An efficient deterministic test for Kloosterman sum zeros

Omran Ahmadi
omran.ahmadi@ucd.ie

Robert Granger
rgranger@computing.dcu.ie

Claude Shannon Institute
University College Dublin
Dublin 4
Ireland

April 19, 2011

Abstract

We propose a simple deterministic test for deciding whether or not a non-zero element $a \in \mathbb{F}_{2^n}$ or $\mathbb{F}_{3^n}$ is a zero of the corresponding Kloosterman sum over these fields, and analyse its complexity. The test seems to have been overlooked in the literature. For binary fields, the test has an expected operation count dominated by just two $\mathbb{F}_{2^n}$-multiplications when n is odd (with a slightly higher cost for even extension degrees), making its repeated invocation the most efficient method to date to find a non-trivial Kloosterman sum zero in these fields. The analysis depends on the distribution of Sylow p-subgroups in two corresponding families of elliptic curves, which we prove using a theorem due to Howe.

Keywords: Kloosterman sums, elliptic curves, Sylow p-subgroups

1 Introduction

For a finite field $\mathbb{F}_{p^n}$, the Kloosterman sum $\mathcal{K}_{p^n} : \mathbb{F}_{p^n} \to \mathbb{C}$ can be defined by

$$\mathcal{K}_{p^n}(a) = 1 + \sum_{x \in \mathbb{F}_{p^n}^{\times}} \zeta^{\mathrm{Tr}(x^{-1}+ax)},$$

where ζ is a primitive p-th root of unity and Tr denotes the absolute trace map $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$, defined by

$$\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}.$$

Note that in some contexts the Kloosterman sum is defined to be just the summation term without the added '1' [18]. As one would expect, a Kloosterman (sum) zero is simply an element $a \in \mathbb{F}_{p^n}^{\times}$ for which $\mathcal{K}_{p^n}(a) = 0$.

Kloosterman sums have recently become the focus of much research, most notably due to their applications in cryptography and coding theory (see [7, 29] for example). In particular, zeros of $\mathcal{K}_{2^n}$ lead to bent functions from $\mathbb{F}_{2^{2n}} \rightarrow \mathbb{F}_2$ [9], and similarly zeros of ternary Kloosterman sums give rise to ternary bent functions [15].

It was recently shown that zeros of Kloosterman sums only exist in characteristics 2 and 3 [20], and hence these are the only cases we consider. Finding such zeros is regarded as being difficult, and recent research has tended to focus on characterising Kloosterman sums modulo small integers [28, 23, 10, 8, 24, 11, 13, 12]. While these results are interesting in their own right, they also provide a sieve which may be used to eliminate elements of a certain form prior to testing whether they are Kloosterman zeros or not, by some other method.

Following work by Katz and Livné [18], Lachaud and Wolfmann [21] and Moisio [27], Lisoněk has exploited a connection between Kloosterman sums and the group orders of two families of elliptic curves [23]. In particular, for $p \in \{2, 3\}$ the Kloosterman sum $\mathcal{K}_{p^n}(a)$ is equal to one minus the trace of Frobenius of an associated elliptic curve $E_{p^n}(a)$. Using p-adic methods — originally due to Satoh [31] — computing the group orders of these elliptic curves asymptotically takes $O(n^2 \log^2 n \log \log n)$ bit operations and requires $O(n^2)$ memory (see Vercauteren's thesis [35] for contributions and a comprehensive survey). Lisoněk also suggests that if instead one only wants to determine whether a given element is a zero, one can do so by checking whether a random point on $E_{p^n}(a)$ has order p^n. Asymptotically, this has a similar bit complexity to the point counting approach, requires less memory, but is randomised. Using this method he was able to find a Kloosterman zero of $\mathcal{K}_{2^n}$ for $n \leq 64$ and $\mathcal{K}_{3^n}$ for $n \leq 34$, in a matter of days [23].

In this paper we take the elliptic curve interpretation to its logical conclusion, in terms of proving divisibility results of Kloosterman sums by powers of the characteristic. In particular we give an efficient deterministic algorithm to compute the Sylow 2- and 3-subgroups of the associated elliptic curves in characteristics 2 and 3 respectively, along with a generator (these subgroups are cyclic in the cases considered). Moreover, the average case running-time of these algorithms is analysed, and is considerably faster than the two methods mentioned.

Finding a single Kloosterman zero — which is often all that is needed in applications — is then a matter of testing field elements until one is found. This crucially depends on the number of Kloosterman zeros, see [18] and §6.3. We note that should one want to find *all* Kloosterman zeros over $\mathbb{F}_{2^n}$, then one can use the fast Walsh-Hadamard transform (see [3] for an overview), which has complexity $O(2^n \cdot n)$, or complex multiplication [2], whereas our method would take $O(2^n \cdot n \log n)$ in the best case.

2 Connection with elliptic curves

The following two lemmas were used by Lisoněk, while the third was proven in [23].

