NOTES ON THE WEIL CONJECTURES FOR CURVES

TRISTRAM DE PIRO

Abstract. We summarise the proof of the Weil conjectures for curves, which was later generalised to higher dimensions by Deligne, and his application to exponential sums in one variable. We extend his result on exponential sums to include rational functions.

Lemma 0.1. *Let C be a smooth projective curve of genus g, $g \neq 1$, defined over a finite field F_q, with $q = p^n$, p prime. Let N be the number of points of C, rational over F_q, then $N = 1 - a + q$, with $|a| \leq 2g\sqrt{q}$.*

Proof. Let F be the n'th power of Frobenius, $\Gamma \subset C \times C$ the graph of F, and $\Delta \subset C \times C$ the diagonal. By the adjunction formula, see [1], we have that;

$$g(\Gamma) = 1 + \frac{(\Gamma^2 + \Gamma.K)}{2}$$

Hence, $\Gamma^2 = 2(g-1) - \Gamma.K$, as Γ and C are birational. Let $l = [x_0 \times C] \subset C \times C$, for $x_0 \in C$, $m = [C \times y_0] \subset C \times C$, for $y_0 \in C$. We have, again using the adjunction formula, that;

$$K.l = 2(g(x \times C) - 1) - l^2 = 2(g-1)$$

$$K.m = 2(g(C \times y) - 1) - m^2 = 2(g-1), \ (*)$$

as $l^2 = m^2 = 0$, because, $(x_0 \times C) \cap (x \times C) = (C \times y) \cap (C \times y_0) = \emptyset$, for $x \neq x_0$, $y \neq y_0$, and $x_0 \times C$, $C \times y_0$ are C are birational. Let $D = K - 2(g-1)m$, then $D.l = 0$, as $l.m = 1$. Let $D_n = D + nl$, we have, by Riemann-Roch, that;

$$h^1(D_n) - h^0(D_n) = 1 + g + \frac{D_n.(D_n - K)}{2}$$

Hence;

$$h^0(D_n) \geq -(1+g) - \frac{D_n.(D_n-K)}{2} = -(1+g) + \frac{K.D - D^2 + 2n(g-1)}{2}$$

It follows that, if $g = 0$, taking $n \leq \frac{K.D-D^2}{2} - 2$, or if $g \geq 2$, taking $n \geq \frac{2(2+g)-(K.D-D^2)}{2(g-1)}$, that $h^0(D_n) \geq 1$. Choosing an effective representative of the class D_n, we have that $D_n.l = 0$, hence, $D_n = \bigcup_{1 \leq i \leq r}(x_i \times C)^{m_i}$, with $x_i \leq x_0$, therefore $D_n = tl$, where $t = \sum_{i=1}^{r} m_i$. It follows that $D = (t-n)l$, and, $K = (t-n)l + 2(g-1)m$. Using $(*)$, and the fact that $l.m = 1$, $m^2 = 0$, we obtain $K = 2(g-1)(l+m)$. Then;

$$\Gamma^2 = 2(g-1) - \Gamma.K$$

$$= 2(g-1) - \Gamma.(2(g-1)(l+m))$$

$$= 2(g-1)(1 - \Gamma.(l+m))$$

We have that $\Gamma.l = card(\{y : F(x_0) = y\}) = 1$, and $\Gamma.m = card(\{x : F(x) = y_0\}) = q$. Hence;

$$\Gamma^2 = 2(g-1)(1-(1+q)) = 2q(1-g)$$

We have that $\Gamma.\Delta = Card(\{x : F(x) = x\} = N$, as the intersection of Γ with Δ is transverse. Let $D = (s_1\Gamma + s_2\Delta)$, with $\{s_1, s_2\} \subset \mathcal{Z}$. We have that $\Gamma.l = 1$, $\Gamma.m = q$, $\Delta.l = 1$ and $\Delta.m - 1$, hence, $D.l = s_1 + s_2$ and $D.m = s_1q + s_2$. Then, by Castelnouvo and Severi's inequality, see [4];

