FINITE FIELDS AND THEIR APPLICATIONS **1**, 399–404 (1995)

On Artin's Conjecture over Function Fields

FRANCESCO PAPPALARDI

Departimento di Matematica, Terza Università delgi Studi, Via C. Segre, 2/6, 00146, Rome, Italy
E-mail: pappa@mat.uniroma3.it

AND

IGOR SHPARLINSKI

School of MPCE, Macquarie University, Sydney, New South Wales 2109, Australia
E-mail: igor@mpce.mq.edu.au

Communicated by Stephen D. Cohen

Received June 17, 1994; revised October 6, 1994

We prove an unconditional analog of Artin's conjecture for the function field of a curve over a finite field. © 1995 Academic Press, Inc.

In this paper we consider an analog of Artin's conjecture for polynomials and rational functions over the finite fields $\mathbb{F}_q$ of q elements. A proof of the original Artin's conjecture was given by Hooley in [H] under the assumption of the Generalized Riemann Hypothesis (see also [N] for a survey of many other relevant results). We show that similar considerations (a kind of sieve method) can be used (in a much simpler form) for the case of function fields as well. Moreover, because for function fields an analog of the Generalized Riemann Hypothesis has been obtained by Weil (see [L-N] for details), we get an unconditional result. We also mention the papers [B] and [L] where similar (and even more general) questions were considered. However, the asymptotic formulas obtained there do not contain any estimates of the error terms.

Let $r(x) \in \mathbb{F}_q(x)$ be a rational function over the finite field $\mathbb{F}_q$ of q elements. One of many possible analogs of Artin's conjecture is the question

1071-5797/95 $12.00

about the number of monic irreducible polynomials $p(x) \in \mathbb{F}_q[x]$ of degree n such that $r(x)$ is a primitive root modulo $p(x)$, i.e., such that the powers

$$r(x)^i, \qquad i = 0, 1, \ldots,$$

generate all nonzero elements of the residue ring $\mathbb{F}_q[x]/p(x)$. In this paper we consider this and an even more general but similar question for arbitrary function fields over a finite field.

Let $\mathcal{C}$ be a nonsingular irreducible curve over $\mathbb{F}_q$ of degree d: this means that it is defined by a system of polynomial equations of total degree d over $\mathbb{F}_q$. In particular, its genus g does not exceed $(d-1)(d-2)/2$. We denote by $\mathbb{K} = \mathbb{F}_q(\mathcal{C})$ the function field of the curve $\mathcal{C}$.

For a divisor $\mathfrak{U}$ let us denote by $\mathcal{O}_{\mathfrak{U}}$ the local ring of $\mathfrak{U}$, namely

$$\mathcal{O}_{\mathfrak{U}} = \{f \in K \mid f \quad \text{is regular on supp } \mathfrak{U}\}.$$

A rational function $r(X) \in \mathbb{K}$ is said be a primitive root modulo a prime divisor $\mathfrak{P}$ if all the powers

$$r(X)^i, \qquad i = 0, 1, \ldots,$$

generate all the nonzero elements of the residue ring

$$\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} \simeq \mathbb{F}_{q^n}.$$

Let $N(r, \mathbb{K}, n)$ denote the number of prime divisors $\mathfrak{P}$ of $\mathcal{C}$ of degree n such that $r(X)$ is a primitive root modulo $\mathfrak{P}$. Let $\nu(k)$ and $\varphi(k)$ denote the number of distinct prime divisors of an integer k and the Euler function, respectively.

THEOREM. *Let $\mathbb{K} = \mathbb{F}_q(\mathcal{C})$ be the function field of a nonsingular irreducible curve $\mathcal{C}$ of degree d over $\mathbb{F}_q$ and let $r(X) \in \mathbb{K}$ be a rational function of degree $m > 0$. Suppose that for all integers $k > 1$, $k \mid q^n - 1$, $r(X)$ is not the* kth *power of a rational function from the function field on $\mathcal{C}$ over the algebraic closure of $\mathbb{F}_q$. Then, for all integers n,*

$$\left| N(r, \mathbb{K}, n) - \frac{\varphi(q^n - 1)}{n} \right| \le 1.5(d+1)(d+2m)n^{-1}2^{\nu(q^n-1)}q^{n/2}.$$

Proof. Let $\mathbb{F}_{q^n}$ be a fixed field of q^n elements. It is known that, for any prime divisor $\mathfrak{P}$ of degree n,

$$\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} \simeq \mathbb{F}_{q^n}$$

and the isomorphism is given by $\Psi(X) \leftrightarrow \psi(Q)$, where $\Psi(X)$ is the image in $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ of a function $\psi(X) \in \mathbb{K}$ and Q is a $\mathbb{F}_{q^n}$-rational point on $\mathcal{C}$ corresponding to $\mathfrak{P}$. Thus, $r(X)$ is a primitive root modulo $\mathfrak{P}$ if and only if $r(Q)$ is a primitive root of the field $\mathbb{F}_{q^n}$.

