpha = (1 + \sqrt{5})/2, \ \bar{\alpha} = (1 - \sqrt{5})/2.$$

This yields Binet's formula:

$$f_k = 1/\sqrt{5} \cdot (\alpha^k - \bar{\alpha}^k).$$

There is a striking resemblance with the closed form for the defect of a curve from having the maximal number of points, a consequence of the Frobenius operator on the Tate module satisfying a certain characteristic polynomial:

$$a_k = 1 + q^k - N_k = \alpha^k + \bar{\alpha}^k, \ CharPoly(\phi) = (1 - \alpha T)(1 - \bar{\alpha} T).$$

In both cases (quadratic extensions), conjugation is the non-trivial Galois automorphism.

5.3. **Localization and Riemann-Weil Zeros.** How is the Fourier Series / Localization picture related with the interpretation of zeros as periods? The characteristic polynomial is similar to a recursive/differential equation. Is there a simpler convolution algebra affording an operator playing the role of the Frobenius?

The inverse of the Riemann-Weil roots should be interpreted as periods. For the general case of hyper elliptic curves, it is probably better to focus (study) $a_p(n) = 1 + p^n - N_n$, as the "defect", which probably is related to the Fourier Transform of the periodization of the function representing the coefficients of the polynomial defining the curve:

$$1 + p^n - N_n = \sum_1^{2g} \alpha_i^n, \quad \alpha_i \text{ ``}periods''of?.$$

So, the *generating function $G(T)$ of the number of finite points* has a better interpretation in terms of partial fractions decomposition, which *is* related to Fourier Transform [43], Ch.7.

5.4. Riemann zeros for elliptic curves.

For the EC $X : y^2 = c - bx + x^3$ Weil poly

$$P_1(T) = 1 - aT + qT^2 = (1 - \alpha T)(1 - \bar{\alpha} T), \ \alpha = q^{1/2+i\gamma} = \sqrt{q} e^{i\theta},$$

with $Re(\alpha) \in \frac{1}{2} Z$.

What is the geometric meaning of the generalized Pythagoras relation?

$$\sqrt{N}^2 = 1 + \sqrt{q}^2 - 2\cos\theta, \ \theta = \gamma \log q.$$

(Modular lattice, Coxeter group of symmetries ...?)

See also EC/group laws / Silverman? (Primes and crypto?)

There should be a relation between the Galois group of $f(x)$ (cyclotomic polynomials) and Weil poly:

$$\text{“}prime\ poly\text{''} \ \Phi(x) \ \Leftrightarrow \ primes \ F_p$$

What are the irreducible poly of degree 3? No $x - k$ factors; Euclid's trick DNWork.

Study the correlation $f(x) \in SpecF_p[X]$ and Riemann zeros γ_f. Relate it with Jacobi sums as 2-cocyles of Gauss sums (extensions / deformations?). Modulo twist $f_b(x) = 1 + bx + x^3$; $b \mapsto a$?.

Any f splits eventually in F_q, $q = p^r$, $r \leq 3!$. Is this the reason the zeta function is rational?

What is the Weil poly for $X : y^2 = (x - a)(x - b)(x - c)$, with $a, b, c \in F_p$?

What about $(y - y_1)(y - y_2) = (x - x_1)(x - x_2)(x - x_3)$: transversal intersections? (Towards Lefshetz theory).

6. The Cyclotomic Elliptic Curve $y^2 = 1 - x^3$

First we look at the “base case” of points over the primary field F_p, and then consider points over extensions to F_{p^l}), i.e. higher dimensional representations.

This is just the intersection in $F_p \times F_p$ of the p-cycle $(x, f(x))$ (graph of $f(x)$) and the “parabola” (x, x^2) (graph of x^2).

It's s a problem suited for intersection theory and Lipschitz indexes framework.

6.1. Lefschetz intersection theory and physics interpretation.

Alternatively, one can investigate the *intersection number* of the two cycles on the q-torus $F_q \times F_q$ (here $q = 5$):

$$Graph\ of\ x^2,\ and\ Graph\ of\ x^5.$$

The String Theory interpretation is clear: “What is the nodal interaction (Veneziano amplitude?) of the 6-mode with the 2-mode on a 5-string”?

Are the Riemann zeros “resonances”, i.e. Laplacian eigenvalues?

6.2. **The projective vs. affine curve.** The projective curve is $Y^2Z = Z^3 - X^3$, and if $Z = 0$ then $X = 0$, therefore the curve has just one point "at infinity": $(0 : \pm 1 : 0)$:

$$|\tilde{\mathcal{C}}(F_p)| = 1 + \mathcal{C}(F_p).$$

6.3. **Counting branching indexes.** As before, $N(x^3 = a)$ and $N(y^2 = b)$ are the branching orders at various points. Then, viewing the defining equation as a linear combination of monomials:

$$y^2 = a,\ x^3 = b,\ a + b = 1,$$

yields

$$|\mathcal{C}(F_p)| = \sum_{a+b=F_p} N(y^2 = a)N(x^3 = b).$$

The branching orders can be expressed in terms of the orbit of the corresponding character, and roots of unity:

1) If $f(x) = x^3 : F_p^\times \to F_p^\times$ has trivial kernel, i.e. if there are no roots of unity, $N(x^3 = b) = 1$; this is the case when 3 does not divide $p - 1$;

2) If $3|p - 1$, then $x^3 : F_p^\times \to F_p^\times$ has index 3, and $N(x^3 = b) = 0$ if b is not in the image of $f(x)$, or $N = 3$ if it is. In this case, it can be represented as a Fourier series of a multiplicative character of order 3, for example in terms of $\chi(x) = x^3$:

$$N(x^3 = b) = \chi^0(b) + \chi(b) + \chi^2(b).$$

Remark 6.1. Is there a general "paradigm" if we consider the polynomials as the algebra of monomials x^n, viewed as branching covers of the p-cycle F_p, and its tori / extensions?

