Canad. J. Math. Vol. **57** (2), 2005 pp. 338–350

Certain Exponential Sums and Random Walks on Elliptic Curves

Tanja Lange and Igor E. Shparlinski

Abstract. For a given elliptic curve $\mathbf{E}$, we obtain an upper bound on the discrepancy of sets of multiples z_sG where z_s runs through a sequence $\mathcal{Z} = (z_1, \dots, z_T)$ such that $kz_1, \dots, kz_T$ is a permutation of $z_1, \dots, z_T$, both sequences taken modulo t, for sufficiently many distinct values of k modulo t.

We apply this result to studying an analogue of the power generator over an elliptic curve. These results are elliptic curve analogues of those obtained for multiplicative groups of finite fields and residue rings.

1 Introduction

We denote by $\mathbb{Z}_m$ the residue ring modulo an integer $m \geq 1$ and by $\mathcal{U}_m$ the group of units of this ring, that is, the collection of residue classes which are relatively prime to m. We identify $\mathbb{Z}_m$ with the set $\{0, 1, \dots, m-1\}$. For $q = p^\gamma$ a power of a prime p, let $\mathbb{F}_q$ denote the finite field of q elements.

As in [6, 7], we say a sequence $\mathcal{Z} = (z_1, \dots, z_T)$ of T elements from $\mathbb{Z}_t$ is $\mathcal{K}$*-invariant* if there exists a set $\mathcal{K} \subseteq \mathcal{U}_t$ such that the sequence $kz_1, \dots, kz_T$, taken modulo t, is a permutation of the original sequence $z_1, \dots, z_T$ for each $k \in \mathcal{K}$.

Let $\mathbf{E}$ be an elliptic curve over $\mathbb{F}_q$, given by an affine *Weierstraß equation* of the form

$$Y^2 + (a_1X + a_3)Y = X^3 + a_2X^2 + a_4X + a_6,$$

with coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$, such that the partial derivatives $a_1Y - 3X^2 - a_2X - a_4$ and $2Y + a_1X + a_3$ do not vanish simultaneously at points of the curve $(x, y) \in \mathbf{E}(\overline{\mathbb{F}}_q)$ over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, see [2, 27]. We put $h(X) = a_1X + a_3$ and $f(X) = X^3 + a_2X^2 + a_4X + a_6$, thus the Weierstraß equation becomes

$$Y^2 + h(X)Y - f(X) = 0.$$

For $p > 2$ one can always take $h = 0$ and for $p > 3$ also $a_2 = 0$; for $p = 2$ at least one of a_1, a_3 must be nonzero.

It is known, see [2, 27], that the set $\mathbf{E}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of $\mathbf{E}$ forms an *Abelian group* under an appropriate composition rule, which we call *addition* and denote $\oplus$, and with the point at infinity $\mathcal{O}$ as the neutral element. Thus, given a point $Q \in \mathbf{E}(\mathbb{F}_q)$ and an integer z we write zQ for the sum of z copies of Q. We also recall that

$$|\#\mathbf{E}(\mathbb{F}_q) - q - 1| \leq 2q^{1/2},$$

Received by the editors February 4, 2003; revised September 1, 2004.
AMS subject classification: Primary: 11L07, 11T23, 11T71; secondary: 14H52, 94A60.

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

where $\#\mathbf{E}(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points, including the point at infinity $\mathcal{O}$. Given a point $Q \in \mathbf{E}(\mathbb{F}_q)$ with $Q \neq \mathcal{O}$ we denote by $x(Q)$ and $y(Q)$ its affine components, $Q = \big(x(Q), y(Q)\big)$.

Let $G \in \mathbf{E}(\mathbb{F}_q)$ be a point of order t, that is, t is the size of the cyclic group $\langle G \rangle$ generated by G.

Let us denote by $\mathcal{X}$ the set of all *additive characters* χ of $\mathbb{F}_q$. It is useful to recall that $\mathcal{X}$ consists of the functions $\chi_a(z) = \exp(2\pi i \operatorname{Tr}(az)/p)$, where $a \in \mathbb{F}_q$ and

$$\operatorname{Tr}(u) = \sum_{j=0}^{\gamma-1} u^{p^j}$$

is the trace of $u \in \mathbb{F}_q = \mathbb{F}_{p^\gamma}$ in $\mathbb{F}_p$, see[21]. The character χ_0 is called the *trivial character*. Accordingly, we denote by $\mathcal{X}^*$ the set of all *nontrivial additive characters*.

For an additive character χ of $\mathbb{F}_q$, we consider exponential sums

$$S_{\mathcal{Z}}(\mathbf{E}, G, \chi) = \sum_{s=1}^{T} \chi\left(x(z_s G)\right)$$

with a sequence $\mathcal{Z} = (z_1, \dots, z_T)$ of nonzero elements of $\mathbb{Z}_t$ (thus $z_s G \neq \mathcal{O}$ and $x(z_s G)$ is always defined). If $\mathcal{Z}$ is $\mathcal{K}$-invariant for a sufficiently large set $\mathcal{K}$, we obtain an upper bound on these sums which is analogous to those of [6, 7] obtained for multiplicative groups of residue rings and finite fields, that is, for character sums with g^{z_s}, where g is a fixed element of multiplicative order t. Similar results can also be obtained for sums with $y(z_s G)$, or more generally with linear combinations $ax(z_s G) + by(z_s G)$.

