ACTA ARITHMETICA
LXXXII.4 (1997)

On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol

by

Christian Mauduit (Marseille) and András Sárközy (Budapest)

1. Introduction. In the last 60 years numerous papers have been written on pseudorandom sequences (we shall also write PR for pseudorandomness). In these papers a wide range of goals, approaches, and tools is presented; even the concept of "pseudorandomness" is interpreted in different ways (depending mostly on the applications in mind). In the majority of the papers constructions of pseudorandom sequences are given and/or tested for pseudorandomness. In several other papers, inspired mostly by cryptography, methods of mathematical logic, probability theory and combinatorics are used to study pseudorandomness (see e.g., [C-T], [Ko], [ML]; further references are given in [Kn]). These latter papers do a very valuable work in analysing and explaining the concept of pseudorandomness but, on the other hand, they are of not much use when it gets to constructing and testing special pseudorandom sequences. In this series we will focus on problems of the first type, i.e., on constructing and testing, more exactly, on apriori or, as Knuth calls it, "theoretical" testing.

The concept of "pseudorandom sequence" can be interpreted in three different ways:

1) $[0,1)$ sequences,
2) pseudorandom sequences of integers selected from $\{1,\dots,N\}$,
3) pseudorandom binary, or more generally, b-ary sequences.

Another related concept is that of the pseudorandom subset.

(Here we shall study only the case when the target distribution is uniform, i.e., the case of "uniform PR-sequence".)

1991 *Mathematics Subject Classification*: Primary 11K45.

Research of the second author partially supported by Hungarian National Foundation for Scientific Research, Grant No. T017433 and CEE fund No. CIPA-CT92-4022. This paper was written while the second author was visiting the Institut de Mathématiques de Luminy (UPR 9016 CNRS), Marseille.

Knuth [Kn] gives an excellent survey of these concepts. He does not distinguish sharply between the three concepts, which is completely justified by the fact that the three concepts are closely related, and there are simple transition algorithms as described in [Kn]. Indeed, recently several papers [Ge], [F-M1], [F-M2], [M-S1], [M-S2] have been written on arithmetic properties of integers characterized by digit properties, and all these papers point to the direction that the arithmetic properties and digit properties are independent. This independence can be utilized by using the principle of "double twist": if we want to construct, say, a PR-sequence of type 2, then first we may use a number theoretic principle to construct a PR-sequence of type 3 ("first twist") and then we apply a transition algorithm ("second twist"), which destroys the original arithmetic structure, in order to get a PR-sequence of type 2.

In spite of the close connection between the three types of PR-sequences, there are also certain differences and, in particular, the study of the different PR-concepts may inspire different approaches and construction principles. So far mostly PR-sequences of type 1 and 2 have been studied; excellent surveys of the theory of uniform PR-sequences are given by Niederreiter in [Ni1], [Ni2] (see also the monograph [Ni3] and the more recent papers [EH-N1], [EH-N2], [EH-N3], [E-L-T]). In these papers Niederreiter gives a brief description and analysis of the methods of PR-sequence generation, starting from the most classical and widely used linear congruential method, and ending with the most promising, recently introduced method studied mostly by Eichenauer-Herrmann, Lehn, Niederreiter and Topuzoğlu which is based on the concept of the multiplicative inverse. A common feature of all these methods is that the construction of the PR-sequence

$$X = (x_1, x_2, \dots, x_N) \tag{1.1}$$

is given by a recursion

$$x_n = f(x_{n-1}, x_{n-2}, \dots, x_{n-k}). \tag{1.2}$$

An important advantage of this sort of constructions is that the elements of the PR-sequence (1.1) can be computed by a (usually) simple algorithm. On the other hand, there are disadvantages as well; later we shall return to such a difficulty.

Niederreiter (later with coauthors) did a work of basic importance in justifying the use of these construction methods by carrying out the "serial test" in all these cases, i.e., he showed that the $[0, 1)$ PR-sequences (1.1) constructed by these methods are such that the discrepancy of the sequence

$$(x_1, x_2, \dots, x_s), \dots, (x_n, x_{n+1}, \dots, x_{n+s-1}), \dots, (x_{N-s+1}, x_{N-s+2}, \dots, X_N)$$

of s-dimensional vectors is "small" (for fixed s).

