Zeroes and Poles of Zeta functions

The following is a "baby" version of the classic argument of Hadmard and de la Vallée Poussin, later generalized by Deligne in his second proof of the Weil conjectures.

Let (α_i) and (β_i) be two finite sequences of complex numbers, with $\alpha_i \neq \beta_j$ for all i and j. Let

$$Z(T) := \prod \frac{1-\alpha_i T}{1-\beta_i T}.$$

Let

$$f(T) := \frac{TZ'(T)}{Z(T)} = \sum_i \left(\frac{\beta_i T}{1-\beta_i T} - \frac{\alpha_i T}{1-\alpha_i T}\right).$$

Then

$$f(T) = \sum_{n \geq 1} a_n T^n, \quad \text{where} \quad a_n = \sum_i \beta_i^n - \alpha_i^n.$$

Let $b : \max(|\beta_i|)$ and $a := \max(|\alpha_i|)$.

Theorem: Suppose $a_n \geq 0$ for all n. Then $b \geq a$. Furthermore, if r is the cardinality of the set of i with $\alpha_i = b$ and s is the cardinality of the set of i with $|\beta_i| = b$, then $r \leq s$. If $s = 1$ and $|\beta_i| = b$, then in fact $\beta_i = b$. In this case if also $r = 1$, and $|\alpha_j| = b$, then $\alpha_j = -b$.

Lemma: Let $(\lambda_1, \ldots, \lambda_r)$ be a finite sequence of complex numbers of absolute value 1. Then there exists an increasing sequence of natural numbers (n_k) such that $(\lambda_i^{n_k})$ tends to 1 for all i.

Proof: The set of $\lambda := (\lambda_1, \ldots, \lambda_r)$ is a compact topological space, namely $(\mathbf{S}^1)^r$. Hence the sequence (λ^m) has a convergent subsequence (m_j). This sequence is Cauchy. So for every number i, there is a number K_i such that

$$||\lambda^{m_j} - \lambda^{m_k}|| < 1/i,$$

whenever j and k are at least K_i, (where $||\ ||$ means for example the sup norm). Then $||\lambda^{m_j - m_k} - 1|| < 1/i$ for $j, k \geq K_i$. In particular, if $n_1 := m_{K_1+1} - m_{K_1}$, then $||\lambda^{n_1} - 1|| < 1$. Suppose that $n_1 < n_2 < \cdots < n_i$ have been chosen so that $||\lambda^{n_j} - 1|| < 1/j$ for $j \leq i$. Let

$$n_{i+1} := m_{K_{i+1}+n_i+1} - m_{K_{i+1}}.$$

Then $n_{i+1} > n_i$ and $||\lambda^{n_{i+1}} - 1|| < 1/(i+1)$. Thus we have constructed the desired sequence by induction.

To prove the theorem, let $m := \max(a, b)$. We assume that $m > 0$, and dividing by m, we may assume that $m = 1$. Let r be the number of i such that $\alpha_i = m$ and s the number of i such that $\beta_i = m$. Then for all k,

$$a_{n_k} = \sum_i \beta_i^{n_k} - \alpha_i^{n_k} \geq 0.$$

Taking the limit as k tends to infinity, we see that each term converges to zero except for those with absolute value 1, which converge to 1. Hence the limit of a_{n_k} is $s - r$. This implies that $s - r \geq 0$, hence that $b \geq a$.

Now suppose that $s = 1$ and $|\beta_1| = b$. Again we assume without of generality that $b = 1$. Assume first that $r = 0$. We have $a_n = \beta_1^n + \epsilon_n$, where ϵ_n tends to zero. By the lemma we find a sequence (n_k) such that $\beta_1^{n_k}$ converge to 1. Then β^{n_k+1} converges to β and hence $a_{n_k+1} = \beta^{n_k+1} + \epsilon_{n_k+1}$ converges to β. Since a_{n_k+1} is always real and nonnegative it follows that β is also. Hence $\beta = b$. Now suppose that $r = 1$. By a similar argument, we find a sequence (n_k) such that $\alpha_1^{n_k}$ and $\beta_1^{n_k}$ converge to 1. Then

$$a_{n_k+1} = \beta^{n_k+1} - \alpha^{n_k+1} + \epsilon_{n_k+1}$$

converges to $\beta - \alpha$ and

$$a_{n_k+2} = \beta^{n_k+2} - \alpha^{n_k+2} + \epsilon_{n_k+2}$$

converges to $\beta^2 - \alpha^2$. It follows that $\beta - \alpha$ and $\beta^2 - \alpha^2$ are real and nonnegative. Hence $\beta + \alpha$ is also real, and hence α and β are real. Thus β and α are both plus or minus 1, and $\alpha = -\beta$. Since $\beta \geq \alpha$, it is β that is positive.

Corollary Let $X/\mathbf{F}_q$ be a smooth, proper, and geometrically connected curve of genus g. Let a_n be the number of $\mathbf{F}_{q^n}$-valued points of $X/\mathbf{F}_q$. Then $|\alpha_i| < q$ for all i, and there exists an $r < 1$ such that

$$|a_n - (q^n + 1)| \leq 2gq^{nr}$$

for all $n \geq 1$.

Proof: We know that $a_n = 1 + q^n - \sum \alpha_i^n$ for all $n \geq 1$. The theorem says that all $|\alpha_i|$ are less than $|q|$, except for the possibility that for one i, $\alpha_i = -q$. But we know this can't happen—by making a base change to $\mathbf{F}_{q^2}$, for example. Hence $|\alpha_i| < q$ for all i. The result follows.

Corollary Let $\pi\colon X \to Y$ be a separable morphism of degree 2 of smooth projective curves over $P\mathbf{F}_p$. For each n let a_n^+ be the cardinality of the set of $y \in Y(\mathbf{F}_q^n)$ with two inverse images in $X(\mathbf{F}_{q^n})$ and let a_n^- be the cardinality of the set of y with no inverse images, and let a_n be the cardinality of the set of all points in $Y(\mathbf{F}_{q^n})$. Then

$$\lim \frac{a_n^+}{a_n} = \lim \frac{a_n^-}{a_n} = 1/2.$$

Proof: Let $a_n(X)$ be the cardinaliy of $X(\mathbf{F}_{q^n})$. For each $y \in Y(\mathbf{F}_{q^n}$, let c_y be the cardinlaity of $\pi^{-1}(y)$. Then $c_y \in \{0, 1, 2\}$. Furthermore $c_y = 1$ if and only if y is ramified, and the total number a_n^0 of such points is uniformly bounded. Hence:

$$a_n(X) = \sum_y c_y = \sum_y (c_y - 1) + a_n(Y) = a_n^+ - a_n^- + a_n(Y)$$

Write $a_n(X) = q^n + \epsilon_n(X)$ and $a_n(Y) = q^n + \epsilon_n(Y)$. Then

$$a_n^+ - a_n^- = \epsilon_n(X) - \epsilon_n(Y) \text{ and}$$

$$a_n^+ + a_n^- = a_n(Y) + a_n^0.$$

Our estimates imply that $\epsilon_n(X)/a_n(Y)$ and $\epsilon_n(Y)/a_n(Y)$ tend to zero with n, where ϵ_n means either $\epsilon_n(X)$ or $\epsilon_n(Y)$. Moreover a_n^0 is bounded. It follows that

$$\lim \frac{a_n^+ - a_n^-}{a_n} = 0 \text{ and } \lim \frac{a_n^+ + a_n^-}{a_n} = 1.$$

The theorem follows.