Bull. Aust. Math. Soc. **89** (2014), 19–32
doi:10.1017/S0004972712001116

ON THE MERTENS CONJECTURE FOR ELLIPTIC CURVES OVER FINITE FIELDS

PETER HUMPHRIES

(Received 4 October 2012; accepted 23 October 2012; first published online 28 February 2013)

Abstract

We introduce an analogue of the Mertens conjecture for elliptic curves over finite fields. Using a result of Waterhouse, we classify the isogeny classes of elliptic curves for which this conjecture holds in terms of the size of the finite field and the trace of the Frobenius endomorphism acting on the curve.

2010 *Mathematics subject classification*: primary 11N56; secondary 11G20.

Keywords and phrases: Mertens conjecture, elliptic curve, finite field, function field.

1. The Mertens conjecture

Let $\mu(n)$ denote the Möbius function, so that for a positive integer n,

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^t & \text{if } n \text{ is the product of } t \text{ distinct primes,} \\ 0 & \text{if } n \text{ is divisible by a perfect square.} \end{cases}$$

The Mertens conjecture states that the summatory function of the Möbius function,

$$M(x) = \sum_{n \leq x} \mu(n),$$

satisfies the inequality

$$|M(x)| \leq \sqrt{x} \tag{1.1}$$

for all $x \geq 1$. This conjecture stems from the work of Mertens [8], who in 1897 calculated $M(x)$ from $x = 1$ up to $x = 10\,000$ and arrived at the conjecture (1.1). Notably, this conjecture implies that all of the nontrivial zeroes of the Riemann zeta function $\zeta(s)$ lie on the line $\mathrm{Re}(s) = 1/2$ (that is, that the Riemann hypothesis is true), and also that all such zeroes are simple.

However, Ingham [6] showed in 1942 that a consequence of the Mertens conjecture is that the imaginary parts of the zeroes of $\zeta(s)$ in the upper half-plane must be

This research was partially supported by an Australian Postgraduate Award.

linearly dependent over the rational numbers, a relation that seems unlikely; while there is yet to be found strong theoretical evidence for the falsity of such a linear dependence, some limited numerical calculations have failed to find any such linear relations [1, 2]. Using methods closely related to the work of Ingham, Odlyzko and te Riele [9] disproved the Mertens conjecture in 1984, and in fact showed that

$$\limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}} > 1.06,$$
$$\liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}} < -1.009.$$

These bounds have since been improved to 1.218 and −1.229 respectively by Kotnik and te Riele [7], and most recently to 1.6383 and −1.6383 respectively by Best and Trudgian [2]. It seems likely that

$$\limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}} = \infty,$$
$$\liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}} = -\infty,$$

and, from the work of Ingham [6], this is known to follow from the assumption of the Riemann hypothesis and the linear independence over the rational numbers of the imaginary parts of the zeroes of $\zeta(s)$ in the upper half-plane.

2. The Mertens conjecture for curves over finite fields

A natural variant of this problem is to formulate an analogue of the Mertens conjecture in the setting of global function fields, that is, for nonsingular projective curves over finite fields. The advantage of this function field setting, as opposed to the classical case, is that the Riemann hypothesis is proved, and the associated zeta functions have only finitely many zeroes. Indeed, when the curve is simply the projective line $\mathbb{P}^1$, so that the associated function field is $\mathbb{F}_q(t)$, the Mertens conjecture is true for trivial reasons, as in this case the summatory function of the Möbius function is bounded in absolute value by q; see [3, p. 5]. In this paper, we study the Mertens conjecture in the next-most simple case, namely when the genus of the curve is one, that is to say, the case of elliptic curves over finite fields. Our main result is Theorem 2.1, where we state that it is indeed possible for certain elliptic curves to satisfy a formulation of the Mertens conjecture, and we classify which curves satisfy this conjecture in terms of the size of the finite field q and the trace of the Frobenius endomorphism acting on the elliptic curve.

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. For an effective divisor N of E, we define the Möbius function of $E/\mathbb{F}_q$ to be

$$\mu_{E/\mathbb{F}_q}(N) = \begin{cases} 1 & \text{if } N \text{ is the zero divisor,} \\ (-1)^t & \text{if } N \text{ is the sum of } t \text{ distinct prime divisors of } E, \\ 0 & \text{if a prime divisor of } E \text{ divides } N \text{ with order at least two.} \end{cases}$$

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

We are interested in the behaviour of the summatory function of the Möbius function of $E/\mathbb{F}_q$,

$$M_{E/\mathbb{F}_q}(X) = \sum_{0 \leq \deg(N) \leq X-1} \mu_{E/\mathbb{F}_q}(N),$$

where X is a positive integer. We wish to determine the validity of the following conjecture.

