Canad. Math. Bull. Vol. **55** (4), 2012 pp. 850–857
http://dx.doi.org/10.4153/CMB-2011-126-x
© Canadian Mathematical Society 2011

Character Sums with Division Polynomials

Igor E. Shparlinski and Katherine E. Stange

Abstract. We obtain nontrivial estimates of quadratic character sums of division polynomials $\Psi_n(P)$, $n = 1, 2, \dots$, evaluated at a given point P on an elliptic curve over a finite field of q elements. Our bounds are nontrivial if the order of P is at least $q^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$. This work is motivated by an open question about statistical indistinguishability of some cryptographically relevant sequences that was recently brought up by K. Lauter and the second author.

1 Division Polynomials and Character Sums

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic $p \geq 3$. Denote by $E(\mathbb{F}_q)$ the group of points of E defined over $\mathbb{F}_q$. We refer to [9] for background on elliptic curves.

For an integer n, let Ψ_n be the n-th division polynomial; $nP = \mathcal{O}$, where $\mathcal{O}$ is the point at infinity, see [9, Exercise 3.34]. For a given point $P \in E(\mathbb{F}_q)$, the sequence $\Psi_n(P)$ is often called an *elliptic divisibility sequence*. It satisfies the following recurrence relation [9, Exercise 3.34]

$$\Psi_{h+i}(P)\Psi_{h-i}(P)\Psi_j(P)^2 + \Psi_{i+j}(P)\Psi_{i-j}(P)\Psi_h(P)^2 + \Psi_{j+h}(P)\Psi_{j-h}(P)\Psi_i(P)^2 = 0 \tag{1.1}$$

Furthermore, the sequence $\Psi_n(P)$ is necessarily periodic with some period T and T is always a multiple of the order of P (see Lemma 3.1 below). For background on elliptic divisibility sequences, see [2, 11, 12].

Note that elliptic divisibility sequences can be viewed as a generalisation of *Lucas sequences*. We recall that a Lucas sequence (of the first kind) is a sequence satisfying a recurrence of the form

$$L_n = aL_{n-1} + bL_{n-2}, \quad L_0 = 0, \quad L_1 = 1,$$

in given coefficients a and b. Lucas sequences, including Fibonacci numbers, satisfy an analogue of (1.1) after an appropriate scaling (multiplication of the n-th term by λ^{n^2-1} for some λ); see [9, Exercise 3.34] and [12, Section VI].

Received by the editors December 29, 2009; revised March 18, 2010.
Published electronically June 27, 2011.
During the preparation of this paper, the first author was supported in part by ARC Grant DP0881473 and the second author was supported in part by NSF Fellowship 0802915 and NSERC PDF-373333.
AMS subject classification: **11L40**, 14H52.
Keywords: division polynomial, character sum.

In this paper, for a fixed point $P \in E(\mathbb{F}_q)$ and a positive integer $N \leq T$, we obtain nontrivial estimates of sums of the form

$$S_P(N) = \sum_{n=1}^{N} \chi\left(\Psi_n(P)\right),$$

where χ is the quadratic character of $\mathbb{F}_q$ (as usual, we set $\chi(0) = 0$). Character sums with linear recurrence sequences were studied in [8]. See also [2, Chapter 5] for a survey of estimates of exponential and character sums with various recurrence sequences. However, to our knowledge, for elliptic divisibility sequences no results have been obtained prior to this work.

2 Motivation

This question also has a cryptographic connection. In [5] the following *elliptic divisibility sequence residue problem* was considered: given two points $P, Q \in E(\mathbb{F}_q)$ such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, where, as before, $\mathcal{O}$ is the point at infinity, and $\operatorname{ord}(P) \geq 4$, calculate $\chi(\Psi_k(P))$ for the smallest positive k such that $Q = kP$. To find k given the points P and Q is the well-known *elliptic curve discrete logarithm problem* and its assumed difficulty is the basis of elliptic curve cryptography. To solve the residue problem it certainly suffices to solve the discrete logarithm problem. However, it may be possible to solve the residue problem without first calculating k. It was shown in [5, Theorem 1.1] that solving either of these problems in subexponential time leads to a solution of the other in subexponential time. For perspective, the calculation of $\chi(\Psi_{k+1}(P)/\Psi_k(P))$ takes only polynomial time from P and Q, and does not reveal k, see [5, Section 8]. This has raised the general question of what can be said about the residuosity of $\Psi_n(P)$. More specifically, it has been shown in [5] that the difficulty of a certain distinguishability problem of cryptographic interest depends on the bias between the quadratic residues and nonresidues amongst consecutive terms of the sequence $\Psi_n(P)$, $n = 1, \dots, N$, which is in turn equivalent to estimating the sums $S_P(N)$.