Why Fourier series represents the index $N(x^n = b)$?

The above sum can be estimated using Jacobi sums, and the Hasse-Weil bound is obtained.

6.4. **Extending the field / dimension of representation space.** The main goal is to identify the "global object", having all the points of field extensions F_{p^n}.

Extending the field from F_p to F_{p^n} means representing the operator T with characteristic polynomial and eigenvalues $det(I - \lambda T) = P(T) = 0$ to higher dimensions.

Counting the points of the *projective closure* gives a nicer formula; is it because of Bezout Theorem, as part of the Intersection Theory framework, or because of the 2D-representation in projective space (Mobius transformations)?

Remark 6.2. A more categorical oriented framework avoids fractions, which can be interpreted as the result of evaluating morphisms: $Ev(g : a \to b) = ba^{-1} = b/a$.

6.5. **Weil form and Jacobi sums.** Counting the points via Jacobi sums yields

$$N_r = 1 + p^r + J + \bar{J}, \ J = (\chi_2 * \chi_3)(1),$$

where the convolution is over F_{p^r}.

In our example, the root $\alpha = J(\chi_2, \chi_3)$ is a Jacobi sum of the corresponding two characters. Note that the Jacobi sum is a Hochschild 2-coboundary [41]:

$$J = dG.$$

Then, what is the significance when looking at N_1 as an "Lefschetz" intersection number of χ_2 and $1 - \chi_3$? Same as $I(\chi_2, \chi_3)$?

Remark 6.3. The **Theory of Jacobi and Gauss sums** yield the Riemann Hypothesis for EC/ff:

$$|J| = \sqrt{p}^r.$$

Does it yield also the power r dependency? Will a deformation argument together with a twist, yield the general case for EC from $y^2 = 1 - x^3$?

6.6. **The Weil form of the Zeta Function.** Then we have the Weil form of the ZF:

$$Z(X,t) = \frac{(1+Jt)(1+\bar{J}t)}{(1-q^0t)(1-qt)}.$$

Remark 6.4. The main point is to notice how $N_r = (1-\alpha^r)(1-\bar{\alpha}^r)$ is determined by $N_1 = (1-\alpha)(1-\bar{\alpha})$, where α and its conjugate are the eigenvalues of an operator on $X(Q_p)$ induced by the Frobenius on $X(\bar{F}_p)$.

So, the main focus is to understand N_1!

Why $N_r = deg(1-\phi^r)$ (degree of the Frobenius), and how it can be represented as a determinant on the l-adic curve $= det(1-\phi^r)$?

Is this the setup for a "homotopic contraction" $\phi^r, r \to \infty$ argument? and how it related to p-adic roots of unity via Teichmuler character? ... Homotopy contraction in Q_p, via lifting F_p?

Is the "infinitesimal case" (f.f. level F_{p^n}) due to the Theory of Jacobi-Gauss sums? (Feynman integrals / p-string theory amplitudes).

6.7. **SAGE Exercise: compute Jacobi-Gauss sums / R-Spec.** Focus on the "cyclotomic EC" $y^2 = 1 - x^3$, and determine R-Spec ($|R - Spec| = 2 \times genus$) for a few primes:

$$R - spectrum(g=1) : \{e^{\pm i\gamma}\}.$$

1) See how $e^{i\gamma}$ correlates with the prime p; is it $p^{i\theta}, \theta = \gamma/2\pi \log p$ more relevant? (or similar? see [19]).

2) Generalize to the case $y^2 = f(x)$ and see how $e^{i\theta}$ correlates with the coefficient / roots of $f(x)$.

3) How hyper-elliptic curves (higher genus) "generate" more R-frequencies/periods? Compare with the theory of Hodge cycles (Jacobi variety? Liouville action variables?).

7. The Cyclotomic EC $y^2 = x^3 + 2$ and $p = 7$

For $q = p = 7$, counting the points: $N_1 = |E(F_7)|$ by computer [39] p.19., the Weil-Betti polynomial $P_1(T; q)$ is:

$$1 + T + 7T^2,\ a = -1,\ N_1 = 1 + q - a = 9, N_2 = (1 + q)^2 - a^2 = 63.$$

Remark 7.1. Is $N_r = (1+q)^r - a^r$? some recursive relation (finite differences equation) ... (like Fibonacci sol. etc.). (instead of as Taylor coefficient loc. cit. p.11).

The solution should be

$$N_r = (1 - \alpha^r)(1 - \bar{\alpha}^r) = (1 + q^r) - (\alpha^r + \bar{\alpha}^r),\ \alpha = q^{1/2+i\gamma},$$

where $\alpha, \bar{\alpha}$ are the zeros of the Frobenius polynomial [39], p.18, and $\rho = 1/2 \pm i\gamma$ are the Riemann zeros for finite fields ("local zeros").

Why are $\alpha^r + \bar{\alpha}^r = q^{r/2}(q^{i\gamma r} + q^{-i\gamma r})$ integers? They are Jacobi sums ($J = dG$ cocycles of Gauss sums - Feynman Integrals/ Veneziano Amplitudes ...)

How do they build up the "global" Riemann zeros?

Study the relationship between $f(x) = 1 + bx + x^3$ forget the twist; see how the perturbation affects the a, N and the zeros, in correlation with the primes (level 1: π_1 / Hodge basis).