The Mertens Conjecture for Elliptic Curves over Finite Fields. *Let E be an elliptic curve over $\mathbb{F}_q$, and let $M_{E/\mathbb{F}_q}(X)$ be the summatory function of the Möbius function of $E/\mathbb{F}_q$. Then, for all sufficiently large positive integers X,*

$$\left|M_{E/\mathbb{F}_q}(X)\right| \leq q^{X/2}.$$

Note that in the definition of $M_{E/\mathbb{F}_q}(X)$, we are summing over effective divisors N of E for which $0 \leq \deg(N) \leq X - 1$, as opposed to the classical case, where $M(x)$ is a sum over positive integers n for which $1 \leq n \leq x$. It is also noteworthy that the classical form of the Mertens conjecture states that $|M(x)| \leq \sqrt{x}$, whereas our function field version instead states that $|M_{E/\mathbb{F}_q}(X)| \leq q^{X/2}$. The reason that q^X replaces x is due to the fact that the absolute norm of an effective divisor N of E is $q^{\deg(N)}$, whereas the absolute norm of a positive integer n is merely n itself.

Our main result is the following theorem.

Theorem 2.1. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. Then the Mertens conjecture for $E/\mathbb{F}_q$ is true if and only if the order of the finite field q and the trace a of the Frobenius endomorphism acting on E over $\mathbb{F}_q$ satisfy precisely one of the following conditions:*

(1) *$q = p^m$ with $a = 2$, where either m is arbitrary and $p \neq 2$, or $m = 1$ and $p = 2$;*
(2) *$q = p^m$ with $a = \sqrt{q}$, where m is even and $p \not\equiv 1 \pmod 3$;*
(3) *$q = p^m$ with $a = 0$, where either m is even and $p \not\equiv 1 \pmod 4$, or m is odd.*

In all these cases, we have that

$$\left|M_{E/\mathbb{F}_q}(X)\right| \leq q^{X/2}$$

for all $X \geq 1$, and also that for every $\varepsilon > 0$, there exist infinitely many positive integers X, dependent on q and a, for which

$$\left|M_{E/\mathbb{F}_q}(X)\right| > (1 - \varepsilon)q^{X/2}.$$

In a related article [5], the author studies the Mertens conjecture for higher-genus curves C over finite fields $\mathbb{F}_q$. There is as yet no classification of isogeny classes for curves of a given genus g outside of Waterhouse's classification of elliptic curves [11], as well as the recent classification of Howe, Nart, and Ritzenthaler of curves of genus two [4], so it is no longer possible to determine directly the isogeny classes of curves for which the Mertens conjecture holds. Instead, the author studies the average number

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

of curves satisfying the Mertens conjecture in a particular family of curves over finite fields, and shows that for a curve C in the chosen family, we ought to expect that

$$\limsup_{X\to\infty} \frac{|M_{C/\mathbb{F}_q}(X)|}{q^{X/2}} > 1.$$

3. Explicit expressions for $M_{C/\mathbb{F}_q}(X)/q^{X/2}$

To study $M_{E/\mathbb{F}_q}(X)$, we must first introduce the zeta function of $E/\mathbb{F}_q$, $Z_{E/\mathbb{F}_q}(u)$. This is defined initially for a complex variable u in the open disc $|u| < q^{-1}$ via the absolutely convergent series

$$Z_{E/\mathbb{F}_q}(u) = \exp\biggl(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{u^n}{n}\biggr).$$

Equivalently, $Z_{E/\mathbb{F}_q}(u) = \zeta_{E/\mathbb{F}_q}(s)$ for $u = q^{-s}$, where

$$\zeta_{E/\mathbb{F}_q}(s) = \sum_{D\geq 0} \frac{1}{\mathcal{N}D^s}.$$

Here the sum is over all effective divisors D of E, and $\mathcal{N}D = q^{\deg(D)}$ denotes the absolute norm of D. This Dirichlet series is absolutely convergent for $\mathrm{Re}(s) > 1$, with an Euler product expansion

$$\zeta_{E/\mathbb{F}_q}(s) = \prod_P \frac{1}{1 - \mathcal{N}P^{-s}},$$

where the product is over all prime divisors P of E. This in turn implies that $Z_{E/\mathbb{F}_q}(u)$ is nonvanishing in the open disc $|u| < q^{-1}$. Much more than this is true: $Z_{E/\mathbb{F}_q}(u)$ extends meromorphically to the entire complex plane, satisfies a certain functional equation, and also a certain form of the Riemann hypothesis.

