ISSN 0012-9593

quatrième série - tome 49 *fascicule 5* *septembre-octobre 2016*

ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

Byungchul CHA & Daniel FIORILLI & Florent JOUVE

Prime number races for elliptic curves over function fields

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Annales Scientifiques de l'École Normale Supérieure

Publiées avec le concours du Centre National de la Recherche Scientifique

Rédaction / *Editor*

Annales Scientifiques de l'École Normale Supérieure,
45, rue d'Ulm, 75230 Paris Cedex 05, France.
Tél. : (33) 1 44 32 20 88. Fax : (33) 1 44 32 20 80.
annales@ens.fr

Édition / *Publication*

Société Mathématique de France
Institut Henri Poincaré
11, rue Pierre et Marie Curie
75231 Paris Cedex 05
Tél. : (33) 01 44 27 67 99
Fax : (33) 01 40 46 90 96

Abonnements / *Subscriptions*

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 09
Fax : (33) 04 91 41 17 51
email : smf@smf.univ-mrs.fr

Tarifs

Europe : 519 €. Hors Europe : 548 €. Vente au numéro : 77 €.

ISSN 0012-9593

Directeur de la publication : Stéphane Seuret
Périodicité : 6 nos / an

Ann. Scient. Éc. Norm. Sup.
4ᵉ série, t. 49, 2016, p. 1239 à 1277

PRIME NUMBER RACES FOR ELLIPTIC CURVES OVER FUNCTION FIELDS

BY BYUNGCHUL CHA, DANIEL FIORILLI AND FLORENT JOUVE

ABSTRACT. – We study the prime number race for elliptic curves over the function field of a proper, smooth and geometrically connected curve over a finite field. This constitutes a function field analogue of prior work by Mazur, Sarnak and the second author. In this geometric setting, we can prove unconditional results whose counterparts in the number field case are conditional on a Riemann Hypothesis and a linear independence hypothesis on the zeros of the implied L-functions. Notably we show that in certain natural families of elliptic curves, the bias generically dissipates as the conductor grows. This is achieved by proving a central limit theorem and combining it with generic linear independence results that will appear in a separate paper. Also we study in detail a particular family of elliptic curves that have been considered by Ulmer. In contrast to the generic case we show that the race exhibits very diverse outcomes, some of which are believed to be impossible in the number field setting. Such behaviors are possible in the function field case because the zeros of Hasse-Weil L-functions for those elliptic curves can be proven to be highly dependent among themselves, which is a very non generic situation.

RÉSUMÉ. – Nous étudions une version du biais de Chebyshev pour les courbes elliptiques sur le corps de fonctions d'une courbe lisse, propre, et géométriquement irréductible. Il s'agit de l'analogue, dans le cas des corps de fonctions, de travaux de Mazur, Sarnak, et Fiorilli. Le cadre géométrique dans lequel on se place permet d'établir inconditionnellement des résultats qui, sur les corps de nombres, nécessitent de supposer l'hypothèse de Riemann ou la conjecture de simplicité généralisée pour les zéros des fonctions L intervenant. On démontre notamment que, dans certaines familles naturelles de courbes elliptiques, il y a dissipation générique du biais lorsque le conducteur tend vers l'infini. La preuve s'appuie sur des résultats d'indépendance linéaire de zéros de fonctions L qui font l'objet d'un autre article des mêmes auteurs. Nous étudions par ailleurs la famille de courbes elliptiques d'Ulmer, et nous montrons qu'elle se comporte de manière pathologique, comparée au cas générique. Divers biais sont mis en évidence pour cette famille, dont certains sont conjecturalement impossibles à réaliser dans le cas des corps de nombres.

1. Introduction and statement of the main results

1.1. Background

It was first noticed by Chebyshev that primes are biased in their distribution modulo 4, in that there seems to be more primes of the form $4n+3$ than of the form $4n+1$ in initial intervals of the integers. A number of papers have been written on this phenomenon and its generalizations, and it is now known that such a bias appears in many number theoretical contexts, such as primes in arithmetic progressions, Frobenius elements in conjugacy classes of the Galois group of extensions of number fields, Fourier coefficients of modular forms, prime polynomials in residue classes over $\mathbb{F}_q(t)$, and so on.

In their seminal paper [18], Rubinstein and Sarnak have given a framework to study questions of this type. One of the features of their work is the quantification of the so-called *Chebyshev bias* in terms of an associated measure which is expressed using an explicit formula as a function of the nontrivial zeros of the involved L-functions.

In the case of Chebyshev's original question, Rubinstein and Sarnak determined that the logarithmic density [(1)] of the set of x for which $\pi(x;4,3) > \pi(x;4,1)$ exists and is given by $\delta(4;3,1) \approx 0.9959$. (Here, $\pi(x;q,a)$ is the count of primes $\leq x$ that are congruent to a modulo q.) Their results are conditional on the Generalized Riemann Hypothesis (GRH), and on the assumption (the Linear Independence hypothesis, or LI in short) that the multiset of (the ordinates of) all nontrivial zeros of the involved L-functions is linearly independent over $\mathbb{Q}$. One might think that the modulus 4 is not exceptional here, and that there should exist other moduli q and residue classes a and b modulo q such that $\delta(q;a,b)$, the logarithmic density of the set of $x \geq 1$ for which $\pi(x;q,a) > \pi(x;q,b)$, is also very close to 1. It turns out that as Rubinstein and Sarnak have shown, $\delta(q;a,b)$ approaches $\frac{1}{2}$ as $q \to \infty$, hence races of large moduli are very moderately biased. One can also quantify the rate of convergence here, showing for example as in [11] that whenever $\delta(q;a,b) \neq \frac{1}{2}$, we have $|\delta(q;a,b) - 1/2| = q^{-\frac{1}{2}+o(1)}$.