Find a "simple" model for Frobenius morphism on Tate's module. Does it matter if $f(x) = 0$ is solvable in Q_p? (Hensel's Lemma)

case 1: $f(x) = 0$ one solution / point in $E(F_p)$;

case 2: $f(x) = 1$ (quadratic residue in any F_p); $N(f(x) = a) = |Ind(f; a)|$. For example when $f(x) = 1 - x^3, Ind = 1$ etc. How does the index vary with a? Is there a nice Lefshetz formula? (orientation matters? de Rham vs. Lebesgue)

case 3: $f(x) = a$ quadratic non-residue, so there is no solution.

Why this has to do with Frobenius filtration and eigenvalues, which in Q_p are the roots of unity (Teichmuller character):

$$\omega(j) = \lim j^{p^n},\ \Phi(\omega(j)) = \omega(j).$$

Perron-Frobenius eigenvalue of 1? Are there other eigenvalues?

8. Turning On The Golden Key: Riemann Roch Theorem

The Euler form of the zeta function is expressed naturally in terms of Frobenius orbits, in the context of the category of field extensions. Grothendieck's approach, via Grothendieck covers, is to use l-adic cohomology in this context, as a Weil cohomology to derive the Weil form. Yet the Riemann zeros are not well accounted for in this way.

Instead, we directly look for an algebraic-geometric object behind the Weil form, probably the analog of the Jacobian variety / zero-Picard group, which should emerge in the finite field case from Gauss sums and their 2-cocycle, the Jacobi sum.

8.1. **Weil form and Riemann Roch genus.** The Weil form defines a genus as $q = Int(dimC/2)$, which should coincide with $g = dimL(K_C)$, where K_C is the canonical divisor (flow) on the curve (Riemann surface for complex numbers).

Riemann-Roch formula has also a symmetric form which exhibits duality [46]. As a confirmation, Tate, in his thesis, calls the adelic Poisson summation formula (Fourier duality), the Riemann-Roch Theorem.

So, what is the complex which implements the algebraic topology concepts (see [47]), having the Jacobi sum as a 2-cocyle? probably Gauss sums play the role of Feynman path integrals $\int_C e^{S(C)}$ (period on Z_n for the n-th degree character). Or better the powers $x^k : Z_n \to Z_n$ play the role of "standing waves" (nodes), and the convolution $J(c, c') = c \star c'(1)$ is a Veneziano amplitude ... (to be made precise later :).

8.2. **Riemann-Roch and Poisson Trace Formula.** Underlying RR - Poisson SF (trace formula), there is the localization - Fourier duality connection: partial fractions decomposition (localization at roots of unity $z^n = 1$, i.e. iso to Z_n), gives the Fourier coefficients of the periodic arithmetic function $a \in Hom(Z_n, \mathbf{C})$.

Relate this with the counting of points of $y^2 = f(x)$ via Jacobi sums.

9. Weil zeros as Gaussian periods

9.1. **Recall.** The Euler form has the category of finite field extensions as the associated algebraic object, with the Frobenius orbits providing the degrees of closed points of the variety. Tate-Weil formalism leads to the Weil form in an indirect way, while Grothendieck l-adic cohomology uses the Grothendieck cover and homological algebra machinery for this.

9.2. **The "missing link": analog of the Jacobian variety.** The "missed" algebraic-geometric object, analog to the Jacobian variety/zero-Picard group, is the algebra of cyclotomic constants (see [48]; see also [50, 49]), with Gaussian periods conjecturally corresponding to the Weil zeros:

$$P_1(T) \quad \leftrightarrow \quad det(xI - C) = \prod_0^{e-1} (x - \theta_i), \ \theta_i : \ Gaussian\ periods.$$

The author's conjecture is based on a path integral interpretation, in analogy with complex analysis case, where the role of path integrals is played by Gauss sums, with their 2-cocycle the Jacobi sum which counts the points of the hyper-elliptic curve (is it related to the fusion rule of cyclotomic constants? associativity / 2-cocycle condition).

Moreover, the Gaussian periods framework emulates the Frobenius generator of the Galois group whose orbits yield the zeta function, which in this finite case is played by the automorphism $\sigma(\xi) = \xi^g$ corresponding to a primitive root of unity $(Aut(F^\times, \cdot)$, $F^\times = Aut(Z_p, +))$.

Finally, the Riemann spectrum should be generated "freely" by Weil zeros, since the Euler form of the RZF is a product of local factors; their renormalization (deformation) should conjecturally correspond to the Weil factors $1/(1-\sqrt{p}e^{i\theta})$, for pairs of conjugated Riemann zeros (Birkhoff decomposition). At least the relation between these concepts should be investigated.

9.3. Duality: Riemann-Roch a.k.a. Poisson Summation Formula.

The function field / spectrum paradigm of Algebraic-geometry applies here via Galois Theory and its interpretation as a Klein geometry.

Riemann-Roch relation is really a duality relation (see [13]); in the finite case the duality appears first via Fourier duality. But the hidden geometric interpretation of Riemann-Roch, which for the complex case steams from the Jacobian variety as a consequence of the path-integral duality (homotopy -¿ homology), can be mimicked via Gauss sums (Feynman Path Integrals). The genus should be the dimension of the integral basis of cyclotomic units.

9.4. A finite 3j-symbols theory?

The corresponding fusion algebra, in the context of Galois groups and Quadratic Reciprocity (and duality in Ab_f), seems to be a finite version of 3j-symbols theory (spin / $SL_2(Z_n)$ - recoupling theory for Discrete String Theory), and its relation with link invariants (Jones polynomial -¿ Weil poly?).

