ON WEIL CONJECTURES (FEB. 2015)

LUCIAN M. IONESCU

Abstract. We review and comment on the Weil conjectures.

Contents

1. Introduction

The Weil conjectures are usually approached by example, and proved "constructively", bottom-up. We first review and comment on a few examples, and the proof provided in [1]. Our goal is a graduate level direct proof, avoiding the "heavy" machinery of Grothendieck's Lefshets formula for etale cohomology (see [1], p.6), either via finite de Rham cohomology (iso to Hochschild; and with singular cohomology in the complex case), or via Degree Theory (Lefschetz), by interpreting Jacobi sums as 2-cocycles of Gauss sums, which are discrete Feynman path integrals.

2. Computing the zeta function of a variety

The zeta function $Z_X(t)$ of a variety X is defined as the generating function keeping track of the number of solutions $N_n(X) = |X(F_{p^n})|$ of the algebraic equation $P(x, y) = 0$, over the tower of finite fields in characteristic p (§2.4.2) [1]. But first, a few examples are in order: counting the number of points on curves over finite fields ("volume").

2.1. **Example 1 - the complex "circle".** Let $\mathcal{C}$ be the affine curve $x^2 + y^2 = 1$ over F_p^2 [2].

[1] See also [2].

[2] We'll interpret these "points" geometrically soon, as affordable representations by symmetries of the corresponding "discrete vector space" (Z-module).

2.1.1. *The "angle" parameterization.* The standard algebraic-geometry parametrization by lines / slopes [1] ("linearizing the circle") [3], yields the bijection:

$$t : F_p - \{t | t^2 + 1 = 0 \ mod \ p\} \to \mathcal{C}(F_p) - \{(-1, 0)\}$$

So the number of points of the curve is $p - 2 + 1$ if -1 is a quadratic residue, and $p + 1$ if not:

$$|\mathcal{C}(F_p)| = p - L_p(-1),$$

where L_p is the Legendre symbol (the unique character of index 2); it corresponds to $x^2 : F_p \to F_p$, i.e. to the y^2-term of the equation defining the variety.

The above equation can be interpreted as follows:

$$|\mathcal{C}(F_p)| = \int_{\mathcal{C}} ds = \int_{F_p} dx - Index(x^2),$$

where we look at x^2 as a branching cover of F_p (analog of the z^n basis for complex functions).

2.1.2. *The projective curve.* When considering the projective curve $\tilde{C}$ instead:

$$X^2 + Y^2 = Z^2, \ X, Y, Z \in F_p,$$

its number of points is $\tilde{C}(F_p) = p + 1$ irrespective of the type of prime p, i.e. whether F_p has or has not a "complex structure" $i^2 = -1$.

Remark 2.1. Why the presence of "rotation" by i affects the number of points? When $-1 = a^2$, the homogeneous equation is equivalent to $x^2 + y^2 + z^2 = 0$ (cone) ...

2.1.3. *The Riemann Surface / Splitting field approach.* A "brute force" approach just solves locally the equation, in the appropriate extension of F_p

$$y = \pm\sqrt{1 - x^2} = \pm\sqrt{1 - x}\sqrt{1 + x}, \ x \in F_p.$$

Here it is perhaps better to think of the "Riemann surface"

$$y^2 = f(x), \ f(x) = 1 - x^2,$$

as a way to represent multi-valued functions, e.g. $y = \pm\sqrt{}$, in terms of path integration. Then the path integral can be reinterpreted as a genuine function on a Riemann surface.

In this way the homotopy groupoid of the path integration pairing is represented as the homology of a space, the Riemann Surface. This would provide a natural framework for a de Rham cohomology model of F_p.

Regarding the additional points of the curve when enlarging the field from F_p to F_{p^n}, the "maximal curve" should correspond to the splitting field of of $f(x)$, that is $F_p[x]/(f(x))$, unless further ramifications of linear factors are involved (?).

[3] "Rational points" are "true points" of the projective space, reflecting the advantage of thinking of fraction fields as the finite part of the projective space of the corresponding ring of integers.

Then the number of points of the curve is

$$|C(F_p)| = \sum_{x\in F_p} \big(L_p(1-x^2)+1\big)$$
$$= p + \sum_{x\in F_p} L_p(1-x^2).$$

Remark 2.2. How to interpret this relation? Some transversality? or "total index" of y^2 on the image of $f(x) = 1-x^2$, with "multiplicity" if f collapses points?