Lemma 2.1 ([21])**.** *Let $a \in \mathbb{F}_{2^n}^{\times}$ and define the elliptic curve $E_{2^n}(a)$ over $\mathbb{F}_{2^n}$ by*

$$E_{2^n}(a) : y^2 + xy = x^3 + a.$$

Then $\#E_{2^n}(a) = 2^n + \mathcal{K}_{2^n}(a)$.

Lemma 2.2 ([27])**.** *Let $a \in \mathbb{F}_{3^n}^{\times}$ and define the elliptic curve $E_{3^n}(a)$ over $\mathbb{F}_{3^n}$ by*

$$E_{3^n}(a) : y^2 = x^3 + x^2 - a.$$

Then $\#E_{3^n}(a) = 3^n + \mathcal{K}_{3^n}(a)$.

Lemma 2.3 ([23])**.** *Let $p \in \{2, 3\}$, let $a \in \mathbb{F}_{p^n}^{\times}$, and let $0 \leq k \leq n$. Then $p^k \mid \mathcal{K}_{p^n}(a)$ if and only if there exists a point of order p^k on $E_{p^n}(a)$.*

Lemma 2.3 is a simple consequence of the structure theorem for elliptic curves over finite fields. Note that for $p \in \{2, 3\}$, by Lemmas 2.1 and 2.2 we have $\mathcal{K}_{p^n}(a) = 0$ if and only if $E_{p^n}(a)$ has order p^n. By Lemma 2.3, this is equivalent to $E_{p^n}(a)$ having a point of order p^n, and hence finding a point of order p^n proves that $\mathcal{K}_{p^n}(a) = 0$. For the remainder of the paper, when we refer to a prime p we implicitly mean $p \in \{2, 3\}$.

3 Determining the Sylow p-subgroup of $E_{p^n}(a)$

It is easy to show that $\mathcal{K}_{2^n}(a) \equiv 0 \pmod 4$ and $\mathcal{K}_{3^n}(a) \equiv 0 \pmod 3$ for all $a \in \mathbb{F}_{2^n}$ and $\mathbb{F}_{3^n}$ respectively. One way to see this is to observe that $E_{2^n}(a)$ possesses a point of order 4 (see §4) and $E_{3^n}(a)$ possesses a point of order 3 (see §5), and hence by Lagrange's theorem, $4 \mid \#E_{2^n}(a)$ and $3 \mid \#E_{3^n}(a)$.

For an integer x, let $\mathrm{ord}_p(x)$ be the exponent of the maximum power of p that divides x. For a given $a \in \mathbb{F}_{p^n}^{\times}$, let $k = \mathrm{ord}_p(\#E_{p^n}(a))$, so that the Sylow p-subgroup $S_p(E_{p^n}(a))$ has order p^k. Since by Lemma 2.3, $S_p(E_{p^n}(a))$ is cyclic, it contains $(p-1)p^{k-1}$ generators. Multiplying these by p results in $(p-1)p^{k-2}$ generators of the order p^{k-1} subgroup. Continuing this multiplication by p process, after $k-1$ steps one arrives at the p-torsion subgroup, consisting of $p-1$ order p points and the identity element $\mathcal{O}$. These considerations reveal the structure of the p-power torsion subgroups, which one may view as a tree, with $\mathcal{O}$ as the root. The root has $p-1$ children which are the non-identity points in $E_{p^n}(a)[p]$. If $k > 1$ each of these $p-1$ vertices has p children: the elements of $E_{p^n}(a)[p^2] \setminus E_{p^n}(a)[p]$. For $1 < i < k$, at the i-th level, each of the $(p-1)p^{i-1}$ vertices have p children.

Using a division polynomial approach Lisoněk was able to prove a condition on a such that $\mathcal{K}_{2^n}(a)$ is divisible by 16, and likelise a condition on a such that $\mathcal{K}_{3^n}(a)$ is divisible by 9. While other methods have pushed the divisibility of $\mathcal{K}_{2^n}(a)$ by 2^k up to 64 [13] and $\mathcal{K}_{3^n}(a)$ by 3^k up to 27 [12], these use p-adic methods; the division polynomial approach seemingly being too cumbersome to progress any further.

However, the process outlined above — taking a generator of $S_p(E_{p^n}(a))$ and multiplying by p repeatedly until the non-identity elements of the p-torsion are obtained — can be reversed, easily and efficiently, using point-halving in even characterstic, and point-thirding in characteristic three, as we demonstrate in the following two sections. Furthermore, due to the cyclic structure of $S_p(E_{p^n}(a))$, at each level, either all points are divisible by p, or none are. This means one can determine the height of the tree by using a depth-first search, but without any backtracking. When a point P on a particular level can not be halved or thirded, this level is $\log_p |S_p(E_{p^n}(a))|$, and P is a generator. Furthermore, one can do this without ever computing the group order of the curve. This process has been considered previously by Miret *et al.*, in the case of determining the Sylow 2-subgroup of arbitrary elliptic curves [25], and for all other primes $l > 2$ [26], with the exception of the cases $l = p$. The case $l = p = 2$ follows easily from point halving, which is well studied in cryptographic circles [19, 32, 14, 1], and known to be faster than point doubling in many cases. The case $l = p = 3$ has not been explicitly addressed before, and we do so here for the family $E_{3^n}(a)$.

