

ON PRIMES OF DEGREE ONE IN FUNCTION FIELDS

GREG W. ANDERSON AND ROBERT INDIK

ABSTRACT. We show that over the algebraic closure of a finite field, every point of the jacobian of a curve annihilated by a power of a prime l is the l -primary component of a point in the image of the curve.

Let X be a smooth, projective, geometrically connected curve of genus $g > 0$ defined over the algebraic closure $\bar{\mathbf{F}}_q$ of the field \mathbf{F}_q of q elements. Fixing a basepoint x_0 of X in $\bar{\mathbf{F}}_q$, let $\varphi: X \rightarrow J$ denote the embedding assigning to each point x of X the divisor class of the difference of x and x_0 . Let l be any prime number and let $\lambda: J(\bar{\mathbf{F}}_q) \rightarrow J(\bar{\mathbf{F}}_q)_l$ denote the projection of the torsion group $J(\bar{\mathbf{F}}_q)$ onto its l -primary component. The object of this note is to prove the following

THEOREM. *The map $\lambda \circ \varphi: X(\bar{\mathbf{F}}_q) \rightarrow J(\bar{\mathbf{F}}_q)_l$ is surjective.*

For the proof we need a lemma giving control over the distribution of primes of degree one in arithmetic progressions. Let K/k be an abelian unramified extension of global fields of positive characteristic. Let g be the genus of k and suppose that \mathbf{F}_q is the field of constants of both K and k . For each prime v of k let $F_v \in \text{Gal}(K/k)$ denote the corresponding arithmetic Frobenius.

LEMMA. *If there exists $\sigma_0 \in \text{Gal}(K/k)$ such that $F_v \neq \sigma_0$ for all primes v of k of degree one, then $q \leq (2g[K:k] + 3)^2$.*

PROOF. By hypothesis

$$(*) \quad \sum_v 1 = - \sum_v \sum_{\psi} \overline{\psi(\sigma_0)} \psi(F_v),$$

where v runs through all the primes of k of degree one (i.e., of residue field coinciding with \mathbf{F}_q), and ψ runs through all the nontrivial complex-valued characters of $\text{Gal}(K/k)$. Now by the Riemann Hypothesis (see Appendix 5 of [W]) the left side of $(*)$ is bounded below by $q + 1 - 2g\sqrt{q}$; the right side is bounded above by $([K:k] - 1)(2g - 2)\sqrt{q}$. The desired conclusion follows immediately.

Turning now to the proof of the theorem, suppose that some point $d \in J(\bar{\mathbf{F}}_q)$ fails to be in the image of $\lambda \circ \varphi$. Assume, as is permissible, that X is the base-change of a smooth projective curve X_0 defined over \mathbf{F}_q , x_0 is \mathbf{F}_q -rational, and d is an \mathbf{F}_q -rational point of the jacobian J_0 of X_0 . Fix a rational prime r distinct from l . Let k denote the function field of X_0 , \bar{k} an algebraic closure of k , and v_0 the prime of degree one of k

Received by the editors April 3, 1984.

1980 *Mathematics Subject Classification.* Primary 12A80; Secondary 14H99.

©1985 American Mathematical Society
 0002-9939/85 \$1.00 + \$.25 per page

to which x_0 corresponds. For each positive integer n let k_n denote the compositum in \bar{k} of k and the unique extension of \mathbf{F}_q in \bar{k} of degree r^n . Let K_n denote the maximal unramified abelian extension of k_n in \bar{k} of degree a power of l in which v_0 splits completely. Letting $\alpha_1, \dots, \alpha_{2g}$ denote the reciprocal roots of the numerator of the zeta function of X_0 over \mathbf{F}_q , we have

$$|[K_n : k_n]|_l = \prod_{j=1}^{2g} |1 - \alpha_j^{r^n}|_l,$$

where $|\cdot|_l$ is any extension to $\bar{\mathbf{Q}}$ of the l -adic absolute value of \mathbf{Q} , whence $[K_n : k_n]$ is bounded. But for all n the Artin symbol $(d, K_n/k_n) \in \text{Gal}(K_n/k_n)$ fails to equal the arithmetic Frobenius F_v for all primes v of k_n of degree one, whence, via the lemma, an estimate

$$q^{r^n} \leq (2g[K_n : k_n] + 3)^2,$$

a contradiction. This proves the theorem.

ACKNOWLEDGEMENT. Thanks to Robert Coleman for suggesting the problem.

REFERENCES

[W] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138

DEPARTMENT OF MATHEMATICS, BRANDEIS UNIVERSITY, WALTHAM, MASSACHUSETTS 02254 (Current address of Robert Indik)

Current address (G. W. Anderson): Department of Mathematics, University of California, Berkeley, California 94720