Publ. Math. Debrecen
80/1-2 (2012), 199–213
DOI: 10.5486/PMD.2011.5057

Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters

By LÁSZLÓ MÉRAI (Budapest)

Abstract. In this paper a large family of pseudorandom binary sequences is proposed by using multiplicative characters and elliptic curves. The construction generalize several earlier ones and both the well-distribution and correlation measures are estimated.

1. Introduction

Pseudorandom sequences play a crucial role in many areas (e.g. in cryptography and communication systems). There are many definitions for pseudorandomness depending on specific application, see [15]. However, we will apply the definition of pseudorandomness given in [14].

It is well known than elliptic curves over finite fields have good pseudorandom properties thus they are widely used for generating pseudorandom sequences (see [3], [4], [5], [6], [8], [7], [12], [24]).

In 1994 Hallgren [11] proposed the *linear congruent generator* from elliptic curves. The linear congruent generator builds a sequence of points on the curve $\mathcal{E}$ by the rule $s_0 = P_0$ for some $P_0 \in \mathcal{E}$ and

$$s_n = P \oplus s_{n-1} = nP \oplus P_0$$

By using the definition of pseudorandomness given in [14], Chen [3], and Chen,

Mathematics Subject Classification: 11K45.
Key words and phrases: pseudorandom, binary sequence,elliptic curve, character.
Research partially supported by Hungarian National Foundation of Scientific Research, Grants No. K 67676 and by the Momentum fund of the Hungarian Academy of Sciences.

Li and Xiao [4] studied binary sequences derived from this generator where they used the Legendre symbol and the discrete logarithm of finite fields.

In this paper we extend this study by using general multiplicative character over finite field and sufficient conditions will be given to guarantee the good pseudorandom properties. In Section 2 we summarize some basic facts about elliptic curves, in Section 3 we recall the definition of pseudorandomness introduced in [14], analyze the constructions proposed in [3], [4], and introduce the new construction. In Section 4 we prove that the construction has strong pseudorandom properties, and in Section 5 we give some conditions for the applicability of the theorems proved in the previous section.

2. Elliptic curves

Let p be an odd prime, $\mathbb{F}_p$ be the finite field of p elements which we represent by the elements $\{0, 1, \dots, p-1\}$, $\mathbb{F}_p^*$ be the set of non-zero elements and $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$.

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$ defined by the Weierstrass equation

$$y^2 = x^3 + Ax + B$$

with coefficients $A, B \in \mathbb{F}_p$ and non-zero discriminant (see [25]). The $\mathbb{F}_p$-rational points $\mathcal{E}(\mathbb{F}_p)$ of $\mathcal{E}$ form an Abelian group with the point in infinity $\mathcal{O}$ as the neutral element, where the group operation is denoted by $\oplus$ (and its inverse operation is denoted by $\ominus$). For a rational point $R \in \mathcal{E}(\mathbb{F}_p)$, a multiple of R is defined by $nR = \bigoplus_{i=1}^{n} R$.

Let $\mathbb{F}_p(\mathcal{E})$ be the function field of $\mathcal{E}$ over $\mathbb{F}_p$. For a rational function $f \in \mathbb{F}_p(\mathcal{E})$ and point $R \in \mathcal{E}(\overline{\mathbb{F}}_p)$, R is a *zero* (resp. *pole*) of f if $f(R) = 0$ (resp. $f(R) = \infty$). Any function of $\mathbb{F}_p(\mathcal{E})$ has finitely many zeros and poles. The *divisor* of f is defined by

$$\operatorname{div}(f) = \sum_{R \in \mathcal{E}(\overline{\mathbb{F}}_p)} \operatorname{ord}_R(f)[R],$$

where $\operatorname{ord}_R(f)$ is the order of f in R.

The set of zeros and poles of f

$$\operatorname{Supp}(f) = \{R \in \mathcal{E}(\overline{\mathbb{F}}_p) \mid \operatorname{ord}_R(f) \neq 0\}$$

is the *support* of $\operatorname{div}(f)$.

The translation map by $W \in \mathcal{E}(\mathbb{F}_p)$ on $\mathcal{E}(\mathbb{F}_p)$ is defined by

$$\begin{aligned} \tau_W : \mathcal{E}(\mathbb{F}_p) &\to \mathcal{E}(\mathbb{F}_p), \\ P &\mapsto P \oplus W. \end{aligned}$$

We define the exponential sum respect to a multiplicative character of $\mathbb{F}_p$ by

$$S(\omega, \chi, f) = \sum_{R \in \mathcal{E}(\mathbb{F}_p)} \omega(R)\chi(f(R))$$

where ω is a character of $\mathcal{E}(\mathbb{F}_p)$, χ is a multiplicative character of $\mathbb{F}_p$, $f \in \mathbb{F}_p(\mathcal{E})$ is a rational function, and R runs on the $\mathbb{F}_p$-rational points except the zeros and poles of f. $S(\omega, \chi, f)$ was investigated in [2], [21], [22]. The incomplete sum was studied in [4]:

