ON WEIL ZEROS
(W. SAGE SUPPORT - 2014)

LUCIAN M. IONESCU

Abstract. We investigate the zeros of the Betti portion of the Weil rational zeta function for elliptic curves, towards a direct understanding of the Weil conjectures. Examples are provided and various directions of investigations are considered.

Contents

1. Introduction

To understand what Riemann zeros really are, we must first understand Weil zeros.

Although Weil conjectures have been proven in various ways, starting from the Euler form towards the Weil rational form, the main algebraic-geometric object underlying the Weil zeta function as its graded Euler characteristic is still missing [2].

The natural analog of a path integral from the complex numbers case, with its Jacobi variety, is the Gauss sum and its 2-cocycle the Jacobi sum[1], which allows to count the number of points of the curve [3].

To have a better grasp of the basic “players”, we investigate here ground-up the Weil zeros of the “cyclotomic” elliptic curve $EC : y^2 = 1 - x^3$

Recall the notation:

$$Z(x) = (1-x)^{-1} P_1(x)(1-px)^{-1},\ P_1(x) = 1 - ax + px^2,$$

$$Defect:\ a = 1 + p - N_1,\ Number\ of\ points:\ N_1 = |EC(F_p)|,$$

Date: April 21, 2022.

where a is the "defect" from what one would expect as the number of points $1+p$ (counting the point at infinity), $P_1(x)$ is the Weil-Betti polynomial with Weil roots $\alpha = c + id, c^2 + d^2 = p$ (Riemann hypothesis: $|\alpha| = \sqrt{p}$).

Except for $p = 2$, for our EC all reductions are "good": the roots of $f(x) = 1 - x^3$ are distinct in F_p.

1.1. **Case $3 \nmid p - 1$.** In this case the multiplicative character $x^3 : F_p^\times \to F_p^\times$ has no kernel, and $f(x) = 1 - x^3$ is a bijection of F_p, thus the number of solutions of $y^2 = f(x)$ is $N_1 = 1 + p$:

$$y = 0 : \ one, \ y \neq 0 : 2 \times (p-1), \ P = \infty, \quad N_1 = 1 + 2 \cdot \frac{p-1}{2} + 1 = 1 + p, \ a = 0.$$

Remark 1.1. The projective closure of the EC belongs to the corresponding projective space $P^1F_p = F_p \times F_p / \sim$. One may start comparing with the complex case, and consider the theory of Mobius transformations $SL_2(F_p)$ "interacting" with the symmetries of the "discrete vector space" (Z-module) $Aut_{Ab}(F_p, +) \cong (F_p^\times, \cdot)$.

For example, using SAGE (See Annex, [2]), we obtain:

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

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

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

$$p = 17 \ mod \ 4 = 1 \ N_1(p) = 18 \ a := 1 + p - N_1 = 0 \ P_1(x) = 1 - 0x + 17x^2 \ p - 1 = 2^4.$$

The Weil-Betti polynomial is $P_1(x) = 1 + px^2$, $a = 2c = 0$ and the Weil zero $\alpha = \sqrt{p}i$ [1].

Remark 1.2. The Weil zeros belong to the quadratic extension $Z[i]$, wether p splits or not, i.e. irrespective of the existence of a 4th root of unity in F_p.

Questions:[2]
1) What is the corresponding Gauss and Jacobi sum?
2) What are the Gauss periods?

1.2. **Case $3|p-1$.** Here $|kerx^3| = 3$, the order of $\chi_3(x) = x^3$ is $(p-1)/3$. Restricting to $F_p^\times$, and using the notation $\chi_n(x) = x^n$, $Im(\chi_3)$ and $Im(\chi_2)$ are "transversal" (the exponents 2 and 3 are relatively prime), so the intersection has $(p-1)/(2 \cdot 3)$ points. Then, N_1 results from the following sum:

$$y = 0 : \ 3 \ points, \ y \neq 0 : \ 2 \times |(p-1)/6, \ N_1 = 3 + (p-1)/3 + 1 = 4 + (p-1)/3.$$

Remark 1.3. Note that $f(x)$ and χ_3 differ by a translation. In the more general case when $f(x)$ splits and is transversal to χ_2, the same argument yields the same formula.

