ERRATUM: "PRIME NUMBER RACES FOR ELLIPTIC CURVES OVER FUNCTION FIELDS"

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.

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

$$E_d \colon y^2 + xy = x^3 - t^d \,.$$

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,*

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

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

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

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

The statement about the rank of $E_d/\mathbb{F}_q(t)$ in [1, Prop. 3.1] is 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 $t, 1-2^4 3^3 t^d, \infty$, respectively. Overall,

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

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

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

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 $L(E/k(T),T)$ (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 $E/k(T)$). 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 $\overline{k}$, 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 $Y \to F_d/\Gamma$ is the result of blowing up x_0 we have by "multiplicativity of zeta functions"

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

(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 $Z(X\times_k \operatorname{Spec} k_r, T^r) = \prod_{i=1}^r Z(X,\xi^i T)$, where $\xi\in\mathbb{C}$ is a primitive r-th root of 1.) Combining theses facts on zeta functions, we deduce that

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

One possibly has to iterate the above process several times (depending on the number of blow-ups that are necessary to construct $\mathcal{E}_d$ from F_d/Γ). However each time a point is blown up, the zeta function for the resulting variety only differs from that of the initial variety by a factor $1-qT$ or $1+qT$. Of course a factor $1-qT$ affects the rank of $E_d/k(T)$, but the rank is known by [2, Th. 9.2]. We deduce that g_d has to be a power of the polynomial $1+qT$ and that the exponent is necessarily η_d by (ii) above.

□

We deduce the following corrected version of [1, Prop. 3.2].

Proposition 1.2. *Let $c_\pm(X)$ be defined by*

$$c_\pm(X) := \begin{cases} q/(q-1) & \text{for even } X,\\ \sqrt{q}/(q-1) & \text{for odd } X.\end{cases}$$

Then

$$T_d(X) = -c_{\pm}(X) + \frac{\epsilon_d}{1-q^{-\frac{1}{2}}} + \frac{\eta_d \mathrm{e}^{\mathrm{i}\pi X}}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e\mid d\\ e\nmid 6}} \phi(e) \frac{q^{-(X \bmod o_e(q))/2}}{1-q^{-o_e(q)/2}} + o_{X\to\infty}(1) \tag{4}$$

for X large enough, where $0 \le (X \bmod \ell) \le \ell - 1$ is the remainder in the Euclidean division of X by ℓ.

Proof. We combine [1, Cor. 2.10] and Proposition 1.1 to obtain that

$$T_d(X) = -c_{\pm}(X) + \frac{\epsilon_d}{1-q^{-\frac{1}{2}}} + \frac{\eta_d \mathrm{e}^{\mathrm{i}\pi X}}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e\mid d\\ e\nmid 6}} \frac{\phi(e)}{o_e(q)} \sum_{k=0}^{o_e(q)-1} \frac{\mathrm{e}^{2\pi \mathrm{i} k X/o_e(q)}}{1-q^{-\frac{1}{2}}\mathrm{e}^{-2\pi \mathrm{i} k/o_e(q)}} + o_{X\to\infty}(1)\,. \tag{5}$$

The end of the proof of [1, Prop. 3.2] remains valid. □

The definition of the "periodic part" of $T_d(X)$ has to be corrected accordingly. We set (compare with [1, (44)])

$$T_d^{\mathrm{per}}(X) := -c_{\pm}(X) + \frac{\epsilon_d}{1-q^{-\frac{1}{2}}} + \frac{\eta_d \mathrm{e}^{\mathrm{i}\pi X}}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e\mid d\\ e\nmid 6}} \phi(e) \frac{q^{-(X \bmod o_e(q))/2}}{1-q^{-o_e(q)/2}}.$$

The statement of [1, Cor. 3.4] remains valid (in the proof, one has to replace the flawed expression for $T_d(X)$ by (4) but this has no impact on the statement of [1, Cor. 3.4] since $\eta_d \ge 0$).