We summarise this process in Algorithm 1. Regarding notation, we say that a point P is p-divisible if there exists a point Q such that $pQ = P$, and write $Q = P/p$.

Algorithm 1: **DETERMINE** $S_p(E_{p^n}(a))$

```
INPUT:  $a \in \mathbb{F}_{p^n}^{\times}$,  $P \in E_{p^n}(a)[p] \setminus \{\mathcal{O}\}$
OUTPUT: $(k, P_k)$ where $k = \mathrm{ord}_p(\#E_{p^n}(a))$ and $\langle P_k \rangle = S_p(E_{p^n}(a))$

counter $\leftarrow 1$;
While $P$ is $p$-divisible do:
    P := P/p;
    counter++;
Return (counter, $P$)
```

4 Binary fields

We now work out the details of Algorithm 1 for the family of curves $E_{2^n}(a)$. For a fixed n, given a point $P = (x, y) \in E_{2^n}(a)$, $2P = (\xi, \eta)$ is given by the formula:

$$\begin{aligned} \lambda &= x + y/x, \\ \xi &= \lambda^2 + \lambda, \\ \eta &= x^2 + \xi(\lambda + 1). \end{aligned} \tag{1}$$

We therefore need to reverse this process. Given $Q = (\xi, \eta)$, to find $P = (x, y)$ such that $[2]P = Q$, we do the following.

First, we solve $\lambda^2 + \lambda = \xi$, if possible. This is solvable in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\xi) = 0$, since the trace of the left-hand side is zero for every $\lambda \in \mathbb{F}_{2^n}$. For odd n this can be solved using the *half trace* (we defer the treatment for even n until §4.1),

$$H(c) = \sum_{i=0}^{(n-1)/2} c^{2^{2i}}.$$

One can check that $\lambda = H(\xi)$ solves equation (1). We then have

$$\begin{aligned} x &= (\eta + \xi(\lambda + 1))^{1/2}, \\ y &= x(x + \lambda). \end{aligned}$$

This completes the halving of the point $Q = (\xi, \eta)$. Note that $\lambda = H(\xi) + 1$ provides the other point whose duplicate is Q. There is a unique 2-torsion point $(0, a^{1/2})$, which when halved by the above method gives the point $P_4 = (a^{1/4}, a^{1/2})$ of order 4, which we use as the base point in the following algorithm.

ALGORITHM 2: **DETERMINE** $S_2(E_{2^n}(a))$

```
INPUT:  $a \in \mathbb{F}_{2^n}^{\times}$, $x = a^{1/4}, y = a^{1/2}$
OUTPUT: $(k, P_k)$ where $k = \mathrm{ord}_2(\#E_{2^n}(a))$ and $\langle P_k \rangle = S_2(E_{2^n}(a))$

counter $\leftarrow 2$;
While Tr$(x) = 0$ do:
    $\lambda \leftarrow H(x)$;
    $x \leftarrow (y + x(\lambda + 1))^{1/2}$;
    $y \leftarrow x(x + \lambda)$;
    counter++;
Return (counter, $P = (x, y)$)
```

Observe that if the point P_4 satisfies $\mathrm{Tr}(a^{1/4}) = \mathrm{Tr}(a) = 0$, then there is a point of order 8, and hence $8 \mid \mathcal{K}_{2^n}(a)$, which was first proven in [15] and later in [23].

4.1 Solving $\lambda^2 + \lambda = \xi$ for even extension degrees

When n is even, the half trace approach will not work. Instead, fix an element $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta) = 1$. Then a solution to equation (1) is given by [4, Chapter II]

$$\lambda = \sum_{i=0}^{n-2} \left(\sum_{j=i+1}^{n-1} \delta^{2^j} \right) \xi^{2^i}. \tag{2}$$

The inner sums can be precomputed, and for a general δ the computation of λ would require $n-1$ multiplications in $\mathbb{F}_{2^n}$, which together with the 2 multplications coming from steps 4 and 5 of Algorithm 2, totals $n+1$ multiplications.

However, should $\mathbb{F}_{2^n}$ contain a proper subfield with extension degree a power of 2, then one can reduce this cost significantly. Let $n = 2^i m$ with $i \geq 1$ and m odd. Fix a $\delta \in \mathbb{F}_{2^{2^i}}$ with $\mathrm{Tr}_{\mathbb{F}_{2^{2^i}}/\mathbb{F}_2}(\delta) = 1$. Then

$$\mathrm{Tr}_{\mathbb{F}_{2^{2^i \cdot m}}/\mathbb{F}_2}(\delta) = m \cdot \mathrm{Tr}_{\mathbb{F}_{2^{2^i}}/\mathbb{F}_2}(\delta) = 1.$$

