Accepted Manuscript

The distribution and density of cyclic groups of the reductions of an elliptic curve over a function field

Márton Erdélyi

PII: S0022-314X(17)30023-9
DOI: http://dx.doi.org/10.1016/j.jnt.2016.11.025
Reference: YJNTH 5648

To appear in: *Journal of Number Theory*

Received date: 30 September 2016
Revised date: 2 November 2016
Accepted date: 4 November 2016

Please cite this article in press as: M. Erdélyi, The distribution and density of cyclic groups of the reductions of an elliptic curve over a function field, *J. Number Theory* (2017), http://dx.doi.org/10.1016/j.jnt.2016.11.025

The distribution and density of cyclic groups of the reductions of an elliptic curve over a function field

Márton Erdélyi *

Abstract

Let K be a global field of finite characteristic $p \geq 2$, and let E/K be a non-isotrivial elliptic curve. We give an asympotoic formula of the number of places ν for which the reduction of E at ν is a cyclic group. Moreover we determine when the Dirichlet density of those places is 0.

Keywords: Elliptic curves; Function fields of positive characteristics; Prime distributions, Chebotarev density theorem; Group structures; Wild ramification.

1 Statement of results

Let K be a global field of characteristic p and genus g_K, and let $k = \mathbb{F}_q \subset K$ $(q = p^f)$ be the algebraic closure of $\mathbb{F}_p$ in K. We denote by V_K the set of places of K. For $\nu \in V_K$, we denote by k_ν the residue field of K at ν, and by $\deg(\nu) := [k_\nu : \mathbb{F}_q]$ the degree of ν. Let $\overline{k}$ be an algebraic closure of k. Denote $\phi : (x \mapsto x^q) \in \mathrm{Gal}(\overline{k}/k)$ the q-Frobenius. Let $k_r|k$ be the unique degree r extension in $\overline{k}$.

Let E/K be an elliptic curve over K with j-invariant $j_E \notin k$, which we shall standardly call non-isotrivial. We denote by $V_{E/K}$ the set of places of K for which the reduction E_ν/k_ν is smooth and $|\overline{V}_{E/K}| = \sum_{\nu \notin V_{E/K}} \deg(\nu)$. For $n \in \mathbb{N} \setminus \{0\}$ let $V_{E/K}(n) = \{\nu \in V_{E/K} | \deg(\nu) = n\}$.

From the theory of elliptic curves we know that for $\nu \in V_{E/K}$, $E_\nu(k_\nu) \simeq \mathbb{Z}/d_\nu\mathbb{Z} \times \mathbb{Z}/d_\nu e_\nu\mathbb{Z}$ for nonzero integers d_ν, e_ν, uniquely determined by E and ν. We call the integers d_ν and $d_\nu e_\nu$ the elementary divisors of E_ν.

The goal of this paper is to extend the results of [CT] about the distribution of the places $\nu \in V_{E/K}$ for which $E_\nu(k_\nu)$ is a cyclic group. Such questions have been investigated for the reductions of an elliptic curve defined over $\mathbb{Q}$ (e.g. in [BaSh], [Co1], [Co2], [CoMu], [GuMu], [Mu1], [Mu2], [Se2]), mainly in relation with the elliptic curve analogue of Artin's primitive root conjecture formulated by Lang and Trotter in [LaTr]. This latter conjecture was investigated in the function field setting E/K by Clark and Kuwata [ClKu], and by Hall and Voloch [HaVo] (see also Voloch's work on constant curves [Vo1], [Vo2]). In [ClKu], a particular emphasis was placed on the study of the cyclicity of $E_\nu(k_\nu)$. Recently Cojacaru, Toth and Voloch [CTV] established distribution results also for the question of places with reductions of square-free orders (which is a more strict condition, than cyclicity).

In this paper we obtain an explicit asymptotic formula for the number of places $\nu \in V_{E/K}$, of fixed degree, for which $E_\nu(k_\nu)$ is cyclic. Our result is a direct extension of the work of [CT] which worked in finite characteristic $p > 3$.

Theorem 1. *Let E/K be a non-isotrivial elliptic curve. For all $\varepsilon > 0$ there exists $c = c(K, E, \varepsilon)$ such that for all $n \in \mathbb{N}$ we have*

$$\left| \# \left(\nu \in V_{E/K}(n) | E_\nu(k_\nu) \text{ is cyclic} \right) - \delta(E/K, 1, n) \frac{q^n}{n} \right| \leq c \frac{q^{n/2+\varepsilon}}{n},$$

where

$$\delta(E/K, 1, n) = \sum_{m | q^n - 1} \frac{\mu(m) \mathrm{ord}_m(q)}{|K(E[m]) : K|},$$

a μ is the Moebius function and $\mathrm{ord}_m(q)$ *denotes the multiplicative order of q modulo m for $m \in \mathbb{N}$, $(m, q) = 1$.*

*Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences (MTA)
Reáltanoda u. 13-15, H-1053 Budapest, Hungary
merdelyi@freestart.hu