On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields

David R. Kohel[1] and Igor E. Shparlinski[2]

[1] School of Mathematics and Statistics
University of Sydney, NSW 2006, Australia
kohel@maths.usyd.edu.au
[2] Department of Computing
Macquarie University, NSW 2109, Australia
igor@mpce.mq.edu.au

Abstract. In the paper an upper bound is established for certain exponential sums, analogous to Gaussian sums, defined on the points of an elliptic curve over a prime finite field. The bound is applied to prove the existence of group generators for the set of points on an elliptic curve over $\mathbb{F}_q$ among certain sets of bounded size. We apply this estimate to obtain a deterministic $O(q^{1/2+\varepsilon})$ algorithm for finding generators of the group in echelon form, and in particular to determine its group structure.

1 Introduction and Notations

Let $q = p^k$ be a prime power and let $\mathcal{E}$ be an elliptic curve over a finite field $\mathbb{F}_q$ of q elements given by a *Weierstrass* equation

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

The set $\mathcal{E}(\mathbb{F}_q)$ of points over $\mathbb{F}_q$, together with the point O at infinity as identity, forms an abelian group. The cardinality of $\mathcal{E}(\mathbb{F}_q)$ is N, where

$$|N - q - 1| \le 2q^{1/2}.$$

Moreover, as a group, $\mathcal{E}(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/M \times \mathbb{Z}/L$ for unique integers M and L with $L \mid M$ and $N = ML$. The number M is called the *exponent* of $\mathcal{E}(\mathbb{F}_q)$. Points P and Q in $\mathcal{E}(\mathbb{F}_q)$ are said to be *echelonized generators* if the order of P is M, the order of Q is L, and any point in $\mathcal{E}(\mathbb{F}_q)$ can be written in the form $mP + \ell Q$ with $1 \le m \le M$ and $1 \le \ell \le L$.

Although there exists a deterministic polynomial time algorithm to find the number of $\mathbb{F}_q$-rational points N due to R. Schoof [11] (see also [4, 5, 16] for references to further theoretical and practical improvements of this algorithm), finding the group structure, or equivalently the exponent M, appears to be a much harder problem.

Once the group order N and the factorization of $r = \gcd(q-1, N)$ are known, there exists a probabilistic algorithm to compute the group structure in expected polynomial time (see [9, 10]). We note that the existence of the *Weil pairing* (see [18]) implies that L divides r. Thus, using the factorization of r and the nondegeneracy of the Weil pairing, the algorithm finds the value of L. The best possible bound on r is $q^{1/2}+1$, but for a random curve the value of r tends to be small, in which case the algorithm is efficient.

We now describe the exponential sums which are the subject of study in this work. Let P and Q be echelonized generators for $\mathcal{E}(\mathbb{F}_q)$. For a real number z or element of $\mathbb{Z}/n\mathbb{Z}$, we define

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

The group $\Omega = \mathrm{Hom}(\mathcal{E}(\mathbb{F}_q), \mathbb{C}^*)$ of characters on $\mathcal{E}(\mathbb{F}_q)$ can be described by the set:

$$\Omega = \{\omega \,|\, \omega(mP + \ell Q) = \mathbf{e}_M(am)\,\mathbf{e}_L(b\ell) \text{ for } 0 \le a < M,\ 0 \le b < L\}.$$

Similarly the group $\Psi = \mathrm{Hom}(\mathbb{F}_q, \mathbb{C}^*)$ of additive characters on $\mathbb{F}_q$ can be described by the set:

$$\Psi = \{\psi \,|\, \psi(z) = \mathbf{e}_p(\mathrm{Tr}(\alpha z)) \text{ for } \alpha \in \mathbb{F}_q\},$$

where $\mathrm{Tr}(x)$ is the trace of $x \in \mathbb{F}_q$ to $\mathbb{F}_p$ (see Chapter 2 of [8]). The identity elements of the groups Ω and Ψ are called *trivial* characters.