2.1.4. *The linear combination of monomials interpretation of X.* Another way to count the points [1] consists in viewing the defining polynomial as a linear combination of monomials, in this example x^2 and y^2:

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

Now the number of solutions $N(x^2 = a)$ is $1+L(a)$, with $L(x)$ the legendre character, and it is the "ramification index" of $f(x) = x^2$ over a.

Remark 2.3. Combining the two ways of counting, yields a relation not so easy to prove:

$$L_p(-1) + \sum_{x\in F_p} L_p(1-x^2) = 0.$$

relation which we will atempt to interprete geometrically as Poincare-Hopf Theorem for the "discrete (displacement) field" $f(x) = 1-x^2$, with divisor $div(f) = |1> +| - 1>$ (roots of unity).

2.1.5. *Using Jacobi sums/ Euler Beta Integrals / Veneziano Amplitudes.* **Question:** Why the p-circle has two points at infinity when $|X| = p-1$, and none, when $|X| = p+1$?

Counting "finite" solutions (affine curve):

$$N_1 = |X(F_p)| = \sum_{a+b=1, a,b\in F_p} N(y^2 = a)N(x^2 = b), \tag{1}$$
$$= \sum_{a+b=1} (1+L(a))(1+L(b)).$$

Remark 2.4. As before, the number of solutions of $x^n = a$ is either 0 when $a \ni Im(x^n)$ or else it is the number of nth roots of unity, in which case it is

$$N(x^n = a) = (1 + \chi + \chi^2 + ... + \chi^{n-1})(a) = \frac{1}{1-\chi}(a)$$

for a character χ of order n.

Question: Is there a way to unify these two cases, and interpret in terms of Intersection Theory (indexes)?

Is the Jacoby sum $\sum_{a+b=1} N(x^n = a)N(f(x) = b)$ related to the "Cauchy Integral"?

$$Ind_n(f; a) = \sum_{a \in F_p} \frac{N(f(x) = 1 - a)}{1 - \chi(a)}$$

and Discrete Fourier Transform of $f(x)$ via partial fractions decompositions?

The above sum is an *Euler Beta integral* (convolution value at 1) with an important meaning: the Veneziano amplitude of the interference of the two modes of the p-astring F_p, i.e. the inner product of the left and right movers $\chi_1(x)$ and $\chi_2(1-x)$ on the p-string F_p:

$$(\chi_1 * \chi_2)(1) = \int_{x \in F_p} \chi(x)\chi_2(1-x) =< \chi_1, \chi_2^* >,$$

where the "Riemann symmetry" $s \mapsto 1 - s$ corresponds to complex conjugation (reference?).

It expands bilinearly as a sum of the following terms:

$$1 * 1 = p,\ (1 * L)(1) = \int_{F_p} L(a)da =< 1, L^* >= 0,\ (L * 1)(1) = 0,\ < L, L^* > .$$

Therefore [4]

$$|X(F_p)| = 1 + ||L||^2.$$

When considering the points at "infinity", i.e. in the projective closure, we get $(1 + L)(-1)$ additional points (0 or 2), for a total which must be as before $p + 1$:

$$|\bar{X}(F_p)| =< 1, 1 > + < L, L* > +N(x^2 = -1)$$

$$=< 1, 1 > + < L, L^* > +(1 + L)(-1) =< 1, 1 > +1.$$

2.1.6. *The Maurer-Cartan of a p-String.* Therefore this Jacobi sum (Veneziano amplitude) satisfies the equation

$$< L, L^* > +L(-1) = 0$$

analog to the relation for $1 - x^2$, [1], p.2.

Question Is $L(-1)$ an Lefshetz index? Is there a String Theory interpretation for it?

We call this equation the *Maurer-Cartan String Equation*:

$$< L, L^* > +\delta_2 * L = 0.^5$$

Alternatively (and plainly; $|F_p^\times|/2 = (p-1)/2$):

$$< L, L^* > +(-1)^{\frac{p-1}{2}} = 0.$$

[4] Is it worth emphasizing the norm?

[5] Kind of forcing the interpretation ...

One way or another $X(F_p) \cong Z/pZ \cup \{\infty\} = P^1(Z/pZ)$, the natural "bi-field" ("Riemann sphere") associated to the field F_p.

