Canad. Math. Bull. Vol. **38** (2), 1995 pp. 167–173

GENERALIZED ARTIN'S CONJECTURE FOR PRIMITIVE ROOTS AND CYCLICITY MOD $\mathfrak{p}$ OF ELLIPTIC CURVES OVER FUNCTION FIELDS

DAVID A. CLARK AND MASATO KUWATA

ABSTRACT. Let $k = \mathbf{F}_q$ be a finite field of characteristic p with q elements and let K be a function field of one variable over k. Consider an elliptic curve E defined over K. We determine how often the reduction of this elliptic curve to a prime ideal $\mathfrak{p}$ is cyclic. This is done by generalizing a result of Bilharz to a more general form of Artin's primitive roots problem formulated by R. Murty.

1. **Introduction.** Let $k = \mathbf{F}_q$ be a finite field of characteristic p with q elements and let K be a function field of one variable over k. We consider an elliptic curve E defined over K. Let $\mathfrak{p}$ be a prime ideal in K. The reduction of E, denoted by $\bar{E}_\mathfrak{p}$, is defined over the residue field $k_\mathfrak{p}$, which is a finite extension of $\mathbf{F}_q$. It is well-known that $\bar{E}_\mathfrak{p}(k_\mathfrak{p})$ is a finite abelian group of the form

$$\bar{E}_\mathfrak{p}(k_\mathfrak{p}) \cong \mathbf{Z}/m_1\mathbf{Z} \oplus \mathbf{Z}/m_1\mathbf{Z}, \quad m_2 \mid m_1,\ p \nmid m_2.$$

(*cf.* [Si, Chapter III Corollary 6.4], for example.) In this note we study how often the group $\bar{E}_\mathfrak{p}(k_\mathfrak{p})$ becomes cyclic. In [S2] Serre raised the same question for elliptic curves over $\mathbf{Q}$, and following Hooley's work [Ho] on Artin's primitive root conjecture, he showed that the density of such prime numbers is non zero, assuming the Generalized Riemann Hypothesis (GRH). Gupta and Murty [GM2] removed the GRH and proved that the number of primes $p \leq x$ for which $\bar{E}(\mathbf{F}_p)$ is cyclic is $\gg x/\log^2 x$ so long as E has a non-rational 2-torsion point.

As for Artin's conjecture for primitive roots, before Hooley [Ho] proved it under GRH, Bilharz [B] proved its analogue for function fields of one variable over finite fields. He, too, assumed the GRH at the time, but the GRH for function fields was subsequently proved by Weil [W].

In this note we prove an analogous result for elliptic curves defined over a function field K over a finite field by generalizing Bilharz's result to a more general form of Artin's problem formulated following R. Murty [M].

Let K_m be the smallest extension of K in which all the m-torsion points of E are defined. Our main result is:

The second author was supported by a Natural Sciences and Engineering Research Council of Canada International Postdoctoral Fellowship.

Received by the editors May 13, 1992; revised March 1, 1994 and December 5, 1994.

AMS subject classification: 11R58 11G05.

Key words and phrases: elliptic curves, function fields.

THEOREM 1.1. *The Dirichlet density δ of the set of prime ideals $\mathfrak{p}$ such that $\bar{E} \bmod \mathfrak{p}$ is cyclic is given by*

$$\delta = \sum_{(m,p)=1} \frac{\mu(m)}{[K_m : K]}.$$

In [LT] Lang and Trotter posed the following question: Let E be an elliptic curve defined over $\mathbf{Q}$ and P be a rational point of infinite order in E. What is the density of prime numbers p for which the group $\bar{E}(\mathbf{F}_p)$ of rational points $\bmod p$ is generated by the reduction of $P \bmod p$? This is an obvious generalization of Artin's conjecture for primitive roots. Once again, this question has an obvious analogue for elliptic curves over function fields. Since $\bar{E} \bmod \mathfrak{p}$ must be a cyclic group to be generated by a single element, our result is a first step toward answering this question. In Section 4 we discuss this question further.

The authors would like to thank Professor R. Murty for suggesting this problem to us and for useful conversations.

2. **Generalization of Bilharz's result.** In this section we will generalize Bilharz's result in [B] in view of application to our problem.

Let $k = \mathbf{F}_q$ be a finite field of characteristic p with q elements. A function field of one variable over k is a field K that satisfies:

(1) the transcendence degree of K/k is 1;
(2) K is finitely generated over k; and
(3) k is algebraically closed in K.