Other advantages and deficiencies of these constructions have been studied as well. In particular, as Niederreiter [Ni1] writes, a deficiency of the most often used linear congruential method is: "Other known regularities in sequences of linear congruential pseudorandom numbers are certain long-range correlations. These regularities can be disruptive in simulations where random irregularities are desired". In general, this analysis of the known constructions leads to the conclusion that, although the new constructions are superior to the previous ones from many points of view, there is a price paid for this (e.g., better structure but more complicated generating algorithm) so that there is no perfect construction. Thus the selection of the construction method to be applied must depend on the application in mind; the construction which is superior in a certain situation may fail in another one. This also means that the search for new approaches and new constructions should be continued.

Less attention has been paid to PR-sequences of type 3 (see, e.g., [MW-S]); here the most intensively studied construction is the shift-register method.

Based on the observations above, in this series we will focus on the least intensively studied type of PR-sequences, i.e., on *pseudorandom binary sequences*. Our goal is first to analyse the random properties of several known important binary sequences and also to give further constructions. In order to analyse and compare all these constructions and to try to eliminate certain deficiencies of the previous methods, first we shall have to introduce a new measure (or measures) of pseudorandomness.

We emphasize that our goal is not the search for new constructions superior to *all* previous ones; this clearly would be too optimistic. Instead, we are aiming at constructions superior to the previous ones at least in certain special situations; besides we will gather new information on random-type properties of special binary sequences playing an important role in number theory and in other fields of mathematics.

2. Measures of pseudorandomness of binary sequences. Before proposing a measure for pseudorandomness of binary sequences, we formulate and discuss the most important requirements to be fulfilled by such a measure.

First, we expect that this measure should reflect the most important and intensively studied random properties such as

1. normality;
2. well-distribution relative to arithmetic progressions;
3. small multiple correlations.

Indeed, in the case of *infinite* sequences $E = (e_1, e_2, \ldots) \in \{-1, 1\}^\infty$ these

random properties can be defined in the following way:

For $k \in \mathbb{N}$, $M \in \mathbb{N}$, $X = (x_1, \dots, x_k) \in \{-1,1\}^k$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $D = (d_1, \dots, d_k) \in \mathbb{N}^k$, $d_1 < \dots < d_k$, write

$$T(E,M,X) = |\{n : 0 \le n < M,\ (e_{n+1}, e_{n+2}, \dots, e_{n+k}) = X\}|, \tag{2.1}$$

$$U(E,M,a,b) = \sum_{j=1}^{M} e_{a+jb} \tag{2.2}$$

and

$$V(E,M,D) = \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k}. \tag{2.3}$$

Then E is said to be *normal* (Knuth uses the term "∞-distributed") if

$$|T(E,M,X) - M/2^k| = o(M) \tag{2.4}$$

for all fixed k and X, as $M \to \infty$, while the second and third random property above can be expressed as

$$U(E,M,a,b) = o(M), \tag{2.5}$$

resp.

$$V(E,M,D) = o(M) \tag{2.6}$$

for all fixed a, b and D, as $M \to \infty$. (Note that the "serial test" in [Kn] corresponds to proving (2.4).) It is easy to see that the two requirements (2.4) and (2.6) are *equivalent*. Moreover, by an important theorem of Niven and Zuckerman [N-Z] (see also [C]) the normality of E implies that E possesses random property 2 in the strong sense that for all $k, m \in \mathbb{N}$, E must be "(m,k)-distributed" (see [Kn, p. 148]), i.e., roughly speaking, E is normal with respect to arithmetic progressions of difference m and strings of length k.

In view of these facts, in the case of *infinite* binary sequences it suffices to require normality.

Before trying to formulate *finite* analogues of these random properties, first we will pose two further requirements of different nature.

To explain the next requirement, as an illustration first consider the following definition of pseudorandomness of finite binary sequences given by Knuth [Kn, p. 162]:

Definition 1. A finite sequence $E_N = (e_1, \dots, e_N) \in \{-1,1\}^N$ is said to be *PR* if for all $k \in \mathbb{N}$ with

$$k \le \frac{\log N}{\log 2}, \tag{2.7}$$

and for all $X \in \{-1,1\}^k$ we have

$$\left| T(E_N, N+1-k, X) - \frac{N+1-k}{2^k} \right| \le \frac{1}{\sqrt{N}}. \tag{2.8}$$

(On the left hand side the frequency of the string X in E_N is compared with the expectation for it.)