9.5. Conclusions and Plan.

The best approach at this point is to try a couple of good examples ("a theory"): for EC and HEC, compute N_1 (and higher) via Jacobi sums, and compare Gaussian periods with Weil zeros.

10. Weil Zeros and Gauss Periods

10.1. Definitions.

Chinese Remainder Th. allows to reduce component wise to the case of prime powers (p-adic numbers).

Let $n = p$ be prime (tangent space; no infinitesimal deformations yet ...).

10.1.1. *The Jacobian Variety, Picard group and Riemann-Roch Th.*

The Jacobian variety over an *arbitrary field* was constructed by Weil (1948), as part of the proof of the Riemann hypothesis for curves over a finite field.

Definition 10.1. The *Jacobin variety* of a curve C is $J(C) = H^0(\Omega^1)^*/H_1(C)$ [14], i.e. the quotient of of the dual of holomorphic differentials by the lattice L of functionals $[\gamma] \mapsto \int_\gamma \omega$.

It is derived from the path integral $\int_\gamma \omega$ of holomorphic differentials on loops, which descends to their homology class, yielding the lattice of (co)periods (?):

$$\int : H_1(C) \times \Omega^1(C) \to C, \quad \int^{\#} : H_1(C) \to H^1(C)^*, \quad J(C) = coker \int^{\#}.$$

Why one needs to take the connected component of holomorphic forms?

What are the *periods* in this context?

As a group the Jacobian variety is iso to the zero-Picard group (connection between duality and Riemann-Roch): $J(C) \cong Pic^0(C)$. Therefore the Jacobian has more structure then just the quotient of formal sums of divisors.

In the discrete finite field case $F_p^\times \to Aut(F_p, +)$, the analog of path integration is the Gauss sum, which is a duality pairing a character (exponential of "integration with a propagator", as an additive functional $exp(\int \omega)$), with a subgroup $H \subset F_p^\times$ ("loop/cycle"), the analog of the lattice is the Gaussian periods (maybe), and the Jacobian variety some quotient of this duality pairing.

The analog of homotopies, yielding the homology via abelianization, is the "2-category structure" of $Aut(Aut(F_p, +))$, i.e. the symmetries of primitive roots of unity (cyclotomic constants etc. - see next subsection).

For higher genus one has to consider the multiple valued map [51]:

$$(x_1, ...x_n) \mapsto (\sum_{i=1}^{g} \int_a^{x_i} \omega_1, ..., \sum_{i=1}^{g} \int_a^{x_i} \omega_g),$$

where $\omega_1, ..., \omega_g$ is a basis of holomorphic differentials. This defines a map

$$Sym^g C \to C^g/\Lambda := J(C),$$

where Λ is the lattice of periods. The target is called the Jacobian variety, and is isomorphic as a group with the zero-Picard group.

10.1.2. *Gauss sums.* A Gaussian sum is

$$G_\psi(\xi) = \sum_{r \in Z_n} \xi(r)\psi(r) \quad <-> \quad <\xi, \psi>,$$

where $\psi(r) = exp(2\pi ira/n)$ is an additive character and ξ is a multiplicative character (e.g. Dirichlet, Hacke etc.).

The case *originally considered by Gauss* was the quadratic Gauss sum, with ξ the Legendre symbol, having the alternative form:

$$G(\xi) = \sum_{r \in F_p} e^{2\pi i r^2/p} \quad <-> \quad \sum_{r \in F_p} exp(\xi(r)),$$

which has a different interpretation (beware of generalizations!):

$$\begin{tikzcd}
F_p \arrow[r, "exp"] & U_p \arrow[r] & C \\
F_p \arrow[u, "\xi"] \arrow[ur, "e^\xi"'] & &
\end{tikzcd}$$

$$G(\xi) = \int_{F_p} e^\xi.$$

In this case $G(\xi) = \sqrt{p}$ or $i\sqrt{p}$, depending on $p \ mod \ 4$ (prime split or inert in $Z[i]$). This form of Gauss sums is generalized to Kummer sums.

The Gauss sum of a Dirichlet (multiplicative) character ξ modulo n is

$$G(\xi)=\sum_{a\in Z_n}\xi(a)e^{2\pi ia/n},\quad \hat{\xi}(1)=(\xi\star e_1)(0).$$

It is closely elated to the finite Fourier transform of the Dirichlet character, and the corresponding convolution of characters (here e_1 is one of the primitive characters of Z_n).

If ξ is primitive then $|G(\xi)|=\sqrt{n}$ (like a Weil zero). If n_0 is the conductor of ξ then

$$G(\xi)=\mu(n/n_0)\xi_0(n/n_0)\ G(\xi_0).$$

Also $G(\bar{\xi})=\xi(-1)G\bar{(}\xi)$. The Gauss sum is not multiplicative, and for relatively prime moduli has the following 2-cocycle:

$$G(\xi)G(\xi')=\xi(n)\xi(n')G(\xi)G(xi').$$

The multiplier looks like a symmetric bilinear form.