Hence this δ can be used in (2). As $\delta^{2^{2^i}} = \delta$, upon expanding (2) in terms of $\{\delta^{2^0}, \delta^{2^1}, \ldots, \delta^{2^{2^i-1}}\}$, we see that at most 2^i multiplications of elements of $\mathbb{F}_{2^{2^i}}$ by elements of $\mathbb{F}_{2^n}$ are required. So the smaller the maximum power of 2 dividing n, the faster one can solve equation (1). In the case where $n = 2m$ with m odd, only 2 such 'mini' multiplications are necessary. Note that when n itself is odd, we set $\delta = 1$ and so no multiplications are needed. At the other end of the extreme, if $n = 2^i$, then one requires $n-1$ full multiplications and 2 more for steps 4 and 5 of Algorithm 2. So in this case we obtain no improvement over the naive initial method of (2).

5 Ternary fields

Let $Q = (\xi, \eta) \in E_{3^n}(a)$. To find $P = (x, y)$ such that $[3]P = Q$, when possible, we do the following. As in [26, §4], we have

$$x([3]P) = x(P) - \frac{\Psi_2(x,y)\Psi_4(x,y)}{\Psi_3^2(x,y)},$$

or

$$(x - \xi)\Psi_3^2(x,y) - \Psi_2(x,y)\Psi_4(x,y) = 0,$$

where Ψ_l is the l-th division polynomial. Working modulo the equation of E_{3^n}, this becomes

$$x^9 - \xi x^6 + a(1-\xi)x^3 - a^2(a+\xi) = 0,$$

whereupon substituting $X = x^3$ gives

$$f(X) = X^3 - \xi X^2 + a(1-\xi)X - a^2(a+\xi) = 0. \tag{3}$$

To solve (3), we make the transformation

$$g(X) = X^3 f\left(\frac{1}{X} - \frac{a(1-\xi)}{\xi}\right) = \frac{a^2\eta^2}{\xi^3}X^3 - \xi X + 1.$$

Hence we must solve

$$X^3 - \frac{\xi^4}{a^2\eta^2}X + \frac{\xi^3}{a^2\eta^2} = 0.$$

Writing $X = \frac{\xi^2}{a\eta}\bar{X}$ this becomes

$$\bar{X}^3 - \bar{X} + \frac{a\eta}{\xi^3} = 0. \tag{4}$$

Hence our thirding condition is simply that $\mathrm{Tr}(a\eta/\xi^3) = 0$, since as before, for every element of $\mathbb{F}_{3^n}$ we have $\mathrm{Tr}(\bar{X}^3 - \bar{X}) = 0$. To solve (4) we use a function similar to the half trace: for $n \equiv 2 \pmod 3$ we define

$$H_3(c) = c + \sum_{i=1}^{(n-2)/3} c^{3^{3i}} - c^{3^{3i-1}}.$$

One can check that this solves the stated equation, the other two solutions being $H_3(c) \pm 1$. For $n \equiv 1 \pmod 3$ one can define a similar function, whereas for $n \equiv 0 \pmod 3$ one can use an analogue of the binary solution given in §4.1.

Unrolling the transformations leads to the following algorithm, with input the 3-torsion point $P_3 = (a^{1/3}, a^{1/3})$.

ALGORITHM 3: **DETERMINE** $S_3(E_{3^n}(a))$

```
INPUT:  $a \in \mathbb{F}_{3^n}^{\times}$,  $x = a^{1/3}, y = a^{1/3}$
OUTPUT: $(k, P_k)$ where $k = \mathrm{ord}_3(\#E_{3^n}(a))$ and $\langle P_k \rangle = S_3(E_{3^n}(a))$

counter $\leftarrow 1$;
While Tr$(ay/x^3) = 0$ do:
    $\lambda \leftarrow H_3(-ay/x^3)$;
    $x \leftarrow \left(\frac{ay}{x^2\lambda} - \frac{a(1-x)}{x}\right)^{1/3}$;
    $y \leftarrow \left(x^3 + x^2 - a\right)^{1/2}$;
    counter++;
Return (counter, $P = (x, y)$)
```

Observe that as with Algorithm 2, if the point P_3 satisfies $\mathrm{Tr}(a \cdot a^{1/3}/a) = \mathrm{Tr}(a) = 0$, then there is a point of order 9, and hence $9 \mid \mathcal{K}_{3^n}(a)$, which was first proven in [34], and later in [23] and [11].

6 Heuristic analysis of Algorithms 2 and 3

In this section we present an heuristic analysis of the expected computational cost of Algorithms 2 and 3. We first address the estimated cost of each iteration (which may be subject to several efficiency improvements), and then address the number of iterations that are performed.

6.1 Cost per iteration

The cost of each iteration in Algorithm 2 is dominated by 2 $\mathbb{F}_{2^n}$-multiplications, the addition, trace, half trace being almost negligible, while squaring and square-rooting are cyclic shifts when using normal bases, and are also very efficient in polynomial bases. We refer the reader to [14, 1] for the state of the art in point halving techniques.

