

quatrième série - tome 54 fascicule 5 septembre-octobre 2021

*ANNALES
SCIENTIFIQUES
de
L'ÉCOLE
NORMALE
SUPÉRIEURE*

Byungchul CHA & Daniel FIORILLI & Florent JOUVE

*Erratum: “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

Responsable du comité de rédaction / *Editor-in-chief*

YVES DE CORNULIER

Publication fondée en 1864 par Louis Pasteur

Continuée de 1872 à 1882 par H. SAINTE-CLAIRE DEVILLE
de 1883 à 1888 par H. DEBRAY
de 1889 à 1900 par C. HERMITE
de 1901 à 1917 par G. DARBOUX
de 1918 à 1941 par É. PICARD
de 1942 à 1967 par P. MONTEL

Comité de rédaction au 1^{er} octobre 2021

S. CANTAT G. GIACOMIN
G. CARRON D. HÄFNER
Y. CORNULIER D. HARARI
F. DÉGLISE C. IMBERT
A. DUCROS S. MOREL
B. FAYAD P. SHAN

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.
Email : annaes@ens.fr

Édition et abonnements / *Publication and subscriptions*

Société Mathématique de France
Case 916 - Luminy
13288 Marseille Cedex 09
Tél. : (33) 04 91 26 74 64. Fax : (33) 04 91 41 17 51
Email : abonnements@smf.emath.fr

Tarifs

Abonnement électronique : 437 euros.
Abonnement avec supplément papier :
Europe : 600 €. Hors Europe : 686 € (\$ 985). Vente au numéro : 77 €.

© 2021 Société Mathématique de France, Paris

En application de la loi du 1^{er} juillet 1992, il est interdit de reproduire, même partiellement, la présente publication sans l'autorisation de l'éditeur ou du Centre français d'exploitation du droit de copie (20, rue des Grands-Augustins, 75006 Paris).

All rights reserved. No part of this publication may be translated, reproduced, stored in a retrieval system or transmitted in any form or by any other means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the publisher.

ISSN 0012-9593 (print) 1873-2151 (electronic)

Directeur de la publication : Fabien Durand
Périodicité : 6 n^{os} / an

ERRATUM: “PRIME NUMBER RACES FOR ELLIPTIC CURVES OVER FUNCTION FIELDS”

BY BYUNGCHUL CHA, DANIEL FIORILLI AND FLORENT JOUVE

ABSTRACT. – The paper mentioned in the title contains a mistake in Proposition 3.1. The expression for the L -function of the elliptic curve $E/\mathbb{F}_q(t)$ is wrong by a small uniformly bounded number of linear factors in $\mathbb{Z}[T]$. In this note we fix the problem and its minor consequences on other results in the same paper.

RÉSUMÉ. – L'article auquel le titre fait référence contient une erreur dans la proposition 3.1. L'expression donnée pour la fonction L de la courbe elliptique $E/\mathbb{F}_q(t)$ diffère de la valeur correcte par un nombre uniformément borné de facteurs linéaires dans $\mathbb{Z}[T]$. Le but de cette note est de corriger cette erreur ainsi que les conséquences mineures qu'elle a entraînées sur d'autres résultats du même article.

1. The L -function of elliptic curves in Ulmer's family

First recall some notation used in [1, §3]. Let $\mathbb{F}_q(t)$ be the rational function field over a finite field \mathbb{F}_q of characteristic $p \geq 3$. Following [2], fix $d \in \mathbb{Z}_{>0}$ and define $E_d/\mathbb{F}_q(t)$ to be the elliptic curve over $\mathbb{F}_q(t)$ given by the Weierstrass equation

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

The following explicit description of the Hasse-Weil L -function of $E_d/\mathbb{F}_q(t)$ is essential to the analysis of Chebyshev's bias for Ulmer's family performed in [1]. This corrects the flawed expression for $L(E_d/\mathbb{F}_q(t), T)$ given in [1, Prop. 3.1].