For every given prime divisor $\mathfrak{P}$ of degree n there are exactly n different $\mathbb{F}_{q^n}$-rational points corresponding to it, namely,

$$\text{Frob}^i(Q), \qquad i = 0, \ldots, n-1,$$

where Frob is the Frobenius isomorphism over $\mathbb{F}_q$. We deduce that $nN(r, \mathbb{K}, n)$ equals the number of $\mathbb{F}_{q^n}$-rational points Q on $\mathcal{C}$ corresponding to at least one prime divisor of degree n for which $r(Q)$ is a primitive root of $\mathbb{F}_{q^n}$.

Moreover, we may count only $\mathbb{F}_{q^n}$-rational points Q because if Q corresponds to a divisor of degree less than n, then Q is a rational point in some proper subfield of $\mathbb{F}_{q^n}$; thus $r(Q)$ is an element of the same subfield and, therefore, it cannot be a primitive root of $\mathbb{F}_{q^n}$.

Hence, we have that

$$N(r, \mathbb{K}, n) = n^{-1}T(r, \mathcal{C}, n),$$

where $T(r, \mathcal{C}, n)$ is the total number of $\mathbb{F}_{q^n}$-rational points Q on $\mathcal{C}$ for which $r(Q)$ is a primitive root of $\mathbb{F}_{q^n}$.

Let Ξ be the set of all multiplicative characters of $\mathbb{F}_{q^n}$. For $\chi \in \Xi$ define its order ord χ as the least positive integer t such that χ^t is the trivial character. Further let $\mathcal{R}_n$ denote the set of $\mathbb{F}_{q^n}$-rational points Q on $\mathcal{C}$ which are neither poles nor zeros of $r(X)$. Applying the Weil estimate for the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{C}$ (see for example the comments to Section 6.4 in [L-N]) and taking into account that $r(X)$ has a total of at most m poles and zeros, we find that

$$\left| |\mathcal{R}_n| - q^n - 1 \right| \le 2gq^{n/2} + m \le (d-1)(d-2)q^{n/2} + m.$$

Now, it is known (see Problem 5.14 of [L-N] or Proposition 2.2 of [N]) that, for any $\rho \in \mathbb{F}_{q^n}$,

$$\frac{\varphi(q^n-1)}{q^n-1} \sum_{\delta | q^n - 1} \frac{\mu(\delta)}{\varphi(\delta)} \sum_{\substack{\chi \in \Xi \\ \text{ord}\, \chi = \delta}} \chi(\rho) = \begin{cases} 1, & \text{if } \rho \text{ is a primitive root,} \\ 0, & \text{otherwise,} \end{cases}$$

where $\mu(k)$ is the Möbius function. Therefore, we have

$$T(r, \mathscr{C}, n) = \frac{\varphi(q^n - 1)}{q^n - 1} \sum_{Q \in \mathscr{R}_n} \sum_{\delta | q^n - 1} \frac{\mu(\delta)}{\varphi(\delta)} \sum_{\substack{\chi \in \Xi \\ \text{ord } \chi = \delta}} \chi(r(Q))$$

$$= \frac{\varphi(q^n - 1)}{q^n - 1} \sum_{\delta | q^n - 1} \frac{\mu(\delta)}{\varphi(\delta)} \sum_{\substack{\chi \in \Xi \\ \text{ord } \chi = \delta}} \sum_{Q \in \mathscr{R}_n} \chi(r(Q)).$$

Since $r(X)$ is not a power of any other rational function, we can apply Perelmuter's bound (see Theorem 2 in [P]),

$$\left| \sum_{Q \in \mathscr{R}_n} \chi(r(Q)) \right| \leq (d^2 + 2dm - 3d) q^{n/2},$$

to every non-trivial multiplicative character χ. Note that this is a particular case of the result of Perelmuter. In fact, Theorem 2 of [P] deals with general sums of additive and multiplicative characters along a curve and is a consequence of the famous Weil result on the Riemann Hypothesis over function fields.