$$D^2 = (s_1\Gamma + s_2\Delta)^2 = s_1^2\Gamma^2 + 2s_1s_2(\Gamma.\Delta) + s_2^2\Delta^2 \leq 2(s_1+s_2)(s_1q+s_2)$$

$$2s_1^2q(1-g) + 2Ns_1s_2 + s_2^2(2-2g) \leq 2s_1^2q + 2s_1s_2 + 2s_1s_2q + s_2^2$$

as $\Delta^2 = 2 - 2g$, see Ex V.1.6(a) of [4]. Hence, for $s_1 \neq 0$;

$$2q(1-g) + 2N\tfrac{s_1}{s_2} + (2-2g) \leq 2q + 2\tfrac{s_2}{s_1} + 2q\tfrac{s_2}{s_1} + 2(\tfrac{s_2}{s_1})^2$$

$$2q(1-g) + 2Nt + (2-2g)t^2 \leq 2q + 2t + 2qt + 2t^2$$

$$(-2g)t^2 + t(2N - 2 - 2q) - 2qg \leq 0$$

$$(2N-2-2q)^2 - 4(2g)(2qg) \leq 0$$

$$(2N-2-2q)^2 \leq 16qg^2$$

$2N - 2 - 2q \leq 4g\sqrt{q}$

$2N - 2 \leq 2q + 4g\sqrt{q}$

$N - 1 \leq q + 2g\sqrt{q}$

Let $N = 1 - a + q$, then $q - a \leq q + 2g\sqrt{q}$ and $|a| \leq 2g\sqrt{q}$

as required.

□

Lemma 0.2. *Using the same notation as Lemma 0.1, let C be a smooth projective curve of genus $g = 1$, defined over F_q, with $q = p^n$, p prime, then $N = 1 - a + q$, with $|a| \leq 2\sqrt{q}$.*

Proof. Again, using the same notation as Lemma 0.1, we have that $P \in C(F_q)$ iff $F(P) = P$, hence, $C(F_q) = Ker(1 - F) = deg(1 - F)$, as $1 - F$ is seperable, ([1]). We have that $deg : C \to \mathcal{Z}$ is a positive definite quadratic form, hence;

$|deg(1 - F) - deg(1) - deg(F)| \leq 2\sqrt{deg(1)deg(F)} = 2\sqrt{q}$

$|N - 1 - q| \leq 2\sqrt{q}$

□

Lemma 0.3. *Again, let notation be as in Lemma 0.1, let C be a smooth projective curve of genus g, defined over F_q, with $q = p^n$, p prime, then the eigenvalues of F, the n'th power of Frobenius, on $H^1(C, \mathcal{Q}_l)$, with $(l, p) = 1$, all have absolute value $q^{\frac{1}{2}}$.*

Proof. We let $N_r = Card(C(F_{q^r}))$, $N_r = 1 - a_r + q^r$. By the above, $|a_r| \leq 2gq^{\frac{r}{2}}$. Using the Lefschetz Fixed Point Formula, see Theorem 4.2 of [3], we have that;

$Z(C, t) = exp(\sum_{r=1}^{\infty} \frac{N_r t^r}{r}) = \frac{P_1(t)}{P_0(t)P_2(t)} = \frac{\prod_{i=1}^{2g}(1-\alpha_i t)}{(1-t)(1-qt)}$ (†)

where $P_i(t) = det(1 - F^* t; H^i(C, \mathcal{Q}_l)$, $0 \leq i \leq 2$, and $\{\alpha_i : 1 \leq i \leq 2g\}$ are the eigenvalues of Frobenius on $H^1(C, \mathcal{Q}_l)$. From (†), we obtain that;