3 Prerequisites Concerning Division Polynomials

We recall some classical results, the first of which describes the ratio $\Psi_{n+r}(P)/\Psi_n(P)$. By [10, Theorem 8] (see also [12, Theorem 8.1]), we have the following lemma.

Lemma 3.1 *Let $P \in E(\mathbb{F}_q)$ be of order $r \geq 3$. Then for all positive $s, k \in \mathbb{Z}$,*

$$\Psi_{sr+k}(P) = a^{ks} b^{s^2} \Psi_k(P),$$

where a and b are given by

$$a = \frac{\Psi_{r-2}(P)}{\Psi_{r-1}(P)\Psi_2(P)}, \qquad b = \frac{\Psi_{r-1}(P)^2\Psi_2(P)}{\Psi_{r-2}(P)}.$$

https://doi.org/10.4153/CMB-2011-126-x Published online by Cambridge University Press

Furthermore, by [10, Lemma 6], we also have the following lemma.

Lemma 3.2 *Let n and m be positive integers. Then*

$$\Psi_{nm}(P) = \Psi_n(mP)\Psi_m(P)^{n^2}.$$

We remark that in general, for $P \in E(\mathbb{F}_q)$ of order $r \geq 3$, the period T of the sequence $\Psi_n(P)$ may be as large as $r(q-1)$; see [10, Corollary 9]. In turn, r can be of order q as well, for example, if P is a generator of the cyclic group of points.

However, the following result, which is immediate from Lemma 3.1, shows that the sequence $\chi(\Psi_n(P))$ is of smaller period.

Lemma 3.3 *Let $P \in E(\mathbb{F}_q)$ be of order $r \geq 3$. Then the sequence $\chi(\Psi_n(P))$ is periodic with period which is a divisor of $R = 2r$.*

Thus, we see from Lemma 3.3 that bounds of character sums $S_P(N)$ are of interest only for the values of $N \leq R = 2r$.

4 Prerequisites Concerning Character Sums

It is well known that for an elliptic curve E over $\mathbb{F}_q$ we have

$$E(\mathbb{F}_q) \sim \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/L\mathbb{Z}$$

for unique integers M and L satisfying $L \mid M$. The point G_1 and G_2 are called *echelonized generators* if G_1 has order M, G_2 has order L, and any point $Q \in E(\mathbb{F}_q)$ can be written in the form $Q = mG_1 + \ell G_2$ with $1 \leq m \leq M$ and $1 \leq \ell \leq L$.

Let $\Omega = \mathrm{Hom}(E(\mathbb{F}_q), \mathbb{C}^*)$ be the group of characters ω on $E(\mathbb{F}_q)$; these are given explicitly by $\omega(Q) = \mathbf{e}_M(am)\mathbf{e}_L(b\ell)$, for some integers a and b with $0 \leq a < M$, $0 \leq b < L$, where $Q = mG_1 + \ell G_2$ and for a positive integer K, we define

$$\mathbf{e}_K(z) = \exp(2\pi i z/K).$$

The following multiplicative analogue of a result of [4] is essentially Proposition 1 of [1], which in turns comes from [6] (note that in [1] it is formulated only for prime fields but the proof extends to arbitrary fields without any difficulties).

Lemma 4.1 *Let η be a non-principal multiplicative character on $\mathbb{F}_q^*$ of order $m \mid q-1$. Let $\mathbb{K} = \mathbb{F}_q(E)$ be the function field of an elliptic curve E over $\mathbb{F}_q$, and $f \in \mathbb{K}$ be of degree d and such that $f \neq g^m$ for any function g in the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. Let $\omega \in \Omega$. Then*

$$\Big|\sum_{Q\in E(\mathbb{F}_q)}^{*} \omega(Q)\eta(f(Q))\Big| \leq 2d\sqrt{q}$$

where $\sum^*$ indicates that the sum is over $Q \in E(\mathbb{F}_q)$ such that $f(Q) \neq \infty$.