PROPOSITION 1.1. – *Suppose that d divides $p^n + 1$ for some n , and let $L(E_d/\mathbb{F}_q(t), T)$ be the Hasse-Weil L -function of E_d over $\mathbb{F}_q(t)$. Then,*

$$(1) \quad L(E_d/\mathbb{F}_q(t), T) = (1 - qT)^{\epsilon_d} (1 + qT)^{n_d} \prod_{\substack{e|d \\ e \neq 6}} \left(1 - (qT)^{o_e(q)}\right)^{\phi(e)/o_e(q)}.$$

Here, $\phi(e) = \#(\mathbb{Z}/e\mathbb{Z})^*$ is the Euler-phi function and $o_e(q)$ is the (multiplicative) order of q in $(\mathbb{Z}/e\mathbb{Z})^*$. Further, ϵ_d and η_d are defined as

$$\epsilon_d := \begin{cases} 0 & \text{if } 2 \nmid d \text{ or } 4 \nmid q-1 \\ 1 & \text{if } 2 \mid d \text{ and } 4 \mid q-1 \end{cases} + \begin{cases} 0 & \text{if } 3 \nmid d \\ 1 & \text{if } 3 \mid d \text{ and } 3 \nmid q-1 \\ 2 & \text{if } 3 \mid d \text{ and } 3 \mid q-1; \end{cases}$$

$$\eta_d := \begin{cases} 0 & \text{if } 2 \nmid d \text{ or } 4 \mid q-1 \\ 1 & \text{if } 2 \mid d \text{ and } 4 \nmid q-1 \end{cases} + \begin{cases} 0 & \text{if } 3 \nmid d \text{ or } 3 \mid q-1 \\ 1 & \text{if } 3 \mid d \text{ and } 3 \nmid q-1. \end{cases}$$

Note that Proposition 1.1 only differs from its original version [1, Prop. 3.1] by the factor $(1+qT)^{\eta_d}$ appearing in (1). In particular the assumptions as well as the statement about the rank of $E_d/\mathbb{F}_q(t)$ in [1, Prop. 3.1] are unchanged.

Proof of Proposition 1.1. – We combine three arguments in order to obtain the expression stated in the proposition for $f_d(T) := L(E_d/\mathbb{F}_q(t), T)$ as an element of $\mathbb{Z}[T]$.

- (i) We first compute the degree of $f_d(T)$ using the conductor-degree formula.
- (ii) We use our knowledge of $\deg f_d(T)$ and the work of Ulmer ([2, Cor. 7.7, Prop. 8.1 and Th. 9.2]) to obtain the following factorization of $f_d(T)$ in $\mathbb{Z}[T]$:

$$f_d(T) = (1 - qT)^{\epsilon_d} g_d(T) P_2(T),$$

where P_2 is the product over divisors e of d not dividing 6 appearing in (1), and $g_d(T) \in \mathbb{Z}[T]$ has degree η_d .

- (iii) We use the geometric construction described in [2, §5] explaining that the difference between $P_2(T)$ and $f_d(T)$ is the result of blowing up some relevant quotient F_d/Γ of a Fermat surface at points that are either defined over \mathbb{F}_q or over a quadratic extension of \mathbb{F}_q (these points are cube roots or fourth roots of 1).

In the rest of the proof we let $k = \mathbb{F}_q$. For (i) we use [3, §3.1.7] and the reduction data [2, §2] for $E_d/k(T)$ to deduce that

$$\deg f_d = -4 + \left(1 + d + \begin{cases} 0 & \text{if } 6 \mid d \\ 2 & \text{if } 6 \nmid d \end{cases} \right),$$

where the first summand -4 on the right-hand side comes from the fact that the base curve is \mathbb{P}^1/k and the three remaining summands correspond to the contributions of the bad reduction places above t , $1 - 2^4 3^3 t^d$, ∞ , respectively. Overall

$$(2) \quad \deg f_d = \begin{cases} d - 3 & \text{if } 6 \mid d, \\ d - 1 & \text{if } 6 \nmid d. \end{cases}$$

As expected, the geometric invariant $\deg f_d$ does not depend on k , but only on d .