We apply our results to studying the distribution of the *power generator* on elliptic curves. Namely, given a point $G \in \mathbf{E}(\mathbb{F}_q)$ of order t, we fix an integer e with $\gcd(e, t) = 1$, put $W_0 = G$ and consider the sequence

$$W_n = eW_{n-1}, \quad n = 1, 2, \dots. \tag{1}$$

In a more explicit form we have $W_n = e^n G$. Traditionally this generator has been considered over residue rings, thus producing sequences of the form g^{e^n}, see [3, 17, 22]. However, recently elliptic curve analogues of several pseudo random number generators have been considered, see [1, 4, 10, 11, 14, 15, 18, 24, 26]. Here we obtain some analogues of the results of [6, 7, 9] and show that the sequence (1) is rather uniformly distributed, provided t and the multiplicative order T of e modulo t are large enough.

Our approach follows the path of [6], and thus relates exponential sums $S_{\mathcal{Z}}(\mathbf{E}, G, \chi)$ to certain exponential sums with rational functions of controlled degree. However, studying when these rational functions degeneralise takes significantly more effort than in the case of [6] (where this issue does not cause any complications at all). In particular, we must study linear combinations of *division polynomials* on elliptic curves. We also remark that some of the parameters involved in this method behave differently compared to [6], so we must optimize them in a different way which in turn leads to a different bound.

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

We also show that our basic arguments combined with some modifications of the approach of [12, 25] lead to a lower bound on the linear complexity of the sequence (1).

We recall that the *linear complexity* of an infinite sequence u_n of a ring $\mathcal{R}$ is the length s of the shortest linear recurrence relation

$$u_{n+s} = a_{s-1}u_{n+s-1} + \cdots + a_0 u_n, \quad n = 0, 1, \ldots, \tag{2}$$

with $a_0, \ldots, a_{s-1} \in \mathcal{R}$, which is satisfied by this sequence, see [3, 22].

The sequence (1) as well as other sequences from the aforementioned works present an attempt to imitate a "random walk" on an elliptic curve. Certainly cryptography could be one of the main "consumers" of such streams of random, or pseudo random, points. Other transformations $\mathcal{T}$ of points on $\mathbf{E}$ can be considered, which can be iterated to generate sequences of points of the form $V_n = \mathcal{T}(V_{n-1})$, $n = 1, 2, \ldots$, that may lead to a number of new interesting number theoretic questions as well as to new useful cryptographic constructions. These constructions can also be generalized to Jacobians of larger genus curves and more general algebraic varieties.

Throughout the paper, the implied constants in the symbols "O", "$\ll$" and "$\gg$" may sometimes depend on the integer parameter $\nu \geq 1$ and are absolute otherwise (we recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$).

2 Preparations

We start with the following simple statement which is Lemma 2 of [6].

Lemma 1 *For any set $\mathcal{K} \subseteq \mathcal{U}_t$ of cardinality $K = \#\mathcal{K}$, any fixed $\delta > 0$ and any integer $J \geq t^\delta$ there exists an integer $r \in \mathcal{U}_t$ such that the congruence*

$$rk \equiv j \pmod{t}, \quad k \in \mathcal{K}, \ 1 \leq j \leq J-1,$$

has $M_r(J) \gg JK/t$ solutions.

We also need some properties of division polynomials on elliptic curves (for more details see for example [2, 19, 23, 27].)

We put $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, and $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

The *division polynomials* $\psi_m(X,Y) \in \mathbb{F}_q[X,Y]/(Y^2 + h(X)Y - f(X))$, $m \geq 0$, are recursively defined by the relations

$$\begin{aligned}
\psi_0 = 0, \ \psi_1 = 1, \ \psi_2 &= 2Y + h(X), \\
\psi_3 &= 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8, \\
\psi_4 &= (2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 \\
&\quad + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2))\psi_2, \\
\psi_{2k+1} &= \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3, \quad k \geq 2, \\
\psi_{2k} &= \psi_k(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2)/\psi_2, \quad k \geq 3.
\end{aligned}$$

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

If q is even or both q and m are odd then $\psi_m(X,Y) \in \mathbb{F}_q[X]$ is univariate and $\psi_m(X,Y) \in \psi_2(X,Y)\mathbb{F}_q[X]$ if q is odd and m is even. Therefore, as $\psi_2^2(X,Y) = 4f(X) + h^2(X)$, we have $\psi_m^2(X,Y), \psi_{m-1}(X,Y)\psi_{m+1}(X,Y) \in \mathbb{F}_q[X]$. In particular, we may write $\psi_{2k+1}(X)$ and $\psi_m^2(X)$.

The division polynomials can be used to state multiples of a point. Let $Q = (x,y) \neq \mathcal{O}$, then the first coordinate of mQ is given by

$$x(mQ) = \frac{\theta_m(x)}{\psi_m^2(x)}, \qquad \text{where } \theta_m(X) = X\psi_m^2 - \psi_{m-1}\psi_{m+1}.$$

The zeros of the denominator $\psi_m^2(X)$ are exactly the first coordinates of the nontrivial m-torsion points, that is, the points $Q = (x,y) \in \overline{\mathbb{F}_q}^2$ on $\mathbf{E}$ with $mQ = \mathcal{O}$. Note, that these points occur in pairs $Q = (x,y)$ and $-Q = (x, -h(x) - y)$, which coincide only if $2Q = \mathcal{O}$, that is, if x is a zero of $\psi_2^2(X)$.