Lemma 4.2 *Under the assumptions of Lemma 4.1, let $H \subseteq E(\mathbb{F}_q)$ be a subgroup. Then*

$$\Big|\sum_{Q\in H}^{*} \omega(Q)\eta(f(Q))\Big| \leq 2d\sqrt{q},$$

where $\sum^*$ indicates that the sum is over $Q \in H$ such that $f(Q) \neq \infty$.

https://doi.org/10.4153/CMB-2011-126-x Published online by Cambridge University Press

Proof Let $\Omega_H \subseteq \Omega$ be the subset of characters ϑ such that $H \subseteq \ker(\vartheta)$. Then Ω_H is dual to $E(\mathbb{F}_q)/H$. So by the orthogonality property of characters of abelian groups, we have

$$\frac{1}{|\Omega_H|}\sum_{\vartheta\in\Omega_H}\vartheta(Q) = \begin{cases} 1 & Q \in H,\\ 0 & Q \notin H.\end{cases}$$

Therefore,

$$\begin{aligned}\sum_{Q\in H}{}^{*}\,\omega(Q)\eta(f(Q)) &= \frac{1}{|\Omega_H|}\sum_{Q\in E(\mathbb{F}_q)}{}^{*}\sum_{\vartheta\in\Omega_H}\vartheta(Q)\omega(Q)\eta(f(Q))\\ &= \frac{1}{|\Omega_H|}\sum_{\vartheta\in\Omega_H}\Bigl(\sum_{Q\in E(\mathbb{F}_q)}{}^{*}(\vartheta\cdot\omega)(Q)\eta(f(Q))\Bigr).\end{aligned}$$

Applying Lemma 4.1, we obtain the desired result. ■

5 Main Results

Here we estimate the incomplete sum $S_P(N)$. Following the standard approach, we start with estimates of complete sums twisted with an additive character.

As before, let $R = 2r$, where r is the order of P. Then for an integer a we define the sums

$$T_P(a) = \sum_{n=1}^{R}\chi(\Psi_n(P))\mathbf{e}_R(an)$$

which can be of independent interest.

Theorem 5.1 *For any integer a, we have*

$$T_P(a) = O(R^{5/6}q^{1/12}(\log q)^{1/3}).$$

Proof Let $a \in \mathbb{Z}$. Fix an integer $L \geq 3$ and let $\mathcal{L}$ denote the set of odd primes ℓ such that $\ell < L$ and $\ell \nmid R$. Since R has at most $O(\log R) = O(\log q)$ prime divisors, we see, say, for

$$L \geq (\log q)^2 \tag{5.1}$$

and sufficiently large q we have

$$\#\mathcal{L} \geq \frac{L}{2\log L}. \tag{5.2}$$

Let $\ell \in \mathcal{L}$. As n runs through all residue classes modulo R, so does ℓn. Since both sequences $\chi(\Psi_n(P))$ and $\mathbf{e}_R(an)$, $n = 1, 2, \dots$, are periodic with period R, (see Lemma 3.3), we have

$$T_P(a) = \sum_{n=1}^{R}\chi(\Psi_{\ell n}(P))\mathbf{e}_R(a\ell n).$$

https://doi.org/10.4153/CMB-2011-126-x Published online by Cambridge University Press

We average over all choices of $\ell \in \mathcal{L}$ and set

$$W = \sum_{\ell \in \mathcal{L}} \sum_{n=1}^{R} \chi(\Psi_{\ell n}(P)) \mathbf{e}_R(a\ell n).$$

Then we have

$$T_P(a) = \frac{1}{\#\mathcal{L}} W. \tag{5.3}$$

To estimate W, we change the order of summation, and then apply the Cauchy inequality:

$$|W|^2 \le R \sum_{n=1}^{R} \Bigl| \sum_{\ell \in \mathcal{L}} \chi(\Psi_{\ell n}(P)) \mathbf{e}_R(a\ell n) \Bigr|^2.$$

Now we apply Lemma 3.2:

$$\begin{aligned} |W|^2 &\le R \sum_{n=1}^{R} \Bigl| \sum_{\ell \in \mathcal{L}} \chi(\Psi_{\ell n}(P)) \mathbf{e}_R(a\ell n) \Bigr|^2 \\ &= R \sum_{n=1}^{R} \Bigl| \sum_{\ell \in \mathcal{L}} \chi(\Psi_{\ell}(nP)) \chi(\Psi_n(P)^{\ell^2}) \mathbf{e}_R(a\ell n) \Bigr|^2. \end{aligned}$$