In the recent paper [10], the second author considered the more general race between two subsets A and B of the invertible reduced residues modulo q. It turns out that when studying the inequality $\pi(x;q,A) > \pi(x;q,B)$ with

$$\pi(x;q,A) := \sum_{a \in A} \pi(x;q,a),$$

things can become dramatically different from the previous case where only two residue classes were involved. Indeed, one can show under GRH and a multiplicity assumption on the zeros of $L(s,\chi)$ that there exist sequences of moduli $\{q_k\}$ and subsets $\{A_k\}$ and $\{B_k\}$ such that the associated lower and upper densities $\underline{\delta}(q_k;A_k,B_k)$ get arbitrarily close to 1. (Note also that it is known $\overline{\delta}(q;A,B) < 1$ for any q, A, B.) In other words, there exist 'highly biased prime number races'. Under the additional assumption that LI holds, it is also proven that in order to obtain highly biased prime number races, the moduli q_k need to have many prime factors, and hence highly biased prime number races are very rare. Most races are very moderately biased, in the sense that $\delta(q;A,B)$ is usually very close to $\frac{1}{2}$.

[(1)] The logarithmic density of a set $S \subset \mathbb{N}$ is defined by $\delta(S) := \lim_{N\to\infty} \frac{1}{\log N} \sum_{\substack{n \leq N \\ n \in S}} \frac{1}{n}$, if this limit exists.

In the context of elliptic curves, Mazur [16] introduced the race between the primes for which $a_p(E)$, the trace of the Frobenius at a prime p, is positive, against those for which $a_p(E)$ is negative. Sarnak's framework [(2)] in [19] to study this question turned out to be very effective, and explained this race very well in terms of the zeros (and potential poles) of $L(\mathrm{Sym}^n E, s)$, the symmetric power L-functions attached to E, conditional on a Riemann Hypothesis and LI. Sarnak also remarked that one can study a related race by focusing on the sign of the summatory function of $a_p(E)/\sqrt{p}$ using the zeros of $L(E,s)$ alone. For this race, Sarnak uncovered the influence of the analytic rank of E on the bias.

Building on Sarnak's work, the second author studied in [9] the following question: is it possible to find highly biased prime number races in the context of elliptic curves over $\mathbb{Q}$, or are all races of this type only moderately biased? It turns out that conditionally on a Riemann Hypothesis and the assumption that the multiplicity of nonreal zeros of $L(E,s)$ is uniformly bounded (which is referred to as a bounded multiplicity assumption), the key to finding such races is to find curves E whose analytic rank is significantly larger than $\sqrt{\log N_E}$, where N_E is the conductor of E. Interestingly, the two existing conjectures (stated in [8] and [20]) on the growth of the rank of elliptic curves over $\mathbb{Q}$ both imply the existence of the aforementioned curves. Note also that elliptic curves of large rank are extremely rare. It is widely believed that 100% of the elliptic curves over $\mathbb{Q}$ have rank either 0 or 1, depending on the root number of $L(E,s)$. One can show, as is explained in [19], that the bias for such curves dissipates as $N_E \to \infty$. Hence, highly biased elliptic curve prime number races over $\mathbb{Q}$ are very rare.

Coming back to the original Chebyshev bias, but in the function field setting, the first author showed in [4] that the framework of Rubinstein and Sarnak can be replicated in the one-variable polynomial ring $\mathbb{F}_q[t]$ over a finite field $\mathbb{F}_q$ of q elements. One of the advantages in this setting is that much more is known about the (inverse) zeros of L-functions. First of all, the Riemann Hypothesis is known to be true in this context. Also, one can explicitly calculate the zeros of relevant L-functions in some specific cases and prove the function field version of LI (see the definition of Grand Simplicity Hypothesis in [4] and also Definition 4.1 below).

The goal of the current paper is to present an unconditional analysis of the Chebyshev bias for elliptic curves E over a function field K (in particular it can be seen as a partial 2-dimensional generalization of [4]). More precisely we study the sign of the summatory function of the (normalized) trace $a_v(E)/q^{\deg v/2}$ of the Frobenius at v, where v runs over the places of the function field of a smooth proper geometrically connected curve over a finite field $\mathbb{F}_q$. In Section 2 we present the analogue of the work of Sarnak [19] in our geometric setting; as in *loc. cit.*, our analysis is more general than what is needed to study bias phenomena in the distribution of the traces of Frobenius. Indeed it involves an arbitrary smooth function of the angles θ_v of the local Frobenius traces, and as such zeros of higher symmetric power L-functions come into play. Section 3 is devoted to the study of Chebyshev's bias for Ulmer's family of elliptic curves E_d over the rational function field $\mathbb{F}_q(t)$ given by the Weierstrass equation

$$E_d : y^2 + xy = x^3 - t^d.$$

[(2)] Granville independently worked out the link between these types of prime number races and the distribution of the zeros of Hasse-Weil L-functions, and explained it to the second author.