We recall that the group of m-torsion points $\mathbf{E}[m]$, for an elliptic curve $\mathbf{E}$ defined over a field of characteristic p, is isomorphic to $\mathbb{Z}_m^2$ if $p \nmid m$.

If m is a power of p then $\mathbf{E}[m]$ is either isomorphic to $\mathbb{Z}_m$ or to $\{\mathcal{O}\}$. In the second case the curve is called supersingular, otherwise non-supersingular or ordinary.

On supersingular curves the discrete logarithm problem is much weaker than on ordinary curves, and thus these may probably introduce some weaknesses in the pseudo random number generator (1) too. In the sequel, we therefore concentrate only on the non-supersingular curves.

By induction one can show that $\theta_m(X) \in \mathbb{F}_q[X]$ is monic of degree $\deg \theta_m = m^2$.

Lemma 2 *Let* $\mathbf{E}$ *be a non-supersingular elliptic curve defined over* $\mathbb{F}_q$*. For any integer* d *we have that there exists at least one point* $Q \in \mathbf{E}\left(\overline{\mathbb{F}}_q\right)$ *of exact order* d*.*

Proof Let $d = d_0 p^j$ with integers $j \geq 0$ and $\gcd(d_0, p) = 1$. For an integer $m = m_0 p^i$ with integers $i \geq 0$ and $\gcd(m_0, p) = 1$, there are $M_m = m_0^2 p^i$ points of order dividing m. Thus for the number N_d of points of exact order d, by the inclusion-exclusion principle, we have

$$N_d = \sum_{m|d} \mu\left(\frac{d}{m}\right) M_m = \sum_{m_0|d_0} \sum_{i=0}^{j} \mu\left(\frac{d}{m_0 p^i}\right) m_0^2 p^i,$$

where $\mu(k)$ is the Möbius function.

If $j = 0$, thus $d = d_0$, $m = m_0$ in the above sums, we obtain

$$\begin{aligned} N_d &= \sum_{m|d} \mu\left(\frac{d}{m}\right) m^2 = d^2 \sum_{m|d} \mu\left(\frac{d}{m}\right)\left(\frac{m}{d}\right)^2 \\ &= d^2 \sum_{m|d} \frac{\mu(m)}{m^2} = d^2 \prod_{\substack{\ell|d \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell^2}\right). \end{aligned}$$

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

If $j \geq 1$, only the terms with $i = j$ and $i = j - 1$ are present in the above sum. Hence,

$$\begin{aligned} N_d &= \sum_{m_0 | d_0} \Bigl(\mu\Bigl(\frac{d}{m_0 p^j}\Bigr) m_0^2 p^j + \mu\Bigl(\frac{d}{m_0 p^{j-1}}\Bigr) m_0^2 p^{j-1} \Bigr) \\ &= \sum_{m_0 | d_0} \Bigl(\mu\Bigl(\frac{d_0}{m_0}\Bigr) m_0^2 p^j + \mu\Bigl(\frac{d_0 p}{m_0}\Bigr) m_0^2 p^{j-1} \Bigr) \\ &= \sum_{m_0 | d_0} \Bigl(\mu\Bigl(\frac{d_0}{m_0}\Bigr) m_0^2 p^j - \mu\Bigl(\frac{d_0}{m_0}\Bigr) m_0^2 p^{j-1} \Bigr) \\ &= \bigl(p^j - p^{j-1}\bigr) \sum_{m_0 | d_0} \mu\Bigl(\frac{d_0}{m_0}\Bigr) m_0^2 = d_0^2 \bigl(p^j - p^{j-1}\bigr) \prod_{\substack{\ell | d_0 \\ \ell \text{ prime}}} \Bigl(1 - \frac{1}{\ell^2}\Bigr). \end{aligned}$$

Thus in each case $N_d > 0$. ■

The following statement deals with linear combinations of multiples of a point G. It is similar to Lemma 6 of [26] (which treats the special case of $D < p = q$). In fact the degree bounds are straightforward, only the non-vanishing of the polynomials is not immediately obvious.

Lemma 3 *Fix integers $1 \leq d_1 < \cdots < d_s \leq D$ and fix elements $c_1, \dots, c_s \in \mathbb{F}_q$ with $c_s \neq 0$. Let $\mathbf{E}$ be a non-supersingular elliptic curve defined over $\mathbb{F}_q$. Let us consider the following rational function*

$$L(X) = \sum_{i=1}^{s} c_i \frac{\theta_{d_i}(X)}{\psi_{d_i}^2(X)} \in \mathbb{F}_q(X).$$

There are nonzero polynomials $H_1, H_2 \in \mathbb{F}_q[X]$ with $\deg H_1, \deg H_2 < sD^2$ such that

$$L(X) = \frac{H_1(X)}{H_2(X)}.$$

Furthermore, $L(X)$ has a pole of multiplicity one.