2. Corrected versions of [1, Th. 1.5] and of some related statements

The fact that the expression for $T_d(X)$ was incorrect in [1] has consequences on some of the results of [1] on Chebyshev's bias in Ulmer's family $(E_d/\mathbb{F}_q(t))$. In this section we state and prove the following corrected version of [1, Th. 1.5].

Theorem 2.1. *For the family $\{E_d/\mathbb{F}_q(t)\}$ (where we recall that the integer d and the characteristic p of $\mathbb{F}_q$ are linked by the relation $d \mid p^n + 1$ for some $n \ge 1$), one has the following cases of extreme bias.*

(i) *Suppose that $3 \mid d$ and $3 \mid q-1$ and that either d is odd or $4 \mid q-1$. Then, $T_d(X) > 0$ for all large enough X, and thus $\underline{\delta}(E_d) = \overline{\delta}(E_d) = 1$.*

(ii) *If $q = p^k$ with p large enough and $d = p^n + 1$ for some $1 \le n \le \mathrm{e}^{q^{\frac{1}{2}}/6}$ with $n \equiv 0 \bmod k$, then $T_d(X) > 0$ for all large enough X, and thus $\underline{\delta}(E_d) = \overline{\delta}(E_d) = 1$.*

(iii) *Fix $\epsilon > 0$. There exists primes $d \ge 3$ and p such that p is a primitive root modulo d, and such that if we pick $q = p^{\frac{d+1}{2}}$, then the associated curve E_d has analytic rank 1 (resp. 2) if $(d-1)/2$ is even (resp. odd) and*

$$0 < \underline{\delta}(E_d) \le \overline{\delta}(E_d) < \epsilon\,.$$

Note that the statement (iii) is unchanged, compared with [1, Th. 1.5(iii)], but since its proof has to be amended, we chose, for completeness, to give a full corrected statement for [1, Th. 1.5].

Proof of Theorem 2.1(i). If d and q satisfy the stated assumptions, then $\epsilon_d \in \{2,3\}$ and $\eta_d = 0$. Then, the statement easily follows because

$$\begin{aligned} -c_{\pm}(X) + \frac{\epsilon_d}{1-q^{-\frac{1}{2}}} + \frac{\eta_d \mathrm{e}^{\mathrm{i}\pi X}}{1+q^{-\frac{1}{2}}} &\geq -\frac{1}{1-q^{-1}} + \frac{\epsilon_d}{1-q^{-\frac{1}{2}}} - \frac{\eta_d}{1+q^{-\frac{1}{2}}} \\ &= \frac{-1+\epsilon_d - \eta_d + q^{-\frac{1}{2}}(\epsilon_d+\eta_d)}{1-q^{-1}} > 0, \end{aligned}$$

thus using Proposition 1.2 we see that $T_d(X) > 0$ for all large enough X. □

Proof of Theorem 2.1(ii). By Proposition 1.2 and by positivity, we have that (recall that p is large enough, and therefore so is d)

$$\begin{aligned} T_d(X) &= -c_{\pm}(X) + \frac{\epsilon_d}{1-q^{-\frac{1}{2}}} + \frac{\eta_d \mathrm{e}^{\mathrm{i}\pi X}}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e \mid d \\ e \nmid 6}} \phi(e) \frac{q^{-(X \bmod o_e(q))/2}}{1-q^{-o_e(q)/2}} + o_{X\to\infty}(1) \\ &\geq \phi(d) q^{-(X \bmod o_d(q))/2} - 1 - \eta_d + o_{p\to\infty}(1) + o_{X\to\infty}(1) \\ &\geq \phi(d) q^{-(o_d(q)-1)/2} - 3 + o_{p\to\infty}(1) + o_{X\to\infty}(1). \end{aligned}$$