Step (ii) merely consists in extracting information from Ulmer's work [2]. Since we assume that $d \mid p^n + 1$ for some n , we deduce from [2, Cor. 7.7, Prop. 8.1] that $L(E/k, T)$ is divisible in $\mathbb{Z}[T]$ by

$$P_2(T) := \prod_{\substack{e \mid d \\ e \nmid 6}} \left(1 - (qT)^{o_e(q)} \right)^{\phi(e)/o_e(q)}.$$

Note that this factor depends a priori on q since making a field extension k'/k will result in replacing q by $|k'|$ each time it occurs in the expression for P_2 . Moreover, invoking [2, Th. 9.2], we obtain an extra factor (a power of $1-qT$) for $L(E/k(t), T)$ so that overall we deduce that in $\mathbb{Z}[T]$, the polynomial f_d is a multiple of

$$(3) \quad h_d(T) := (1 - qT)^{\epsilon_d} \prod_{\substack{e|d \\ e \neq 6}} \left(1 - (qT)^{o_e(q)}\right)^{\phi(e)/o_e(q)}.$$

Again note that ϵ_d depends on d and on k ; precisely its value is affected by the presence of cube roots or fourth roots of 1 in k . In particular as soon as we work over a field extension k'/k containing the cube and fourth roots of 1, the parameter ϵ_d becomes independent of any further base extension.

Let $g_d := \frac{f_d}{h_d} \in \mathbb{Z}[T]$ and let $\eta_d = \deg g_d$. From (2) and (3) we deduce the formula for η_d stated in the proposition. In particular, the expression for η_d shows that $g_d = 1$ when k contains both the groups of cube roots and fourth roots of 1, and that in any case $\eta_d = \deg g_d \leq 2$.

We finally turn to (iii). From [4, (6.3)] we know precisely how the zeta function of \mathcal{E}_d relates to $L(E_d/k(T), T)$ (here the notation is as in [2, §3]: \mathcal{E}_d/k is the elliptic surface which is regular, proper and relatively minimal when seen as fibered over \mathbb{P}^1 , and which has generic fiber $E_d/k(T)$). Also \mathcal{E}_d is constructed (see [2, §5]) from some quotient F_d/Γ of the diagonal Fermat surface F_d/k by a sequence of blow-ups at k -points of μ_3 and μ_4 (the groups of cube roots and fourth roots of 1 in \bar{k} , respectively), as explained in [2, §5.6].

By [2, Cor. 7.7] the polynomial P_2 is the characteristic polynomial of the Frobenius acting on the middle étale cohomology of F_d/Γ . The “missing” factor g_d thus comes as the arithmetic translation of the sequence of blow-ups leading from F_d/Γ to \mathcal{E}_d . Let x_0 be a k' -rational point of F_d/Γ which is blown up in the process of constructing \mathcal{E}_d . As already mentioned, x_0 corresponds to an element of $\mu_3 \cup \mu_4$ seen as a subset of \bar{k} . In particular, k' either equals k or is a quadratic extension of k . In any case we can choose k' to be a quadratic extension of k such that x_0 is defined over k' . Then if $Y \rightarrow F_d/\Gamma$ is the result of blowing up x_0 we have by “multiplicativity of zeta functions” that

$$Z(Y/k', T) = \frac{Z((F_d/\Gamma)/k', T)}{1 - q^2 T}.$$

(Here we use the standard fact asserting that if X/k is a variety and if Y is a closed subvariety of X , then $Z(X, T) = Z(Y, T) \cdot Z(U, T)$ where U is the complement $U := X \setminus Y$. This is readily obtained from the definition of the zeta function of a variety over a finite field as an exponential generating series.) Also one has the following base change formula:

$$Z(Y/k', T^2) = Z(Y/k, T) \times Z(Y/k, -T).$$

(Again this is a standard fact obtained by coming back to the definition of the zeta function of a variety over a finite field X/k and by exploiting elementary properties of r -th roots of 1 in \mathbb{C} , to show that if k_r/k is an extension of degree r , then one has $Z(X \times_k \text{Spec } k_r, T^r) = \prod_{i=1}^r Z(X, \xi^i T)$, where $\xi \in \mathbb{C}$ is a primitive r -th root of 1.) Combining these facts on zeta