Theorem 3.1 (See [10, Theorems 5.9 and 5.10]). *Given an elliptic curve E over $\mathbb{F}_q$, there exists a quadratic polynomial $P_{E/\mathbb{F}_q}(u)$ such that for $|u| < q^{-1}$,*

$$Z_{E/\mathbb{F}_q}(u) = \frac{P_{E/\mathbb{F}_q}(u)}{(1-u)(1-qu)}. \tag{3.1}$$

This yields a meromorphic extension of $Z_{E/\mathbb{F}_q}(u)$ to the whole complex plane, with simple poles at $u = q^{-1}$ and $u = 1$. Furthermore, $Z_{E/\mathbb{F}_q}(u)$ satisfies the functional equation

$$Z_{E/\mathbb{F}_q}(u) = q^{g-1}u^{2(g-1)}Z_{E/\mathbb{F}_q}\Bigl(\frac{1}{qu}\Bigr).$$

Finally, the polynomial $P_{E/\mathbb{F}_q}(u)$ is of the form

$$P_{E/\mathbb{F}_q}(u) = 1 - au + qu^2,$$

with a an integer satisfying $|a| \leq 2\sqrt{q}$, so that $a = 2\sqrt{q}\cos\theta$ for some $0 \leq \theta \leq \pi$.

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

The polynomial $P_{E/\mathbb{F}_q}(u) = 1 - au + qu^2$ factorises over $\mathbb{C}$ as

$$P_{E/\mathbb{F}_q}(u) = (1 - \gamma_1 u)(1 - \gamma_2 u)$$

for some complex numbers γ_1, γ_2 with $\gamma_1 = \overline{\gamma_2}$; we call these the inverse zeroes of $\zeta_{E/\mathbb{F}_q}(s)$. Without loss of generality, we may assume that $\mathrm{Im}(\gamma_1) \geq 0$. As $\gamma_1 + \overline{\gamma_1} = a$ and $\gamma_1\overline{\gamma_1} = q$, we have that

$$\gamma_1 = \sqrt{q}e^{i\theta},$$
$$\gamma_2 = \sqrt{q}e^{-i\theta},$$

where

$$\theta = \arccos\left(\frac{a}{2\sqrt{q}}\right). \tag{3.2}$$

Geometrically, the integer a is the trace of the Frobenius endomorphism acting on the elliptic curve E over $\mathbb{F}_q$; the angle θ is called the Frobenius angle of $E/\mathbb{F}_q$. Notably, there are several restrictions on the possible values that a may take. The following lemma fully characterises the possible values of a.

Lemma 3.2 (Waterhouse [11, Theorem 4.1]). *Let a be an integer. Then a is the trace of the Frobenius endomorphism acting on some elliptic curve E over a finite field $\mathbb{F}_q$ of characteristic p if and only if one of the following conditions is satisfied:*

(1) $a \not\equiv 0 \pmod{p}$ *and* $|a| < 2\sqrt{q}$; *for such an integer a, the associated Frobenius angle θ is such that θ/π is irrational;*

(2) (i) $q = p^m$ *with* $a = 2\sqrt{q}$, *where m is even, so that* $\theta = 0$;

(2) (ii) $q = p^m$ *with* $a = -2\sqrt{q}$, *where m is even, so that* $\theta = \pi$;

(3) (i) $q = p^m$ *with* $a = \sqrt{q}$, *where m is even and* $p \not\equiv 1 \pmod{3}$, *so that* $\theta = \pi/3$;

(3) (ii) $q = p^m$ *with* $a = -\sqrt{q}$, *where m is even and* $p \not\equiv 1 \pmod{3}$, *so that* $\theta = 2\pi/3$;

(4) (i) $q = 2^m$ *with* $a = \sqrt{2q}$, *where m is odd, so that* $\theta = \pi/4$;

(4) (ii) $q = 2^m$ *with* $a = -\sqrt{2q}$, *where m is odd, so that* $\theta = 3\pi/4$;

(4) (iii) $q = 3^m$ *with* $a = \sqrt{3q}$, *where m is odd, so that* $\theta = \pi/6$;

(4) (iv) $q = 3^m$ *with* $a = -\sqrt{3q}$, *where m is odd, so that* $\theta = 5\pi/6$;

(5) $q = p^m$ *with* $a = 0$, *where either m is even and* $p \not\equiv 1 \pmod{4}$, *or m is odd, so that* $\theta = \pi/2$.

That is, there is a bijective correspondence between the isogeny classes of elliptic curves over $\mathbb{F}_q$ and the values of the integer a given in the above conditions.

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

The method of proof of Theorem 2.1 involves determining an explicit expression for $M_{E/\mathbb{F}_q}(X)$ in terms of a and q by first studying the Dirichlet series

$$\sum_{D\geq 0} \frac{\mu_{E/\mathbb{F}_q}(D)}{\mathcal{N}D^s}. \tag{3.3}$$

This has previously been done for arbitrary nonsingular projective curves over finite fields by Cha [3], who uses the resulting expression to study the average size of the quantity

$$\limsup_{X\to\infty} \frac{|M_{C/\mathbb{F}_q}(X)|}{q^{X/2}}$$

when averaged over a particular family of curves C, in the limit as the size of the finite field $\mathbb{F}_q$ tends to infinity. Our results are similar and follow the same method, but by restricting ourselves to the case of curves of genus one, we are able to determine exact formulas, while we also have the advantage of using the classification in Lemma 3.2 of the possible values of the trace of the Frobenius endomorphism.