However, we have that $q^{2n/k} \equiv 1 \bmod d$, that is $o_d(q) \mid 2n/k$. We conclude that

$$\begin{aligned} T_d(X) &\geq \phi(d) q^{\frac{1}{2}} q^{-\frac{n}{k}} - 3 + o_{p\to\infty}(1) + o_{X\to\infty}(1) \\ &= \phi(d) q^{\frac{1}{2}} (d-1)^{-1} - 3 + o_{p\to\infty}(1) + o_{X\to\infty}(1). \end{aligned}$$

This quantity is positive for large enough X since, for d large enough, we have that $\phi(d)/(d-1) \geq (\mathrm{e}^{-\gamma} + o(1))/\log\log d$ and the condition on n implies that $\log\log(p^n+1) \leq q^{\frac{1}{2}}/6 + \log\log p + 1$. Since $6\exp(-\gamma) > 3$ the proof is complete.

□

The proof of [1, Th. 1.5(iii)] uses [1, Prop. 3.5] which remains valid although parts of its proof require some corrections that we now explain.

Proof of Proposition 3.5 *in* [1]. The argument given in [1] to prove [1, Prop. 3.5(i)] remains valid since the hypotheses on the parameters imply that $\eta_d = 0$.

We turn to the proof of [1, Prop. 3.5(ii)]. The hypotheses imply $\varepsilon_d = 0$ and $\eta_d = 1$. Thus, by Proposition 1.2, one has that

$$T_d(X) = -c_{\pm}(X) + \frac{\mathrm{e}^{\mathrm{i}\pi X}}{1+q^{-\frac{1}{2}}} + \phi(\ell) \frac{q^{-(X \bmod o_\ell(q))/2}}{1-q^{-o_\ell(q)/2}} + \phi(2\ell) \frac{q^{-(X \bmod o_{2\ell}(q))/2}}{1-q^{-o_{2\ell}(q)/2}} + o_{X\to\infty}(1).$$

We have $q^n \equiv (-p^{-1})^n \equiv -1 \bmod d$. We claim that n is the least positive integer such that this congruence holds. Indeed this minimality condition holds by definition for the congruence $p^n \equiv -1 \bmod d$. Now $q \equiv -p^{-1} \bmod d$ and n is even, thus the claim follows. Since q is odd, the property $\ell \mid q^k - 1$ is equivalent to $2\ell \mid q^k - 1$, for all $k \in \mathbb{Z}_{\geq 1}$. In particular we have $o_d(q) = o_{2\ell}(q) = o_\ell(q) = 2n$. Now, let j be an integer such that $4 \leq j \leq 2n-1$. We have that

$$\phi(\ell) \frac{q^{-(j \bmod o_\ell(q))/2}}{1-q^{-o_\ell(q)/2}} + \phi(2\ell) \frac{q^{-(j \bmod o_{2\ell}(q))/2}}{1-q^{-o_{2\ell}(q)/2}} \ll \ell q^{-4/2} \ll p^{n-2(n-1)} = p^{2-n}.$$

If j is odd, we have that $c_\pm(j) \gg q^{-\frac{1}{2}} = p^{(1-n)/2}$ and $\mathrm{e}^{\mathrm{i}\pi j} = -1$. We deduce that for p and X large enough we have $T_d(X) < 0$ (recall $n \geq 4$) as soon as $X \equiv j \bmod 2n$. If j is even, we have that

$$T_d(X) = -c_\pm(j) + \frac{1}{1+q^{-\frac{1}{2}}} + O(p^{2-n}) + o_{X\to\infty}(1) = -\frac{p^{-(n-1)/2}}{1-q^{-1}} + O(p^{2-n}) + o_{X\to\infty}(1).$$

which is < 0 for large enough p and X. Hence

$$0 \leq \underline{\delta}(E_d) \leq \overline{\delta}(E_d) \leq \frac{2}{n}.$$

As for the lower bound, it is given by [1, Cor. 3.4]. □

Proof of Theorem 2.1(iii). This is a direct consequence of [1, Prop. 3.5(i)] and [1, Cor. 3.7] (the argument given in the proof of [1, Th. 1.5(iii)] can be applied without modifications). □

3. Corrected version of [1, Th. 1.7] and of some related results

The corrected version of [1, Th. 1.7] is the following statement.