Remark 2.5. Look for extension of computing Jacobi sums (convolutions) from characters to functions via Fourier Transform:

$$\sum_{a+b=1, a,b \in F_p} N(y^2 = a) N(f(x) = b,$$

using intersection theory instead of fixed point theory $f(x) = g(x)$.

2.2. **Intermezzo - The de Rham cohomology of $(Z/pZ, +)$.** The "discrete 1-D manifold" $(F_p, +) = Z/pZ$, with its Lie-Klein geometry $(F_p^\times, \cdot) \to Aut(Z/pZ, +)$, has a natural differential (finite difference) and corresponding path integral (sum):

$$f \in Hom_{Sets}(Z/pZ, C), f'(x) = f(x+1) - f(x),$$

$$\gamma : \{1, ..., m\} \to F_p, \ \int_\gamma f(x)dx = \sum_1^m f(\gamma(k)),$$

where C is some field of coefficients (e.g. complex numbers), and γ is a *path* in F_p, i.e. an isometry for the natural distance functions: $|\gamma(k+1) - \gamma(k)| = 1$.

The two K-linear operators D (finite differences) and I, path integration from 0, as a natural choice of a base point ($\int$ is rather a pairing), can be represented as usual in the convolution algebra of functions ($\mathcal{F} = (Hom_{Sets}(Z/pZ, K), *)$:

$$Df = f * \mu, \ I(f) = f * 1,$$

in terms of the Mobius function μ, the convolution inverse of the "zeta function" 1 (see [10] for Mobius inversion in the context of aritmetic functions on Z, and [9] for details).

Now the de Rham cohomology of D is dual to Tate cohomology of the cyclic group $G = (Z/pZ, +)$ ([5], p.35):

$$\ldots \longrightarrow Z[G] \xrightarrow{N_G} Z[G] \xrightarrow{x-1} \ldots$$

where the dual of D is multiplication by $x - 1$, and the dual of I is multiplication by $N_G = \sum_0^{p-1} x^k$.

To interprete the above formula counting of elements of C as a discrete analog of Poincare-Hopf Theorem, we first interpret the Legendre symbol of -1 as an index. Then consider the Poincare-Hopf Theorem for the "vector (displacement) field" $f(x) = x^2$, or via Gauss-Bonnett Theorem [3], with the appropriate normalization of the curvature $K = 1$ for the finite torus $T^2 = F_p \times F_p$:

$$\int_{F_p \times F_p} K dx \times dy = \chi(T^2) = Ind(0) + Ind(1).$$

??

...
or study $P(x,y) = x^2 + y^2$ instead?

For additional discrete analogue of traditional mathematics concepts, e.g. the Fourier "analysis" on finite abelain groups, see [4].

2.3. **Example 2 - the elliptic curve $y^2 = 1 - x^3$ over F_p.** 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).

Remark 2.6. It's s setup suited for intersection theory and Lipschitz indexes etc.

2.3.1. *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": $(0 : \pm 1 : 0)$:

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

2.3.2. *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 2.7. 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.

2.4. **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.

2.4.1. *The p-circle $x^2+y^2=1$ over F_{p^n}.* Let's count the points of the p-cycle X : $x^2+y^2=1$ over extensions F_{q^n} of F_q, where $q=p^m$ [1], Ex. 2.5, p.5. We will use Jacobi sums as a route ($L(x)=\chi_2(x)=\chi(x)$ for short):

$$|X(F_{p^n})|=\sum_{a+b=1,a,b\in F_{p^n}} N(x^2=a)N(y^2=1)$$

$$=\sum_{a+b}(1+\chi_2(a)(1+\chi_2(b))=\sum(1+\chi(a)+\chi(b)+\chi(a)\chi(b)$$

$$=|F_{q^n}|+(\chi*\chi)(1)$$

since $\sum\chi(x)=0$ and the Jacobi sum $J(\chi,\chi)=\sum_a\chi(a)\chi(1-a)$ is a convolution value. The "nice" results about Jacobi sums occur in projective space, probably because of the nice intersection theory (Bezout Th. etc.). So we expect $\chi*\chi(1)=0$, and the size of the projective curve in n-dim space over F_q is:

$$N_n(X)=|\tilde{X}(F_{q^n})|=1+q^n$$

Then the zeta function is:

$$Z(X,t)=exp(\sum N_n(X)t^n/n)=exp(\sum(1+q^n)t^n/n)$$

$$=\frac{1}{(1-q^0t)(1-q^nt}.$$

2.4.2. *Zeta function, log and formal path integration.* This is plainly because

$$\log\frac{1}{1-x}=1+x/1+x^2/2+...,$$

so the <u>formal</u> *logarithm integrates the geometric series!*

$$\log(1+x+x^2+x^3+\dots)=1+x+x^2/2+\cdots=\int(1+x+x^2+...),$$

as expected from a *path integral* definition of the *numerical* (convergent, real or complex etc.) logarithm:

$$\log(x)=\int_1^x dt/t.$$

2.4.3. *Why Euler product is the factorization by degrees?* How can the Euler product Lemma 2.3 [1], p.4 have the Weil product form?

$$\prod_{x\in X_{Cl}} \frac{1}{1-t^{deg(x)}} = \frac{1}{\prod_{i=0}^{2d} P_i(t)^{(-1)^i}}$$

The polynomials seem to belong to formal groups (p-adics?), with a factorization in terms of the "periods" α_j^i (Jacobian variety?):

$$P_i(t) = 1 + \alpha_1^i t + \alpha_2^i t^2 + ...$$

In the p-cycle example $P_1(t) = 1$, but in the EC case (see later on), it is not 1, so how can (here $q = p$):

$$\frac{1 - a_p t + pt^2}{(1-t)(1-qt)} = \frac{(1+Jt)(1+\bar{J}t)}{(1-t)(1-pt)}$$

equal

$$\prod_{x\in X_{Cl}} \frac{1}{(1-t^{deg(x)})}?$$

What are the closed points (orbits)? Does the Frobenius (Galois generator) generates the orbits?

... and why not work with the "de Rham differential forms" of primes, i.e. the exterior algebra of primes, with super-grading the Mobius function μ, so we would have

$$Z^-(X,t) = 1/Z(X,t) = P_0 \cdot P_1^{-1} \cdot P_2 ... = exp(Tr(D)).$$

2.4.4. *Galois, Frobenius and roots of unity (p-adic fields).* Note that the field extensions are cyclotomic (uniqueness of extensions), so one expects a "selection by sectors" operated by the polynomial $f(x)$ defining the variety $X : y^2 = f(x)$, on the cyclotomic polinomials defining the extensions. In other words, there should be a correlation between the "roots" of $f(x)$ and the roots of unity. This is reminiscent of *Kroneker-Weber Theorem* that the maximal abelian ("homology, not homotopy") extension Q^{Ab} of Q (better lift to algebraic adeles) is generated by roots of unity, all present in the unramified extensiond of the p-adic numbers (see *canonical / Frobenius lift* and vershibung maps [7]; the Teicmuller representation of p-adic integers are Witt vectors, suitable for algebraically representing the carry-over cocycles / deformation of component-wise addition and products of power series).

So, $f(x) = 1 + ... + x^d$ is a deformation of a cyclotomic polynomial $1 - x^d$; then the corresponding curve is a deformation of the torus (Z/MZ conductor?), which is a product of (finite) circles of roots of unity Z_{p^k} (CRTr.) The Laplace spectrum (or better Dirac equation/ quaternions, not to "stumble" on $p = 1/3$ *mod* 4, i.e. to split all rational prime nicely, for enough "rotations"; everything is the theory of $SL_2(Z)$), should follow suit.

2.4.5. *Zeta function of the elliptic curve $y^2 = 1 - x^3$ over F_{p^n}.* Counting the points of the projective closure gives a nice formula (b/c Bezout Theorem?).

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}.

Remark 2.8. 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 $y^2 = 1 - x^3$?

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 2.9. 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 $X(\bar{F}_p)$ (see [8]).

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).

2.4.6. *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 [12]).

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? Liuville action variables?).

2.4.7. *Zeta function of the hyper-elliptic curve* $y^2 = 1 - x^6$. Keep studying the "cyclotomic hyper-EC" (finite Riemann Surfaces), consider $n = 6$, i.e. genus $g = Integer[(6-1)/2] = 2$ [8] [6]. Let $q = 5$ as before. The Zeta function in its Weil form is:

$$Z(T)^{-1} = (1-T)P(T)^{-1}(1-qT),$$

with the expected characteristic polynomial

$$P(T) = (1 - aT + 5T^2)(1 - bT + 5T^2),$$

of an operator on the cohomology of this "Riemann Surface" (to be identified!). Its degree is $deg(P) = dim(H^1) = 2 \cdot g$ ($\chi(X) = 2 - 2g$).