Let K be a function field of one variable and $\mathcal{F}$ be a family of finite Galois extensions of K. Denote by $L(\mathcal{F})$ the lattice of fields spanned by $\mathcal{F}$. Let M be a set of prime ideals in K. We say that the Dirichlet density of M *exists* if the limit

$$\frac{\lim_{s \to 1+0} \delta(s, M) = \lim_{s \to 1+0} \sum_{\mathfrak{p} \in M} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \text{ in } K} N\mathfrak{p}^{-s}}$$

exists. We call this limit the *Dirichlet density* of M and denote it by $\delta(M)$.

The *generalized Artin's problem* is to determine the density of primes that do not split completely in any of the fields in $L(\mathcal{F})$ for a given family $\mathcal{F}$. If we take $\mathcal{F} = \{\mathbf{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{a})\}_{\ell: \text{prime}}$ for a given $a \in \mathbf{Q}$, we obtain the original Artin's primitive roots problem. Bilharz solved this problem for $\mathcal{F} = \{K(\sqrt[\ell]{1}, \sqrt[\ell]{a})\}_{\ell: \text{prime}, \ell \neq p}$. In the following we will generalize his result.

Let K be a function field of one variable over a finite field $k = \mathbf{F}_q$ and $\mathcal{F} = \{K_\nu\}_{\nu \in \mathbf{N}}$ be a countable family of Galois extensions of K. Let k_ν be the algebraic closure of k in K_ν. Define $n(\nu) = [K_\nu : K]$ and $c(\nu) = [k_\nu : k]$. Let $g(K_\nu)$ be the genus of K_ν. For a set of positive integers $I = \{\nu_1, \ldots, \nu_r\}$, we define K_I to be the compositum $K_{\nu_1} \cdots K_{\nu_r}$. We define the Möbius function for I by $\mu(I) = (-1)^{|I|}$. With this notation we can state our main result.

THEOREM 2.1. *Suppose that the following conditions hold for the family $\mathcal{F} = \{K_\nu\}_{\nu \in \mathbf{N}}$.*

https://doi.org/10.4153/CMB-1995-023-2 Published online by Cambridge University Press

(1) $\sum_{\nu=1}^{\infty} \frac{1}{n(\nu)} < \infty$,

(2) $\sum_{\nu=1}^{\infty} \frac{1}{c(\nu)q^{\frac{1}{2}c(\nu)}} < \infty$, *and*

(3) There exists a constant C *such that* $g(K_\nu) \leq C\frac{n(\nu)}{c(\nu)}$ *for all* ν.

Let M *be the set of prime ideals in* K *that do not split completely in any of the fields in* $L(\mathcal{F})$. *Then the Dirichlet density of* M *exists and is given by*

$$\delta(M) = \sum_I \frac{\mu(I)}{[K_I : K]}.$$

PROOF. If F is a Galois extension of K, we define (F) to be the set of prime ideals in K that split completely in F. In this notation (K) stands for the set of all prime ideals in K. We set $M_n = \bigcap_{\nu \leq n}[(K) - (K_\nu)]$. Then, on the one hand, we have $M = \lim_{n\to\infty} M_n$. On the other hand,

$$\begin{aligned} M_n &= (K) - \sum_{\nu\leq n}(K_\nu) + \sum_{\nu_1<\nu_2\leq n}(K_{\nu_1}K_{\nu_2}) - \cdots + (-1)^n(K_{\nu_1}\cdots K_{\nu_n}) \\ &= \sum_{I\subset\{1,\ldots,n\}} \mu(I)(K_I) \end{aligned}$$

Thus

$$\delta(s, M) = \lim_{n\to\infty} \delta(s, M_n) = \sum_I \mu(I)\delta\big(s, (K_I)\big).$$

Our task now is to prove that we can exchange the two limits $\lim_{s\to 1+0}$ and $\lim_{n\to\infty}$.