Lemma 1. *Let $Q \in \mathcal{E}(\mathbb{F}_p)$ be a rational point of order N, $\chi \neq \chi_0$ non-principal multiplicative character of $\mathbb{F}_p$, $f \in \mathbb{F}_p(\mathcal{E})$ rational function which is $f(x, y) \neq z^d(x, y)$ for all $z \in \overline{\mathbb{F}}_p(\mathcal{E})$. Then for any $a, b, t \in \mathbb{N}$ with $1 \leq a \leq a + (t-1)b \leq N$ the following bound holds:*

$$\left| \sum_{x=0}^{t-1} \chi(f((a + bx)Q)) \right| < |\operatorname{Supp}(f)| p^{1/2}(1 + \log N).$$

We note that originally the condition $f(x, y) \neq z^l(x, y)$ was required for any factor l of $p - 1$. However it can be easily shown that it is enough to ensure it for $l = d$ (see for example Theorem 4 in [20])

3. Measures of pseudorandomness, the construction

In this paper we follow the approach of Mauduit and Sárközy [14]: For a given binary sequence

$$E_N = \{e_1, \ldots, e_N\} \in \{-1, +1\}^N$$

the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|,$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ such that $1 \leq a \leq a+(t-1)b \leq N$, and the *correlation measure of order ℓ* of E_N is defined as

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, \dots, d_\ell)$ and M such that $0 \le d_1 < d_2 < \cdots < d_\ell \le N - M$.

The sequence E_N is considered as a "good" pseudorandom sequence if both these measures $W(E_N)$ and $C_\ell(E_N)$ (at least for small ℓ) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$). This terminology is justified since for a truly random sequence E_N each of these measures is $\ll \sqrt{N \log N}$. (For a more precise version of this result see [1].)

Using the Legendre symbol, Goubin, Mauduit and Sárközy [9] showed (extending a result of Mauduit and Sárközy [14]) that the sequence $E_p = \{e_1, \dots, e_p\}$ defined by

$$e_n = \begin{cases} \left(\dfrac{f(n)}{p}\right) & \text{if } \ f(n) \neq 0 \\ +1 & \text{otherwise,} \end{cases} \tag{1}$$

has strong pseudorandom properties:

$$W(E_{p-1}) \ll \deg f p^{1/2} \log p, \quad C_\ell(E_{p-1}) \ll \deg f \ell p^{1/2} \log p.$$

if f satisfies certain conditions.

In [10] Gyarmati (generalizing [23]) introduced the following sequence:

$$e_n = \begin{cases} +1 & \text{if } \ 1 \le \operatorname{ind} f(n) \le p/2 \\ -1 & \text{if } p/2 < \operatorname{ind} f(n) < p \text{ or } p \mid f(n), \end{cases} \tag{2}$$

where ind is the index (discrete logarithm) in $\mathbb{F}_p$ with respect to a given primitive root g. She proved, that if f satisfies certain conditions, then the sequence also has strong pseudorandom properties.

In [3], Chen adapted the Legendre symbol construction to elliptic curves. He defined a binary sequence in the following way: let p be a prime, $\mathcal{E}(\mathbb{F}_p)$ be the $\mathbb{F}_p$-rational points of an elliptic curve which is cyclic, let G be a generator of $\mathcal{E}(\mathbb{F}_p)$ with order T, and finally let $f \in \mathbb{F}_p(\mathcal{E})$. Then the sequence $E_T = \{e_1, \dots, e_T\}$ is defined by:

$$e_n = \begin{cases} \left(\dfrac{f(nG)}{p}\right) & \text{if } \ nG \notin \operatorname{Supp}(f) \\ +1 & \text{otherwise.} \end{cases} \tag{3}$$

He proved that its well-distribution measure is small and he also studied its linear complexity profile.

In [4], Chen, Li and Xiao extended the discrete logarithm construction to elliptic curves: they defined the sequence $E_T = \{e_1, \dots, e_T\}$ by

$$e_n = \begin{cases} +1 & \text{if } \ 1 \le \operatorname{ind} f(nG) \le p/2 \\ -1 & \text{if } p/2 < \operatorname{ind} f(nG) < p \text{ or } f(nG) \in \operatorname{Supp}(f). \end{cases} \tag{4}$$

As in the classical case [16] we can extend construction (3) and (4) by using arbitrary multiplicative character in (3) instead of the Legendre symbol. More precisely let χ be a multiplicative character of $\mathbb{F}_p$ and define the sequence $E_T = (e_1, \dots, e_T)$ by

$$e_n = \begin{cases} +1 & \text{if } \arg(\chi(f(nG))) \in [0, \pi) \text{ for } nG \notin \operatorname{Supp}(f), \\ -1 & \text{otherwise,} \end{cases} \tag{5}$$

where $\arg z$ is the argument of z

If χ is the Legendre symbol we get construction (3), while if we define χ by $\chi(g) = e^{2\pi i/(p-1)}$ (where g is a generator), then we get construction (4).