For the same modulus $n=n'$, with $\xi\xi'$ primitive also, the 2-cocycle is the Jacobi sum:

$$J(\xi,\xi')=G(\xi)G(\xi')/G(\xi\xi').$$

10.1.3. *Gaussian periods.* Given a subgroup $H\to G=Z_n^\times$ of the multiplicative group of the cyclic group (symmetries of a higher dimensional torus), a *Gaussian period* is a sum of primitive n-th roots of unity ζ^a, where a runs over a fixed coset of H in G, i.e. the integral over a fiber:

$$\begin{tikzcd} G \arrow[r, "exp"] \arrow[d, "\pi"] & S^1 & \textit{Periodization/Orbit Integrals} \\ G/H & & P([g])=\int_{\pi^{-1}([g])} exp(a)da. \end{tikzcd}$$

Gaussian periods are related to Gauss sums $G(\xi)=G_{e_1}(\xi)$, where $H=ker\xi$. For example, Gauss quadratic sum is the sum of two Gaussian periods:

$$G(\xi)=P-P^*,\ P=\zeta+\zeta^4+\zeta^9+...,\ P^*=\zeta^2+...$$

where P is the sum over quadratic residues, and P^* is the sum over quadratic non-residues.

In general, Gauss sums are linear combinations of Gaussian periods, being *each other's Fourier transforms.*

Gaussian periods generally lie in smaller fields, while Gaussian sums have nicer algebraic properties.

What about the Jacobi sums which enter in process of counting the number of points of a hyper-elliptic curve over a finite field?

Remark 10.1. Gaussian periods framework in F_p is similar to that of Frobenius orbits in the category of field extensions of F_p, which leads to the Euler form, and from there, via l-adic cohomology, to Weil form of the zeta function.

What is the relation between Gaussian periods and Weil zeros? Is the Riemann spectrum algebraically generated by Weil-Spectrum?

For additional detail on Gaussian periods see [52, 48]. The graphical nature of Gaussian periods (crystallographic groups, orbifolds, quantum orbitals related, maybe?), see [53].

Remark 10.2. Gaussian periods should be collectively viewed as a function on $G/H = \cup gH$, in a framework similar to periodization operator and Poisson Summation Formula (Riemann-Roch Theorem), especially in connection with Kummer sums, which play the role of a zeta function. Gauss sums also play the role of the Gamma function (Mellin transform of the exponential, the fixed point of Fourier transform).

11. Examples, computations and conjectures

We review some of the considerations from §6, regarding the EC $y^2 = 1 - x^3$. Don't change the EC; look instead for a correlation between Weil zeros and $p-1$ ($F_p^\times$ as the symmetries of our discrete Klein geometry on F_p / Galois group action), to be justified via Gauss sums, Fourier duality, and Hochschild cohomology (Jacobi sums: $J = dG$).

11.1. **The "branching cover" character $\xi(x) = x^s$.**

When counting points over F_p, $N(x^s = a)$ is relevant. We may reduce s modulo $p-1$, so we should consider the bicharacter:

$$\xi : F_p^\times \times Z_{p-1} \to F_p,\ \xi(a,s) = a^s.$$

This is analogous to the RZF one $\xi(n,s) = n^s$, who's periodization over N yields the RZF.

Exclude $a = 0$. Then a has $x = a$ has a multiplicative structure in $F_p^\times$ via the Chinese Remainder Theorem and a choice of *primitive root* ζ s.t. $< \zeta >= F_p^\times$:

$$\eta : F_p^\times \to Z_{p-1} \to \prod_{prime\ q|p-1} Z_{q^{\nu(q)}}, \quad a = \zeta^k,\ k \mapsto (k\ mod\ q^\nu).$$

The minimal orbits of $F_p^\times \to Aut(Z_p, +)$ are essential for the understanding of Gaussian periods.

To study the number of solutions $N(x^m = a)$ in $F_p^\times$ assume $m|p-1$ (it depends only on $gcd(m, p-1)$). Then this is either zero or m [41], p.5, the size of the multiplicative subgroup $U_m \subset F_p^\times$ of m-roots of unity.

Remark 11.1. If $q = p^n$ and $m|q-1$ then $m = dd'$ with $d|p-1$ and $d'|1+p+...+p^{n-1}$; does this give any structure to N_r, when $r > 1$? How is this related to the fact that only genus g N_r's are algebraically independent?

The following Lemma ([41], p.5) represents the number of points as a character sum (here ϵ is the trivial character), by duality.

Lemma 11.1.

$$N(x^m = a) = \sum_{\xi^m=\epsilon} \xi(a).$$

Proof 3. *For $a = 0$ this is trivial. If $a = b^m \in F_p^\times$, i.e. $a \in Im\zeta_m$, with $\zeta_m(x) = x^m$ the corresponding character, then*

$$\sum_{\xi^m=\epsilon} \xi(a) = \sum_{\xi^m=\epsilon} \epsilon(b) = m = N(x^m = a).$$

If a is not an m^{th} power, then there is a character of order m not orthogonal on a, under the Fourier duality for $(F_p^\times, \cdot)$, i.e. $\chi'(a) \neq 1$. In general (group property):

$$\sum_{\xi^m=\epsilon} \chi(a) = \chi'(a) \sum_{\xi^m=\epsilon} \chi(a).$$

But now $\chi'(a) \neq 1$ implies the sum vanishes, so it equals $N(x^m = a)$.

Remark 11.2. On can restate the content of the above Lemma and its proof in the context of Fourier analysis in the multiplicative group $F_p^\times$. Viewed additively, it is a multi-dimensional torus (Chinese Reminder Th.), and the sum is the Fourier Series of the characteristic function of the image of $\xi(x) = x^m$. Example $p = 7$ ...

Remark 11.3. The factor $2|p-1$ plays the role of the square in $y^2 = f(x)$, giving the "surface property" to the Riemann surfaces. Can this idea be made more substantial? It can be also associated to the two orientations on the cycle Z_{p-1}; or the cone-like structure.