Remark 2.10. Formal manifolds/groups (deformations and diffeos etc.) lead to graded cohomology rings? $deg(Z^{-1}) = 2 - deg(P) = \chi(X) = \sum_0^D (-1)^k dim(H^k), D = 2$ via some augmentation homomorphism.

This time $Z(T)$ is determined by two coefficients $N_1 = 6$ and $N_2 = 46$, counted by computer.

The Taylor series of $\log Z(T)$ (from the Weil form) yields:

$$\log Z(T) = (6 - a - b)T + (23 - \frac{1}{2}(a^2 + b^2))T^2 + ...$$

and comparing with $exp(N_1 T + N_2 T^2/2 + ...) \pmod{T^3}$, yields

$$6 - a - b = 6,\ 23 - \frac{1}{2}(a^2 + b^2) = 46/2 \quad \Rightarrow a + b = 0, a^2 + b^2 = 0 \Rightarrow a = 0, b = 0.$$

Remark 2.11. It is tempting to interpret $a + b = Tr(?), a^2 + b^2 = N(?) = det(?)$ ... or maybe as zero zeta sums $S_k = \sum_0^1 a_i^k$ ... ??

Now let's compute the coefficients N_r by "hand":

$$N_1 = 1 + \sum_{a+b=1} N(y^2 = a)N(x^6 = b).$$

Remark 2.12. For the homogeneus eq., for genus $g > 0$ ($n > 2$) we always get just one point "at infinity" (projective):

$$Y^2X^4 + X^6 = Z^6,\ Z = 0\ \Rightarrow X = 0.$$

So why real hyper-elliptic curves have 2 points? (Multiplicity?)

As before, the computation reduces via

$$N(x^2 = a) = 1 + \chi_2(a),\ N(x^6 = a) = \sum_0^5 \chi^k(a),\ N_1 = 1 + \sum_{i=0..1, j=0..4} \chi_2^i * \chi_6^j(1)$$

[6] If $deg(f(x)) = 2g + 1$ it is an imaginary hyper-EC, with one point at infinity; if the degree is $2g + 2$ it is a real hyper-EC, with 2 points at infinity (see Wiki).

to Jacobi sums: $\chi_2 * \chi_6$, since higher relatively prime powers "don't interact" and by "rotational symmetry" (primitive roots) the case reduces to the above "fundamental resonance, to be evaluated using SAGE (for several primes).

Remark 2.13. Since $2|6$ one expects a "nice" answer, computable directly by "symmetry" arguments.

$x^5 = x$ in F_5, so $N(x^6 = b) = N(x^2 = b)$, and

$$N_1 = 1 + |F_5| + 2\sum_a \chi_2(a) + \sum_a \chi_2(a)\chi_2(1-a) = 6,$$

since the other sums are zero as before.

In F_{25} is more complicated

$$N_2 = \sum_{a+b=1, a,b\in F_{25}} (1+\chi_2(a))(1+\chi_6(b)+...)$$

$$= 2\sum_{a\in ker(\chi_2)} (1+\chi_6(1-a)+...)$$

Why for 2D-case Jacobi sums are no longer trivial?

$$N_2 = 1 + |F_{5^2}| + 20 = 46.$$

Check with SAGE.

2.4.8. *Lefschetz intersection theory.* 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?

2.4.9. *Main points / relations.* Investigate the relation between the degree n of the cyclotomic polynomial $f(x) = 1 - x^n$, the prime modulus $q = p$ and the coefficients of the Betti polynomial

$$P(T) = (1 - a_1T + pT)...(1 - a_gT + pT),\ a_j = \sqrt(p)(e^{i\gamma_j} + e^{-i\gamma_j}),\ j = 1..g,$$

with a_i given by Viete's relations in terms of the *reciprocal* of the Riemann zeros $\rho_j = 1/\sqrt{p}\ e^{i\gamma_j}$.

Since Chinese remainder Theorem should apply to the structure of $F_{p^m} = Hom(C_p, C_m)$, one should study the prime sectors of the Zeta function: $m = q^l$ a prime power.