Consider the zeta function of K/k:

$$\zeta(s, K/k) = \prod_{\mathfrak{p}\in(K)} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1}.$$

Taking the logarithm, we have

$$\log\zeta(s, K/k) = -\sum_{m=1}^{\infty} \sum_{\mathfrak{p}\in(K)} \frac{1}{mN\mathfrak{p}^{ms}}.$$

Since the first term is the dominant part near $s = 1$, we can rewrite the definition of the Dirichlet density as follows.

$$\lim_{s\to 1+0} \delta(s, M) = \lim_{s\to 1+0} \frac{\sum_{m=1}^{\infty}\sum_{\mathfrak{p}\in M}(mN\mathfrak{p}^{ms})^{-1}}{\sum_{m=1}^{\infty}\sum_{\mathfrak{p}\in(K)}(mN\mathfrak{p}^{ms})^{-1}} = \lim_{s\to 1+0} \frac{\sum_{m=1}^{\infty}\sum_{\mathfrak{p}\in M}(mN\mathfrak{p}^{ms})^{-1}}{\log\zeta(s, K/k)}$$

Suppose that a prime ideal $\mathfrak{p}$ in K splits completely in K_ν; *i.e.*,

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_{n(\nu)}; \quad N\mathfrak{P}_i = N\mathfrak{p}.$$

Then we have

$$\sum_{m=1}^{\infty} \sum_{\mathfrak{p}\in(K_\nu)} \frac{1}{mN\mathfrak{p}^{ms}} = \frac{1}{n(\nu)} \sum_{m=1}^{\infty} \sum_{\substack{\mathfrak{P} \text{ in } K_\nu \\ \deg\mathfrak{P}=1}} \frac{1}{mN\mathfrak{P}^{ms}} \leq \frac{1}{n(\nu)} \log\zeta(s, K_\nu/k_\nu).$$

https://doi.org/10.4153/CMB-1995-023-2 Published online by Cambridge University Press

Thus we have

$$\delta\big(s,(K_\nu)\big) = \frac{\sum_{m=1}^{\infty}\sum_{\mathfrak{p}\in M}(mN\mathfrak{p}^{ms})^{-1}}{\sum_{m=1}^{\infty}\sum_{\mathfrak{p}\in(K)}(mN\mathfrak{p}^{ms})^{-1}} \le \frac{1}{n(\nu)}\frac{\log\zeta(s,K_\nu/k_\nu)}{\log\zeta(s,K/k)}.$$

Since $M_n \supset M$ and $M_n \setminus M \subset \sum_{\nu>n}(K_\nu)$, it suffices to show that the series

$$\sum_\nu \frac{1}{n(\nu)}\left|\frac{\log\zeta(s,K_\nu/k_\nu)}{\log\zeta(s,K/k)}\right|$$

converges uniformly in $1 < s \le s_0$ for some s_0.

The zeta function for a function field of one variable over a finite field can be written as $\zeta(s,K/k) = Z(q^{-s},K/k)$, where

$$Z(t,K/k) = \frac{L(t,K/k)}{(1-t)(1-qt)};\ L(t,K/k) = \prod_{i=1}^{2g(K)}(1-\omega_i t), \quad |\omega_i| = q^{\frac{1}{2}}.$$

From this it follows that

$$\sum_\nu \frac{1}{n(\nu)}\left|\frac{\log\zeta(s,K_\nu/k_\nu)}{\log\zeta(s,K/k)}\right| = \sum_\nu \frac{1}{n(\nu)}\left|\frac{\log L(q^{-sc(\nu)},K_\nu/k_\nu)}{\log\zeta(s,K/k)}\right| + \sum_\nu \frac{1}{n(\nu)}\left|\frac{\log(1-q^{-sc(\nu)})(1-q^{(1-s)c(\nu)})}{\log\zeta(s,K/k)}\right|,$$

where $k_\nu(X)$ is a rational function field with coefficients in k_ν. It is easy to see that the quantity

$$\left|\frac{\log\zeta(s,k_\nu(X)/k)}{\log\zeta(s,K/k)}\right|$$

converges as $s \longrightarrow 1+0$. Thus, it follows from the condition (1) that the second term converges. To prove the convergence of the first term, we first observe that for $s > 1$

$$L(q^{-sc(\nu)},K_\nu/k_\nu) = \prod_{i=1}^{2g(K_\nu)}(1-\omega_i q^{-sc(\nu)}) \begin{cases} \le (1+q^{-\frac{sc(\nu)}{2}})^{2g(K_\nu)} < (1+q^{-\frac{c(\nu)}{2}})^{Cn(\nu)/c(\nu)} \\ \ge (1-q^{-\frac{sc(\nu)}{2}})^{2g(K_\nu)} > (1-q^{-\frac{c(\nu)}{2}})^{Cn(\nu)/c(\nu)}. \end{cases}$$