In order to use these constructions one need further conditions to the rational function f as the following example shows:

Example 3.1. Consider the elliptic curve defined by

$$y^2 = x^3 - 2x$$

over $\mathbb{F}_{19}$. This curve has 20 points and $(2, 2)$ is a generator. Let $f(x, y) = x$. Then the sequence defined as in (3) is

n	nG	e_n	n	nG	e_n
1	(2,2)	-1	11	(18 ,1)	-1
2	(7,14)	+1	12	(16 ,6)	+1
3	(15,1)	-1	13	(10,12)	-1
4	(11,6)	+1	14	(5,18)	+1
5	(13,10)	-1	15	(13,9)	-1
6	(5 ,1)	+1	16	(11,13)	+1
7	(10 ,7)	-1	17	(15,18)	-1
8	(16 ,13)	+1	18	(7,5)	+1
9	(18 ,18)	-1	19	(2,17)	-1
10	(0 ,0)	-1	20	$\mathcal{O}$	-1

The second order correlation $C_2(E_{20})$ is large:

$$e_n \cdot e_{n+10} = \left(\frac{f(nG)}{19}\right) \cdot \left(\frac{f((n+10)G)}{19}\right) = \left(\frac{f(nG) \cdot f(nG+10G)}{19}\right)$$
$$= \left(\frac{f(nG) \cdot f(nG+(0,0))}{19}\right) = \left(\frac{x \cdot \left(\left(\frac{y}{x}\right)^2 - x\right)}{19}\right) = 1,$$

since the function $x \cdot \left(\left(\frac{y}{x}\right)^2 - x\right)$ is the constant -2 function over the curve.

Similar examples can be given if the order of $\mathcal{E}(\mathbb{F}_p)$ has small prime divisor.

As in [9], in order to describe the "good" rational functions, we will need the definition of admissibility:

Definition 2. Let $\mathcal{A}$ and $\mathcal{B}$ be multisets of elements of $\mathbb{Z}_m$ such that the multiplicities of the elements of $\mathcal{A}$ and $\mathcal{B}$ are less than d. If $\mathcal{A}+\mathcal{B}$ represents every element of $\mathbb{Z}_m$ with multiplicity divisible by d, i.e., for all $c \in \mathbb{Z}_m$ the number of solution of

$$a + b = c, \quad a \in \mathcal{A}, b \in \mathcal{B} \tag{6}$$

(the a's and b's are counted with their multiplicities) is divisible by d, then $\mathcal{A}+\mathcal{B}$ is said to have *property* $P(d)$.

Definition 3. If $k, \ell, m, d \in \mathbb{N}$ and $k, \ell \le m$, then (k, ℓ, m) is said to be *d-admissible triple*, if there are no multisets $\mathcal{A}$ and $\mathcal{B}$ of elements of $\mathbb{Z}_m$ such that the number of distinct elements of $\mathcal{A}$ is less than or equal to k, the number of distinct elements of $\mathcal{B}$ is less than or equal to ℓ, all multiplicities of elements $a \in \mathcal{A}$ are co-prime to d and $\mathcal{A}+\mathcal{B}$ possesses property $P(d)$.

Theorem 1. *Let p be an odd prime, χ be a multiplicative character of $\mathbb{F}_p$ of even order d, $\mathcal{E}(\mathbb{F}_p)$ be cyclic group of order T, $f \in \mathbb{F}_p(\mathcal{E})$ which is not an l-th power for $l \mid d$ in $\overline{\mathbb{F}}_p(\mathcal{E})$. If we define the binary sequence $E_T = \{e_1, \ldots, e_T\}$ by* (5) *then we have*

$$W(E_T) \le 2|\operatorname{Supp}(f)|p^{1/2}(1+\log T)\log d + |\operatorname{Supp}(f)| \tag{7}$$

Theorem 2. *Let p, χ, d, f and E_T be as in Theorem 1. Let us assume that the order of zeros and poles of f which are not divisible by d are co-prime to d, and $\ell \in \mathbb{N}$ such that the triple $(|\operatorname{Supp}(f)|, \ell, T)$ is d-admissible, then we have*

$$C_\ell(E_T) \le 4^\ell |\operatorname{Supp}(f)|p^{1/2}(1+\log T)(\log d)^\ell + \ell|\operatorname{Supp}(f)| \tag{8}$$

Remark 1. For odd d it can be shown that

$$W(E_T) \le 2|\operatorname{Supp}(f)|p^{1/2}(1+\log T)\log d + |\operatorname{Supp}(f)| + \frac{T}{d}$$

and

$$C_\ell(E_T) \le 5^\ell|\operatorname{Supp}(f)|p^{1/2}(1+\log T)(\log d)^\ell + \ell|\operatorname{Supp}(f)| + \frac{M}{d^\ell}.$$

These bounds are trivial if d is small however there is no nontrivial upper bound in this case as it was shown by an example in [16] in a similar situation.

This construction is perhaps less elementary and natural than some other modular constructions but perhaps this is compensated by the fact that this construction provides large new families of binary sequences which are proved to possess strong pseudorandom properties. Besides this sequences can be generated relatively fast, there are many program language (e.g. SAGE) which include fast elliptic curve computation algorithm and e.g. the Legendre symbol can be also computed fast via Jacobi symbol.

4. Proofs

Since the proof of Theorems 1 and 2 are slightly elementary we just sketch the proof.

Throughout the paper χ_0 denotes the principal character and to avoid any confusion we denote the general multiplicative character by γ.

We will need the following result (see [17], [23]):

Lemma 4. *Let g be a generator of $\mathbb{F}_q$, then*

$$\sum_{\gamma^d=\chi_0}^{*} \frac{1}{|1-\gamma(g)|} < d\log d,$$

where γ runs over the non-principal characters of $\mathbb{F}_q$ such that $\gamma^d = \chi_0$.