Proof We have

$$L(X) = \sum_{i=1}^{s} c_i \frac{\theta_{d_i}(X)}{\psi_{d_i}^2(X)} = \frac{H_1(X)}{\psi_{d_1}^2(X) \dots \psi_{d_s}^2(X)} = \frac{H_1(X)}{H_2(X)}.$$

Obviously,

$$\deg H_1 \leq d_s^2 + \sum_{i=1}^{s-1} (d_i^2 - 1) < sD^2 \quad \text{and} \quad 0 < \deg H_2 = \sum_{i=1}^{s} (d_i^2 - 1) < sD^2.$$

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

By Lemma 2 there exists a point $Q \in \mathbf{E}(\overline{\mathbb{F}}_q)$ of exact order d_s. Then $\theta_{d_s}(X)/\psi^2_{d_s}(X)$ has a pole at $x(Q)$, while none of the other $\theta_{d_i}(X)/\psi^2_{d_i}(X)$, $1 \le i < s$, can have a pole there. Hence, $L(X)$ has a pole at $x(Q)$ and hence it cannot be constant on $\mathbf{E}$. Moreover, this pole is of multiplicity one. ■

We also need the following upper bound which is a special partial case of Corollary 1 of [16].

Lemma 4 *Let $\mathbf{E}$ be a non-supersingular elliptic curve defined over $\mathbb{F}_q$. Let $f(X)$ be a rational function of degree N having a pole of multiplicity one. Then the bound*

$$\max_{\chi \in \mathcal{X}^*} \Bigl| \sum_{\substack{Q \in \mathcal{H} \\ f(x(Q)) \neq \infty}} \chi(f(x(Q))) \Bigr| = O\left(N q^{1/2}\right)$$

holds, where $\mathcal{H}$ is an arbitrary subgroup of $\mathbf{E}(\mathbb{F}_q)$.

In particular, Lemma 3 and Lemma 4 imply the following result which forms the basis of our arguments.

Corollary 5 *Fix integers $1 \le d_1 < \cdots < d_s \le D$ and fix $c_1, \ldots, c_s \in \mathbb{F}_q$ with $c_s \neq 0$. Let $\mathbf{E}$ be a non-supersingular elliptic curve defined over $\mathbb{F}_q$. Then the following bound holds:*

$$\max_{\chi \in \mathcal{X}^*} \Bigl| \sum_{\substack{Q \in \mathcal{H} \\ Q \neq \mathcal{O}}} \chi\Bigl(\sum_{i=1}^{s} c_i x(d_i Q)\Bigr) \Bigr| = O\left(s D^2 q^{1/2}\right),$$

where $\mathcal{H}$ is an arbitrary subgroup of $\mathbf{E}(\mathbb{F}_q)$ of order $t = \#\mathcal{H}$ such that

$$\gcd(t, d_1 \ldots d_s) = 1.$$

Finally, we need the following simple statement:

Lemma 6 *Let a sequence u_n, $n = 0, 1, \ldots$, satisfy a linear recurrence relation of the form (2) over $\mathbb{F}_q$. Then for any $s+1$ pairwise distinct non-negative integers $h_1, \ldots, h_{s+1}$, there exist $c_1, \ldots, c_{s+1} \in \mathbb{F}_q$, not all equal to zero, such that*

$$\sum_{i=1}^{s+1} c_i u_{n+h_i} = 0, \qquad n = 0, 1, \ldots .$$

Proof The set of all solutions of any linear recurrence relation over any field $\mathbb{F}$ is a vector space of dimension s over $\mathbb{F}$, for example, see Chapter 8 of [21]. Therefore, any $s + 1$ solutions are linearly dependent. In particular, the $s + 1$ sequences $u_{n+h_1}, \ldots, u_{n+h_{s+1}}$, $n = 0, 1, \ldots$, are linearly dependent. ■

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

3 Main Result

The following bound is an analogue of Lemma 4 of [6]. Accordingly our proof follows along the same lines as that of [6]. However, the proof is also based on the results of Section 2 which are new and use special properties of elliptic curves. Thus the final result is different.

Theorem 7 *Let $\mathcal{Z} = (z_1, \dots, z_T)$ be a $\mathcal{K}$-invariant sequence of nonzero elements of $\mathbb{Z}_t$ with respect to the set $\mathcal{K} \subseteq \mathcal{U}_t$ of cardinality $K = \#\mathcal{K}$ and let N be the number of solutions of the congruence $z_r \equiv z_s \pmod t$, $1 \le r, s \le T$. Let $\mathbf{E}$ be a non-supersingular elliptic curve defined over $\mathbb{F}_q$. Let $G \in \mathbf{E}(\mathbb{F}_q)$ be of order $t \ge q^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$. Then for any integer $\nu \ge 1$ the following bound holds:*

$$\max_{\chi \in \mathcal{X}^*} |S_{\mathcal{Z}}(\mathbf{E}, G, \chi)| \ll N^{1/2\nu} T^{1-1/\nu} t^{(\nu+1)/\nu(\nu+2)} K^{-1/(\nu+2)} q^{1/4(\nu+2)}.$$

Proof Fix some $\varepsilon > 0$ and put

$$J = \left\lceil t^{(\nu+1)/(\nu+2)} K^{-\nu/(\nu+2)} q^{-1/2(\nu+2)} \right\rceil.$$

In this case $J \ge t^{1/(\nu+2)} q^{-1/2(\nu+2)} \ge q^{\varepsilon/(\nu+2)}$, thus Lemma 1 applies.