Let $\mathbb{F}_q(\mathcal{E})$ be the function field of the curve $\mathcal{E}$. It is generated by the functions x and y, satisfying the Weierstrass equation (1) of the curve, and such that $P = (x(P), y(P))$ for each $P \in \mathcal{E}(\mathbb{F}_q) - \{O\}$.

For characters $\omega \in \Omega$ and $\psi \in \Psi$, and a function $f \in \mathbb{F}_q(\mathcal{E})$, we define the sum

$$S(\omega, \psi, f) = \sum_{\substack{P \in \mathcal{E}(\mathbb{F}_q) \\ f(P) \neq \infty}} \omega(P)\psi(f(P)).$$

In this work we estimate the exponential sums $S(\omega, \psi, f)$. In particular we will be interested in the sums for $f = x$ or $f = y$. The bounds obtained generalize and improve previous bounds from [13, 14]. We apply this bound to design a deterministic algorithm to compute the group structure of $\mathcal{E}(\mathbb{F}_q)$ and to find echelonized generators in time $O(q^{1/2+\varepsilon})$.

In the next section we recall some classical results on L-functions of curves, and relate these to $S(\omega, \psi, f)$.

Throughout the paper $\log z$ denotes the natural logarithm of z.

2 *L*-functions of Curves

Let $\mathcal{C}$ be an irreducible projective curve over $\mathbb{F}_q$ of genus g. The divisor group is the free abelian group of formal sums of prime places $\mathfrak{P}$ of $\mathbb{F}_q(\mathcal{C})$. For a fixed

algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ we can identify a prime place $\mathfrak{P}$ with a Galois orbit $\{P_1, \ldots, P_d\}$ of points in $\mathcal{C}(\overline{\mathbb{F}}_q)$, and define $d = \deg(\mathfrak{P})$ to be its degree.

A character χ of the divisor group of $\mathbb{F}_q(\mathcal{C})$ is a map to $\mathbb{C}$, with image in a finite set $\{0\} \cup \mathbf{e}_n(\mathbb{Z})$ and which is a homomorphism to $\mathbb{C}^*$ on divisors with support outside of a finite set of prime places. Associated to χ is a cyclic Galois cover $\pi : \mathcal{X} \to \mathcal{C}$ and a divisor $\mathfrak{f}(\chi)$ called the *conductor*, such that π is unramified outside of the support of $\mathfrak{f}(\chi)$.

We define the following character sums

$$\sigma_m(\chi) = \sum_{\deg\mathfrak{P} \leq m} \deg(\mathfrak{P})\chi(\mathfrak{P}), \quad m = 1, 2, \ldots,$$

taken over all prime places $\mathfrak{P}$ of $\mathbb{F}_q(\mathcal{C})$ of degree $\deg\mathfrak{P} \leq m$. We define an *L-function*

$$L(\mathcal{C}, t, \chi) = \exp\left(\sum_{m=1}^{\infty} \sigma_m(\chi) t^m/m\right),$$

where $\exp : t\mathbb{C}[[t]] \longrightarrow \mathbb{C}[[t]]$ is given by

$$\exp(h(t)) = \sum_{n=0}^{\infty} \frac{h(t)^n}{n!}.$$

The following proposition for $L(\mathcal{C}, t, \chi)$ appears as Theorem A of [2] or Theorem 6 of Chapter 7 of [20].

Proposition 1. *$L(\mathcal{C}, t, \chi)$ is a polynomial of degree*

$$D = 2g - 2 + \deg\mathfrak{f}(\chi)$$

where $\mathfrak{f}(\chi)$ is the conductor of χ. If χ is a product of two characters χ_1 and χ_2 which are ramified in disjoint sets of divisors then

$$\deg\mathfrak{f}(\chi) = \deg\mathfrak{f}(\chi_1) + \deg\mathfrak{f}(\chi_2).$$

We remark the second statement is applicable in particular if one of characters is totally unramified.

We next recall the statement of the Riemann Hypothesis for function fields.