The contribution to $T(r, \mathscr{C}, n)$ of the trivial character (i.e., the character of order $d = 1$) is

$$|\mathscr{R}_n| \frac{\varphi(q^n - 1)}{q^n - 1} = \varphi(q^n - 1) + \Delta,$$

where

$$\Delta \leq \frac{\varphi(q^n - 1)}{q^n - 1} (2 + (d - 1)(d - 2) q^{n/2} + m \leq (d - 1)(d - 2) q^{n/2} + m + 2.$$

Further, it is easy to see that

$$\sum_{\delta | k} |\mu(\delta)| = 2^{\nu(k)}.$$

Since Ξ is a cyclic group (see Corollary 5.9 of [L-N]), there are exactly $\varphi(d)$ characters $\chi \in \Xi$ with ord $\chi = d$. Taking this into account, we obtain

$$\begin{aligned}
|T(r, \mathscr{C}, n) - \varphi(q^n - 1)| &\leq (d - 1)(d - 2) q^{n/2} + m + 2 \\
&\quad + (d^2 + 2dm - 3d) q^{n/2} \sum_{\delta | q^n - 1} |\mu(\delta)| \\
&\leq 2^{\nu(q^n - 1)} q^{n/2} ((d - 1)(d - 2)/2 \\
&\quad + m/2 + 1 + d^2 + 2dm - 3d) \\
&\leq 1.5(d + 1)(d + 2m) 2^{\nu(q^n - 1)} q^{n/2},
\end{aligned}$$

which is the claimed estimate. ■

COROLLARY 1. *For any* $\varepsilon > 0$,

$$N(r, \mathbb{K}, n) = \frac{\varphi(q^n - 1)}{n}(1 + O(d(d+m)q^{-n(1/2-\varepsilon)})),$$

where the implied constant depends only on ε.

Proof. From the well-known inequalities

$$\nu(k) = O(\log k/\log\log k), \qquad k/\varphi(k) = O(\log\log k),$$

we get

$$2^{\nu(q^n-1)} = O(q^{n\varepsilon/2}), \qquad (q^n - 1)/\varphi(q^n - 1) = O(q^{n\varepsilon/2}),$$

and the estimate follows. ■

In the special case of the rational function field over a finite field, that is, when $d = 1$, $\mathbb{K} = \mathbb{F}_q(x)$, $N(r, \mathbb{F}_q, n)$ is the number of irreducible polynomials $p(x)$ of degree n such that $r(x)$ is a primitive root of $\mathbb{F}_q[x]/p(x)$. Then, we get

$$N(r, \mathbb{F}_q, n) = \frac{\varphi(q^n - 1)}{n}(1 + O(mq^{-n(1/2-\varepsilon)}))$$

for any given rational function $r(x) \in \mathbb{F}_q(x)$ of degree m.

COROLLARY 2. *Given a rational function* $r(X) \in \mathbb{K}$ *of degree* m, *there is a prime divisor* $\mathfrak{P}$ *of degree*

$$\deg \mathfrak{P} = O(\log_q (d + m) + 1)$$

for which $r(X)$ *is a primitive root modulo* $\mathfrak{P}$.

Proof. It is easy to see that the least n such that $N(r, \mathbb{K}, n) > 0$ is of order $O(\log_q (d + m) + 1)$. ■

We define the norm an integer divisor $\mathfrak{U}$ as

$$\mathrm{Nm}(\mathfrak{U}) = q^{\deg \mathfrak{U}}.$$

We conclude with

COROLLARY 3. *If q is fixed then, for any rational function $r(X) \in \mathbb{K}$ of degree m and for any $\varepsilon > 0$, there is a prime divisor $\mathfrak{P}$ of norm*

$$\mathrm{Nm}\,(\mathfrak{P}) = O((d(d+m))^{2+\varepsilon})$$

for which $r(X)$ is a primitive root modulo $\mathfrak{P}$.

Proof. It is easy to see that for q fixed, the minimal n such that $N(r, \mathbb{K}, n) > 0$ is of order $(2+\varepsilon)\log_q((d+1)(d+m)) + O(1)$. ■

ACKNOWLEDGMENTS

The authors thank Steve Cohen and Pieter Moree for many valuable comments and critical remarks.

REFERENCES

[H] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.

[B] H. Bilharz, Primdivisoren mit vorgegebener Primitivwurzel, *Math. Ann.* **114,** (1937), 476–492.

[L] H. W. Lenstra, On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.* **42** (1977), 201–224.

[L-N] R. Lidl and H. Niederreiter, "Finite Fields," Addison-Wesley, Reading, Massachusetts, 1983.

[N] W. Narkiewicz, "Classical Problems in Number Theory, PWN, Warsaw, 1986.

[P] G. I. Perelmuter, A bound of the sum along a curve, *Mat. Zametki* **5**, No. 3 (1969), 373–380. [in Russian]