CORRECTION TO "NONVANISHING OF HYPERELLIPTIC ZETA FUNCTIONS OVER FINITE FIELDS"

JORDAN S. ELLENBERG, WANLIN LI, AND MARK SHUSTERMAN

published in *Algebra and Number Theory* **14**:7 (2020), 1895–1909

REVISION OF THEOREM 1.7 AND COROLLARY 1.8

A few corrections are required in the part of the paper that treats superelliptic curves of degree $\ell > 2$; we summarize these corrections below, then for ease of reading include corrected versions of Theorem 1.7 and Corollary 1.8 and their proofs.

- The statement of Theorem 1.7 part 1 is modified to reflect the fact that the cycle lengths k_i being mutually coprime implies $q \equiv 1 \bmod \ell$, and changing the assertion "every zero of Z_C is simple" to the correct "every zero of Z_C has degree ℓ-1."
- In the statement of Theorem 1.7 part 2, when q is congruent to 1 mod ℓ and $r = 2$, we added the requirement that the two cycles are of odd length.
- In the proof of Theorem 1.7, we corrected the statement that the permutation π acts trivially on $\mathbb{F}_\ell div(y)$ (instead it acts as multiplication by q), removed a footnote that rested on that statement, and clarified some discussion in the penultimate paragraph where the not-well-defined expression $\sqrt{q}$ was used in the original draft.
- The statement of Corollary 1.8 is changed to include necessary conditions on the order of q modulo ℓ, and the proof is rewritten with more details.
- A new reference [1] is added.

The authors apologize for any inconvenience incurred by the lapses in the original paper.

Theorem 1.7. *Let ℓ be an odd prime different from the characteristic of $\mathbb{F}_q$. Let C be a smooth projective curve over $\mathbb{F}_q$ which admits a degree ℓ map $f : C \to \mathbb{P}^1_{\mathbb{F}_q}$ such that f is Galois over $\mathbb{F}_q$ with Galois group isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. Let $S \subset \mathbb{P}^1(\overline{\mathbb{F}}_q)$ be the set of branch points of f. Let π be the permutation induced by the Frobenius action on S, and suppose that π is the composition of disjoint cycles of orders $k_1, k_2, \ldots, k_r$, all prime to ℓ.*

(1) *Suppose the k_i are mutually coprime and $r \leq 3$. Then every zero of Z_C has degree $\ell - 1$.*
(2) *Define κ_i to be k_i if k_i is odd and $k_i/2$ if k_i is even. Suppose that either*
   - *q is congruent to 1 modulo ℓ and $r = 2$, with both cycles of odd length; or*
   - *There is no i such that q^{κ_i} is congruent to 1 modulo ℓ.*

   Then the point $s = \frac{1}{2}$ is not a zero of Z_C.

Proof. Let $x_1, \ldots, x_m$ be the ramification points of the $(\mathbb{Z}/\ell\mathbb{Z})$-cover of $\mathbb{P}^1$ in S, where $m = k_1 + \cdots + k_r$. The Jacobian $J(C)$ of C carries an action of $\mathbb{Z}[(\mathbb{Z}/\ell\mathbb{Z})]$; write $\lambda \in \mathbb{Z}[(\mathbb{Z}/\ell\mathbb{Z})]$ for $\zeta_\ell - 1$, where ζ_ℓ is a generator of $(\mathbb{Z}/\ell\mathbb{Z})$. A Riemann-Hurwitz computation shows that the genus of C is $(m-2)(\ell-1)/2$, so the Tate module $T_\ell J(C)$ is a free $\mathbb{Z}_\ell[\zeta_\ell]$-module of rank $m - 2$, and $J(C)[\lambda]$ has dimension $m - 2$.

The λ-torsion subgroup of $J(C)$ is spanned by the degree-0 λ-torsion divisors $x_i - x_j$. That is, the group of divisors of the form $\sum a_i x_i$ with $\sum a_i = 0$ surjects onto $J(C)[\lambda]$. This surjection is not an isomorphism; there is a 1-dimensional kernel, which we can describe as follows. Over $\overline{\mathbb{F}}_q$, the curve C has an affine model of the form $y^\ell = f(x)$ with f a rational function with no zeroes or poles at ∞. Then the principal divisor associated to y is $\sum a_i x_i$ where $a_i = \mathrm{ord}_{x_i} f$. We have now expressed $J(C)[\lambda]$ as an explicit subquotient of $\mathbb{F}_\ell^m$.