Lemma 5. *Let χ be a multiplicative character of even order d and let $n \neq 0$. Then we have*

$$\frac{2}{d}\sum_{\gamma^d=\chi_0}^{*} \frac{1-\bar\gamma(g)^{d/2}}{1-\bar\gamma(g)}\cdot\gamma(n) = \begin{cases} +1 & \text{if } \arg\big(\chi(n)\big) \in [0,\pi) \\ -1 & \text{otherwise,} \end{cases}$$

where γ runs over the non-principal characters of $\mathbb{F}_q$ such that $\gamma^d = \chi_0$, and g is a generator such that $\chi(g) = e(1/d)$.

PROOF. The statement of this lemma is a part of the proof of Theorem 1 in [17], although it was not formulated there a form of a lemma. □

PROOF OF THEOREM 1. To prove the theorem consider $a \in \mathbb{Z}$ and $b, t \in \mathbb{N}$ such that

$$1 \le a \le a + (t-1)b \le T, \quad b < T. \tag{9}$$

If we define the set $\mathcal{N}$ by

$$\mathcal{N} = \{n \mid nG \notin \operatorname{Supp}(f)\},$$

then by Lemma 5 we have

$$|U(E_T, t, a, b)| \le \frac{2}{d} \sum_{\gamma^d=\chi_0}^{*} \left| \sum_{\substack{0 \le j < t \\ a+jb \in \mathcal{N}}} \gamma(f((a+jb)G)) \right| \left| \frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)} \right| + |\operatorname{Supp}(f)|.$$

and since f is not a l-th power for $l \mid d$, by Lemmas 1 and 4 we have

$$\sum_{\gamma^d=\chi_0}^{*} \left| \sum_{\substack{0 \le j < t \\ a+jb \in \mathcal{N}}} \gamma(f((a+jb)G)) \right| \left| \frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)} \right| \le |\operatorname{Supp}(f)|\, p^{1/2}(1+\log t) \sum_{\gamma^d=\chi_0}^{*} \frac{2}{|1-\gamma(g)|}$$

which implies the theorem. □

PROOF OF THEOREM 2. In order to prove the theorem consider any $M < T$ and $D = (d_1, \ldots, d_\ell)$ such that $0 \le d_1 < \cdots < d_\ell \le T - M$. Then by Lemma 5 we have

$$|V(E_T, M, D)| \le \frac{2^\ell}{d^\ell} \sum_{\gamma_1^d=\chi_0}^{*} \cdots \sum_{\gamma_\ell^d=\chi_0}^{*} \left| \frac{1-\gamma_1(g)^{\frac{d}{2}}}{1-\gamma_1(g)} \cdots \frac{1-\gamma_\ell(g)^{\frac{d}{2}}}{1-\gamma_\ell(g)} \right| \cdot \left| \sum_{\substack{1 \le n \le M: \\ n+d_i \in \mathcal{N} \\ i=1,\ldots,\ell}} \gamma_1(f((n+d_1)G)) \ldots \gamma_\ell(f((n+d_\ell)G)) \right| + \ell |\operatorname{Supp}(f)|. \tag{10}$$

Let us define δ_u for $u = 1, \ldots, \ell$ by

$$\gamma_u = \chi^{\delta_u},$$

where

$$0 \le \delta_u < d \quad \text{for } u = 1, \dots, \ell.$$

Using this notation we have

$$\gamma_1(f((n+d_1)G)) \dots \gamma_\ell(f((n+d_\ell)G)) = \chi\left(f^{\delta_1} \circ \tau_{d_1 G}(nG) \dots f^{\delta_\ell} \circ \tau_{d_\ell G}(nG)\right),$$

if $n + d_i \in \mathcal{N}$ for $i = 1, \dots, \ell$.

Write $F_{\gamma_1,\dots,\gamma_\ell} = F_{\delta_1,\dots,\delta_\ell} = f^{\delta_1} \circ \tau_{d_1 G} \cdot \dots \cdot f^{\delta_\ell} \circ \tau_{d_\ell G}$. It suffices to show:

Lemma 6. *If f, k, ℓ are defined as in Theorem 2 and not all of the δ_i's are zeros, then $F_{\delta_1,\dots,\delta_\ell}$ is not a d-th power.*

Indeed, by separating the main term with $\delta_1 = \dots = \delta_\ell = 0$, by (10), Lemmas 1 and 4, we have

$$\begin{aligned} |V(E_T, M, D)| &\le \frac{2^\ell}{d^\ell} \ell |\operatorname{Supp}(f)| p^{1/2} (1 + \log M) \left(\sum_{\gamma^d = \chi_0}^{*} \frac{2}{|1 - \gamma(g)|} \right)^\ell + \ell |\operatorname{Supp}(f)| \\ &\le \frac{2^\ell}{d^\ell} \ell |\operatorname{Supp}(f)| p^{1/2} (1 + \log M)(2d \log d)^\ell + \ell |\operatorname{Supp}(f)|, \end{aligned}$$

which implies the theorem. □

It remains to prove Lemma 6.

Proof of Lemma 6. In order to prove that the function $F_{\delta_1,\dots,\delta_\ell}$ is not a d-th power, it is enough to show that at least one of the coefficients of its divisor is not divisible by d.