[1] It is in fact the reciprocal of the Weil zero, for the purpose of comparing with the Riemann zeros.

[2] ... for later.

Examples using SAGE:

$$p = 7\ mod\ 4 = 3\ N_1(p) = 12\ a = -4, P_1(x) = 1 + 4x + 7x^2 p - 1 = 2 * 3$$
$$p = 13\ mod\ 4 = 1\ N_1(p) = 12\ a = 2, P_1(x) = 1 - 2x + 13x^2, p - 1 = 2^2 * 3$$

1.2.1. *Primes $p = 2^k * 3 + 1$.* The data suggests the conjecture:

Conjecture 1.1. *The discriminant $\Delta = a^2 - 4p$ of the Weil-Betti polynomial is essentially the number of symmetries of the finite field as a discrete vector space (Klein-Galois geometry).*

$$\Delta = 4(p - 1).$$

Proof 1. *(... analize χ_3 and QR ...)*

1.3. **The relation between Δ and $Aut_{Ab}(F_p, +)$.** Weil-Betti polynomial reduced modulo a prime p, is an element of $F_p[x]$. The Weil zeros belong to the corresponding extension $F_p(\Delta)$.

1.4. **Questions.** 1) What is the meaning of the factors of Δ, e.g. $2^k * 3$ when considering such a field extension? What is the structure of the prime ideals of the corresponding ring of integers? Do those primes split? (Yes).

2) Does it mean that the Galois group is not enough to "reveal" the geometry of the field extension? Is the theory of $SL_2(Z(\Delta))$ more relevant?

3) For other primes, such that the summands of $Aut(F_p, +)$ are higher order polynomial p-adic numbers, is there an "interference" due to some Kuneth formula for tensoring finite field extensions?

4) Is the case of prime exponents easier to understand? (e.g. $p = 2^q * 3^l + 1$, with q, l prime).

2. Appendix

More data obtained using SAGE.

2.1. **$p - 1 = 2^k * 3^2$.**

$$k = 1\ p\ mod4 = 3N1 = 2^2 * 3a = 8p - 1 = 2 * 3^2 - Delta/4 : 3$$
$$k = 2\ p\ mod4 = 1N1 = 2^4 * 3a = -10p - 1 = 2^2 * 3^2 - Delta/4 : 2^2 * 3$$
$$k = 3\ p\ mod4 = 1N1 = 2^2 * 3 * 7a = -10p - 1 = 2^3 * 3^2 - Delta/4 : 2^4 * 3$$
$$k = 2 * 3\ p\ mod4 = 1N1 = 2^4 * 3 * 13a = -46p - 1 = 2^6 * 3^2 - Delta/4 : 2^4 * 3$$
$$k = 7\ p\ mod4 = 1N1 = 2^2 * 3 * 7 * 13a = 62p - 1 = 2^7 * 3^2 - Delta/4 : 2^6 * 3$$
$$k = 11\ p\ mod4 = 1N1 = 2^6 * 3 * 97a = -190p - 1 = 2^11 * 3^2 - Delta/4 : 2^6 * 3 * 7^2$$
$$k = 2 * 7\ p\ mod4 = 1N1 = 2^8 * 3 * 193a = -766p - 1 = 2^14 * 3^2 - Delta/4 : 2^8 * 3$$
$$k = 17\ p\ mod4 = 1N1 = 2^2 * 3 * 7 * 14029a = 1214p - 1 = 2^17 * 3^2 - Delta/4 : 2^6 * 3 * 5^2 * 13^2$$

References

[1] L. M. Ionescu, On Weyl conjectures, Gauss and Jacobi sums, ISU Algebra Seminar presentation.

[2] L. M. Ionescu, On Riemann and Weyl zeros (TBA).

[3] Goren, "Gauss and Jacobi sums, Weyl conjectures", https://www.math.mcgill.ca/goren/SeminarOnCohomology/mycohomologytalk.pdf

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