This identification is equivariant for the Frobenius action on both sides, so it allows us to describe the mod ℓ Galois representation afforded by $J(C)$ in terms of the permutation π which Frobenius induces on $x_1, \ldots, x_m$.

The action of π splits $x_1, \ldots, x_m$ into cycles of length $k_1, \ldots, k_r$, which by hypothesis are prime to ℓ, and which must be multiples of d, where d is the order of q in $\mathbb{F}_\ell^*$. So the eigenvalues of π in its action on $\mathbb{F}_\ell^m$ are the union (as multisets) $\bigcup_{j=1}^r \mu_{k_j}$. Now the composition factors of $\mathbb{F}_\ell^m$ as a representation of the cyclic group $\langle \pi \rangle$ are $J(C)[\lambda]$, $\mathbb{F}_\ell \mathrm{div}(y)$, and the π-trivial one-dimensional representation onto which $\mathbb{F}_\ell^m$ maps by summing coordinates. The action of π on the latter factor is trivial, while π acts on $\mathbb{F}_\ell \mathrm{div}(y)$ as multiplication by q. If the zeta function Z_C had a zero at $1/2$, then $\sqrt{q}$ would be a Frobenius eigenvalue of C, which would mean that some eigenvalue μ of the action of π on $J(C)[\lambda]$ satisfied $\mu^2 = q$.

In case q is congruent to 1 modulo ℓ (i.e., $d = 1$) the eigenvalues of π in its action on $J(C)[\lambda]$ are the multiset $\bigcup_{j=1}^r \mu'_{k_j}$ together with $r-2$ copies of 1, where μ'_n denotes the nontrivial nth roots of unity. The hypotheses $r = 2$ and k_j odd now guarantee that the eigenvalues of π on $J(C)[\lambda]$ contain no copies of either 1 or -1, completing the proof in this case.

If $d > 1$, we note that our condition on q^{κ_j} can be satisfied only when d is even. (If d is odd, then κ_j is always a multiple of d, so $q^{\kappa_j} = 1$.) When d is even, our condition in fact says precisely that each k_i is a multiple of d but not of $2d$. The two square roots of q in $\bar{\mathbb{F}}_\ell^*$ both have order $2d$, and thus neither can appear among the eigenvalues of Frobenius on $J(C)[\lambda]$.

We now turn to the first assertion of the theorem. We note that the coprimality of the k_i implies that $d = 1$, or in other words that q is conguent to 1 modulo ℓ. The fact that $J(C)$ carries an action of $\mathbb{Z}/\ell\mathbb{Z}$ defined over $\mathbb{F}_q$ with trivial invariant subspace implies that the Frobenius eigenvalues on $J(C)$ all appear with multiplicity a multiple of $\ell - 1$, and that a root of multiplicity $k(\ell-1)$ reduces to a root of multiplicity k in the action of Frobenius on $J(C)[\lambda]$. So we just need to show that the action of Frobenius on $J(C)[\lambda]$ has no repeated eigenvalues. The coprimality of the k_i guarantees that the union $\bigcup_{j=1}^r \mu'_{k_j}$ is disjoint; the remaining eigenvalues are $r-2$ copies of 1, so since $r \leq 3$ we are done.

□

Corollary 1.8. *Let ℓ be an odd prime different from the characteristic of $\mathbb{F}_q$. Let d be the order of $(q \bmod \ell)$ in $(\mathbb{Z}/\ell\mathbb{Z})^*$. Let $N(X)$ be the number of primitive degree ℓ Dirichlet characters $\chi_f : (\mathbb{F}_q[t]/f)^* \to \mathbb{C}^*$ with conductor f satisfying $q^{\deg f} \leq X$ and $L(1/2, \chi_f) \neq 0$. We show the following:*

- *if $d = 1$, then $N(X) \gg \frac{X}{\log X}$ for $X \to \infty$;*

- *if d is even, then $N(X) \gg \frac{X}{(\log X)^{1-\frac{\ell-1}{2d}}}$ for $X \to \infty$. In particular, since $d \mid \ell - 1$, we have $N(X) \gg \frac{X}{(\log X)^{1/2}}$ for $X \to \infty$.*

We do not get a lower bound of this quality in the case where q has odd order modulo ℓ.

Proof. We first consider the case $d = 1$ (i.e., q is congruent to 1 modulo ℓ).