Let $\mathcal{R}$ be a co-set of $\mathcal{E}(\mathbb{F}_p)$ in $\mathcal{E}(\overline{\mathbb{F}}_p)$. Since $\mathcal{E}(\mathbb{F}_p)$ is cyclic, $\mathcal{R}$ has the form

$$\mathcal{R} = \{S \oplus aG \mid a = 1, \dots, T\}$$

with arbitrary $S \in \mathcal{R}$.

For a given co-set $\mathcal{R}$ let the divisor of f respect to this co-set be

$$\operatorname{div}_{\mathcal{R}}(f) = \sum_{R \in \mathcal{R}} \operatorname{ord}_R(f)[R]$$

where now

$$\operatorname{div}(f) = \sum_{\mathcal{R}} \operatorname{div}_{\mathcal{R}}(f).$$

If $R \in \mathcal{R}$ is a zero (or a pole) of f, then all of the zeros (and poles) of $F_{\delta_1,\dots,\delta_\ell}$ in $\mathcal{R}$ have the form $R \oplus aG \ominus d_iG$ ($a \in \{1,\dots,T\}$, $i \in \{1,\dots,\ell\}$) and no other zero (and pole) belongs to this $\mathcal{R}$. Thus the divisor of $F_{\delta_1,\dots,\delta_\ell}$ respect to $\mathcal{R}$ is

$$\begin{aligned}\operatorname{div}_{\mathcal{R}}(F_{\delta_1,\dots,\delta_\ell}) &= \operatorname{div}_{\mathcal{R}}(f^{\delta_1} \circ \tau_{d_1G} \dots f^{\delta_\ell} \circ \tau_{d_\ell G}) = \sum_{R\in\mathcal{R}} \sum_{i=1}^{\ell} \delta_i \operatorname{ord}_R(f)[R \ominus d_iG] \\ &= \sum_{a=1}^{T} \sum_{i=1}^{\ell} \delta_i \operatorname{ord}_{S\oplus aG}(f)[S \oplus aG \ominus d_iG]. \qquad (11)\end{aligned}$$

where S is a fixed element of $\mathcal{R}$.

Let us fix a co-set $\mathcal{R}$ such that it contains at least one zero or pole of f whose order is co-prime to d, and let $\mathcal{A}$ be the multiset of a's ($a = 1,\dots,T$) with multiplicity $\operatorname{ord}_{R\oplus aG}(f)$ modulo d and $\mathcal{B}$ be the multiset of $-d_i$'s with multiplicity δ_i ($i = 1,\dots,\ell$). All of the orders $\operatorname{ord}_R(f)$ $R \in \operatorname{Supp}(f)$ are co-prime to d, the number of distinct elements of $\mathcal{B}$ is less than or equal to ℓ and $(|\operatorname{Supp}(f)|, \ell, T)$ is d-admissible, then there is an Q whose multiplicity in $\mathcal{A}+\mathcal{B}$ is not divisible by d, so its coefficient in the divisor of $F_{\delta_1,\dots,\delta_\ell}$ is not divisible by d. □

5. Admissibility

In order to use Theorem 2 one needs criteria for a triple (k,ℓ,T) being d-admissible.

Theorem 3. *Let us denote the least prime factor of m by $p(m)$. Then*

(i) *If $k, m, d \in \mathbb{N}$, $k < p(m)$ then the triple $(k, 2, m)$ is d-admissible.*

(i) *If $k, \ell, m, d \in \mathbb{N}$, $k < m$ and*

$$(4\ell)^k < p(m), \qquad (12)$$

then the triple (k,ℓ,m) is d-admissible.

(i) *If T is prime, all of the prime factors of d are primitive roots modulo m, then for every pair $k, \ell \in \mathbb{N}$ with $k < m$, $\ell < m$, the triple (k,ℓ,m) is d-admissible.*

Throughout this section we will denote the multiplicity of a in $\mathcal{A}$ by $m_{\mathcal{A}}(a)$.

First we show that it is enough to prove the theorem, when d is a prime number:

Lemma 7. *If for all of the prime divisors p of d (k,ℓ,m) is p-admissible, then (k,ℓ,m) is d-admissible.*

PROOF. Assume that there are multisets $\mathcal{A}$, $\mathcal{B}$ such that $\mathcal{A}+\mathcal{B}$ possess property $P(d)$.

Let $d = p_1^{\alpha_1}\dots p_r^{\alpha_r}$, and let p_i be a prime divisor such that $p_i^{\alpha_i}$ does not divide all of the multiplicities $m_{\mathcal{B}}(b)$ $(b\in\mathcal{B})$.

If there is an element $b\in\mathcal{B}$ such that $p_i \nmid m_{\mathcal{B}}(b)$ then let us define $\mathcal{A}'$ (resp. $\mathcal{B}'$) by taking the element $a\in\mathcal{A}$ with multiplicity $m_{\mathcal{A}}(a) \mod p_i$ (resp. $b\in\mathcal{B}$ with multiplicity $m_{\mathcal{B}}(b) \mod p_i$). Clearly $\mathcal{A}'$ and $\mathcal{B}'$ are not empty (i.e. not all of the multiplicities $m_{\mathcal{A}}(a)$, $m_{\mathcal{B}}(b)$ are divisible by p_i) and $\mathcal{A}'+\mathcal{B}'$ has property $P(p_i)$.