To begin, we note that the Möbius function of $E/\mathbb{F}_q$ is multiplicative and satisfies $\mu_{E/\mathbb{F}_q}(P) = -1$ and $\mu_{E/\mathbb{F}_q}(P^t) = 0$ whenever $t \geq 2$ for any prime divisor P of E, and so the Dirichlet series (3.3) has the Euler product

$$\sum_{D\geq 0} \frac{\mu_{E/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \prod_P (1 - \mathcal{N}P^{-s})$$

for $\mathrm{Re}(s) > 1$, which, upon comparing Euler products, yields the identity

$$\sum_{D\geq 0} \frac{\mu_{E/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \frac{1}{\zeta_{E/\mathbb{F}_q}(s)}, \tag{3.4}$$

which is valid for all $\mathrm{Re}(s) > 1$. On the other hand,

$$\sum_{D\geq 0} \frac{\mu_{E/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \sum_{D\geq 0} \frac{\mu_{E/\mathbb{F}_q}(D)}{q^{\deg(D)s}} = \sum_{N=0}^{\infty} \frac{1}{q^{Ns}} \sum_{\deg(D)=N} \mu_{E/\mathbb{F}_q}(D). \tag{3.5}$$

So determining an expression for the coefficients of the Dirichlet series for $1/\zeta_{E/\mathbb{F}_q}(s)$ using the known factorisation (3.1) of $\zeta_{E/\mathbb{F}_q}(s)$ and then comparing coefficients will lead us to a precise formula for $M_{E/\mathbb{F}_q}(X)$.

Lemma 3.3 (See Cha [3, Proposition 2.2]). *For each $N \geq 0$ and any $T > 0$,*

$$\frac{1}{2\pi i} \oint_{C_T} \frac{1}{u^{N+1}} \frac{1}{Z_{E/\mathbb{F}_q}(u)}\, du = \sum_{\deg(D)=N} \mu_{E/\mathbb{F}_q}(D) + \sum_{\gamma} \operatorname*{Res}_{u=\gamma^{-1}} \frac{1}{u^{N+1}} \frac{1}{Z_{E/\mathbb{F}_q}(u)}, \tag{3.6}$$

where the sum is over the inverse zeroes γ of $Z_{E/\mathbb{F}_q}(u)$, counted without multiplicity, and $C_T = \{z \in \mathbb{C} : |z| = q^T\}$. Furthermore, the left-hand side of (3.6) vanishes for $N \geq 1$.

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

Proof. This is essentially proved in [3, Proposition 2.2] in more generality; the chief difference here is the use of a varying contour. Consider the contour integral

$$\frac{1}{2\pi i}\oint_{C_T}\frac{1}{u^{N+1}}\frac{1}{Z_{E/\mathbb{F}_q}(u)}\,du, \tag{3.7}$$

where $C_T = \{z \in \mathbb{C} : |z| = q^T\}$. We can write $1/Z_{E/\mathbb{F}_q}(u)$ in two ways; via (3.1), and via (3.4) and (3.5), yielding the identities

$$\frac{1}{Z_{E/\mathbb{F}_q}(u)} = \frac{(1-u)(1-qu)}{(1-\gamma_1 u)\,(1-\gamma_2 u)}, \tag{3.8}$$

$$\frac{1}{Z_{E/\mathbb{F}_q}(u)} = \sum_{N=0}^{\infty} u^N \sum_{\deg(D)=N} \mu_{E/\mathbb{F}_q}(D), \tag{3.9}$$

where the first identity is valid for all $u \in \mathbb{C} \setminus \{\gamma_1^{-1}, \gamma_2^{-1}\}$, and the second identity is valid for all $|u| < q^{-1}$. So the singularities of the integrand of (3.7) in the interior of the closed curve C_T occur at $u = 0$ and at $u = \gamma^{-1}$ for each zero γ^{-1} of $Z_{E/\mathbb{F}_q}(u)$. At the singularity $u = 0$, we have by (3.9) that

$$\operatorname*{Res}_{u=0} \frac{1}{u^{N+1}}\frac{1}{Z_{E/\mathbb{F}_q}(u)} = \sum_{\deg(D)=N} \mu_{E/\mathbb{F}_q}(D).$$

The identity (3.6) now follows by Cauchy's residue theorem. Now (3.8) and the fact that $|u| = q^T$ and $|\gamma_1| = |\gamma_2| = \sqrt{q}$ imply that

$$\begin{aligned}\left|\frac{1}{2\pi i}\oint_{C_T}\frac{1}{u^{N+1}}\frac{1}{Z_{E/\mathbb{F}_q}(u)}\,du\right| &\le \frac{1}{2\pi}\oint_{C_T}\left|\frac{1}{u^{N+1}}\frac{1}{Z_{E/\mathbb{F}_q}(u)}\right|\,|du| \\ &\le \frac{\left(q^T+1\right)\left(q^{1+T}+1\right)}{(q^{1/2+T}-1)^2}q^{-NT}.\end{aligned}$$

As the right-hand side of (3.6) is independent of T, we may take the limit as T tends to infinity in order to find that the contour integral above is zero if $N \ge 1$. □

We are now able to determine an explicit expression for $M_{E/\mathbb{F}_q}(X)/q^{X/2}$. We must consider two cases: when $Z_{E/\mathbb{F}_q}(u)$ has only simple zeroes, and when $Z_{E/\mathbb{F}_q}(u)$ has a zero of order two. For the first case, we have the following result.