Proposition 2. *Let $\vartheta_1, \ldots, \vartheta_D$ be zeros of $L(C, t, \chi)$ in $\mathbb{C}$. Then*

$$\sigma_m(\chi) = -(\vartheta_1^m + \ldots + \vartheta_D^m),$$

and each zero satisfies $|\vartheta_i| = q^{1/2}$.

3 Exponential Sums on Elliptic Curves

We recall the following standard lemma on character groups of abelian groups.

Lemma 1. *Let G be an abelian group and let $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ be its dual group. Then for any element χ of $\widehat{G}$, we have*

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \begin{cases} 1, & \text{if } \chi = \chi_0, \\ 0, & \text{if } \chi \neq \chi_0, \end{cases}$$

where $\chi_0 \in \widehat{G}$ is the trivial character.

In particular, we apply the bound to the pairs $\{\Psi, \mathbb{F}_q\}$ and $\{\mathcal{E}(\mathbb{F}_q), \Omega\}$. By the canonical isomorphism of G with the dual of $\widehat{G}$, the lemma is symmetrical in G and $\widehat{G}$.

As an immediate application of Lemma 1 we observe that if ψ_0 is the trivial character, then

$$S(\omega, \psi_0, f) = \sum_{\substack{P\in\mathcal{E}(\mathbb{F}_q)\\ f(P)\neq\infty}} \omega(P) = -\sum_{\substack{P\in\mathcal{E}(\mathbb{F}_q)\\ f(P)=\infty}} \omega(P).$$

Thus we see that the interesting part of the exponential sum comes from the character $\psi \circ f$, which defines an Artin-Schreier extension of $\mathbb{F}_q(\mathcal{E})$, as studied in Bombieri [2, Section VI]. We also remark that the exponential sums $S(\omega_0, \psi, f)$ with the trivial character $\omega_0 \in \Omega$ have been estimated in [2].

Let f be a nonconstant function on $\mathcal{E}$. We write the divisor of poles of f as

$$(f)_\infty = \sum_{i=1}^{t} n_i \mathfrak{P}_i,$$

where, in particular,

$$\deg(f) = \sum_{i=1}^{t} n_i \deg(\mathfrak{P}_i). \tag{2}$$

In particular, $degf = 2$ if $f = x$, and $degf = 3$ if $f = y$. With this notation we have the following theorem.

Theorem 1. *The character ω determines an unramified character, and $\psi \circ f$ determines a character of conductor $\sum_{i=1}^{t} m_i \mathfrak{P}_i$, where $m_i \leq n_i + 1$ with equality if and only if $(n_i, q) = 1$. The exponential sum satisfies the bound*

$$|S(\omega, \psi, f)| \leq \sum_{i=1}^{t} m_i \deg(\mathfrak{P}_i) q^{1/2}.$$

Proof. The character ω determines an unramified character mapping through $\mathcal{E}(\mathbb{F}_q)$. Specifically, a prime divisor $\mathfrak{P}$ with associated Galois orbit $\{P_1, \ldots, P_d\}$ contained in $\mathcal{E}(\overline{\mathbb{F}}_q)$ maps to the point $P = \sum_i P_i$ in $\mathcal{E}(\mathbb{F}_q)$, and we define $\omega(\mathfrak{P}) = \omega(P)$. The character thus defines a Galois character on the unramified cover defined by the isogeny $\mathcal{E} \to \mathcal{E}$ with kernel $\mathcal{E}(\mathbb{F}_q)$. In particular the character is unramified and its conductor is trivial. Applying Proposition 1 we reduce to the consideration of the conductor of the character defined by $\psi \circ f$.