Here, we used the condition (3) to have the last inequality. Since

$$0 < \log(1+q^{-\frac{c(\nu)}{2}}) < q^{-\frac{c(\nu)}{2}}$$

and

$$0 < -\log(1-q^{-\frac{c(\nu)}{2}}) < \frac{q^{\frac{c(\nu)}{2}}}{q^{\frac{c(\nu)}{2}}-1}q^{-\frac{c(\nu)}{2}} < 4q^{-\frac{c(\nu)}{2}},$$

we have

$$|\log L(q^{-sc(\nu)},K_\nu/k_\nu)| < 4C\frac{n(\nu)}{c(\nu)}.$$

In the meantime, since $\zeta(s,K/k)$ has a pole at $s=1$, there exists a constant C' for any $s_0 > 1$ such that

$$0 < \frac{1}{\log\zeta(s,K/k)} < C' \quad \text{for } 1 < s \le s_0.$$

https://doi.org/10.4153/CMB-1995-023-2 Published online by Cambridge University Press

From all these we have

$$\left|\frac{1}{n(\nu)}\frac{\log L(q^{-sc(\nu)}, K_\nu)}{\log \zeta(s, K/k)}\right| < 4CC'\frac{1}{c(\nu)q^{\frac{c(\nu)}{2}}}.$$

The sum of the right hand side for all ν converges by the condition (2). This completes the proof of the theorem. ∎

3. **Elliptic curves over a function field.** Let E be an elliptic curve defined over K. Suppose that the j-invariant of E is non constant. Let K_m be the smallest Galois extension of K in which the m-torsion points are defined. We define $\mathcal{F} = \{K_\ell\}_{\ell:\text{prime},\ell\neq p}$. Note that the field K_p is is excluded because the p-torsion part of $E \bmod \mathfrak{p}$ is always cyclic. The group $E \bmod \mathfrak{p}$ is cyclic if and only if $\mathfrak{p}$ does not split completely in any of the fields in $L(\mathcal{F})$. In order to prove Theorem 1.1 we will show that the family $\mathcal{F}$ satisfies the conditions for Theorem 2.1.

PROOF OF THEOREM 1.1. Let j be an indeterminant variable. Consider an elliptic curve E_j defined over $\mathbf{F}_q(j)$ whose j-invariant coincides with j. Igusa [I] determined the Galois group and the ramification of the extension $\mathbf{F}_q(j)_\ell/\mathbf{F}_q(j)$. For simplicity, we assume $p \geq 5$. The proof for the cases $p = 2, 3$ is essentially the same. For details, see [I]. When $p \geq 5$, we have

$$\mathrm{Gal}\left(\bar{\mathbf{F}}_q(j)_\ell/\bar{\mathbf{F}}_q(j)\right) \cong \mathrm{SL}(2, \mathbf{Z}/\ell\mathbf{Z}),$$

where $\bar{\mathbf{F}}_q$ is the algebraic closure of $\mathbf{F}_q$. Also, the extension $\mathbf{F}_q(j)_\ell/\mathbf{F}_q(j)$ is tamely ramified.

Equating the indeterminant j and the j-invariant of E/K, we can regard K as an extension of $\mathbf{F}_q(j)$. Since K_ℓ is the compositum of K and $\mathbf{F}_q(j)_\ell$, we have

$$\begin{aligned} n(\ell) &= |\mathrm{Gal}(K_\ell/K)| \geq \left|\mathrm{Gal}\left(\mathbf{F}_q(j)_\ell/\mathbf{F}_q(j)\right)\right|/[K : \mathbf{F}_q(j)] \geq |\mathrm{SL}(2, \mathbf{Z}/\ell\mathbf{Z})|/[K : \mathbf{F}_q(j)] \\ &= \ell(\ell-1)(\ell+1)/[K : \mathbf{F}_q(j)]. \end{aligned}$$

This proves the condition (1).

Since the Weil pairing on the torsion group is equivariant with the Galois action, K_ℓ must contain the ℓth roots of unity. Thus, we have $c(\ell) = [k_\ell : k] \geq [k(\sqrt[\ell]{1}) : k]$, and the last quantity equals $\ell - 1$ for almost ℓ. This proves the condition (2).

Since $\mathbf{F}_q(j)_\ell/\mathbf{F}_q(j)$ is tamely ramified, so is K_ℓ/K. Hence, the condition (3) follows immediately from the Riemann-Hurwitz formula. This concludes the proof of Theorem 1.1. ∎

4. **A remark on the Lang-Trotter conjecture.** Let P be a K-rational point of E. P generates the group $\bar{E} \bmod \mathfrak{p}$ if and only if the Artin symbol $\left(\frac{K_\ell/K}{\mathfrak{p}}\right)$ does not belong to a certain set S_ℓ for all prime numbers ℓ (*cf.* [LT]). In order to answer the question

https://doi.org/10.4153/CMB-1995-023-2 Published online by Cambridge University Press

posed by Lang and Trotter, we have to generalize the formulation of Artin's problem in Section 2 even further.