Proposition 3.4. *Let E be an elliptic curve over $\mathbb{F}_q$, and suppose that $Z_{E/\mathbb{F}_q}(u)$ has only simple zeroes. Then*

$$\frac{M_{E/\mathbb{F}_q}(X)}{q^{X/2}} = 2\sqrt{\frac{q+1-a}{4q-a^2}}\cos(\omega + X\theta), \tag{3.10}$$

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

where a is the trace of the Frobenius endomorphism, the Frobenius angle $\theta \in [0, \pi]$ is given by (3.2), and $\omega \in (-\pi/2, \pi/2)$ is given by

$$\omega = \arctan\left(\frac{a-2}{\sqrt{4q-a^2}}\right).$$

We remark that (3.10) is equivalent to

$$\frac{M_{E/\mathbb{F}_q}(X)}{q^{X/2}} = \cos(X\theta) - \frac{a-2}{\sqrt{4q-a^2}}\sin(X\theta) \tag{3.11}$$

via the cosine angle-sum formula.

Proof. We write γ for γ_1 and $\overline{\gamma}$ for γ_2. The fact that $Z_{E/\mathbb{F}_q}(u)$ has only simple zeroes is equivalent to $\gamma \neq \overline{\gamma}$, and hence that $a \neq \pm 2\sqrt{q}$, and consequently

$$\begin{aligned}\operatorname*{Res}_{u=\gamma^{-1}} \frac{1}{u^{N+1}}\frac{1}{Z_{E/\mathbb{F}_q}(u)} &= \lim_{u\to\gamma^{-1}}\left(u-\gamma^{-1}\right)\frac{1}{u^{N+1}}\frac{(1-u)(1-qu)}{(1-\gamma u)(1-\overline{\gamma}u)}\\ &= -\gamma^N\frac{(\gamma-1)(\overline{\gamma}-1)}{\overline{\gamma}-\gamma}.\end{aligned}$$

Similarly,

$$\operatorname*{Res}_{u=\overline{\gamma}^{-1}} \frac{1}{u^{N+1}}\frac{1}{Z_{E/\mathbb{F}_q}(u)} = \overline{\gamma}^N\frac{(\gamma-1)(\overline{\gamma}-1)}{\overline{\gamma}-\gamma}.$$

It follows that when $N = 0$, the left-hand side of (3.6) is equal to 1, as the sum over the inverse zeroes $\gamma, \overline{\gamma}$ on the right-hand side of (3.6) vanishes when $N = 0$, whereas

$$\sum_{\deg(D)=0} \mu_{E/\mathbb{F}_q}(D) = 1,$$

as the only effective divisor of E of degree zero is the zero divisor. Thus,

$$\sum_{\deg(D)=N} \mu_{E/\mathbb{F}_q}(D) = \frac{(\gamma-1)(\overline{\gamma}-1)}{\overline{\gamma}-\gamma}\left(\gamma^N-\overline{\gamma}^N\right) + \begin{cases}1 & \text{if } N=0,\\ 0 & \text{otherwise.}\end{cases}$$

Summing this expression from $N = 0$ to $N = X - 1$ and evaluating the resulting geometric series,

$$M_{E/\mathbb{F}_q}(X) = \frac{\overline{\gamma}-1}{\overline{\gamma}-\gamma}\gamma^X + \frac{\gamma-1}{\gamma-\overline{\gamma}}\overline{\gamma}^X,$$

and hence

$$\frac{M_{E/\mathbb{F}_q}(X)}{q^{X/2}} = 2\mathrm{Re}\left(\frac{\overline{\gamma}-1}{\overline{\gamma}-\gamma}e^{iX\theta}\right) = \frac{\sqrt{q+1-2\sqrt{q}\cos\theta}}{\sqrt{q}\sin\theta}\cos(\omega+X\theta),$$

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

where

$$\omega = \arctan\left(\frac{\sqrt{q}\cos\theta - 1}{\sqrt{q}\sin\theta}\right),$$

and we have used the fact that $\gamma = \sqrt{q}e^{i\theta}$. We complete the proof by noting that

$$2\sqrt{q}\sin\theta = \sqrt{4q - a^2}$$

as $a = 2\sqrt{q}\cos\theta$ with $0 \le \theta \le \pi$. □

We also have the following analogous result in the case where $Z_{E/\mathbb{F}_q}(u)$ has a zero of multiple order.