11.2. **Jacobi sums for our example.** We use the above lemma to count the number of points on our main example of an elliptic curve. For the case of projective hepersurfaces, see [41].

$$N(y^2 = 1 - x^3) = \sum_{b=1-a} N(x^2 = b)N(x^3 = a)$$

$$= \sum_{a+b=1} \sum_{\chi_2^2=\epsilon} \sum_{\chi_3^3=\epsilon} \chi_2(b)\chi_3(a).$$

$$= \sum_{chi_2,\chi_3} \sum_{a+b=1} \chi_2(b)\chi_3(a) = \sum_{chi_2,\chi_3} J(\chi_2, \chi_3),$$

with

Definition 11.1. $J(\chi, \chi') = \sum_{a+b=1} \chi(a)\chi'(b)$, called the Jacobi sum (two variables).

Since here the conductors of the Dirichlet characters χ_2 and χ_3 are relatively prime, the Jacobi sum is related to Gauss sums as follows (§10.1.2, or Wikipedia):

$$J(\chi_2, \chi_3) = G(\chi_2)G(\chi_3)/G(\chi_2\chi_3) = dG(\chi_2, \chi_3),$$

where d is the Hochschild cohomology differential.

Remark 11.4. Recall that

1) for $\chi \neq \epsilon$, $|G(\chi|) = \sqrt{q}$, belonging to the same quadratic extension as the Weil zero.

2) the Gauss sum is essentially the Fourier coefficient of χ ([41], p.3, with $\alpha = 1$; see the role of the additive character $\psi(\alpha) = \zeta_p^{Tr(\alpha)}$):

$$G(\chi) = q\hat{\chi}(-1).$$

11.3. **Questions.** A) What is the geometric interpretation of the Hochschild differential of Fourier coefficient (Gauss sum)? What kind of "curvature" is it?

B) If the Weil polynomial is the characteristic polynomial of an operator defined in the quadratic extension $F_p(\sqrt{p})$, then $a = 2Tr(\alpha)$ (Weil root); what is the relation with the roots of unity and the other trace and determinant (Galois group)? There should be a relation between Weil zero and the factorization of $p - 1$:

$$\alpha = a + ib, \quad a^2 + b^2 = p,$$

Are we here splitting p in the "Gaussian integer plane" of the "finite circle" $Z_{p-1} \cong F_p^\times$? Recall Lagrange sums of squares.

C) What is the numeric coincidences in our example, for a few primes $p = 5, 7, ...$? What is the primes are "simple", i.e. Fermat primes, with $F_p^\times$ "Z-lines" (circles)?

12. On Weil zeros

What are the possible Weil zeros, for various EC and F_p?

12.1. **Emphasis on the multiplicative structure $F_p^\times$.** Let $E : y^2 = 1-g(x), g(x) = x(x^2 - Sx + P)$, so that we can correlate the number of points N_1 of the EC E, with the sizes of the subsets $Ker(g)$ and $Im(g)$ in the *multiplicative group* $F_p^\times$:

$$g : F_p^\times \to F_p^\times,\ Ker(g) = g^{-1}(1).$$

After excluding the point at infinity, the finite points (x, y) of E belong to three different types of conditions:

$$1)\ y = 0\ , x \in Ker(g), \quad 2)\ y \neq 0,\ 0 \neq x \in Im(g) \cap QNR, \quad 3)\ (y = \pm 1, x = 0).$$

Then N_1 has two different, yet possibly related, representations:

$$|Ker(g)| + 2\ |Im(g) \cap QNR| + 2 = N_1 - 1 = p - Tr(\alpha),$$

where α is the Weil zero of the Weil-Betti polynomial $P_1(x) = 1 - Tr(\alpha)x + px^2$.

12.2. **Why Dirichlet characters and Gauss sums: Fourier Series.** Probably a *Fourier series representation of* $g(x)$ in terms of multiplicative characters $\chi(x)$ would relate this "numerical approach with the computation of number of points leading to Jacobi sums. The case $g(x) = x \cdot (x - \beta)^2$ might be of special interest, with its subcase $g(x) = x^3$, or when $g(x) = \chi(x)$ is a multiplicative character.

When $g(x) = \chi(x)$ is a character, $p - 1 = |Ker(g)| \times |Im(g)|$. Since $|QNR| = (p-1)/2$, a possible "Index Theorem" might relate these various sizes (or maybe an Orbit-Stabilizer Theorem argument?).

For example, if $g(x) = x^3$ is the character of order $m = 3$, assuming $3|p-1$, then $|Ker(g)| = 3$ (cubic roots of unity), and $Im(g)$ is a maximal "abelian hyper cone" in $F_p^\times \cong Z/(p-1)Z$. The simplest case is $p = 7$.

12.3. **Goals when using SAGE.** Using SAGE we look for a correlation between N_1, $|Ker(g)$, $|Im(g) \cap QNR|$ (QNR denotes the set of quadratic non-residues), and the discriminant $\Delta = S^2 - 4P$, which determines if $g(x)$ has one or 3 roots in F_p.

Regarding the primes p tested, if $4|p-1$ and $p = c^2 + d^2$ splits, then the Weil zero $\alpha = c + id$ is a "Galois-Gaussian integer", i.e. $\alpha \in F_p[i]$ (How to better express this? Is F_p a "torus" already, with a complex structure? Is there a relation with Sophie Germain primes $p = 2q + 1$, when p does not split?).

Since $N_1 = P_1(1)$ there may be a correlation between the polynomials themselves: $P_1(x)$ and $x^2 - Sx + P$ (or use $1 - SX + Px^2$ standard form?).