Due to the presence of inversions and square-root computations, Algorithm 3 is considerably less efficient than Algorithm 2. Asymptotically, one expects 3-adic point counting methods to be superior. However, for fields of a practical size, comparing Algorithm 3 with the built-in MAGMA point counting functions (introduced in [5]), Algorithm 3 is several orders of magnitude faster (as is Algorithm 2). We leave it as an interesting practical challenge to develop efficient point thirding algorithms and implementations.

6.2 (Heuristic) expected number of iterations

In terms of the number of iterations that must be performed in Algorithms 2 and 3, we first propose the following simple heuristic argument, before giving a proof in §7. We make the assumption that over all $a \in \mathbb{F}_{p^n}^{\times}$, at the start of any iteration, regardless of the height of the tree at that point, the argument of the trace function is uniformly distributed in $\mathbb{F}_{p^n}$. While this assumption may seem an unfounded, in our experiments the resulting estimate is true to within 1% of the actual average value, for the relatively small fields we compared with. We treat the two characteristics separately.

For Algorithm 2, every curve order is divisible by 4, and on the first iteration, $2^{n-1}-1$ of the curves $E_{2^n}(a)$ have $\mathrm{Tr}(a)=0$. On the second iteration, by our assumption, approximately 2^{n-2} curves have trace 0. Summing over all iterations this gives a total of

$$2^{n-1}+2^{n-1}+\cdots+2+1 \approx 2^n,$$

for the number of iterations that need to be performed for all $a \in \mathbb{F}_{2^n}^{\times}$. This is one iteration per element and so the expected order of $S_2(E_{2^n}(a))$ as $n \to \infty$ is $2^{2+1}=8$.

For Algorithm 3, since the trace has probability 1/3 of being zero, the same argument for the expected number of iterations gives the corresponding total

$$3^{n-1}+3^{n-2}+\cdots+3+1 \approx 3^n/2.$$

Hence over all $a \in \mathbb{F}_{3^n}^{\times}$, according to this heursitic we have an expected total of $3^n/2$ iterations, which is 1/2 an iteration per element, and so the expected order of $S_3(E_{3^n}(a))$ as $n \to \infty$ is $3^{1+1/2}=3\sqrt{3}$.

In terms of finding a point of order p^n on $E_{p^n}(a)$, note that one only needs to perform at most $\lceil n/2+\log_p 4\rceil-(4-p)$ iterations of Algorithms 2 and 3 for $p=2$ and $p=3$ respectively, as this determines the curve order uniquely (as p^n). The ceiling is of course the same precision used in the p-adic point counting methods [35].

6.3 Exact formula for average order of $S_p(E_{p^n}(a))$

Let $p^n + t$ be an integer in the Weil interval $W_{p^n} = [p^n + 1 - 2p^{n/2}, p^n + 1 + 2p^{n/2}]$, which is assumed to be divisible by 4 if $p = 2$ and divisible by 3 if $p = 3$. Let $N(t)$ be the number of solutions in $\mathbb{F}_{p^n}^{\times}$ to $\mathcal{K}_{p^n}(a) = t$. Katz and Livné have proven the following [18]. Let $\alpha = (t + \sqrt{t^2 - 4p^n})/2$ for t as above. Then

$$N(t) = \sum_{\text{orders } \mathcal{O}} h(\mathcal{O}),$$

where the sum is over all orders $\mathcal{O} \subset \mathbb{Q}(\alpha)$ which contain $\mathbb{Z}[\alpha]$. Hence the total of the exponents of the Sylow p-subgroups, over all $a \in \mathbb{F}_{p^n}^{\times}$, is

$$T_{p^n} = \sum_{(p^n+t) \in W_{p^n}} N(t) \cdot \mathrm{ord}_p(p^n + t).$$

The expected order of $S_p(E_{p^n}(a))$ is thus $p^{T_{p^n}/(p^n-1)}$. It seems difficult to prove the heuristic of §6.2 by estimating T_{p^n} using the Katz-Livné result directly. However, using a theorem due to Howe [16], we prove Theorem 7.3 below.

7 Main result

We now present our main result, which proves the expected order of the Sylow p-subgroups is as stated in §6.2. To facilitate our analysis, for $1 \leq k \leq n$, we partition T_{p^n} into the counting functions

$$T_{p^n}(k) = \sum_{(p^n+t) \in W_{p^n}, p^k | (p^n+t)} N(t), \tag{5}$$

so that

$$T_{p^n} = \sum_{k=1}^{n} T_{p^n}(k). \tag{6}$$

Observe that since $\#E_{2^n}(a) \equiv 0 \pmod 4$ for all $a \in \mathbb{F}_{2^n}^{\times}$, we have $T_{2^n}(1) = T_{2^n}(2) = 2^n - 1$ and furthermore since $\mathrm{Tr}(a) = 0$ for precisely $2^{n-1} - 1$ elements $a \in \mathbb{F}_{2^n}^{\times}$, we have $T_{2^n}(3) = 2^{n-1} - 1$. Similarly, since $\#E_{3^n}(a) \equiv 0 \pmod 3$ for all $a \in \mathbb{F}_{3^n}^{\times}$, we have $T_{3^n}(1) = 3^n - 1$ and again by the trace condition, we have $T_{3^n}(2) = 3^{n-1} - 1$.