Theorem 3.1. *For the family $\{E_d/\mathbb{F}_q(t)\}$, one has the following cases where $T_d(X)$ is completely unbiased. Fix $p \equiv 3 \bmod 4$ and let $d \geq 5$ be an* odd *divisor of p^2+1. Pick $q = p^{4k+1}$ with $k \geq 1$. Then the analytic rank of E_d is $(d-1)/4$ and we have*

$$\underline{\delta}(E_d) = \overline{\delta}(E_d) = \frac{1}{2}.$$

The proof of [1, Th. 1.7] uses [1, Prop. 3.8], which remains valid although the proof requires some corrections that we now explain.

Proof of Proposition 3.8 in [1]. Under the stated assumptions $q \equiv p \bmod 4$ thus $4 \nmid q-1$ and of course $2 \mid d$. Also since n is even, $3 \nmid d$. We deduce $\epsilon_d = 0$ and $\eta_d = 1$ and, from (4), we obtain the formula

$$T_d(X) = -c_\pm(X) + \frac{\mathrm{e}^{\mathrm{i}\pi X}}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e\mid d\\ e\nmid 6}} \phi(e) \frac{q^{-(X \bmod o_e(q))/2}}{1-q^{-o_e(q)/2}} + o_{X\to\infty}(1).$$

As in [1, Prop. 3.8], one shows that, for each $e \mid d$ with $e \nmid 6$, we have that $o_e(q) \geq 3$.

Using this fact, we have that if $X \equiv 3 \bmod 2n$ (recall $n \geq 2$ so that 3 is an admissible remainder for the Euclidean division by $2n$), then

$$T_d(X) = -c_\pm(X) - \frac{1}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e\mid d\\ e\nmid 6}} \phi(e) \frac{q^{-3/2}}{1-q^{-o_e(q)/2}} + o_{X\to\infty}(1).$$

This last quantity is negative for large enough $X \equiv 3 \bmod 2n$. Indeed $(1+q^{-\frac{1}{2}})^{-1} = 1 + o_{p\to\infty}(1)$, and since X is odd we have $c_\pm(X) = o_{p\to\infty}(1)$. Also,

$$\sum_{\substack{e\mid d\\ e\nmid 6}} \phi(e) \frac{q^{-3/2}}{1-q^{-o_e(q)/2}} \ll q^{-\frac{3}{2}} d \ll p^{n-3(kn+1)/2} \ll p^{-\frac{5}{2}},$$

which is $o_{p\to\infty}(1)$. We conclude by invoking [1, Cor. 3.4].

□

Proof of Theorem 3.1. We argue as in [1, Proof of Th. 1.7] to see that $\epsilon_d = 0$. Moreover, since we assume d is odd and $d \mid p^2+1 \equiv 2 \bmod 3$, we have $\eta_d = 0$ and $d \equiv 1 \mod 4$ (indeed d is an odd divisor of a sum of two coprime squares). Note also that if $e \mid d$ with $e \notin \{1,2\}$ (*i.e.* $e \neq 1$ since d is odd), then $q^2 \equiv p^2 \equiv -1 \bmod e$, hence $o_e(q) = 4$. The rank of E_d is then easily computed with the help of Proposition [1, Prop. 3.1]. Moreover, we deduce from (4) that

$$T_d(X) = -c_\pm(X) + \sum_{\substack{e|d \\ e\neq 1}} \phi(e) \frac{q^{-(X \bmod 4)/2}}{1-q^{-2}} + o_{X\to\infty}(1),$$

hence $T_d^{\mathrm{per}}(X)$ is 4-periodic.