Since χ is the quadratic character and ℓ is odd, we have

$$\chi(\Psi_n(P)^{\ell^2}) = \chi(\Psi_n(P)). \tag{5.4}$$

Therefore,

$$\begin{aligned} |W|^2 &\le R \sum_{n=1}^{R} |\chi(\Psi_n(P))|^2 \Bigl| \sum_{\ell \in \mathcal{L}} \chi(\Psi_{\ell}(nP)) \mathbf{e}_R(a\ell n) \Bigr|^2 \\ &\le R \sum_{n=1}^{R} \Bigl| \sum_{\ell \in \mathcal{L}} \chi(\Psi_{\ell}(nP)) \mathbf{e}_R(a\ell n) \Bigr|^2. \end{aligned}$$

Expanding the square and switching the order of summation again, we obtain

$$\begin{aligned} |W|^2 &\le R \sum_{n=1}^{R} \sum_{\ell_1, \ell_2 \in \mathcal{L}} \chi(\Psi_{\ell_1}(nP)) \mathbf{e}_R(a\ell_1 n) \chi(\Psi_{\ell_2}(nP)) \mathbf{e}_R(-a\ell_2 n) \\ &= R \sum_{\ell_1, \ell_2 \in \mathcal{L}} \sum_{n=1}^{R} \chi\left(\Psi_{\ell_1}(nP)\Psi_{\ell_2}(nP)\right) \mathbf{e}_R(a(\ell_1 - \ell_2)n). \end{aligned}$$

https://doi.org/10.4153/CMB-2011-126-x Published online by Cambridge University Press

We now turn to bounding the inner sum. For $\ell_1 = \ell_2 = \ell$, we have the trivial estimate

$$\sum_{n=1}^{R} \chi(\Psi_\ell(nP)^2) < R.$$

For $\ell_1 \neq \ell_2$ we use Lemma 4.2. The degree of $\Psi_\ell(P)$ (considered as a function in the function field of E) is $(\ell^2 - 1)/2$, so the degree of $\Psi_{\ell_1}(P)\Psi_{\ell_2}(P)$ is

$$\frac{(\ell_1^2 + \ell_2^2 - 2)}{2} < L^2 - 1.$$

It is also easy to see (by examining its zeros) that $\Psi_{\ell_1}(P)\Psi_{\ell_2}(P)$ is not a square of another function from the same function field. Since $R = 2r$ and r is the order of the group $H = \langle P \rangle$ generated by P, we see from Lemma 4.2 that

$$\begin{aligned}
&\Big| \sum_{n=1}^{R} \chi\left(\Psi_{\ell_1}(nP)\Psi_{\ell_2}(nP)\right) \mathbf{e}_R(a(\ell_1 - \ell_2)n) \Big| \\
&\quad = \Big| \sum_{n=1}^{r} \chi\left(\Psi_{\ell_1}(2nP)\Psi_{\ell_2}(2nP)\right) \mathbf{e}_r(a(\ell_1 - \ell_2)n) \Big| \\
&\qquad + \Big| \sum_{n=1}^{r} \chi\left(\Psi_{\ell_1}(2nP - P)\Psi_{\ell_2}(2nP - P)\right) \mathbf{e}_r(a(\ell_1 - \ell_2)n) \Big| \\
&\quad = O(L^2 q^{1/2}).
\end{aligned}$$

Thus, we obtain $|W|^2 = O(R^2 \# \mathcal{L} + RL^2 \sqrt{q}(\#\mathcal{L})^2)$. Substituting this bound in (5.3) and using (5.2), we derive

$$\begin{aligned}
T_P(a) &= O\big(R(\#\mathcal{L})^{-1/2} + q^{1/4}R^{1/2}L\big) \\
&= O\big(RL^{-1/2}(\log L)^{1/2} + q^{1/4}R^{1/2}L\big).
\end{aligned}$$

We now choose $L = \lfloor R^{1/3}q^{-1/6}(\log q)^{1/3} \rfloor$; thus (5.1) is satisfied, provided that q is large enough which implies the desired estimate. ■

We remark that Theorem 5.1 is nontrivial if $R \geq q^{1/2+\varepsilon}$ for a fixed $\varepsilon > 0$ (we recall that the largest possible value of R is of order q).

Now using the standard reduction between complete and incomplete sums, see [3, Section 12.2], we obtain the following corollary.