The "cyclotomic primes" (irreducible) should play a similar role as the rational primes, so maybe study the irreducible pieces of $1 - x^n$; is $1 - x^6 = (1-x)(1+x)(1-x+x^2)(1+x+x^2)$ "equivalent" to a "surgery" on the two spheres $1 \pm x + x^2$?

The Riemann zeros should have a clear meaning in the theory of complex curves, i.e. Riemann surfaces: harmonic basis ... ? The simpler case: Elliptic Curves and Jacobian variety?

2.4.10. *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 [7] 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 2.14. Is $N_r = (1 + q)^r - a^r$? see [8], p.12; 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 [7], 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?

2.4.11. *Quadratic twists:* $ay^2 = c + bx + x^3$. When a is a quadratic non-residue, $V : y^2 = f(x)$ and $V' : ay^2 = f(x)$ have ZF with Weil polynomials related by $a' = -a$ [8], p.18. Example $V : y^2 = x^3 - 1$ over F_5 has $a = 0$ and $V' : 3y^2 = x^3 - 1$ has also $a' = 0$. V' is iso to $y^2 = x^3 - 2$, since $2 \cdot 3 = 1\ mod\ 5$.

What is the meaning of such a symmetry $a \mapsto -a$ (symmetric space)? Here $g(y) = y^2$ and $g'(y) = ay^2$ are "transversal cycles" decompose $F_q = Im(g) \oplus Im(g')$, or rather $F_q^\times = Im(g) \cup Im(g')$, $q - 1 = 2m$ ...

2.5. **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 Pythagora 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).

3. On the proof of Weil Conjectures for Elliptic Curves

The main ingredients are the Tate module and the Weil pairing.

Remark 3.1. Why in order to study the reduction of $EC(Q)$ at p, Tate “deforms” the curve in the direction of $l \neq p$, to have a characteristic zero framework, instead of just using Hensel's philosophy, and deform $EC(Q)$ into $EC(Q_p)$ directly!?

$$\begin{array}{ccc} EC/Q & \xrightarrow{mod\ p} & EC/F_p \\ {\scriptstyle p-deform}\downarrow & \nearrow_{mod\ p} & \downarrow{\scriptstyle l-deform} \\ EC/Q_p & \xrightarrow{iso?} & T_l \cong Z_l \times Z_l. \end{array}$$

Recall that, by Hensel's Lemma, IVPs in Q_p have unique solutions (assuming smooth points on EC), so “infinitesimal points” on $EC(F_p)$ correspond 1:1 to p-adic points on $EC(Q_p)$; extends to unramified extensions too).

We will review the proof following [8] and “run” it on the following example:

$$E/F_7 :\ y^2 = x^3 + 2.$$

The EC has 9 points: $O(0:1:0), (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)$. The zeta function (Weil form) is:

$$Z(E/F_7;T) = \frac{1+T+7T^2}{(1+T)(1+7T)}.$$

The next coefficient is [7], p.19:

$$N_2 = |E(F_{7^2})| = 1 + q^2 + \alpha^2 + frm[o] - - + 7^2 - (1 - 2 \cdot 7),$$

since $\alpha = \sqrt{7}e^{i\theta}$, with $\theta = 2\pi/3$, i.e. $\alpha/\sqrt{7}$ is a cubic root of unity. Thus $\alpha^2 + \beta^2 = \sqrt{7}(\xi^2+\xi) = -7$!? (what's wrong?), or rather $\alpha^2+\bar{\alpha}^2 = (\alpha+\bar{\alpha})^2-2\alpha\bar{\alpha} = (-1)^2-2\cdot 7 = -13$.

3.1. **The Tate Module.**

3.1.1. *The torsion subgroups.* The torsion subgroups of an EC are $V[m] = \{P \in E(\bar{K})|[m]P = O\}$.

Question: For our example, if $m = 3, p = 7$ how to determine $E[m]$? How to "extract" the minimal extension of Fp which implements $E[m]$? More primarily, what is the group law in $E(F7)$?

...

Remark 3.2. The Tate module approach needs the whole category of extensions of F_p, just in order to get to a characteristic zero setup. It also uses the "mysterious" group law: clear geometrically, but unclear its meaning (Intersecting a line and the cubic in the plane: why the intersection is such a 2-cocycle?)

4. In search of the "missing complex"

The Weil polynomial is a characteristic poly of some operator which should occur naturally in the initial context of the EC/f.f. For higher genus g, N_1 does not determine the ZF (the Weil poly).