If $X \equiv 0 \bmod 4$, then

$$T_d(X) = -\frac{q}{q-1} + \sum_{\substack{e|d \\ e\neq 1}} \frac{\phi(e)}{1-q^{-2}} + o_{X\to\infty}(1) \geq -2 + \frac{d-1}{1-q^{-2}} + o_{X\to\infty}(1),$$

which is positive for X large enough.

If $X \equiv 1 \bmod 4$, then

$$T_d(X) = -\frac{q^{\frac12}}{q-1} + \sum_{\substack{e|d \\ e\neq 1}} \frac{\phi(e) q^{-\frac12}}{1-q^{-2}} + o_{X\to\infty}(1) = q^{-\frac12}\left(\frac{d-2-q^{-1}}{1-q^{-2}}\right) + o_{X\to\infty}(1),$$

which is again positive for X large enough.

The analysis of the cases $X \equiv 2, 3 \bmod 4$ is unchanged compared with [1, Proof of Th. 1.7], except for ther index set in the sums $\sum_{e|d, e\neq 1,2}$ which have to be replaced by $\sum_{e|d,e\neq 1}$. □

Remark 3.2. In [1, Th. 1.7], the constraint "d odd" does not appear. However taking into account the correcting factor $(1+qT)^{\eta_d}$ in the expression for $L(E_d/\mathbb{F}_q(t), T)$ (in Proposition 1.1) we now see that this is a necessary restriction. Let us investigate the changes to the above proof implied in case d is *even*. Since $3 \nmid d$ and $4 \nmid q-1$ we still have $\epsilon_d = 0$; however if d is even, we have $\eta_d = 1$. The argument according to which any divisor $e \neq 1, 2$ of d satisfies $o_e(q) = 4$ is still valid and thus Proposition 1.2 gives

$$T_d(X) = -c_\pm(X) + \frac{(-1)^X}{1+q^{-\frac12}} + \sum_{\substack{e|d \\ e\neq 1,2}} \phi(e) \frac{q^{-(X \bmod 4)/2}}{1-q^{-2}} + o_{X\to\infty}(1),$$

hence with notation as before $T_d^{\mathrm{per}}(X)$ is again 4-periodic.

The formula for the rank in [1, Prop. 3.1] provides the explicit value $(d-2)/4$ for the analytic rank of $E_d/\mathbb{F}_q(t)$ (note that d is an even divisor of p^2+1 and thus $d \equiv 2 \mod 4$).

Let us determine the sign of $T_d(X)$ depending on $X \bmod 4$. If $X \equiv 0 \bmod 4$, then

$$T_d(X) = -\frac{q}{q-1} + \frac{1}{1+q^{-\frac12}} + \sum_{\substack{e|d \\ e\neq 1,2}} \frac{\phi(e)}{1-q^{-2}} + o_{X\to\infty}(1) \geq -2 + \frac{1}{1+q^{-\frac12}} + \frac{d-2}{1-q^{-2}} + o_{X\to\infty}(1),$$

which is positive for X large enough.

Likewise for $X \equiv 3 \bmod 4$ the contribution is negative in case d is odd (as seen in the proof above). For even d the factor $(1+qT)^{\eta_d}$ of the L-function produces an extra negative contribution:

$$T_d(X) = -\frac{q^{\frac{1}{2}}}{q-1} - \frac{1}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e|d \\ e\neq 1,2}} \frac{\phi(e) q^{-\frac{3}{2}}}{1-q^{-2}} + o_{X\to\infty}(1)$$

thus $T_d(X)$ is *a fortiori* negative for X large enough.

For $X \equiv 2 \bmod 4$, the contribution remains negative. Indeed we have that

$$T_d(X) = -\frac{q}{q-1} + \frac{1}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e|d \\ e\neq 1,2}} \frac{\phi(e) q^{-1}}{1-q^{-2}} + o_{X\to\infty}(1) = -\frac{q^{-\frac{1}{2}}}{1-q^{-1}} + \frac{(d-2)q^{-1}}{1-q^{-2}} + o_{X\to\infty}(1)$$

$$= \frac{-q^{-\frac{1}{2}} + (d-2)q^{-1} - q^{-\frac{3}{2}}}{1-q^{-2}} + o_{X\to\infty}(1),$$

which is negative for X large enough since $(d-2)q^{-\frac{1}{2}} \leq p^{2-2k-\frac{1}{2}} \leq p^{-\frac{1}{2}}$.