Proposition 3.5. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p, and suppose that $Z_{E/\mathbb{F}_q}(u)$ has zeroes of multiple order, so that $q = p^m$ with $a = \pm 2\sqrt{q}$, where m is even. Then*

$$\frac{M_{E/\mathbb{F}_q}(X)}{q^{X/2}} = -(\pm 1)^X\left(1 \mp \frac{1}{\sqrt{q}}\right)X + (\pm 1)^X. \tag{3.12}$$

Proof. If $a = \pm 2\sqrt{q}$, then $\gamma = \overline{\gamma} = \pm\sqrt{q}$. Now

$$\begin{aligned}\operatorname*{Res}_{u=\pm q^{-1/2}} \frac{1}{u^{N+1}}\frac{1}{Z_{E/\mathbb{F}_q}(u)} &= \lim_{u\to\pm q^{-1/2}} \frac{d}{du}\frac{(u \mp q^{-1/2})^2}{u^{N+1}}\frac{(1-u)(1-qu)}{(1\mp\sqrt{q}u)^2}\\ &= (\pm 1)^{N+1}(\sqrt{q}\mp 1)^2 N q^{(N-1)/2}.\end{aligned}$$

As this vanishes when $N = 0$, we must again have that

$$\frac{1}{2\pi i}\oint_{C_T}\frac{1}{u}\frac{1}{Z_{E/\mathbb{F}_q}(u)}\,du = 1$$

via (3.6), and consequently

$$\sum_{\deg(D)=N}\mu_{E/\mathbb{F}_q}(D) = -(\pm 1)^{N+1}(\sqrt{q}\mp 1)^2 N q^{(N-1)/2} + \begin{cases}1 & \text{if } N = 0,\\ 0 & \text{otherwise,}\end{cases}$$

which leads to the result upon summing over all $0 \le N \le X - 1$ and then dividing through by $q^{X/2}$. □

4. Proof of Theorem 2.1

Using Propositions 3.4 and 3.5, we are now able to determine the quantity

$$\limsup_{X\to\infty}\frac{|M_{E/\mathbb{F}_q}(X)|}{q^{X/2}}$$

for each elliptic curve E over a given finite field $\mathbb{F}_q$. We must consider each possible combination of values for q and a as determined in Lemma 3.2, which will culminate in a proof of Theorem 2.1.

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

(1) If $q = p^m$ with $a \not\equiv 0 \pmod{p}$ and $|a| < 2\sqrt{q}$, then by (3.10),

$$|M_{E/\mathbb{F}_q}(X)| \leq 2\sqrt{\frac{q+1-a}{4q-a^2}}q^{X/2}$$

for all $X \geq 1$. As the Frobenius angle θ is such that θ/π is irrational, the Weyl equidistribution theorem implies that $X\theta$ is equidistributed modulo π as X tends to infinity, and hence

$$\limsup_{X\to\infty} \frac{|M_{E/\mathbb{F}_q}(X)|}{q^{X/2}} = 2\sqrt{\frac{q+1-a}{4q-a^2}} = \sqrt{1 + \frac{(a-2)^2}{4q-a^2}}.$$

So the Mertens conjecture for $E/\mathbb{F}_q$ is true precisely when the inequality

$$\sqrt{1 + \frac{(a-2)^2}{4q-a^2}} \leq 1$$

holds, which can only occur when $a = 2$, provided that $p \neq 2$. Note that even in this case, we nevertheless have via the Weyl equidistribution theorem that for every $\varepsilon > 0$, there exist infinitely many values of X, dependent on q, for which

$$|M_{E/\mathbb{F}_q}(X)| > (1-\varepsilon)q^{X/2}.$$

(2) If $q = p^m$ with $a = \pm 2\sqrt{q}$, where m is even, then from (3.12),

$$\limsup_{X\to\infty} \frac{|M_{E/\mathbb{F}_q}(X)|}{q^{X/2}} = \infty.$$

(3) (i) If $q = p^m$ with $a = \sqrt{q}$, where m is even and $p \not\equiv 1 \pmod{3}$, we have from (3.11) that

$$\frac{M_{E/\mathbb{F}_q}(X)}{q^{X/2}} = \cos\left(\frac{\pi X}{3}\right) - \frac{\sqrt{3}}{3}\left(1 - \frac{2}{\sqrt{q}}\right)\sin\left(\frac{\pi X}{3}\right).$$

We calculate the six cases of $X \pmod{6}$:

$X \pmod{6}$	$M_{E/\mathbb{F}_q}(X)/q^{X/2}$
0	1
1	$1/\sqrt{q}$
2	$-1 + 1/\sqrt{q}$
3	-1
4	$-1/\sqrt{q}$
5	$1 - 1/\sqrt{q}$

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

So for all $X \geq 1$,

$$|M_{E/\mathbb{F}_q}(X)| \leq q^{X/2},$$

with equality occurring infinitely often.