$log(Z(C, t)) = \sum_{r=1}^{\infty} \frac{(1+q^r-a_r)t^r}{r}$

[1] See [7], Corollary 5.5, p79

$= \sum_{i=1}^{2g} log(1-\alpha_i t) - log(1-t) - log(1-qt)$ $(\dagger\dagger)$

Equating coefficients, we have $a_r = \sum_{i=1}^{2g} \alpha_i^r$, $(*)$. We claim that $|a_r| \leq 2gq^{\frac{r}{2}}$ iff $|\alpha_i| \leq q^{\frac{1}{2}}$, for $1 \leq i \leq 2g$, for $q \neq 2$, $(**)$. One direction is clear, otherwise observe that, using $(*)$;

$\sum_{i=1}^{2g} \frac{\alpha_i t}{1-\alpha_i t}$

$= \sum_{i=1}^{2g} \alpha_i t(\sum_{r=0}^{\infty} \alpha_i^r t^r)$

$= \sum_{r=0}^{\infty} \sum_{i=1}^{2g} (\alpha_i^{r+1} t^r)$

$= \sum_{r=0}^{\infty} a_{r+1} t^r$

The power series $\sum_{r=0}^{\infty} a_{r+1} t^r$ converges for $|t| < q^{\frac{-1}{2}}$, $(***)$, using the fact that $|a_{r+1}| \leq 2gq^{\frac{r+1}{2}}$, and $lim_{r\to\infty} |\frac{2gq^{\frac{r+1}{2}} t^r}{2gq^{\frac{r}{2}} t^{r-1}|} < 1$, if $(***)$ holds. If there exists $|\alpha_i| > q^{\frac{1}{2}}$, we obtain a pole of $\sum_{i=1}^{2g} \frac{\alpha_i t}{1-\alpha_i t}$ at $t = \frac{1}{\alpha_i}$, with $|t| < q^{\frac{1}{2}}$, a contradiction, hence $(**)$ is shown. If $q = 2$, a similar claim to $(**)$, namely $|a_r| \leq (max(2, 2g) + \sqrt{2}) q^{\frac{r}{2}}$ iff $|\alpha_i| \leq q^{\frac{1}{2}}$, for $1 \leq i \leq 2g$ holds, using the same proof as for $(**)$. From the functional equation for $Z(C, t)$, which follows from the Riemann-Roch formula, see [4], and $(\dagger)$, we obtain;

$Z(\frac{1}{qt}) = q^{1-g} t^{2-2g} Z(t)$

$\prod_{i=1}^{2g} (t - \frac{\alpha_i}{q}) q^g = \prod_{i=1}^{2g} (t - \frac{1}{\alpha_i}) \prod_{i=1}^{2g} \alpha_i$

Hence, for some permutation $\sigma \in S_{2g}$, $\frac{\alpha_i}{q} = \frac{1}{\alpha_{\sigma(i)}}$, so that $|\alpha_i| = q^{\frac{1}{2}}$, for $1 \leq i \leq 2g$.

□

Remarks 0.4. *Lemmas 0.1 and 0.3, due to Weil, and Lemma 0.2, due to Hasse, can be found as exercises, V.1.10, App. C. 5.7 and V.1.10, respectively, in* [4]. *Lemma 0.3 is often referred to as the Riemann hypothesis, part of the Weil conjectures, for curves, as it implies that the zeros of the associated zeta function to C are all situated on the line* $Res(s) = \frac{1}{2}$. *The proof of 0.2 can also be found in Lemmas 1.1 and 1.2, p138, of* [7]. *The proof of Theorem 4.2 for locally constant sheaves with an action by* $\mathcal{Q}_l$, *in* [3], *is derived from the corresponding*

result Theorem 2.9 in [3]*, for locally constant sheaves with an action by* $\mathcal{Z}/l\mathcal{Z}$*.*