4.1. **A wild guess.**

If $y^2 = f(x) = a_0 + ... + a_n x^n$ over F_p and a_i are reduced mod p, think: linear combination of characters $x^k : F_p^\times \to S_{p-1} - > C$ and p-adic digits a_i. What are the Teichmuller digits and the Teichmuller decomposition of

$$Z/p^{n+1}Z = F_p \times U_1,\ Z/p^{n+1}Z^\times \cong F_p^\times \times Z/p^n Z.$$

Why is the genus $g = Integer[(n-1)/2]$?

It's the other way around: higher degree extensions / representations of $C_{p^n-1} \to Aut(Z/pZ^n, +)$ allow for more eigenspaces and eigenvalues (Riemann zeros) in a "symplectic" / complex way ("everything is $SL_2(C)$"), "producing" more solutions of the given constraint: $f(T) \in H$, where $[G:H] = 2, G \cong C_{p^n-1}$.

So, a direct relation with Fourier transform of ? should exist ...

The key is to understand F_{p^n} as the convolution algebra $A = Hom(C_n, F_p)$: what is a generator X of the $p^n - 1$-cycle?

5. Examples revisited

For an EC $X(F_q) : y^2 = c - bx + x^3$ the Weil form of the ZF is

$$Z(T) = P_1(T)/[(1-T)(1-qT), P1(T) = 1 - aT + qT^2),$$

where $a = 1 + q - N_1$ is the relation with the number of points over F_q, which determines the zeta function, and related to Jacobi sum (via the computation of N_1) by $a = J + \bar{J}$ (in general or just for our main example?). It's also the trace of the Frobenius operator (in Tate's formalism).

Via Viete's relations $a = \alpha + \beta$, sum of the two Riemann zeros ($\beta = \bar{\alpha}$) of the 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 $Re(\alpha) \in \frac{1}{2}Z$.

Remark 5.1. What is the geometric meaning of the generalized Pythagora relation?

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

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

The number of points is determined by the zeros $\alpha, \beta = \bar{\alpha}$ of the Weil polynomial, which correspond to Riemann zeros ρ:

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

5.1. **EC** $y^2 = 2 + x^3$**.** The EC has 9 points over F_7 (localized at $p = 7$): $O(0:1:0), (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)$, so $N_1 = 9$.

Since $a = 1 + q - N_1$ (here $q = p = 7$), The zeta function (Weil form) is:

$$Z(E/F_7; T) = \frac{1 + T + 7T^2}{(1+T)(1+7T)}.$$

The next coefficient is [7], p.19:

$$N_2 = |E(F_{7^2})| = (1 + q^2) - (\alpha^2 + \bar{\alpha}^2) = 1 + 7^2 - (1 - 2 \cdot 7),$$

since $\alpha = \sqrt{7}e^{i\theta}$, with $\theta = 2\pi/3$, i.e. $\alpha/\sqrt{7}$ is a cubic root of unity. Thus $\alpha^2 + \beta^2 = \sqrt{7}(\xi^2 + \xi) = -7$!? (what's wrong?), or rather $\alpha^2 + \bar{\alpha}^2 = (\alpha + \bar{\alpha})^2 - 2\alpha\bar{\alpha} = (-1)^2 - 2 \cdot 7 = -13$.

For $q = p = 7$, counting the points: $N_1 = |E(F_7)|$ by computer [7] 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 5.2. Is $N_r = (1+q)^r - a^r$? see [8], p.12; 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 [7], 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?

6. Appendix

6.1. **Number of solutions $N(\chi(x) = a)$.** For a character $\chi(x)$, e.g. Legendre character of index 2, the number of solutions can be represented as [11], Lemma 3.1, p.5:

$$N(\chi) = \sum \chi^k = \frac{1}{1-\chi}$$

6.2. **On Jacobi and Gauss sums.** see [11].

6.3. **Frobenius morphism.** Our example $y^2 = x^3 - 2, p = 7, q = 1,\ f^{(1)} = f, C^{(1)} = C,\ F : C \to C, F(x, y) = (x^p, y^p) = (x, y)$ is the identity.

For $q = p^2$ ...

Study the "Grothendieck cover" of $K = \bar{F}_p$ as a directed system and the Galois action of frobenius, with $norm = det(L_x)$ and trace =? For Tate/Weil formalism the Char poly is Weil poly, and trace = sum of eigenvalues/ Rioemann zeros.