We select r as in Lemma 1. Let $\mathcal{M}$ denote the subset of $\mathcal{K}$ which satisfies the corresponding congruence and let $M = \#\mathcal{M}$.

Define $R(u)$ as the number of elements $z \in \mathcal{Z}$ with $z \equiv u \pmod t$. Note that

$$\sum_{u \in \mathcal{U}_t} R(u) = T \quad \text{and} \quad \sum_{u \in \mathcal{U}_t} R(u)^2 = N.$$

We also have $R(ku) = R(u)$ for any $k \in \mathcal{K}$ since repetitions in $\mathcal{Z}$ are preserved under the permutation of $\mathcal{Z}$ generated by multiplication by $k \in \mathcal{K}$. Therefore

$$\begin{aligned} S_{\mathcal{Z}}(\mathbf{E}, G, \chi) &= \sum_{u \in \mathcal{U}_t} R(u) \chi\left(x(uG)\right) = \frac{1}{M} \sum_{k \in \mathcal{M}} \sum_{u \in \mathcal{U}_t} R(ku) \chi\left(x(kuG)\right) \\ &= \frac{1}{M} \sum_{k \in \mathcal{M}} \sum_{u \in \mathcal{U}_t} R(u) \chi\left(x(kuG)\right) = \frac{1}{M} \sum_{u \in \mathcal{U}_t} R(u) \sum_{k \in \mathcal{M}} \chi\left(x(kuG)\right). \end{aligned}$$

By the Hölder inequality we have

$$\begin{aligned} |S_{\mathcal{Z}}(\mathbf{E}, G, \chi)|^{2\nu} &\le M^{-2\nu} \Big(\sum_{u \in \mathcal{U}_t} R(u) \Big| \sum_{k \in \mathcal{M}} \chi\left(x(kuG)\right) \Big| \Big)^{2\nu} \\ &= M^{-2\nu} \Big(\sum_{u \in \mathcal{U}_t} \Big(R(u)^2 \Big)^{1/2\nu} R(u)^{(\nu-1)/\nu} \Big| \sum_{k \in \mathcal{M}} \chi\Big(x(kuG) \Big) \Big| \Big)^{2\nu} \\ &\le M^{-2\nu} \Big(\sum_{u \in \mathcal{U}_t} R(u)^2 \Big) \Big(\sum_{u \in \mathcal{U}_t} R(u) \Big)^{2\nu-2} \sum_{u \in \mathcal{U}_t} \Big| \sum_{k \in \mathcal{M}} \chi\Big(x(kuG) \Big) \Big|^{2\nu} \\ &= M^{-2\nu} N T^{2\nu-2} \sum_{u \in \mathcal{U}_t} \Big| \sum_{k \in \mathcal{M}} \chi(x(kuG)) \Big|^{2\nu}. \end{aligned}$$

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

Let $\mathcal{G} = \langle G \rangle$ be the cyclic group generated by G and let $\mathcal{G}^* = \mathcal{G} \backslash \mathcal{O}$. Then,

$$\begin{aligned}
\sum_{u \in \mathcal{U}_t} \Big| \sum_{k \in \mathcal{M}} \chi\left(x(kuG)\right) \Big|^{2\nu} &\leq \sum_{u=1}^{t-1} \Big| \sum_{k \in \mathcal{M}} \chi\left(x(kuG)\right) \Big|^{2\nu} \\
&\leq \sum_{l_1,\dots,l_\nu \in \mathcal{M}} \sum_{k_1,\dots,k_\nu \in \mathcal{M}} \sum_{Q \in \mathcal{G}^*} \chi\Big(\sum_{i=1}^{\nu} \left(x\left(l_i Q\right) - x\left(k_i Q\right)\right)\Big) \\
&\leq \sum_{l_1,\dots,l_\nu \in \mathcal{M}} \sum_{k_1,\dots,k_\nu \in \mathcal{M}} \sum_{Q \in \mathcal{G}^*} \chi\Big(\sum_{i=1}^{\nu} \left(x\left(rl_i Q\right) - x\left(rk_i Q\right)\right)\Big)
\end{aligned}$$

because $\gcd(r,t) = 1$. For the case that $(k_1, \dots, k_\nu)$ is a permutation of $(l_1, \dots, l_\nu)$, we must use the trivial bound and this gives a contribution $O\left(M^\nu t\right)$. In case this does not happen (there are at most $M^{2\nu}$ ways), the inner sum above is a character sum with a rational function of degree at most $2\nu J^2$. By Corollary 5 each of these terms contributes at most $O\left(J^2 q^{1/2}\right)$. Thus

$$\begin{aligned}
\left|S_{\mathcal{Z}}(\mathbf{E}, G, \chi)\right|^{2\nu} &\ll M^{-2\nu} N T^{2\nu-2}\left(M^\nu t + M^{2\nu} J^2 q^{1/2}\right) \\
&= N T^{2\nu-2}\left(M^{-\nu} t + J^2 q^{1/2}\right)
\end{aligned}$$

and so

$$S_{\mathcal{Z}}(\mathbf{E}, G, \chi) \ll N^{1/2\nu} T^{1-1/\nu}\left(M^{-1/2} t^{1/2\nu} + J^{1/\nu} q^{1/4\nu}\right).$$