Finally if $X \equiv 1 \bmod 4$, the contribution is negative (contrary to the case d odd). Indeed we have that

$$T_d(X) = -\frac{q^{\frac{1}{2}}}{q-1} - \frac{1}{1+q^{-\frac{1}{2}}} + \sum_{\substack{e|d \\ e\neq 1,2}} \frac{\phi(e) q^{-\frac{1}{2}}}{1-q^{-2}} + o_{X\to\infty}(1)$$

$$= \frac{-1}{1-q^{-1}} + \frac{q^{-\frac{1}{2}}(d-2)}{1-q^{-2}} + o_{X\to\infty}(1) = \frac{-1-q^{-1}+q^{-\frac{1}{2}}(d-2)}{1-q^{-2}} + o_{X\to\infty}(1)\,.$$

As seen above $(d-2)q^{-\frac{1}{2}} \leq p^{-\frac{1}{2}}$ and thus $T_d(X)$ is negative for large enough X.

As a conclusion, we obtain that under the assumptions of Theorem 3.1 but fixing this time an *even* divisor d of p^2+1, we have $\delta(E_d) = 1/4$.

4. Corrected proof of [1, Th. 1.8] and of some related results

The statement of [1, Th. 1.8] remains valid, however its proof relies on [1, Prop. 3.10], that statement of which remains valid as well, although its proof requires some fixing. We now explain the details.

Proof of Proposition 3.10 *in* [1]. We first see that the hypotheses on the parameters imply that $\epsilon_d = \eta_d = 0$. Indeed, as in [1, Proof of Prop. 3.10] we show that $d \equiv n \equiv 1 \bmod 2$ and that $d \equiv n \bmod 3$. Since n is prime, we deduce that $(6,d) = 1$ as soon as $n > 3$. Now if $n = 3$, the assumption $3 \nmid p+1$ and the fact that $p^3+1 \equiv p+1 \bmod 3$ imply that $d \equiv 1 \bmod 3$ and again we conclude $(6,d) = 1$. Therefore under the assumptions stated in [1, Prop. 3.10], we have $\epsilon_d = \eta_d = 0$.

The rest of the proof of [1, Prop. 3.10] is unchanged.

□

The way [1, Th. 1.8] is deduced from [1, Prop. 3.10] is unchanged.

Acknowledgements. We thank Richard Griffon for helpful discussions that led to the correct computation (1) of the L-function of Ulmer's elliptic curve $E_d/\mathbb{F}_q(t)$.

References

[1] B. Cha, D. Fiorilli, and F. Jouve, *Prime number races for elliptic curves over function fields*, Ann. Sci. Éc. Norm. Supér. (4) **49** (2016), no. 5, 1239–1277.

[2] D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) **155** (2002), no. 1, 295–315.

[3] ———, *Geometric non-vanishing*, Invent. Math. **159** (2005), no. 1, 133–186.

[4] ———, *Elliptic curves over function fields*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280.

Department of Mathematics and Computer Science, Muhlenberg College, 2400 Chew st., Allentown, PA 18104, USA

E-mail address: cha@muhlenberg.edu

Universit Paris-Saclay, CNRS, Laboratoire de mathmatiques d'Orsay, 91405, Orsay, France.

Département de mathématiques et de statistique, Université d'Ottawa, 150 Louis Pasteur pvt, Ottawa, Ontario, K1N 6N5, Canada

E-mail address: daniel.fiorilli@universite-paris-saclay.fr

Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France.

E-mail address: florent.jouve@math.u-bordeaux.fr