Consider the family $\mathcal{F}\{(K_\nu, S_\nu)\}_{\nu\in\mathbf{N}}$, where K_ν is a Galois extension of K and S_ν is a union of conjugacy classes in $\mathrm{Gal}(K_\nu/K)$. Define K_I and S_I for $I = \{\nu_1, \ldots, \nu_r\}$ in an obvious way. Define $s(\nu)$ to be the number of elements in S_ν and $c(\nu)$ to be the same as in Section 2. Denote the Frobenius element of $\mathrm{Gal}(\bar{k}/k)$ by ϕ. Let $a(\nu)$ be a positive integer such that

$$\mathrm{res}_{k_\nu}\, \tau = \mathrm{res}_{k_\nu}\, \phi^{a(\nu)}$$

for every $\tau \in S_\nu$. With these notations, we can generalize our result in Section 2 as follows.

THEOREM 4.1. *Suppose that the following conditions hold for the family* $\mathcal{F} = \{(K_\nu, S_\nu)\}_{\nu\in\mathbf{N}}$.

(1) $\sum_{\nu=1}^{\infty} \frac{s(\nu)}{n(\nu)} < \infty$,

(2) $\sum_{\nu=1}^{\infty} \frac{s(\nu)}{c(\nu)q^{\frac{1}{2}a(\nu)}} < \infty$, *and*

(3) There exists a constant C *such that* $g(K_\nu) \leq C\frac{n(\nu)}{c(\nu)}$ *for all* ν.

Let M *be the set of prime ideals in* K *such that the Artin symbol* $\left(\frac{K_\nu/K}{\mathfrak{p}}\right)$ *does not belong to* S_ν *for all* ν. *Then the Dirichlet density of* M *exists and given by*

$$\delta(M) = \sum_I \frac{\mu(I)|S_I|}{[K_I : K]}.$$

If we take $S_\nu = \{\mathrm{id}\}$, we recover our original result. In that case we have $a(\nu) = c(\nu)$. Unfortunately, in our present situation, S_ν contains enough elements to reduce $a(\nu)$ to 1 (*cf.* [LT]). Thus we can not prove the condition (2). Fried and Jarden [FJ] give a slightly better error estimate for the Čebotarev density theorem, but their estimate still depends on $a(\nu)$. Hence, at the present time, we are not able to prove the existence of the density.

REFERENCES

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

[CP] D. A. Cox and W. P. Parry, *Representations associated with elliptic surfaces*, Pacific J Math. **114**(1984), 309–323.

[FJ] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, Heidelberg, 1986.

[GM1] R. Gupta and M. R. Murty, *Primitive points on elliptic curves*, Compositio Math. **58**(1986), 13–44.

[GM2] ———, *Cyclicity and generation of points* mod *p on elliptic curves*, Invent. Math. **101** (1990), 225–235.

[Ho] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225**(1967), 197–218.

[I] J. Igusa, *Fiber system of Jacobian varieties III*, Amer. J. Math. **81**(1959), 453–476.

[LT] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83**(1977), 289–292.

[M] M. R. Murty, *On Artin's conjecture*, J. Number Theory **16**(1983), 147–168.

[S1] J.-P. Serre, *Abelian l-adic Representation and Elliptic Curves*, Benjamin, New York, 1968.

[S2] ———, *Resumé des cours de l'année scolaire 1976-1977.*

[Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
[W] A. Weil, *Sur les Courbes Algébriques et Variétés qui s'en Déduisent*, Hermann, Paris, 1948.

Department of Mathematics and Statistics
McGill University
805 Sherbrooke St. West
Montréal, Québec
H3A 2K6

Current address:
Department of Mathematics
Brigham Young University
Provo, Utah 84602
U.S.A.
e-mail: clark@math.byu.edu

Department of Mathematics and Statistics
McGill University
805 Sherbrooke St. West
Montréal, Québec
H3A 2K6

Current address:
Département de Mathématiques
Université de Caen
Esplanade de la Paix
14032 Caen cedex
France
e-mail: kuwata@math.unicaen.fr