By Lemma 1 we have $M \gg JK/t$ thus

$$S_{\mathcal{Z}}(\mathbf{E}, G, \chi) \ll N^{1/2\nu} T^{1-1/\nu}\left(t^{(\nu+1)/2\nu} K^{-1/2} J^{-1/2} + J^{1/\nu} q^{1/4\nu}\right).$$

Substituting the chosen value of J, after simple calculations we obtain the stated result. ■

In the most interesting case when

$$\ln K \sim \ln N \sim \ln T \sim \ln t$$

the bound of Theorem 7, taken with $\nu = 1$, yields

$$\max_{\chi \in \mathcal{X}^*} \left|S_{\mathcal{Z}}(\mathbf{E}, G, \chi)\right| \ll t^{5/6+o(1)} q^{1/12},$$

which is nontrivial for $t \geq q^{1/2+\varepsilon}$.

In another interesting special case when $\mathcal{Z}$ is a subgroup of $\mathcal{U}_t$ we can select $\mathcal{K} = \mathcal{Z}$, so we have $N = K = T$, and the bound of Theorem 7 takes the form

$$\max_{\chi \in \mathcal{X}^*} \left|S_{\mathcal{Z}}(\mathbf{E}, G, \chi)\right| \ll T^{1-(3\nu+2)/2\nu(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)}. \tag{3}$$

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

One easily verifies that if $T \geq t^{2/3}q^{1/6+\varepsilon}$ and $t \geq q^{1/2+\varepsilon}$, then taking sufficiently large ν, makes the bound (3) nontrivial. To see this, it is enough to remark that

$$T^{-(3\nu+2)/2\nu(\nu+2)}t^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)} = \left(T^{-1}t^{\alpha_\nu}q^{\beta_\nu}\right)^{(3\nu+2)/2\nu(\nu+2)},$$

where

$$\alpha_\nu = \frac{2}{3}\left(1+\frac{1}{3\nu+2}\right) \quad \text{and} \quad \beta_\nu = \frac{1}{6}\left(1-\frac{2}{3\nu+2}\right).$$

4 Power Generator on Elliptic Curves

Let $\mathbf{E}$ be a non-supersingular elliptic curve defined over $\mathbb{F}_q$ and let $G \in \mathbf{E}(\mathbb{F}_q)$ be of order t.

Let W_n, $n = 0, 1, \dots$, be a sequence generated by (1). It is clear that this sequence is periodic with period T which is the multiplicative order of e modulo t.

Fix a basis $\{\omega_1, \dots, \omega_\gamma\}$ of $\mathbb{F}_q = \mathbb{F}_{p^\gamma}$ over $\mathbb{F}_p$. For two integer vectors $\alpha = (\alpha_1, \dots, \alpha_\gamma)$ and $\beta = (\beta_1, \dots, \beta_\gamma)$ with $0 \leq \alpha_i < \beta_i < p$, $i = 1, \dots, \gamma$, we consider the box

$$B_{[\alpha,\beta)} = \{\xi \in \mathbb{F}_q \mid \xi = \xi_1\omega_1 + \cdots + \xi_\gamma\omega_\gamma,\ \xi_i \in [\alpha_i, \beta_i),\ 1 \leq i \leq \gamma\}$$

of volume

$$\operatorname{volm} B_{[\alpha,\beta)} = \prod_{i=1}^{\gamma}(\beta_i - \alpha_i)$$

and denote by $N(\alpha, \beta)$ the number of points W_n, $n = 0, \dots, T-1$, satisfying $x(W_n) \in B_{[\alpha,\beta)}$.

Let $\mathcal{B}$ denote the set of all such boxes $B_{[\alpha,\beta)}$.

We now denote by $\Delta_e(\mathbf{E}, G)$ the largest deviation of $N(\alpha, \beta)$ from its expected values, that is,

$$\Delta_e(\mathbf{E}, G) = \sup_{B_{[\alpha,\beta)} \in \mathcal{B}} \left| N(\alpha, \beta) - \frac{\operatorname{volm} B_{[\alpha,\beta)}}{q} T \right|.$$

Theorem 8 *Let $\mathbf{E}$ be a non-supersingular elliptic curve defined over $\mathbb{F}_q$. Then for any integer $\nu \geq 1$, the following bound holds:*

$$\Delta_e(\mathbf{E}, G) \ll T^{1-(3\nu+2)/2\nu(\nu+2)}t^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)}(\ln p + 1)^\gamma.$$

Proof We have

$$\sum_{\chi \in \mathcal{X}} \chi(\xi) = \begin{cases} 0 & \text{if } \xi = 0, \\ q & \text{if } \xi \in \mathbb{F}_q^*. \end{cases}$$

Therefore

$$\begin{aligned} N(\alpha, \beta) &= \frac{1}{q}\sum_{n=0}^{T-1}\sum_{\xi \in B_{[\alpha,\beta)}}\sum_{\chi \in \mathcal{X}} \chi(x(W_n) - \xi) \\ &= \frac{1}{q}\sum_{\chi \in \mathcal{X}}\sum_{n=0}^{T-1}\chi(x(W_n)) \sum_{\xi \in B_{[\alpha,\beta)}} \chi(-\xi). \end{aligned}$$