7.1 Estimating $T_{p^n}(k)$

For $k \geq 2$, let $\mathcal{T}_{2^n}(k)$ be the set of $\mathbb{F}_{2^n}$-isomorphism classes of elliptic curves $E/\mathbb{F}_{2^n}$ such that $\#E(\mathbb{F}_{2^n}) \equiv 0 \pmod{2^k}$. Similarly for $k \geq 1$, let $\mathcal{T}_{3^n}(k)$ be the set of $\mathbb{F}_{3^n}$-isomorphism classes of elliptic curves $E/\mathbb{F}_{3^n}$ such that $\#E(\mathbb{F}_{3^n}) \equiv 0 \pmod{3^k}$.

Observe that the elliptic curves $E_{2^n}(a)$ and $E_{3^n}(a)$ both have j-invariant $1/a$ [33, Appendix A], and hence cover all the $\overline{\mathbb{F}}_{2^n}$- and $\overline{\mathbb{F}}_{3^n}$-isomorphism classes of elliptic curves respectively, except $j = 0$. We have the following lemma.

Lemma 7.1. *[6, Lemma 6] Let $E/\mathbb{F}_q$ be an elliptic curve and let $[E]_{\mathbb{F}_q}$ be the set of $\mathbb{F}_q$-isomorphism classes of elliptic curves that are $\overline{\mathbb{F}}_q$-isomorphic to E. Then for $j \neq 0, 1728$ we have $\#[E]_{\mathbb{F}_q} = 2$, and $[E]_{\mathbb{F}_q}$ consists of the $\mathbb{F}_q$-isomorphism class of E and the $\mathbb{F}_q$-isomorphism class of its quadratic twist E^t.*

Let $\#E_{2^n}(a) = 2^n + 1 - t_a$, with t_a the trace of Frobenius. Since $j \neq 0$, by Lemma 7.1 the only other $\mathbb{F}_{2^n}$-isomorphism class with invariant $1/a$ is that of the quadratic twist $E_{2^n}^t(a)$, which has order $2^n + 1 + t_a$. Since $t_a \equiv 1 \pmod 4$, we have $\#E_{2^n}^t(a) \equiv 2 \pmod 4$ and hence none of the $\mathbb{F}_{2^n}$-isomorphism classes of the quadratic twists of $E_{2^n}(a)$ for $a \in \mathbb{F}_{2^n}^\times$ are in $\mathcal{T}_{2^n}(k)$, for $k \geq 2$. By an analogous argument, only the $\mathbb{F}_{3^n}$-isomorphism classes of $E_{3^n}(a)$ for $a \in \mathbb{F}_{3^n}^\times$ are in $\mathcal{T}_{3^n}(k)$, for $k \geq 1$. Furthermore, all curves $E/\mathbb{F}_{2^n}$ and $E/\mathbb{F}_{3^n}$ with $j = 0$ are supersingular [36, §3.1], and therefore have group orders $\equiv 1 \pmod 4$ and $\equiv 1 \pmod 3$ respectively. Hence no $\mathbb{F}_{p^n}$-isomorphism classes of curves with $j = 0$ are in $\mathcal{T}_{p^n}(k)$ for $p \in \{2, 3\}$. As a result, for $2 \leq k \leq n$ we have

$$|\mathcal{T}_{2^n}(k)| = T_{2^n}(k), \tag{7}$$

and similarly, for $1 \leq k \leq n$ we have

$$|\mathcal{T}_{3^n}(k)| = T_{3^n}(k).$$

Therefore in both cases, a good estimate for $|\mathcal{T}_{p^n}(k)|$ is all we need to estimate $T_{p^n}(k)$. The cardinality of $\mathcal{T}_{3^n}(k)$ is naturally related to the study of modular curves; in particular, considering the number of $\mathbb{F}_{p^n}$-rational points on the Igusa curve of level p^k allows one to prove Theorem 7.3 below [17, 30]. However, for simplicity (and generality) we use a result due to Howe on the group orders of elliptic curves over finite fields [16]. Consider the set

$$V(\mathbb{F}_q; N) = \{E/\mathbb{F}_q : N \mid \#E(\mathbb{F}_q)\}/\cong_{\mathbb{F}_q}$$

of equivalence classes of $\mathbb{F}_q$-isomorphic curves whose group orders are divisible by N. Following Lenstra [22], rather than estimate $V(\mathbb{F}_q; N)$ directly, Howe considers the weighted cardinality of $V(\mathbb{F}_q; N)$, where for a set S of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$, this is defined to be:

$$\#'S = \sum_{[E] \in S} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(E)}.$$

For $j \neq 0$ we have $\#\mathrm{Aut}_{\overline{\mathbb{F}}_q}(E) = 2$ [33, §III.10] and since $\{\pm 1\} \subset \mathrm{Aut}_{\mathbb{F}_q}(E)$ we have $\#\mathrm{Aut}_{\mathbb{F}_q}(E) = 2$ also. Therefore, by the above discussion, for $p = 2, k \geq 2$ and $p = 3, k \geq 1$ we have

$$|\mathcal{T}_{p^n}(k)| = 2 \cdot \#'V(\mathbb{F}_{p^n}; p^k), \tag{8}$$

We now present Howe's result.