12.4. **Possible values from Lagrange Sum of Squares Theorem.** Since $\alpha = c+id, c^2+d^2 = p$, the possible values correspond to the ways p splits in $Z[i]$, assuming $p \cong 1 \ mod\ 4$, according to Fermat's Two Squares Theorem. It means that $x^2 + 1$ is reducible in $F_p[x]$, and the solutions correspond to $x^2 = -1, x \in F_p$:

$$x^2 = -1, d = cx, c \in F_p \quad \Rightarrow \quad \alpha = c^2 + d^2 = p.$$

The multiplicity corresponds to 4th roots of unity. See also Wikipedia: "Proofs of Fermat's theorem on sums of two squares".

The geometric analog involves branched covers of Riemann Surfaces [54].

12.5. **Tasks.** 1) List splittings $c^2 + d^2 = p$;

2) Compute Weil zeros / Number of points for EC for $p \cong 1 \ mod\ 4$.

12.6. **Is there a Deformation Theorem for EC?.** How the number of points, viewed as an intersection number of $\chi(x) = x^2$ and $f(x) = a + bx + x^3$ in F_p, depends on the coefficients of the Weiestrass form of the EC (or Lagrange form $y^2 = x(x-1)(x-\lambda))$?

Is it better to represent the equation $y^2 = 1 - xg(x)$ and look at the discriminant of g instead?

The coefficients of the equation are "homotopically deformed" (in the sense of automorphism orbits), the number of the solutions remains the same (the index does not change). This is an analog of Hopf's Theorem for indexes / winding numbers over the complex numbers.

12.7. **Examples using SAGE.** Fix the elliptic curve $y^2 = 1+x^3$. For various primes the number of points etc., are:

$$p = 2 \ mod \ 4 = 2 \ N_1(p) = 3 \ a := 1 + p - N_1 = 0 \ P_1(x) = 1 - 0x + 2x^2 \ p - 1 = 1$$

$$p = 3 \ mod \ 4 = 3 \ N_1(p) = 4 \ a := 1 + p - N_1 = 0 \ P_1(x) = 1 - 0x + 3x^2 \ p - 1 = 2$$

$$p = 5 \ mod \ 4 = 1 \ N_1(p) = 6 \ a := 1 + p - N_1 = 0 \ P_1(x) = 1 - 0x + 5x^2 \ p - 1 = 2^2$$

$$p = 7 \ mod \ 4 = 3 \ N_1(p) = 12 \ a := 1 + p - N_1 = -4 \ P_1(x) = 1 - -4x + 7x^2 \ p - 1 = 2 * 3$$

$$p = 11 \ mod \ 4 = 3 \ N_1(p) = 12 \ a := 1 + p - N_1 = 0 \ P_1(x) = 1 - 0x + 11x^2 \ p - 1 = 2 * 5$$

$$p = 13 \ mod \ 4 = 1 \ N_1(p) = 12 \ a := 1 + p - N_1 = 2 \ P_1(x) = 1 - 2x + 13x^2 \ p - 1 = 2^2 * 3$$

A more detailed study will be provided elsewhere.

13. Conclusions

Proving Weil conjectures goes a long way around the still unknown geometric object (cohomology) which yields the Weil zeta function as a graded Euler characteristic. The study of Weil zeros considered above should provide insight into what this object is.

14. Appendix: SAGE code

The data in the example section was generated with the following SAGE code.

14.1. **Counting** $N(RS(y^2 = f(x); F_p)$**.** Counting the number of points of a hyperelliptic curve $y^2 = f(x)$ over finite fields $GF(p^n,' a')$, for primary finite fields $n = 1$. SAGE Code, as is, follows.

```
# Finite Field Z/pZ, so we are working mod p
# Define the procedure N1EC(p) for EC: y^2=1+x^3
def N1EC(p):
   N=0;
   for x in range(p):
      f=mod(1+x^3,p)
      if f==0:
         N+=1;
      elif kronecker(f,p)==1:
   for y in range(p):
   if mod(y^2,p)==f: N+=1;
   return N+1
# End procedure
# Looping for various primes
```

```
P=Primes();
for k in range(20):
    p=P.unrank(k); N1=N1EC(p); a=1+p-N1
    print “p=”, p, “ mod 4=”, mod(p,4), “ N1(p)=”, N1, “ a:=1+p-N1=”, a,
    “ P1(x)=1-”,a,“x+”, p,“xˆ2”, “ p-1=”, factor(p-1)
```

References

[1] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, GTM Series #84, Springer New York, 2010.

[2] O. Shanker, “Entropy of Riemann zeta zero sequence”, AMO - Advanced Modeling and Optimization, Volume 15, Number 2, 2013, https://camo.ici.ro/journal/vol15/v15b18.pdf

[3] K. Ford and A. Zaharescu, On the distribution of imaginary parts of zeros of the Riemann zeta function, J. reine angew. Math. **579** (2005), 145-158. www.researchgate.net, 2005.

[4] K. Ford, K. Soundararajan, A. Zaharescu, On the distribution of imaginary parts of zeros of the Riemann zeta function, II, 0805.2745, 2009.

[5] L. M. Ionescu, On prime numbers and Riemann zeros, 2017.

[6] L. M. Ionescu, “A statistics study of Riemann zeros”, 2014, to appear.

[7] B. Mazur, W. Stein, *Primes: What is Riemann’s Hypothesis?*, Cambridge University Press, 2016; http://modular.math.washington.edu/rh/rh.pdf

[8] P. Garrett, “Riemann’s explicit/exact formula”, 2015, http://www-users.math.umn.edu/g̃arrett/m/mfms/notes_2015-16/03_Riemann_and_zeta.pdf

[9] V. Munoz and R. P. Marco, Unified treatment of explicit and trace formulas via Poisson-Newton formula, https://arxiv.org/abs/1309.1449

[10] A. Connes, “An essay on the Riemann Hypothesis”, http://www.alainconnes.org/docs/rhfinal.pdf

[11] I. Volovich, Number Theory as the Ultimate Physics Theory.