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

Separating the term T volm $B_{[\alpha,\beta)}/q$, corresponding to χ_0 we derive

$$\left|N(\alpha,\beta) - \frac{\text{volm}\, B_{[\alpha,\beta)}}{q}T\right| \le \frac{1}{q}\sum_{\chi\in\mathcal{X}^*}\left|\sum_{n=0}^{T-1}\chi(x(W_n))\right|\left|\sum_{\xi\in B_{[\alpha,\beta)}}\chi(\xi)\right|.$$

We remark that the set $\mathcal{Z} = \{1, e, \dots, e^{T-1}\}$ is a subgroup of $\mathcal{U}_t$, thus the bound (3) applies to the first sum. Hence, for any integer $\nu \ge 1$,

$$\left|N(\alpha,\beta) - \frac{\text{volm}\, B_{[\alpha,\beta)}}{q}T\right| \le T^{1-(3\nu+2)/2\nu(\nu+2)}t^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)}$$
$$\times\frac{1}{q}\sum_{\chi\in\mathcal{X}^*}\left|\sum_{\xi\in B_{[\alpha,\beta)}}\chi(\xi)\right|.$$

Using this bound and then the inequality

$$\sum_{\chi\in\mathcal{X}}\left|\sum_{\xi\in B_{[\alpha,\beta)}}\chi(\xi)\right| \le q(1+\ln p)^{\gamma}$$

(see [5] or [28, Lemma 6]), we finish the proof. ■

Let $\mathcal{L}_e(\mathbf{E}, G)$ denote the linear complexity of the sequence $x(W_n)$, $n = 0, 1, \dots,$ given by (1).

Theorem 9 *Let* $\mathbf{E}$ *be a non-supersingular elliptic curve defined over* $\mathbb{F}_q$*. Then the following bound holds:*

$$\mathcal{L}_e(\mathbf{E}, G) \gg Tt^{-2/3},$$

Proof Let $s = \mathcal{L}_e(\mathbf{E}, G)$.

Put $J = \lceil t^{1/3}\rceil$. Thus by Lemma 1, there exist $r \in \mathcal{U}_t$ and $M_r(J) \gg JT/t$ values of h, $0 \le h \le T-1$ and j, $0 \le j \le J-1$, with $re^h \equiv j \pmod t$. If $s \ge M_r(J)$, then the bound immediately follows.

Otherwise, for these values of r, let us fix any $s+1 \le M_r(J)$ such pairs (h, j) of them which we call (h_i, j_i), $i = 1, \dots, s+1$. By Lemma 6 we see that there exist $c_1, \dots, c_{s+1} \in \mathbb{F}_q$, not all equal to zero, such that

$$0 = \sum_{i=1}^{s+1} c_i W_{n+h_i} = \sum_{i=1}^{s+1} c_i x\left(e^{n+h_i}G\right) = \sum_{i=1}^{s+1} c_i x\left(e^{h_i}e^nG\right), \quad n = 0, 1, \dots.$$

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

Therefore, the equation

$$\sum_{i=1}^{s+1} c_i x\left(e^{h_i} Q\right) = 0, \qquad n = 0, 1, \dots$$

is satisfied by at least T points $Q \in \langle G \rangle$. Taking into account that for $r \in \mathcal{U}_t$, the map $Q \to rQ$ is a permutation on $\langle G \rangle$, we obtain that the equation

$$\sum_{i=1}^{s+1} c_i x\left(j_i Q\right) = \sum_{i=1}^{s+1} c_i x\left(r e^{h_i} Q\right) = 0, \qquad n = 0, 1, \dots$$

is satisfied by at least T points $Q \in \langle G \rangle$. Using Lemma 3 we derive

$$T \leq (s+1)(J-1)^2$$

which implies the desired result. ■

5 Remarks

We have already remarked that the sequence (1) is an elliptic curve analogue of the power generator in finite fields and residue rings. Unfortunately, as in that case, we do not know how to study the distribution of the s-tuples $(x(W_n), \dots, x(W_{n+s-1}))$, except for the case when e is small (for example $e = 2$), see [9].

Elliptic curve analogues of the more traditional linear congruential generator have been studied as well, see [1, 4, 10, 11, 14, 15, 18]. In this case, one selects a point $G \in \mathbf{E}(\mathbb{F}_q)$ of order t and an arbitrary initial value $U_0 \in \mathbf{E}(\mathbb{F}_q)$ and then computes

$$U_n = U_{n-1} \oplus G, \qquad n = 1, 2, \dots. \tag{4}$$

Thus one gets a sequence (4) of period t at the cost of one addition on $\mathbf{E}(\mathbb{F}_q)$ per point. Obtaining pseudo random points by using (1) is, generally, more expensive. However, for $e = 2$ the addition of distinct points in (4) is replaced by one point doubling. This operation is equally expensive in even characteristic and needs only one extra squaring in $\mathbb{F}_q$ for $p \geq 3$. Thus, provided that the order of 2 modulo t is large, the power generator offers a good alternative. Furthermore, in even characteristic to obtain $W_n = e^n Q$ directly, one can use explicit formulas [13] which save some operations.