If all the multiplicities $m_{\mathcal{B}}(b)$ are divisible by p_i, then let β_i be the largest power such that

$$p_i^{\beta_i} \mid \gcd\{m_{\mathcal{B}}(b) : b\in\mathcal{B}\}$$

Clearly $\beta_i<\alpha_i$. Let $\mathcal{A}'=\mathcal{A}$ and let $\mathcal{B}'$ be the multiset of elements $b\in\mathcal{B}$ with multiplicity $m_{\mathcal{B}}(b)p^{-\beta_i}$. Now not all of the multiplicities $m_{\mathcal{B}'}(b')$ are divisible by p_i and $\mathcal{A}'+\mathcal{B}'$ has property $P(d/p_i^{\beta_i})$. By using the argument above there are $\mathcal{A}''$ and $\mathcal{B}''$ such that $\mathcal{A}''+\mathcal{B}''$ has property $P(p_i)$. □

PROOF OF THEOREM 3. By Lemma 7, we can assume, that d is a prime number. Since the proof is similar to the proof of the original version of this lemma [9], we will leave some of the details to the reader.

Proof of (1) in Theorem 3. Assume that contrary to the assertion, there are $k,m,d\in\mathbb{N}$ with $k<p(m)$ such that the triple $(k,2,m)$ is not d-admissible, i.e. there are multisets $\mathcal{A},\mathcal{B}\subset\mathbb{Z}_m$ such that the number of distinct elements of $\mathcal{A}$ is k, the number of distinct elements of $\mathcal{B}$ is 2 and the number of solutions of (6) is divisible by d for all $c\in\mathbb{Z}_m$.

Let the two distinct elements of $\mathcal{B}$ be r, $r+s$ (where now $s\neq 0$). Every element of $\mathcal{A}+r$ has at least two representations in form (6) whence $\{a+r\,|\,a\in\mathcal{A}\}=\{a+r+s\mid a\in\mathcal{A}\}$ as sets. Therefore $\{a+r\mid a\in\mathcal{A}\}=\{a+r+st\mid a\in\mathcal{A}\}$ for any $t\in\mathbb{N}$. Hence $\mathcal{A}+r$ contains a co-set of a non-trivial subgroup of $\mathbb{Z}_m$ generated by s thus the number of distinct elements of $\mathcal{A}$ is greater or equal to $p(m)$.

Proof of (2) in Theorem 3. Assume that k,ℓ,m satisfy (12), and we have $\mathcal{A},\mathcal{B}\subset\mathbb{Z}_m$, such that the number of distinct elements of $\mathcal{A}$ is k and the number of distinct elements of $\mathcal{B}$ is ℓ.

If $s\in\mathbb{N}$, $(s,m)=1$, then (6) and

$$sa+sb=sc,\quad a\in\mathcal{A},\ b\in\mathcal{B}$$

have the same solutions, and if c runs over the element of $\mathbb{Z}_m$, then here $c'=sc$ does the same. Thus it suffices to show, that there are $s\in\mathbb{N}$, $c\in\mathbb{Z}_m$, $(s,m)=1$

such that the number of the solution of the equation

$$sa + sb = c, \quad a \in \mathcal{A},\ b \in \mathcal{B} \tag{13}$$

is not divisible by d.

For $a \in \mathbb{Z}$, let $r(a)$ denote the absolute least residue of a modulo m, i.e. define $r(a) \in \mathbb{Z}$ by

$$r(a) \equiv a \mod m, \quad -\frac{m}{2} < r(a) \le \frac{m}{2}$$

We need the analogue of Lemma 3 in [9]:

Lemma 8. *If k, ℓ, m, $\mathcal{A}$ are defined as above, and the distinct elements of $\mathcal{A}$ are represented by $a_1, \dots, a_k$, then there is an s such that $(s, m) = 1$ and*

$$|r(sa_i)| \le \frac{1}{2}\left[\frac{m}{\ell}\right] \quad \text{for } i = 1, \dots, k. \tag{14}$$

Proof. Let $\mathcal{J} = \{1, \dots, p(m)\}$. Clearly, if $i, j \in \mathcal{J}$, then $(i - j, m) = 1$ and there is no other set of indices with this property whose cardinality is greater than $|\mathcal{J}|$.

Consider the $p(m)$ k-tuples

$$\underline{u}_j = (r(ja_1), \dots, r(ja_k)), \quad j \in \mathcal{J}. \tag{15}$$

Write $D = \frac{1}{2}\left[\frac{m}{\ell}\right] + 1$ and $Z = \left[\frac{m}{D}\right] + 1$. Then $DZ > m$, thus for all $j \in \mathcal{J}$ there are non-negative integers $t_1 = t_1(j), \dots, t_k = t_k(j)$ such that

$$r(ja_i) \in \left\{-\left[\frac{m}{2}\right] + t_i D, -\left[\frac{m}{2}\right] + t_i D + 1, \dots, -\left[\frac{m}{2}\right] + (t_i + 1)D - 1\right\}$$

where

$$t_i \in \{0, 1, \dots, Z - 1\} \tag{16}$$

for $i = 1, \dots, k$.