Lemma 0.5. *If* $r \in F_q[x]$*, with* $q = p^n$*,* p *prime,* $deg(r) = d$*,* $(p, d) = 1$*, and* $\psi : F_q \to \mathcal{C}$ *is a nontrivial additive character, then;*

$$|\sum_{x \in F_q} \psi(r(x))| \leq (d-1)q^{\frac{1}{2}} + 1$$

If $\{r, s\} \subset F_q[x]$*, with* $q = p^n$*,* p *prime,* $deg(r) = d$*,* $deg(s) = e$*,* $(p, d) = (p, e) = 1$*, and* $\psi : F_q \to \mathcal{C}$ *is a nontrivial additive character, then;*

$$|\sum_{x \in F_q, s(x) \neq 0} \psi(\frac{r(x)}{s(x)})| \leq (1 + d + 2e)q^{\frac{1}{2}} + e$$

Proof. The proof of the first result is contained in [2], but the 1-dimensional case simplifies the presentation. We have that $C \subset A^2$, defined by $t^p - t = r(x)$, is an etale, Galois cover pr_x of A^1, with Galois group F_p, in particular C is nonsingular. It is a straightforward calculation to show that, for $x \in A^1(F_q)$, the action of F on the fibre C_x is given by, $F(x, t) = (x, t + Tr_{F_q/F_p}(r(x)))$. We let $E_l = \mathcal{Q}_l(e^{\frac{2\pi ij}{p}} : 0 \leq j \leq p-1)$, $(l, p) = 1$. Denoting the action of $w \in F_p$ on C, by $w * z$, we can construct constant sheaves $\{F_j : j \in F_p\}$ on P^1, with $(F_j)_x \cong E_l$, for $x \in P^1$, and inclusions $k_j : C \to F_j$, respecting the Galois action, such that $k_j(w * z) = exp(\frac{-2\pi ijw}{p})k_j(z)$, ([2]). Using footnote 2, the Lefschetz fixed point formula for P^1, see Theorem 2.9 of [3], the classification of characters on F_q, the facts that $H^i(P^1, F_j) = H^i(A^1, F_j) = 0$, for $i \neq 1, j \neq 0$, and $H^1(P^1, F_j) = H^1(A^1, F_j)$, we obtain, for $j \in F_p$, $j \neq 0$, that;

$$\sum_{x \in P^1 \cap Fix(F)} Tr(F_x^*, F_{j,x}) = \sum_{i=0}^{2} (-1)^i Tr(F^*, H^i(P^1, F_j))$$

[2] It is straightforward to construct algebraic power series $\eta_{x_0}(x)$, for $x_0 \in A^1$, with $(x, \eta_{x_0}(x)) \in C$, for $x \in A^1$. Interpreting these on etale covers $\{U_k : k \in \mathcal{N}\}$, which are closed under the action of F, where $Card(F_q^{alg}) = Card(\mathcal{N})$, we can construct $F_j|_{A^1}$, using $exp(\frac{-2\pi ijw_{kk'}}{p})$, for the transition $w_{kk'} \in F_p$, between η_k and $\eta_{k'}$ on the intersections $U_k \cap U_{k'}$. For the extension to P^1, we can choose an open $U \subset P^1$, with $\infty \in U$, such that $U \cap \bigcup_{k \neq k'}(U_k \cap U_{k'}) = \emptyset$ and use the trivial transition. By construction, we have that $\eta_k^q - \eta_k = (Tr_{F_q/F_p}(r(x)))$, hence, for $x \in A^1(F_q)$, we have that $Tr(F_x^*, F_{j,x}) = exp(\frac{-2\pi ijTr_{F_q/F_p}(r(x))}{p})$, and, $Tr(F_\infty^*, F_{j,\infty}) = 1$