Theorem 7.2. *[16, Theorem 1.1] There is a constant $C \leq 1/12 + 52/6 \approx 1.262$ such that the following statement is true: Given a prime power q, let r be the multiplicative arithmetic function such that for all primes l and positive integers a*

$$r(l^a) = \begin{cases} \dfrac{1}{l^{a-1}(l-1)}, & \text{if } q \not\equiv 1 \pmod{l^c}; \\ \\ \dfrac{l^{b+1}+l^b-1}{l^{a+b-1}(l^2-1)}, & \text{if } q \equiv 1 \pmod{l^c}, \end{cases}$$

where $b = \lfloor a/2 \rfloor$ and $c = \lceil a/2 \rceil$. Then for all positive integers N one has

$$\left| \frac{\#' V(\mathbb{F}_q; N)}{q} - r(N) \right| \leq \frac{CN\rho(N)2^{\nu(N)}}{\sqrt{q}}, \tag{9}$$

where $\rho(N) = \prod_{p|N}((p+1)/(p-1))$ and $\nu(N)$ denotes the number of prime divisors of N.

Equipped with Theorem 7.2, we now present our main theorem.

Theorem 7.3. *Let $p \in \{2, 3\}$ and let $T_{p^n}(k)$ be defined as above. Then*

(i) For $3 \leq k < n/4$ we have $T_{2^n}(k) = 2^{n-k+2} + O(2^{k+n/2})$,

(ii) For $2 \leq k < n/4$ we have $T_{3^n}(k) = 3^{n-k+1} + O(3^{k+n/2})$,

(iii) $T_{2^n} = 3 \cdot 2^n + O(n \cdot 2^{3n/4})$,

(iv) $T_{3^n} = 3^{n+1}/2 + O(n \cdot 3^{3n/4})$,

(v) $\lim_{n\to\infty} T_{p^n}/(p^n - 1) = \begin{cases} 3 & \text{if } p = 2, \\ 3/2 & \text{if } p = 3. \end{cases}$

Furthermore, in (i) – (iv) the implied constants in the O-notation are absolute and effectively computable.

Proof. By equations (7) and (8), and Theorem 7.2, for $3 \leq k \leq n$ we have

$$\left| \frac{T_{2^n}(k)}{2^{n+1}} - \frac{1}{2^{k-1}} \right| \leq \frac{C \cdot 2^k \cdot 3 \cdot 2}{2^{n/2}},$$

from which part (i) follows immediately. Similarly for $2 \leq k \leq n$ we have

$$\left| \frac{T_{3^n}(k)}{2 \cdot 3^n} - \frac{1}{3^{k-1} \cdot 2} \right| \leq \frac{C \cdot 3^k \cdot (4/2) \cdot 2}{3^{n/2}},$$

from which part (ii) follows. For part (*iii*) we write equation (6) as follows:

$$T_{2^n} = \sum_{k=1}^{n} T_{2^n}(k) = \sum_{k=1}^{\lfloor n/4 \rfloor - 1} T_{2^n}(k) + \sum_{k=\lfloor n/4 \rfloor}^{n} T_{2^n}(k).$$

Considering these two sums in turn, for the first we have

$$\begin{aligned} & 2^n + (2^n + 2^{n-1} + \cdots + 2^{n-\lfloor n/4 \rfloor + 2}) + O(2^{n/2+2} + 2^{n/2+3} + \cdots + 2^{n/2+\lfloor n/4 \rfloor}) \\ = \;& 2^n + \Big(\frac{2^{n+1}-1}{2-1} - \frac{2^{n-\lfloor n/4 \rfloor + 2} - 1}{2-1}\Big) + O(2^{n/2+\lfloor n/4 \rfloor + 1}) \\ = \;& 2^n + \frac{2^{n+1}-1}{2-1} + O(2^{3n/4}). \end{aligned}$$

Observe that $p^{k+1} \mid t \Longrightarrow p^k \mid t$ and so $T_{2^n}(k+1) \leq T_{2^n}(k)$, which gives

$$\sum_{k=\lfloor n/4 \rfloor}^{n} T_{2^n}(k) \leq (3n/4 + 2) \cdot T_{2^n}(\lfloor n/4 \rfloor) = O(n \cdot 2^{3n/4}).$$

Combining these one obtains

$$T_{2^n} = 2^n + \frac{2^{n+1}-1}{2-1} + O(n \cdot 2^{3n/4}),$$

which proves (*iii*). Part (*iv*) follows with the same argument, but without the first term. Part (*v*) now follows immediately from parts (*iii*) and (*iv*). □

Acknowledgements

The authors wish to thank Faruk Göloğlu and Alexey Zaytsev for useful discussions.