See is something similar happens when "Hensel-deforming" (lifting) the curve from F_p to p-adic field Q_p, instead of "up", by extending F_p (is this ramifying the curve?)

Curves correspond to fields, and the Galois Theory gives the directed system ("grothendieck cover"): invariant subfields etc. Extending the curve via extending the coefficients (duality by evaluation), corresponds to extending their fields of functions (separable/"space-like"/horizontally, and ramified/"time-like"/vertically). The uniformizer, tangent space M_p/M_p^2 etc. formalism for function fields of curves, seems to correspond exactly to the deformation formalism, from F_p to Q_p.

The Frobenius morphism captures the ramified component of the curve extension: $K- > L, C(K)- > C(L)$, with the q-th power Frobenius Φ^q (generic Galois group element) an endomorphism purely inseparable (ramified) of degree $deg = q = p^r$.

Forget about the q-th power, deal with the generator: the Frobenius Φ.

How is the Galois action on fields, dual to the action of fields on their discrete vector space (Z-modules)? Is there a "partial reflexivity"?

$$2 - category/Homotopy\ Theory :\ Galois \to Aut(Fields), \quad Field \to Aut(Zp^k)$$

$$Aut(Aut()) \sim Id \quad => \quad Frob.(\bar{F}_p) \mapsto Frob(Qp)...?$$

7. Questions and Problems

7.1. **1/18/2015.** 1) How can the Weil rational form of the ZF equal the algebraic geometry form? see [1], p.4. Lemma 2.3 and Theorem 2.4, p.5:

$$Weil\ Form \quad \prod \frac{P_1 P_3 \ldots}{P_0 P_2 \ldots} = Z(X_0, t) = \prod_{x \in |X_0|} \frac{1}{1 - t^{deg(x)}} \quad AG - Form.$$

Why there is no numerator in the AG-form of the ZF?

What about Example 2.5 (Elliptic Curves)?

2) Riemann-Roch Theorem for Projective Line (Exercise 2.3, [13], p.38).

Let $F : P^1 - > P^1$ (rational function). Then i) $Sum_{f(P)=Q} e(P) = deg(F)$; ii) $deg_s(Q) = |F^{-1}(Q)|$; iii) Prove RR Th. for P1; iv) Prove Hurwitz Th.

8. Collected Examples

8.1. **EC** $y^2 = 1 + x + x^3$**.** From Wikipedia: Counting Points on Elliptic Curves.

Let $p = 5$. Then $C(F_p) = \{(0, \pm 1), (2, \pm 1), (3, \pm 1), (4, 2), (4, 3)\} \cup O$ (point at infinity). So $N_1 = 9, a = 1 + p - N_1 = -3$ and $P_1(T) = 1 + 3T + 5T^2$. Note: $N_1 = P_1(1)$ (any significance? 1 is the multiplicative "origin").

If we look at the projective space / curve, what are the Mobius transformations and how do they relate to the function field of the curve? 3-transitive? preserving circles? Characteristic polynomial of MT and multiplier (elliptic, hyperbolic, loxodromic); is the Frobenius one MT and the roots α, β of Weil poly, its roots?

References

[1] Y. Tian, Weil conjecture I.
[2] P. Ding, L. M. Ionescu, G. F. Seelinger, On zeta functions (project).
[3] Oliver Knill, The theorems of Green-Stokes, Gauss-Bonnet and Poincare-Hopf in graph theory, http://arxiv.org/pdf/1201.6049.pdf
[4] A. Terras, Fourier Analysis on Finite Groups and Applications
[5] R. Sharifi, An introduction to group cohomology, http://math.arizona.edu/s̃harifi/groupcoh.pdf
[6] J. Rabinoff, The theory of Witt vectors.
[7] C. Ritzenthaler, AGM for elliptic curves.
[8] Colin Hayman, The Weil conjectures, Master Thesis 2008.
[9] Fusun Akman, Mobius inversion principle, presentation.
[10] T. Apostol, Analytic Number Theory.
[11] Eyal Z. Goren, Gauss and Jacobi sums, Weil conjectures, http://www.math.mcgill.ca/goren/SeminarOnCohomology/mycohomologytalk.pdf
[12] L. M. Ionescu, On Prime Numbers and Riemann zeros, https://vixra.org/abs/2204.0105
[13] J. Silvermann, The Algebra of Elliptic Curves.

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