There are several more natural questions about the sequence (1) which would be interesting to study. For example, in the case $q = p$, it would be desirable to show that for a random choice of the prime p, a curve $\mathbf{E}$, a point $G \in \mathbf{E}(\mathbb{F}_p)$, and an integer e, the period T of the sequence (1) is likely to be large, in particular, is likely to be above the nontriviality threshold of Theorem 8. For the classical power generator such results are provided by [8]. It seems that combining the upper bounds of [8] on the number of elements of small multiplicative order in "random" residue rings with the results of [20] on the distribution of the number of points on "random" elliptic curves, one can get such results.

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

References

[1] P. Beelen and J. Doumen, *Pseudorandom sequences from elliptic curves.* In: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer-Verlag, Berlin, 2002, pp. 7–52.

[2] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography.* London Math. Society Lecture Note Series 265, Cambridge University Press, 2000.

[3] T. W. Cusic, C. Ding, and A. Renvall, *Stream ciphers and number theory.* North-Holland, Amsterdam, 1998.

[4] E. El Mahassni and I. E. Shparlinski, *On the uniformity of distribution of congruential generators over elliptic curves.* In: Sequences and Their Applications, Springer-Verlag, London, 2002, pp. 257–264.

[5] H. Davenport and D. J. Lewis, *Character sums and primitive roots in finite fields.* Rend. Circ. Mat. Palermo (2) **12**(1963), 129–136.

[6] J. B. Friedlander, J. Hansen, and I. E. Shparlinski, *Character sums with exponential functions.* Mathematika **47**(2000), 75–85.

[7] J. B. Friedlander, S. V. Konyagin, and I. E. Shparlinski, *Some doubly exponential sums over $\mathbb{Z}_m$.* Acta Arith. **105**(2002), 349–370.

[8] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function.* Math. Comp. **70**(2001), 1591–1605 (see also **71**(2002), 1803–1806).

[9] J. B. Friedlander and I. E. Shparlinski, *On the distribution of the power generator.* Math. Comp. **70**(2001), 1575–1589.

[10] G. Gong, T. A. Berson, and D. R. Stinson, *Elliptic curve pseudo random sequence generators.* In: Selected Areas in Cryptography, Lecture Notes in Comput. Sci. 1758, Springer-Verlag, Berlin, 2000, pp. 34–49.

[11] G. Gong and C. C. Y. Lam, *Linear recursive sequences over elliptic curves.* In: Sequences and Their Applications, Springer, London, 2002, pp. 182–196.

[12] F. Griffin and I. E. Shparlinski, *On the linear complexity profile of the power generator.* IEEE Trans. Inform. Theory **46**(2000), 2159–2162.

[13] J. Guajardo and C. Paar, *Efficient algorithms for elliptic curve cryptosystems.* In: Advances in Cryptology—Crypto'97, Lect. Notes in Comput. Sci. 1294, Springer, Berlin, 1997, pp. 342–356.

[14] S. Hallgren, 'Linear congruential generators over elliptic curves', *Preprint CS-94-143*, Dept. of Comp. Sci., Cornegie Mellon Univ., 1994, 1–10.

[15] F. Hess and I. E. Shparlinski, *On the linear complexity and multidimensional distribution of congruential generators over elliptic curves.* Designs, Codes and Cryptography, (to appear).

[16] D. R. Kohel and I. E. Shparlinski, *Exponential sums and group generators for elliptic curves over finite fields.* In: Algorithmic Number Theory, Lecture Notes in Comput. Sci. 1838, Springer, Berlin, 2000, pp. 395–404.

[17] J. C. Lagarias, *Pseudorandom number generators in cryptography and number theory.* In: Cryptology and Computational Number Theory, Proc. Sympos. Appl. Math. 42, Amer. Math. Soc., Providence, RI, 1990, pp. 115–143.

[18] C. C. Y. Lam and G. Gong, *Randomness of elliptic curve sequences.* Research Report CORR 2002-18, Faculty of Mathematics, University of Waterloo, Waterloo, 2002, 1–11.

[19] S. Lang, *Elliptic curves: Diophantine analysis.* Grundlehren der Mathematischen Wissenschaften 231, Springer-Verlag, Berlin, 1978.

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

[21] R. Lidl and H. Niederreiter, *Finite fields.* Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997.

[22] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography.* CRC Press, Boca Raton, FL, 1997.

[23] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p.* Math. Comp. **44**(1985), 483–494.

[24] I. E. Shparlinski, *On the Naor–Reingold pseudo-random number function from elliptic curves.* Appl. Algebra Engrg. Comm. Comput. **11**(2000), 27–34.

[25] ———, *On the linear complexity of the power generator.* Des. Codes Cryptogr. **23**(2001), 5–10.

[26] I. E. Shparlinski and J. H. Silverman, *On the linear complexity of the Naor–Reingold pseudo-random function from elliptic curves.* Des. Codes Cryptogr. **24**(2001), 279–289.

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press

[27] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

[28] A. Winterhof, *Some estimates for character sums and applications.* Des. Codes Cryptogr. **22**(2001), 123–131.

Institute for Information Security and Cryptology
Ruhr-University of Bochum
D-44780 Bochum
Germany
e-mail: lange@itsc.ruhr-uni-bochum.de

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

https://doi.org/10.4153/CJM-2005-015-8 Published online by Cambridge University Press