References

[1] Omran Ahmadi and Alfred Menezes. On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$. *Des. Codes Cryptogr.*, 37(3):493–507, 2005.

[2] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[3] K. G. Beauchamp. *Walsh functions and their applications.* Academic Press [Harcourt Brace Jovanovich Publishers], London, 1975. Techniques of Physics, No. 3.

[4] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[5] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] Wouter Castryck and Hendrik Hubrechts. The distribution of the number of points modulo an integer on elliptic curves over finite fields. Preprint, 2011.

[7] Pascale Charpin and Guang Gong. Hyperbent functions, Kloosterman sums, and Dickson polynomials. *IEEE Trans. Inform. Theory*, 54(9):4230–4238, 2008.

[8] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. The divisibility modulo 24 of Kloosterman sums on GF(2^m), m odd. *J. Combin. Theory Ser. A*, 114(2):322–338, 2007.

[9] John. F. Dillon. *Elementary Hadamard Difference Sets.* PhD Thesis. University of Maryland, 1992.

[10] Kseniya Garaschuk and Petr Lisoněk. On binary Kloosterman sums divisible by 3. *Des. Codes Cryptogr.*, 49(1-3):347–357, 2008.

[11] Faruk Göloğlu, Gary McGuire, and Richard Moloney. Ternary kloosterman sums modulo 18 using stickelberger's theorem. In *SETA*, pages 196–203, 2010.

[12] Faruk Göloğlu, Gary McGuire, and Richard Moloney. Ternary kloosterman sums using stickelberger's theorem and the gross-koblitz formula. Preprint, 2010.

[13] Faruk Göloğlu, Gary McGuire, and Richard Moloney. Binary kloosterman sums using stickelberger's theorem and the gross-koblitz formula. To appear in Acta Arithmetica.

[14] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography.* Springer Professional Computing. Springer-Verlag, New York, 2004.

[15] Tor Helleseth and Victor Zinoviev. On Z_4-linear Goethals codes and Kloosterman sums. *Des. Codes Cryptogr.*, 17(1-3):269–288, 1999.

[16] Everett W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Math.*, 85(2):229–247, 1993.

[17] Jun-ichi Igusa. On the algebraic theory of elliptic modular functions. *J. Math. Soc. Japan*, 20:96–106, 1968.

[18] Nicholas Katz and Ron Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.

[19] Erik Woodward Knudsen. Elliptic scalar multiplication using point halving. In *Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '99, pages 135–149, London, UK, 1999. Springer-Verlag.

[20] K.P. Kononen, M.J. Rinta-aho, and K.O. Väänänen. On integer values of kloosterman sums. *Information Theory, IEEE Transactions on*, 56(8):4011 – 4013, aug. 2010.

[21] Gilles Lachaud and Jacques Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Trans. Inform. Theory*, 36(3):686–692, 1990.

[22] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.

[23] Petr Lisoněk. On the connection between Kloosterman sums and elliptic curves. In *Sequences and their applications—SETA 2008*, volume 5203 of *Lecture Notes in Comput. Sci.*, pages 182–187. Springer, Berlin, 2008.

[24] Petr Lisonk and Marko Moisio. On zeros of kloosterman sums. *Designs, Codes and Cryptography*, 59:223–230, 2011. 10.1007/s10623-010-9457-x.

[25] J. Miret, R. Moreno, A. Rio, and M. Valls. Determining the 2-Sylow subgroup of an elliptic curve over a finite field. *Math. Comp.*, 74(249):411–427 (electronic), 2005.

[26] J. Miret, R. Moreno, A. Rio, and M. Valls. Computing the l-power torsion of an elliptic curve over a finite field. *Math. Comp.*, 78(267):1767–1786, 2009.

[27] Marko Moisio. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. *Acta Arith.*, 132(4):329–350, 2008.

[28] Marko Moisio. The divisibility modulo 24 of Kloosterman sums on GF(2^m), m even. *Finite Fields Appl.*, 15(2):174–184, 2009.

[29] Marko Moisio and Kalle Ranto. Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros. *Finite Fields Appl.*, 13(4):922–935, 2007.

[30] Amílcar Pacheco. Rational points on Igusa curves and L-functions of symmetric representations. *J. Number Theory*, 58(2):343–360, 1996.

[31] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[32] R. Schroeppel. Elliptic curves: Twice as fast! Presentation at the CRYPTO 2000 Rump Session, 2000.

[33] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[34] Gerard van der Geer and Marcel van der Vlugt. Kloosterman sums and the p-torsion of certain Jacobians. *Math. Ann.*, 290(3):549–563, 1991.

[35] F. Vercauteren. *Computing zeta functions of curves over finite fields.* PhD Thesis. Katholieke Universiteit Leuven, 2003.

[36] Lawrence C. Washington. *Elliptic curves.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003. Number theory and cryptography.