The character $\psi \circ f$ defines a Galois character associated to an Artin-Schreier extension of $\mathcal{E}$, as studied in Bombieri [2, Section VI]. In particular the conductor is determined in Theorem 5 of that work. The bound then follows from Proposition 2. □

In particular, from Theorem 1 and the identity (2) we see that the bound

$$|S(\omega, \psi, f)| \leq 2\deg(f) q^{1/2} \tag{3}$$

holds. If the polar divisor of f has support at a single prime divisor, then we have the stronger bound

$$|S(\omega, \psi, f)| \leq (1 + \deg(f)) q^{1/2}.$$

For a subgroup $\mathcal{H}$ of $\mathcal{E}(\mathbb{F}_q)$ we define

$$S_{\mathcal{H}}(\omega, \psi, f) = \sum_{\substack{P \in \mathcal{H} \\ f(P) \neq \infty}} \omega(P)\psi(f(P))$$

Corollary 1. *Let f be a nonconstant function in $\mathbb{F}_q(\mathcal{E})$ and ψ be a nontrivial character, then the bound*

$$|S_{\mathcal{H}}(\omega, \psi, f)| \leq 2\deg(f) q^{1/2}$$

holds.

Proof. Let $\Omega_{\mathcal{H}} \subseteq \Omega$ be the set of characters $\chi \in \Omega$ such that $\ker(\chi)$ contains $\mathcal{H}$. Then $\Omega_{\mathcal{H}}$ is dual to $\mathcal{E}(\mathbb{F}_q)/\mathcal{H}$, so we may apply Lemma 1. Therefore

$$\begin{aligned} S_{\mathcal{H}}(\omega, \psi, f) &= \frac{1}{|\Omega_{\mathcal{H}}|} \sum_{\substack{P \in \mathcal{E}(\mathbb{F}_q) \\ f(P) \neq \infty}} \sum_{\chi \in \Omega_{\mathcal{H}}} \chi(P)\omega(P)\psi(f(P)) \\ &= \frac{1}{|\Omega_{\mathcal{H}}|} \sum_{\chi \in \Omega_{\mathcal{H}}} S(\chi \cdot \omega, \psi, f). \end{aligned}$$

Applying the inequality (3), we obtain the desired estimate. □

4 Distributions of points in intervals

We also require the following standard lemma, which appears, for instance, as Problem 11.c in Chapter 3 of [19].

Lemma 2. *For any positive integers n, s, and r we have*

$$\sum_{k=1}^{n-1} \left| \sum_{a=s}^{s+r} \mathbf{e}_n(ak) \right| \leq n(1 + \log n).$$

We define an *interval* I in $\mathbb{F}_q$ to be a subset of the form $B + \alpha[s, \ldots, s+r]$ for an additive subgroup B of $\mathbb{F}_q$, an element $\alpha \in \mathbb{F}_q$, and nonnegative integers s and r.

Lemma 3. *For any interval I in $\mathbb{F}_q$ the bound*

$$\sum_{\psi \in \Psi} \left| \sum_{\beta \in I} \psi(\beta) \right| \leq q(1 + \log p)$$

holds.

Proof. For an additive subgroup $B \subseteq \mathbb{F}_q$, we define $\Psi_B = \{\psi \in \Psi \mid B \subseteq \ker(\psi)\}$, and note that Ψ_B is dual to $\mathbb{F}_q/B$.

Now suppose $I = B + \alpha[r, \ldots, r+s]$, where $B \subseteq \mathbb{F}_q$ is additive subgroup and $\alpha \notin B$. Since $\sum_{\beta \in B} \psi(\beta) = 0$ for all ψ not in Ψ_B, we can express the sum as

$$\sum_{\psi \in \Psi} \left| \sum_{\beta \in I} \psi(\beta) \right| = \sum_{\psi \in \Psi} \left| \sum_{\beta \in B} \psi(\beta) \sum_{k=r}^{r+s} \psi(k\alpha) \right| = |B| \sum_{\psi \in \Psi_B} \left| \sum_{k=r}^{r+s} \psi(k\alpha) \right|.$$

We set $C = B + \alpha\mathbb{F}_p$, and note that $\psi(k\alpha) = 1$ for all ψ in Ψ_C. Therefore

$$\sum_{\psi \in \Psi} \left| \sum_{\beta \in I} \psi(\beta) \right| = |B||\Psi_C| \sum_{\psi \in \Psi_B/\Psi_C} \left| \sum_{k=r}^{r+s} \psi(k\alpha) \right|.$$