Let f_1, f_2 be two distinct monic irreducible polynomials in $\mathbb{F}_q[t]$ of degrees being odd and prime to ℓ. Let $d_1 = \deg f_1$ and $d_2 = \deg f_2$. Let $e \in \{1, \dots, \ell - 1\}$ be such that $\ell \mid d_1 + ed_2$. The smooth projective curve C with affine model $y^\ell = f_1 f_2^e$ admits a cyclic degree ℓ map to $\mathbb{P}^1_{\mathbb{F}_q}$ where the set of branch points are roots of $f = f_1 f_2$ in the affine line (the condition on $d_1 + ed_2$ guarantees there is no branching at ∞.) By Theorem 1.7(2), the zeta function Z_C does not vanish at $s = 1/2$. Thus, all degree ℓ Dirichlet characters with conductor f have L-functions nonvanishing at the central point. Evidently, the number of such pairs f_1, f_2 with $d_1 + d_2 \leq n$ is at least the number of irreducible polynomials of degree $n - 3$; the number of characters with non-vanishing L-functions is thus bounded below by a constant multiple of $q^n/n = X/(\log X)$. This concludes the proof in the $d = 1$ case.

We now turn to the case where $q \not\equiv 1 \bmod \ell$. We recall that d is the order of q mod ℓ in $(\mathbb{Z}/\ell\mathbb{Z})^*$. Let $\Sigma_{d,2d}$ be the set of monic squarefree polynomials such that all of their irreducible factors have degree divisible by d but not divisible by $2d$. For any $f \in \Sigma_{d,2d}$ there exists a $(\mathbb{Z}/\ell\mathbb{Z})$ field extension $K/\mathbb{F}_q(x)$ with conductor f. The field K is the function field of a curve $C/\mathbb{F}_q$ which admits a cyclic degree ℓ map to $\mathbb{P}^1_{\mathbb{F}_q}$ whose set of branch points are roots of f. By Theorem 1.7(2), the zeta function Z_C does not vanish at $s = 1/2$. Thus, all degree ℓ Dirichlet characters with conductor f have their L-functions do not vanish at the central point. The number of such characters is $(\ell - 1)^{\omega(f)}$ where $\omega(f)$ denotes the number of irreducible factors of f.

So it remains to count the number of degree ℓ Dirichlet characters whose conductor is in $\Sigma_{d,2d}$, which by the above discussion is given by

$$\sum_{f \in \Sigma_{d,2d}, |f| \leq X} (\ell - 1)^{\omega(f)}.$$

To estimate this sum, we start by considering the Dirichlet series

$$G(s) = \sum_{f \in \Sigma_{d,2d}} (\ell - 1)^{\omega(f)} |f|^{-s}$$

where $|f| = q^{\deg f}$. Then $G(s)$ has a Euler product expansion

$$G(s) = \prod_{P \in \Sigma_{d,2d},\ \text{irrd.}} (1 + (\ell - 1)|P|^{-s}).$$

Taking

$$H(s) = \prod_{P \in \Sigma_{d,2d},\ \text{irrd.}} (1 + |P|^{-s})^{2d},$$

we see that $G(s)^{2d}/H(s)^{\ell-1}$ is holomorphic at $s=1$. Now define

$$Z_d(s) = \prod_{d|\deg P,\ P \text{ irrd.}} (1+|P|^{-s})^d$$

so that $H(s) = (Z_d(s))^2/Z_{2d}(s)$. Since $Z_d(s)$ and $Z_{2d}(s)$ each have a simple pole at $s=1$, so does $H(s)$.

We conclude that $G(s)^{2d}$ has a pole at $s=1$ with order $\ell-1$ and is absolutely convergent for $\Re(s)>1$. By [1, Theorem 3.1], the sum of coefficients of $G(s)$ has the following asymptotic relation

$$\sum_{f\in\Sigma_{d,2d'}|f|\leq X} (\ell-1)^{\omega(f)} \sim C\cdot X(\log X)^{\frac{\ell-1}{2d}-1}$$

where the constant

$$C = \frac{|(\lim_{s\to 1} G(s)^{2d}(s-1)^{\ell-1})^{\frac{1}{2d}}|}{\Gamma((\ell-1)/(2d))}.$$

And it gives the desired result.

□

REFERENCES

[1] Ryo Kato, *A remark on the Wiener-Ikehara Tauberian theorem*, Comment. Math. Univ. St. Pauli **64** (2015), no. 1, 47–58. MR3410120