(3) (ii) Similarly, if $q = p^m$ with $a = -\sqrt{q}$, where m is even and $p \not\equiv 1 \pmod 3$,

$$\frac{M_{E/\mathbb{F}_q}(X)}{q^{X/2}} = \cos\left(\frac{2\pi X}{3}\right) + \frac{\sqrt{3}}{3}\left(1 + \frac{2}{\sqrt{q}}\right)\sin\left(\frac{2\pi X}{3}\right).$$

The three cases of $X \pmod 3$ are

$X \pmod 3$	$M_{E/\mathbb{F}_q}(X)/q^{X/2}$
0	1
1	$1/\sqrt{q}$
2	$-1 - 1/\sqrt{q}$

This shows that

$$\limsup_{X\to\infty} \frac{\left|M_{E/\mathbb{F}_q}(X)\right|}{q^{X/2}} = 1 + \frac{1}{\sqrt{q}}.$$

(4) (i) If $q = 2^m$ with $a = \sqrt{2q}$, where m is odd, then

$$\frac{M_{E/\mathbb{F}_{2^m}}(X)}{2^{mX/2}} = \cos\left(\frac{\pi X}{4}\right) - \left(1 - \frac{1}{2^{(m-1)/2}}\right)\sin\left(\frac{\pi X}{4}\right).$$

We analyse the eight cases of $X \pmod 8$:

$X \pmod 8$	$M_{E/\mathbb{F}_{2^m}}(X)/2^{mX/2}$
0	1
1	$2^{-m/2}$
2	$-1 + 2^{-(m-1)/2}$
3	$-\sqrt{2} + 2^{-m/2}$
4	-1
5	$-2^{-m/2}$
6	$1 - 2^{-(m-1)/2}$
7	$\sqrt{2} - 2^{-m/2}$

So when $m = 1$, we have that

$$|M_{E/\mathbb{F}_2}(X)| \leq q^{X/2}$$

for all $X \geq 1$, with equality occurring infinitely often, while for $m \geq 3$,

$$\limsup_{X\to\infty} \frac{|M_{E/\mathbb{F}_{2^m}}(X)|}{2^{mX/2}} = \sqrt{2} - \frac{1}{2^{m/2}}.$$

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

(4) (ii) Likewise, if $q = 2^m$ with $a = -\sqrt{2q}$, where m is odd, then

$$\frac{M_{E/\mathbb{F}_{2^m}}(X)}{2^{mX/2}} = \cos\left(\frac{3\pi X}{4}\right) + \left(1 + \frac{1}{2^{(m-1)/2}}\right)\sin\left(\frac{3\pi X}{4}\right).$$

The table of values of $X \pmod 8$ is

$X \pmod 8$	$M_{E/\mathbb{F}_{2^m}}(X)/2^{mX/2}$
0	1
1	$2^{-m/2}$
2	$1 + 2^{-(m-1)/2}$
3	$\sqrt{2} + 2^{-m/2}$
4	-1
5	$-2^{-m/2}$
6	$-1 - 2^{-(m-1)/2}$
7	$-\sqrt{2} - 2^{-m/2}$

Thus,

$$\limsup_{X\to\infty} \frac{|M_{E/\mathbb{F}_{2^m}}(X)|}{2^{mX/2}} = \sqrt{2} + \frac{1}{2^{m/2}}.$$

(4) (iii) If $q = 3^m$ with $a = \sqrt{3q}$, where m is odd, then

$$\frac{M_{E/\mathbb{F}_{3^m}}(X)}{3^{mX/2}} = \cos\left(\frac{\pi X}{6}\right) - \left(1 - \frac{2}{3^{m/2}}\right)\sin\left(\frac{\pi X}{6}\right).$$

The 12 cases of $X \pmod{12}$ are

$X \pmod{12}$	$M_{E/\mathbb{F}_{3^m}}(X)/3^{mX/2}$
0	1
1	$(\sqrt{3} - 1)/2 + 3^{-m/2}$
2	$-(\sqrt{3} - 1)/2 + 3^{-(m-1)/2}$
3	$-1 + 2 \times 3^{-m/2}$
4	$-(\sqrt{3} + 1)/2 - 3^{-(m-1)/2}$
5	$-(\sqrt{3} + 1)/2 + 3^{-m/2}$
6	-1
7	$-(\sqrt{3} - 1)/2 - 3^{-m/2}$
8	$(\sqrt{3} - 1)/2 - 3^{-(m-1)/2}$
9	$1 - 2 \times 3^{-m/2}$
10	$(\sqrt{3} + 1)/2 + 3^{-(m-1)/2}$
11	$(\sqrt{3} + 1)/2 - 3^{-m/2}$