[12] L.M. Ionescu, “Remarks on physics as number theory”, *Proceedings of the 19th National Philosophy Alliance* Vol. 9, pp. 232-244, http://www.gsjournal.net/old/files/4606_Ionescu2.pdf.

[13] Wikipedia, Riemann-Roch duality.

[14] Wikipedia, Jacobian Variety.

[15] H. Rademacher, *Fourier analysis in number theory*, Collected Works, pp.434-458.

[16] M. Kontsevich, D. Zagier, Periods, IHES 2001, http://www.maths.ed.ac.uk/ãar/papers/kontzagi.pdf

[17] L. M. Ionescu, A natural partial order on the prime numbers, Notes on Number Theory and Discrete Mathematics, Volume 21, 2015, Number 1, Pages 1?9; arxiv.org/abs/1407.6659, 2014.

[18] V. R. Pratt, Every prime has a succinct certificate, SIAM J. Comput. Vol.4, No.3, Sept. 1975, 214-220.

[19] L. M. Ionescu, On Prime Numbers and Riemann zeros, https://vixra.org/abs/2204.0105

[20] D. Lorenzini, An Invitation to Arithmetic Geometry, *Graduate Studies in Mathematics* Vol. 9, 1996.

[21] Wen Wang, Notes on character sums, http://wstein.org/edu/2010/414/projects/wen_wang.pdf

[22] L. M. Ionescu, Topics in Number Theory MAT 410, Fall 2015, Fall 2016, Google presentation.

[23] B. Ossermann, Weil conjectures, https://www.math.ucdavis.edu/ osserman/math/pcm.pdf

[24] L. M. Ionescu, “A natural partial order on the prime numbers”, *Notes on Number Theory and Discrete Mathematics*, Volume 21, 2015, Number 1, Pages 1?9; arxiv.org/abs/1407.6659, 2014.

[25] S. S. Kudla, “Tate’s thesis”, *An Introduction to the Langlands Program*, pp 109-131, Editors: Joseph Bernstein, Stephen Gelbart, Springer, 2004.

[26] K. Conrad, “The character group of *Q*”, http://www.math.uconn.edu/k̃conrad/blurbs/gradnumthy/characterQ.pdf

[27] I. M. Gel'fand M. I. Graev, I. I. Pyateskii-Shapiro, *Representation theory and automorphic forms*, Academic Press, 1990.
[28] F. Gouvea, *p-adic Numbers: An Introduction*, Springer-Verlag, 1993.
[29] L. M. Ionescu, Recent presentations, http://my.ilstu.edu/ lmiones/presentations_drafts.htm
[30] R. Meyer, "A spectral interpretation of the zeros of the Riemann zeta function", math/0412277
[31] J. F. Burnol, "Spectral analysis of the local conductor operator", math/9809119.pdf, 1998.
[32] John Baez, "Quasicrystals and the Riemann Hypothesis", golem.ph.utexas.edu/category/2013/06/quasicrystals_and_the_riemann.html
[33] Freeman Dyson, "Frogs and Birds", AMS 56 (2009), 212-223.
[34] A. M. Odlyzko, "Primes, quantum chaos and computers", *Proc. Symp.*, May 1989, Washington DC, pp.35-46.
[35] Wikipedia: "Riemann Zeta Function".
[36] Y. Tian, Weil conjecture I.
[37] M. Mustaza, Lecture 1: The Hasse-Weil Zeta Functions.
[38] P. Ding, L. M. Ionescu, G. F. Seelinger, On zeta functions (project).
[39] C. Ritzenthaler, AGM for elliptic curves.
[40] Colin Hayman, The Weil conjectures, Master Thesis 2008.
[41] Eyal Z. Goren, Gauss and Jacobi sums, Weil conjectures, http://www.math.mcgill.ca/goren/SeminarOnCohomology/mycohomologytalk.pdf
[42] S. K. Lando, Lectures on generating functions, Student Mathematical Library, Vol.23, AMS,.
[43] M. Beck, S. Robins, Computing the continuous discretely, Springer 2007.
[44] Nivenita, Riemann hypothesis for function fields.
[45] Mathematics Stack Exchange, Frobenius orbits and irreducible polynomials, http://math.stackexchange.com/questions/1093548/orbits-of-frobenius-homomorphism-in-finite-field-extension ; http://math.stackexchange.com/questions/152880/how-many-irreducible-polynomials-of-degree-n-exist-over-mathbbf-p
[46] Jerry Shurman, The elliptic curve group law via the Riemann-Roch Theorem.
[47] Fulton, Algebraic Topology.
[48] F. Thaine, On gaussian periods that are rational integers.
[49] Paramand, Gauss and regular polygons.
[50] Wikipedia: 1) Gaussian period; 2) Gauss sum; 3) Jacobian variety.
[51] Mathematics Stack Exchange, Group Law for an Elliptic curve.
[52] Paramand Singh, Gauss and regular polygons: Gaussian periods.
[53] W. Duke, S.R. Garcia, B. Lutz, The graphic nature of Gaussian periods.
[54] Wikipedia, http://en.wikipedia.org/wiki/Splitting_of_prime_ideals_in_Galois_extensions

Department of Mathematics, Illinois State University, IL 61790-4520
Email address: lmiones@ilstu.edu