Since $C/B \cong \alpha\mathbb{F}_p$ is cyclic of order p and with dual group Ψ_B/Ψ_C, we can apply Lemma 2 together with $|B||\Psi_C| = q/p$ to obtain the stated bound. □

For a character $\omega \in \Omega$, a function $f \in \mathbb{F}_q(\mathcal{E})$, and a subset $S \subseteq \mathbb{F}_q$ we define the

$$\mathcal{T}(S, f, \omega) = \{P \in \mathcal{E}(\mathbb{F}_q) \mid f(P) \in S \text{ and } \omega(P) \neq 1\}.$$

and denote its cardinality by $T(S, f, \omega)$.

Theorem 2. *Let $\mathcal{E}$ be an elliptic curve over a finite field $\mathbb{F}_q$, and let f be a function with poles only at O. Then for any interval $I \subset \mathbb{F}_q$ and character ω of order m, the bound*

$$\left| T(I, f, \omega) - N \frac{(m-1)}{m} \frac{|I|}{q} \right| \leq 2(1 + \deg(f))(1 + \log p) q^{1/2}$$

holds.

Proof. Set $\mathcal{H}$ to be the kernel of ω. Applying Lemma 1 we obtain the expression

$$\begin{aligned} T(I, f, \omega) &= \frac{1}{q} \sum_{\beta \in I} \sum_{\substack{P \in \mathcal{E}(\mathbb{F}_q) \\ P \notin \mathcal{H}}} \big(\sum_{\psi \in \Psi} \psi(f(P) - \beta) \big) \\ &= \frac{1}{q} \sum_{\psi \in \Psi} \sum_{\substack{P \in \mathcal{E}(\mathbb{F}_q) \\ P \notin \mathcal{H}}} \psi(f(P)) \sum_{\beta \in I} \psi(\beta)^{-1} \\ &= \frac{1}{q} \sum_{\psi \in \Psi} \big(S(\omega_0, \psi, f) - S_{\mathcal{H}}(\omega_0, \psi, f) \big) \sum_{\beta \in I} \psi(\beta)^{-1}, \end{aligned}$$

where $\omega_0 \in \Omega$ is the trivial character. Separating out the term corresponding to the trivial character $\psi_0 \in \Psi$, we obtain the expression:

$$T(I, f, \omega) - N \frac{(m-1)}{m} \frac{|I|}{q} = \frac{1}{q} \sum_{\substack{\psi \in \Psi \\ \psi \neq \psi_0}} \big(S(\omega_0, \psi, f) - S_{\mathcal{H}}(\omega_0, \psi, f) \big) \sum_{\beta \in I} \psi(\beta)^{-1}.$$

Applying Theorem 1 and Lemma 3 we obtain the desired result. □

Corollary 2. *Let $\mathcal{E}$ be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p, and take either $f = x$ if $p \neq 2$ or $f = y$ if $p \neq 3$ in $\mathbb{F}_q(\mathcal{E})$. Then for any interval $I \subset \mathbb{F}_q$ of cardinality greater than $5(1 + \deg(f))(1 + \log p) q^{1/2}$, the set*

$$\mathcal{T}(I, f) = \{ P \in \mathcal{E}(\mathbb{F}_q) \,|\, f(P) \in I \}$$

generates $\mathcal{E}(\mathbb{F}_q)$.

Proof. Since $\deg(x) = 2$ and $\deg(y) = 3$, we observe that the lower bound on I implies that $|I| > |\mathbb{F}_q|$ for $q < 100$. But for all $q > 100$, we note that the bound

$$\frac{q}{N} \leq \frac{q}{q - 2q^{1/2} + 1} < 1.25$$

holds. Applying the bound of the previous theorem, we find that the subset $\mathcal{T}(I, f, \omega)$ of $\mathcal{T}(I, f)$, is nonempty for any nontrivial character ω. Therefore $\mathcal{T}(I, f)$ is contained in no proper subgroup of $\mathcal{E}(\mathbb{F}_q)$. □

5 The Algorithm

Theorem 3. *Given any $\varepsilon > 0$, there exists an algorithm which, given an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$, constructs echelonized generators for $\mathcal{E}(\mathbb{F}_q)$ in time $O(q^{1/2+\varepsilon})$.*

Proof. For q large, the algorithm works by the following steps, and for small q we may solve the problem by any method we choose.