$1 + \sum_{x \in F_q} \psi(r(x)) = Tr(F^*, H^1(A^1, F_j))$, $(*)$

We can find a nonsingular projective curve Z and an embedding $b : C \to Z$, defined over F_q, ([3]). As in [2], we have that $b_* pr_x^* : H^1(A^1, F_j) \to H^1(Z, E_l)$ is injective, $(**)$, and $dim(H^1(A^1, F_j)) = d - 1$, for $j \in F_p$, $j \neq 0$, $(***)$. It follows, using $(**)$, $(***)$, Lemma 0.3, ([4]), applied to Z and $H^1(Z, E_l)$, observing that E_l is a constant Q_l sheaf, and, Remark 0.4, that;

$|1 + \sum_{x \in F_q} \psi(r(x))| \leq (d-1)q^{\frac{1}{2}}$

$|\sum_{x \in F_q} \psi(r(x))| \leq (d-1)q^{\frac{1}{2}} + 1$

For the second result, if $\{r, s\} \subset F_q[x]$, we let $C \subset A^2 \cap pr_x^{-1}(s(x) \neq 0)$, be defined by $s(x)(t^p - t) - r(x) = 0$, which defines an etale, Galois cover $pr_x : C \to A^1 \setminus s(x) = 0$, with Galois group F_p. Repeating the construction of the first part of the lemma, for corresponding F_j, with $j \neq 0$, we obtain;

$e + \sum_{x \in F_q, s(x) \neq 0} \psi(r(x)) = Tr(F^*, H^1(A^1 \setminus s(x) = 0, F_j)$

Again, embedding C in a smooth projective curve $b : C \to Z$, over F_q, we obtain that $b_* pr_x^* : H^1(A^1 \setminus s(x) = 0, F_j) \to H^1(Z, E_\lambda)$ is injective. Following [5], see notation there for cl and α, and [6], letting $U = (P^1 \setminus (s = 0 \cup \infty))$, so that $\chi(U) = 2 - 2g(P^1) - (deg(s) + 1) = 1 - e$, we obtain that;

$dim(H^1(A^1 \setminus s(x) = 0, F_j))$

$= \chi(U) cl(F_{j,\eta}) - \sum_{s(x)=0} \alpha_x(F_{j,x}) - \alpha_\infty(F_{j,\infty})$

$= (1 - e) - \sum_{s(x)=0} ord_x(\frac{r(x)}{s(x)}) - ord_\infty(\frac{r(x)}{s(x)}) = K_{d,e}$

where $K_{d,e} \leq 1 + d + 2e$, for $j \in F_p$, $j \neq 0$. Hence, as above, for a nontrivial character ψ on F_q;

$|\sum_{x \in F_q, s(x) \neq 0} \psi(\frac{r(x)}{s(x)})| \leq K_{d,e} q^{\frac{1}{2}} + e \leq (1 + d + 2e) q^{\frac{1}{2}} + e$

[3]However, the projective closure of C, $\overline{C} \subset P^2$ is not smooth at infinity, if $d \neq p$

[4]We can assume that the restriction of F^* to $H^1(A^1, F_j)$ is in Jordan Canonical Form when calculating the trace.

□

References

[1] Complex Algebraic Surfaces, LMS Student Texts 34, A. Beauville, (1996).

[2] La Conjecture de Weil: I, Pierre Deligne, Publications mathematiques de l'I.H.E.S, tome 43, (1974).

[3] Etale Cohomology and the Weil Conjecture, E. Fretag, R. Kiehl, Springer, (1988).

[4] Algebraic Geometry, R. Hartshorne, Springer, ().

[5] Caracteristique d'Euler-Poincare d'un faisceau et cohomolohie des varieyes abeliennes, M. Raynaud, Seminaire Bourbaki, 286, 1964-1966.

[6] Sur les corps locaux a corps residual algebriquement clos, Bulletin de la S.M.F, tome 89, (pp 105-154), J.P. Serre, (1961).

[7] The Arithmetic of Elliptic Curves, 2nd Edition, J. Silverman, Springer, (1986).

Mathematics Department, Harrison Building, Streatham Campus, University of Exeter, North Park Road, Exeter, Devon, EX4 4QF, United Kingdom