The number of the possible k-tuples $t_1, \dots, t_k$ with (16) is, by (12),

$$Z^k = \left(\left[\frac{m}{D}\right] + 1\right)^k < \left(2\frac{m}{D}\right)^k < \left(2\frac{m}{m/2\ell}\right)^k = (4\ell)^k < p(m),$$

thus there are at least two different indices $j_1, j_2 \in \mathcal{J}$ such that

$$t_1 = t_1(j_1) = t_1(j_2), \dots, t_k = t_k(j_1) = t_k(j_2).$$

Then we have

$$-\left[\frac{m}{2}\right] + t_i D \le r(j_1 a_i), r(j_2 a_i) < \left[\frac{m}{2}\right] + (t_i + 1)D$$

whence

$$|r(j_1 a_i) - r(j_2 a_i)| < D \quad \text{for } i = 1, \dots, k.$$

Finally we can define s by $s = |j_1 - j_2|$, so that $(s, m) = 1$. □

In order to complete the proof of (2), consider an s which satisfies (14). Let $b_1, \ldots, b_\ell$ denote the distinct elements of $\mathcal{B}$, and let $1 \le i, j \le \ell$ be indices such that

$$sb_l \notin \{sb_i + 1, \ldots, sb_j - 1\} \quad \text{for } l = 1, \ldots, \ell.$$

By the pigeon hole principle the maximum distance of two consecutive sb_l's is at least $[m/\ell] + 1$.

Let us denote the values of $r(sa_1), \ldots, r(sa_k)$, ordered increasingly, by $r_1, \ldots, r_k$:

$$-\frac{1}{2}\left[\frac{m}{\ell}\right] \le r_1 \le \cdots \le r_k \le \frac{1}{2}\left[\frac{m}{\ell}\right].$$

By (14) we have

$$\begin{aligned}(sb_j + r_1) - (sb_i + r_k) &= (sb_j - sb_i) + r_1 - r_k \\ &\ge \left(\left[\frac{m}{\ell}\right] + 1\right) - \frac{1}{2}\left[\frac{m}{\ell}\right] - \frac{1}{2}\left[\frac{m}{\ell}\right] = 1 > 0.\end{aligned}$$

Consider u, v such that $r(sa_u) = r_1$, $r(sa_v) = r_k$, then the numbers of representation of the numbers

$$sa_v + sb_i \quad \text{and} \quad sa_u + sb_j$$

is the number of pairs $(a, b) = (a_v, b_i)$ and $(a', b') = (a_u, b_j)$ resp., and this is $m_{\mathcal{A}}(a_v)m_{\mathcal{B}}(b_i)$ and $m_{\mathcal{A}}(a_u)m_{\mathcal{B}}(b_j)$ which are co-prime to d.

Proof of (3) of Theorem 3. For any multiset $\mathcal{C} \subset \mathbb{Z}_m$ let us consider the polynomial $P_{\mathcal{C}}(x) \in \mathbb{Z}_d[x]$ defined by

$$P_{\mathcal{C}}(x) = \sum_{c \in \mathcal{C}} x^{r_m(c)}.$$

As in the classical case for any multisets $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_d$, $\mathcal{A} + \mathcal{B}$ has property $P(d)$ if and only if

$$P_{\mathcal{A}}(x)P_{\mathcal{B}}(x) \equiv 0 \mod x^m - 1.$$

If $x^{m-1} + \cdots + 1$ is reducible in $\mathbb{Z}_d[x]$, say $P_1(x)P_2(x) = x^{m-1} + \cdots + 1$, then let us define $\mathcal{A}, \mathcal{B}$ by $P_1(x) = \sum_{a \in \mathcal{A}} x^{r_m(a)}$ and $P_2(x)(x-1) = \sum_{b \in \mathcal{B}} x^{r_m(b)}$. Thus clearly $\mathcal{A} + \mathcal{B}$ has property $P(d)$.

Conversely if $x^{m-1} + \cdots + 1$ is irreducible in $\mathbb{Z}_d[x]$, and $\mathcal{A} + \mathcal{B}$ has property $P(d)$ then $x^{m-1} + \cdots + 1$ must divide $P_{\mathcal{A}}(x)$ or $P_{\mathcal{B}}(x)$ thus $\mathcal{A}$ or $\mathcal{B}$ contains $\mathbb{Z}_m$.

Finally by Theorem 2.47 (in [13] p.65) the polynomial $x^{m-1} + \cdots + 1$ is irreducible in $\mathbb{Z}_d[x]$ if and only if m is prime and d is a primitive root modulo T. □

As in [9] we can define the analogue of "good" numbers:

Definition 9. A positive integer m is said to be *good* respect to d if for any pair $k, \ell \in \mathbb{N}$ with $k < m$, $\ell < m$, the triple (k, ℓ, m) is d-admissible.

By Theorem 3 we can characterize the *good* numbers:

Corollary 10. *The number m is good respect to d, if and only if it is prime and all of the prime factors of d are primitive roots modulo m.*

Proof. It remains to show that if for every numbers $k, \ell \in \mathbb{N}$ the triple (k, ℓ, m) is d-admissible, then for each prime divisor p of d and numbers $k', \ell' \in \mathbb{N}$ the triple (k', ℓ', m) is p-admissible.