1. Find the group order N of $\mathcal{E}(\mathbb{F}_q)$, and factor it to find the set of all divisors.
2. Construct the set $\mathcal{T}(I, f)$ of points $P \in \mathcal{E}(\mathbb{F}_q)$ with $f(P) \in I$, for an appropriate choice of function f and interval I, such that $\mathcal{T}(I, f)$ contains generators for $\mathcal{E}(\mathbb{F}_q)$.
3. Reduce the generator set to a pair of echelon generators.

The group order can be computed in polynomial time using the method of Schoof [11], with practical improvements by Atkin and Elkies [5]. The order can be factored by trial division in time $O(q^{1/2+\varepsilon})$, but faster algorithms are also available [1, 4], so this phase does not present the limiting complexity.

By Corollary 2, if we set f equal to x for $p \neq 2$ or y if $p = 2$, then the set $\mathcal{T}(I, f)$ contains generators for $\mathcal{E}(\mathbb{F}_q)$ for an interval I of size $O(q^{1/2+\delta})$, where $0 < \delta < \varepsilon$. For each $x_0 \in I$ (or $y_0 \in I$), the points (x_0, y_0) in $\mathcal{E}(\mathbb{F}_q)$, if such exist, can be found by solving a quadratic (or cubic) equation. Knowing a quadratic (or cubic) nonresidue, one can extract roots in polynomial time (see [1, 4, 16]). The nonresidue can be computed, for instance, by the $O(q^{1/4+\delta})$-algorithm of [15], which finds a primitive root for $\mathbb{F}_q$. This one time computation has no impact on the complexity of the algorithm. Therefore the complexity of this stage of the algorithm is

$$O(|\mathcal{T}(I, f)|(\log q)^{O(1)}) = O(q^{1/2+\varepsilon}),$$

which defines the complexity of the algorithm.

Using the factorization of the order N, and a set of generators, we can find the exponent M of the group in polynomial time. If P is a point of order m and Q is a point of order n, where $\gcd(n, m) = 1$, then $P + Q$ has order nm. Thus it suffices to produce echelon generators for each subgroup $\mathbb{Z}/r^\mu\mathbb{Z} \times \mathbb{Z}/r^\lambda\mathbb{Z}$, where r is prime and r^μ and r^λ are the largest powers of r dividing M and $L = N/M$, respectively. Finding an element P of order r^μ involves only polynomial time group operations on elements of the set $\mathcal{T}(I, f)$. Likewise a set of generators for the r^λ-torsion group can be produced in polynomial time, by multiplying points in $\mathcal{T}(I, f)$ by an appropriate factor. Setting $P_1 = r^{\mu-\lambda}P$, we take the Weil pairing of P_1 with each element Q of order r^λ to identify an independent generator (see Menezes [10]). The complexity of this step is again

$$O\left(|\mathcal{T}(I, f)|(\log q)^{O(1)}\right) = O\left(q^{1/2+\varepsilon}\right),$$

so the complexity is as asserted. □

6 Remarks

We note that the methods of this paper can be improved or extended in several ways. From the proof of Corollary 2, it is clear that the constant 5 in the bound can be improved to $4 + o(1)$. A more significantly improvement, however, is achieved using standard techniques (see Chalk [3]) to remove the $\log p$ from the bound. In another direction, combining the method of this paper with a simple sieve method, it is possible to prove results on the distribution of points whose order equals the group exponent. In particular, for curves with cyclic point group $\mathcal{E}(\mathbb{F}_q)$, one obtains results on the distribution of cyclic generators in intervals. Since none of these results have consequence to the final complexity of the algorithm of this paper, we have left these results to comments.