Corollary 5.2 *For any $N \leq R$, we have, $S_P(N) = O(R^{5/6}q^{1/12}(\log q)^{4/3})$.*

https://doi.org/10.4153/CMB-2011-126-x Published online by Cambridge University Press

6 Comments

In principle, our approach works for sums of multiplicative characters of arbitrary order $d \mid q-1$. In this case, Lemma 3.3 needs some obvious adjustments. Furthermore, the set $\mathcal{L}$ in the proof of Theorem 5.1 must be chosen to consist of primes $\ell \equiv \pm 1 \pmod{d}$, so (5.4) still holds. For any fixed d the final result is the same, however its strength diminishes as d grows, and, for example, for characters of order $q-1$ leads only to a trivial estimate. Although we do not see any immediate cryptographic significance of such a result, obtaining nontrivial estimates of character sums with arbitrary multiplicative characters is a natural and interesting question. A related open question is obtaining nontrivial estimates on similar sums of additive characters of $\mathbb{F}_q$. In this case, there is no natural analogue of (5.4) and thus our approach does not apply at all.

Finally, we mention an algorithmic question which can be of cryptographic relevance. Given a black box which for every integer n outputs $\chi(\Psi_n(P))$, the question is to recover the "hidden" point P. This admits several modifications depending on whether the curve E and the field $\mathbb{F}_q$ are known or not. This question is analoguous to the more studied cryptographic problem of recovering a hidden polynomial $f(X) \in \mathbb{F}_q[X]$ given a black box which outputs $\chi(f(n))$; see [7] and the references therein.

Acknowledgement The authors would like to thank Kristin Lauter who brought them together and stimulated their joint work on this paper. The authors are also grateful to the Fields Institute for its support and stimulating atmosphere which led to the initiation of this work at the Fields Cryptography Retrospective Meeting, Toronto, May 2009.

References

[1] Z. Chen, *Elliptic curve analogue of Legendre sequences.* Monatsh. Math. **154**(2008), no. 1, 1–10. http://dx.doi.org/10.1007/s00605-008-0520-x

[2] G. Everest, A. J. van der Poorten, I. E. Shparlinski, and T. Ward, *Recurrence Sequences.* Mathematical Surveys and Monographs 104. American Mathematical Society, Providence, RI, 2003.

[3] H. Iwaniec and E. Kowalski, *Analytic Number Theory.* American Mathematical Society Colloquium Publications 53. American Mathematical Society, Providence, RI, 2004.

[4] D. R. Kohel and I. E. Shparlinski, *On exponential sums and group generators for elliptic curves over finite fields.* Lecture Notes in Comput. Sci. 1838, Springer, Berlin, 2000, pp. 395–404.

[5] K. E. Lauter and K. E. Stange, *The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences.* Lecture Notes in Comput. Sci. 5381, Springer-Verlag, Berlin, 2009, pp. 309–327.

[6] M. Perret, *Multiplicative character sums and Kummer coverings.* Acta Arith. **59**(1991), no. 3, 279–290.

[7] A. C. Russell and I. E. Shparlinski, *Classical and quantum function reconstruction via character evaluation.* J. Complexity **20**(2004), no. 2-3, 404–422. http://dx.doi.org/10.1016/j.jco.2003.08.019

[8] I. E. Shparlinski, *Distribution of nonresidues and primitive roots in recurrent sequences.* Mat. Zametki **24**(1978), no. 5, 603–613, 733, (in Russian).

[9] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Second edition. Graduate Texts in Mathematics 106. Springer, Dordrecht, 2009.

[10] ———, *p-adic properties of division polynomials and elliptic divisibility sequences.* Math. Ann. **332**(2005), no. 2, 443–471. http://dx.doi.org/10.1007/s00208-004-0608-0

https://doi.org/10.4153/CMB-2011-126-x Published online by Cambridge University Press

[11] C. Swart, *Elliptic Curves and Related Sequences.* Ph.D. thesis, Royal Holloway and Bedford New College, University of London, 2003.

[12] M. Ward, *Memoir on elliptic divisibility sequences.* Amer. J. Math. **70**(1948), 31–74. http://dx.doi.org/10.2307/2371930

Department of Computing, Macquarie University, North Ryde, Sydney, NSW 2109, Australia
e-mail: igor.shparlinski@mq.edu.au

Department of Mathematics, Stanford University, Stanford, CA 94305, USA
e-mail: stange@pims.math.ca

https://doi.org/10.4153/CMB-2011-126-x Published online by Cambridge University Press