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

Consequently,

$$\limsup_{X\to\infty} \frac{|M_{E/\mathbb{F}_{3^m}}(X)|}{3^{mX/2}} = \frac{\sqrt{3}+1}{2} + \frac{1}{3^{(m-1)/2}}.$$

(4) (iv) Next, if $q = 3^m$ with $a = -\sqrt{3q}$, where m is odd, then

$$\frac{M_{E/\mathbb{F}_{3^m}}(X)}{3^{mX/2}} = \cos\Big(\frac{5\pi X}{6}\Big) + \Big(1 + \frac{2}{3^{m/2}}\Big)\sin\Big(\frac{5\pi X}{6}\Big).$$

Now we have the table

$X \pmod{12}$	$M_{E/\mathbb{F}_{3^m}}(X)/3^{mX/2}$
0	1
1	$-(\sqrt{3}-1)/2 + 3^{-m/2}$
2	$-(\sqrt{3}-1)/2 - 3^{-(m-1)/2}$
3	$1 + 2 \times 3^{-m/2}$
4	$-(\sqrt{3}+1)/2 - 3^{-(m-1)/2}$
5	$(\sqrt{3}+1)/2 - 3^{-m/2}$
6	-1
7	$(\sqrt{3}-1)/2 - 3^{-m/2}$
8	$(\sqrt{3}-1)/2 + 3^{-(m-1)/2}$
9	$-1 - 2 \times 3^{-m/2}$
10	$(\sqrt{3}+1)/2 + 3^{-(m-1)/2}$
11	$-(\sqrt{3}+1)/2 + 3^{-m/2}$

So we have that

$$\limsup_{X\to\infty} \frac{|M_{E/\mathbb{F}_{3^m}}(X)|}{3^{mX/2}} = \frac{\sqrt{3}+1}{2} + \frac{1}{3^{(m-1)/2}}.$$

(5) Finally, if $q = p^m$ with $a = 0$, where either m is even and $p \not\equiv 1 \pmod 4$, or m is odd, then

$$\frac{M_{E/\mathbb{F}_q}(X)}{q^{X/2}} = \cos\Big(\frac{\pi X}{2}\Big) + \frac{1}{\sqrt{q}}\sin\Big(\frac{\pi X}{2}\Big).$$

The four cases of $X \pmod 4$ are

$X \pmod 4$	$M_{E/\mathbb{F}_q}(X)/q^{X/2}$
0	1
1	$1/\sqrt{q}$
2	-1
3	$-1/\sqrt{q}$

Thus, we have the inequality

$$|M_{E/\mathbb{F}_q}(X)| \le q^{X/2}$$

for all $X \ge 1$, with equality occurring infinitely often.

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press

Acknowledgements

The author thanks Jim Borger for his helpful advice and corrections of this paper, and also Mike Zieve for alerting the author to the results in [4].

References

[1] P. T. Bateman, J. W. Brown, R. S. Hall, K. E. Kloss and R. M. Stemmler, 'Linear relations connecting the imaginary parts of the zeros of the zeta function', in: *Computers in Number Theory*, (eds. A. O. L. Atkin and B. J. Birch) (Academic Press, London, 1971), 11–19.

[2] D. G. Best and T. S. Trudgian, 'Linear relations of zeroes of the zeta-function'. arXiv:math.NT/1209.3843.

[3] B. Cha, 'The summatory function of the Möbius function in function fields'. arXiv:math.NT/1008.4711v2.

[4] E. W. Howe, E. Nart and C. Ritzenthaler, 'Jacobians in isogeny classes of abelian surfaces over finite fields', *Ann. Inst. Fourier* **59** (2009), 239–289.

[5] P. Humphries, 'On the Mertens conjecture for function fields'. arXiv:math.NT/1210.0945.

[6] A. E. Ingham, 'On two conjectures in the theory of numbers', *Amer. J. Math.* **64** (1942), 313–319.

[7] T. Kotnik and H. te Riele, 'The Mertens conjecture revisited', in: *Algorithmic Number Theory*, Lecture Notes in Comput. Sci., 4076 (eds. F. Hess, S. Pauli and M. Pohst) (Springer, Berlin, 2006), 156–167.

[8] F. Mertens, 'Über eine zahlentheoretische Funktion', *Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Mathematisch-Naturwissenschaftliche Klasse, Abteilung 2a* **106** (1897), 761–830.

[9] A. M. Odlyzko and H. J. J. te Riele, 'Disproof of the Mertens conjecture', *J. reine angew. Math.* **357** (1985), 138–160.

[10] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, 210 (Springer, New York, 2002).

[11] W. C. Waterhouse, 'Abelian varieties over finite fields', *Ann. Sc. Éc. Norm. Supér., Série 4* **2** (1969), 521–560.

PETER HUMPHRIES, Department of Mathematics, Princeton University,
Princeton, New Jersey 08544, USA
e-mail: peterch@math.princeton.edu

https://doi.org/10.1017/S0004972712001116 Published online by Cambridge University Press