With minimal modification, the results of this paper carry over to a general result on Jacobians of a hyperelliptic curves over $\mathbb{F}_q$ given by an equation of the form $y^2 + a(x)y = b(x)$, where $a(x)$ and $b(x)$ are polynomials over $\mathbb{F}_q$. More precisely, it is possible to prove bounds on the size of sets of points *on the curve* which generate the group of rational points *on the Jacobian*. For elliptic curves, the Weil pairing is used to prove the independence of generators for the group of rational points [9, 10]. Lacking an effective analogue of the Weil pairing, this approach seems to be the only available deterministic method for producing a provable set of elements generating the group.

For finite fields of bounded characteristic there exist deterministic polynomial time algorithms for constructing a polynomial size set of elements containing a primitive element (see [12, 13], and also Chapter 2 of [16]). It remains open whether similar improved bounds hold for the group of rational points on elliptic curves over finite fields of small characteristic.

The exponential sums of this work also have implications for pseudo-random number generators. The bound of Corollary 1 has been used in [17] to show that the elliptic curve of the Naor–Reingold pseudo-random function is uniformly distributed. Our results can also be used to prove that the elliptic curve analogues of the congruencial generator of pseudo-random numbers (see [6, 7]) produce uniformly distributed sequences.

Acknowledgment. The authors are grateful to Hendrik Lenstra for valuable advice and his generous sharing of ideas on the subject of this work.

References

1. E. Bach and J. Shallit. *Algorithmic Number Theory.* MIT Press, Cambridge MA, 1996.
2. E. Bombieri. On exponential sums in finite fields. *Amer. J. Math* **88**, 1966, pp. 71–105.
3. J. H. H. Chalk. Polynomial congruences over incomplete residue systems modulo k. *Proc. Kon. Ned. Acad. Wetensch.*, **A92** (1989), 49–62.

4. H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Berlin, 1997.
5. N. Elkies. Elliptic and modular curves over finite fields and related computational issues. *Computational perspectives on number theory (Chicago, IL, 1995)*, Stud. Adv. Math. **7**, Amer. Math. Soc., Providence, RI, 1998, 21–76.
6. G. Gong, T. A. Bernson and D. A. Stinson. Elliptic curve pseudorandom sequence generators. *Research Report CORR-98-53*, Faculty of Math., Univ. of Waterloo, 1998, 1–21.
7. S. Hallgren. Linear congruential generators over elliptic curves. *Preprint CS-94-143*, Dept. of Comp. Sci., Cornegie Mellon Univ., 1994, 1–10.
8. R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge Univ. Press, Cambridge, 1997.
9. A. J. Menezes, T. Okamoto and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *Trans. IEEE Inform. Theory* **39**, 1993, pp. 1639–1646.
10. A. J. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Acad. Publ., Boston, MA, 1993.
11. R. J. Schoof. Elliptic curves over finite fields and the computation of square roots Mod *p*. *Math. Comp.*, **44** (1985), 483–494.
12. V. Shoup. Searching for primitive roots in finite fields. *Math. Comp.*, **58** (1992), 369–380.
13. I. E. Shparlinski. On primitive elements in finite fields and on elliptic curves. *Matem. Sbornik*, **181** (1990), 1196–1206 (in Russian).
14. I. E. Shparlinski. On Gaussian sums for finite fields and elliptic curves. *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **573** (1992), 5–15.
15. I. E. Shparlinski. On finding primitive roots in finite fields. *Theor. Comp. Sci.*, **157** (1996), 273–275.
16. I. E. Shparlinski. *Finite Fields: Theory and Computation*. Kluwer Acad. Publ., North-Holland, 1999.
17. I. E. Shparlinski. On the Naor–Reingold pseudo-random function from elliptic curves. *Appl. Algebra in Engin., Commun. and Computing* (to appear).
18. J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, Berlin, 1995.
19. I. M. Vinogradov. *Elements of Number Theory*. Dover Publ., NY, 1954.
20. A. Weil. *Basic of Number Theory*. Spinger-Verlag, Berlin, 1974.