Let p be a prime factor of d and α be a power such that $p^\alpha \| d$. Furthermore let $\mathcal{A}$, $\mathcal{B}$ be multisets which posses property $P(p)$. Then let $\mathcal{A}'$ be a multiset which consists the element $a \in \mathcal{A}$ with multiplicity $m_{\mathcal{A}'}(a)$ $(0 \le m_{\mathcal{A}'}(a) < d)$ satisfying

$$m_{\mathcal{A}'}(a) \equiv m_{\mathcal{A}}(a) \mod p^\alpha$$
$$m_{\mathcal{A}'}(a) \equiv 1 \mod d/p^\alpha,$$

and let $\mathcal{B}'$ be a multiset which contains the elements $b \in \mathcal{B}$ with multiplicity $m_{\mathcal{B}}(b) \cdot \frac{d}{p}$.

Then the multiplicity of elements $a \in \mathcal{A}'$ are co-prime to d and $\mathcal{A}' + \mathcal{B}'$ possess property $P(d)$ □

Acknowledgements. I would like to thank to the referee for his valuable remarks.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, Measures of pseudorandomness for finite sequences: typical values, *Proc. Lond. Math. Soc.* **95** (2007), 778–812.

[2] P. H. T. Beelen and J. M. Doumen, Pseudorandom sequences from elliptic curves, in: Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), *Springer-Verlag, Berlin – Heidelberg – New York*, 2002, 37–52.

[3] Z. Chen, Elliptic curve analogue of Legendre sequences, *Monatsh. Math.* **154** (2008), 1–10.

[4] Z. Chen, S. Li and G. Xiao, Construction of pseudo-random binary sequences from elliptic curves by using discrete logarithm, in: Sequences and Their Applications - SETA 2006, Vol. 4086, Lecture Notes in Comput. Sci., *Springer, Berlin*, 2006, 285–294.

[5] E. ElMahassni and I. Shparlinski, On the uniformity of distribution of congruential generators over elliptic curves, in: Sequences and their applications (Bergen, 2001), Discrete Math. Theor. Comput. Sci., *Springer*, *London*, 2002, 257–264.

[6] E. ElMahassni and I. Shparlinski, On the distribution of the elliptic curve power generator, in: Finite fields and applications, Vol. 461, Contemp. Math., *Amer. Math. Soc., Providence, RI*, 2008, 111–118.

[7] G. Gong and C. C. Y. Lam, Linear recursive sequences over elliptic curves, in: Sequences and their applications (Bergen, 2001), Discrete Math. Theor. Comput. Sci., *Springer*, *London*, 2002, 182–196.

[8] G. Gong, T. A. Berson and D. R. Stinson, Elliptic curve pseudorandom sequence generators, in: Selected areas in cryptography (Kingston, ON, 1999), Vol. 1758, Lecture Notes in Comput. Sci., *Springer*, *Berlin*, 2000, 34–48.

[9] L. Goubin, C. Mauduit and A. Sárközy, Construction of large families of pseudorandom binary sequences, *J. Number Theory* **106** (2004), 56–69.

[10] K. Gyarmati, On a family of pseudorandom binary sequences, *Periodica Math. Hungar.* **49** (2004), 45–63.

[11] S. Hallgren, Linear congruential generators over elliptic curves, Tech. Report CS-94-143, *Carnegie Mellon Univ.*, 1994.

[12] T. Lange and I. Shparlinski, Distribution of some sequences of points on elliptic curve, *J. Math. Cryptol.* **1**, no. 1 (2007), 1–11.

[13] R. Lidl and H. Niederreiter, Finite Fields, second ed., *Cambridge University Press*, 1997.

[14] C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol, *Acta Arith.* **82** (1997), 365-377.

[15] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, *CRC Press*, *Boca Raton, FL*, 1997.

[16] L. Mérai, Construction of large families of pseudorandom binary sequences, *Ramanujan J.* **18** (2009), 341–349.

[17] L. Mérai, Construction of pseudorandom binary lattices based on multiplicative characters, *Period. Math. Hungar.* **59** (2009), 43–51.

[18] S. M. Oon, Construction des suites binaires pseudo-aléatories, PhD thesis, *Nancy*, 2005.

[19] S. M. Oon, On pseudo-random properties of certain Dirichlet series, *Ramanujan J.* **15** (2008), 19–30.

[20] G. I. Perel'muter, On certain character sums, *Uspehi Mat. Nauk* **18** (1963), 145–149.

[21] M. Perret, Multiplicative Characters Sums and Nonlinear Geometric Codes, Eurocode '90, *Springer-Verlag*, *Berlin – Heidelberg – New York*, 1991, 158-165.

[22] M. Perret, Multiplicative characters sums and Kummer coverings, *Acta Arith.* **59** (1991), 279-290.

[23] A. Sárközy, A finite pseudorandom binary sequence, *Studia Sci. Math. Hungar.* **38** (2001), 377–384.

[24] I. Shparlinski, Pseudorandom number generators from elliptic curves, in: Recent trends in cryptography, Vol. 477, Contemp. Math., *Amer. Math. Soc., Providence, RI*, 2009, 121–141.

[25] J. H. Silverman, The Arithmetic of Elliptic Curves, *Springer*, *Berlin*, 1995.

László Mérai
Rényi Alfréd Institute
Reáltanoda u. H-1053 Budapest,
Hungary

E-mail: merai@cs.elte.hu

(Received November 30, 2010; revised May 24, 2011)