Note that condition (2.7) expresses the fact that strings of length much greater than $(\log N)/\log 2$ occur only with "small" probability.

The definition above allows two possibilities only: a sequence is either "good" or "bad", i.e., it is either PR or not. Instead, we would like to introduce a more flexible measure of pseudorandomness. Namely, it may occur that, say, a sequence does not satisfy (2.8) but (2.8) holds in the slightly weaker form, with $2/\sqrt{N}$ on the right hand side; however, this slight deficiency can be more than compensated by the fact that certain other random-type properties (playing an especially important role in our application) hold optimally. In such a case, of course, we would like to accept the sequence as a "good" one. Correspondingly, the fourth requirement is:

4. The pseudorandomness of binary sequences should be characterized by a real-valued function defined on the set of all finite binary sequences (so that one should be able to compare two sequences of the same length).

A further natural requirement is that:

5. One should be able to estimate this PR-measure at least for certain "nice" sequences.

Since it is practically hopeless to define a measure which can be estimated reasonably well for the majority of sequences, the last requirement is:

6. This PR-measure should have different levels, and one should be able to estimate at least low level measures, to interpret the result obtained as a "trend", a "partial result" towards pseudorandomness.

In order to define such a PR-measure, first we will introduce PR-measures characterizing the random properties 1, 2, 3 above. Indeed, for each of these properties, there is a quite natural way to assign a measure of pseudorandomness to any given $E_N = (e_1, \dots, e_N) \in \{-1, 1\}^N$:

1. *Normality measure of order k*:

$$N_k(E_N) = \max_{X \in \{-1,1\}^k} \max_{0 < M \le N+1-k} |T(E_N, M, X) - M/2^k|.$$

(See (2.1) and (2.4).)

2. *Normality measure*:

$$N(E_N) = \max_{k \le (\log N)/\log 2} N_k(E_N).$$

(See condition (2.7) in Definition 1.)

3. *Well-distribution measure*:

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

where the maximum is taken over all a, b, t such that $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ and $1 \le a + b \le a + tb \le N$. (See (2.2) and (2.5).)

4. *Correlation measure of order k*:

$$C_k(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \Big| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k} \Big|$$

where the maximum is taken over all $D = (d_1, \dots, d_k)$ and M such that $M + d_k \le N$. (See (2.3) and (2.6).)

5. *Correlation measure*: Here one wants a bound for $C_k(E_N)$ for k "not very large" (for large k the estimate of $C_k(E_N)$ can be extremely difficult). In view of condition (2.7) in Definition 1, one may introduce the correlation measure as

$$C(E_N) = \max_{k \le (\log N)/\log 2} C_k(E_N).$$

(Another option could be $C^*(E_N) = \sum_{k=1}^{\infty} C_k(E_N)/2^k$.)

In the finite case, the connection between normality, well-distribution in arithmetic progressions and correlation is much more complicated than in the infinite case. While in the infinite case normality and small correlation ((2.4) and (2.6)) are equivalent, here the connection is one way:

Proposition 1. *For all N, E_N and $k < N$ we have*

$$N_k(E_N) \le \max_{1 \le t \le k} |C_t(E_N)|. \tag{2.9}$$

Proof. For all $k, N \in \mathbb{N}$, $X = (x_1, \dots, x_k) \in \{-1, 1\}^k$ and $1 \le M \le N + 1 - k$ we have

$$\begin{aligned}
&|T(E_N, M, X) - M/2^k| \\
&\quad = \Big| |\{n : 0 \le n < M,\ (e_{n+1}, e_{n+2}, \dots, e_{n+k}) = X\}| - \frac{M}{2^k} \Big| \\
&\quad = \Big| \sum_{n=0}^{M-1} \frac{x_1 \dots x_k}{2^k} \prod_{j=1}^{k} (e_{n+j} + x_j) - \frac{M}{2^k} \Big| \\
&\quad = \Big| \frac{x_1 \dots x_k}{2^k} \sum_{1 \le d_1 < \dots < d_t \le k} \Big(\prod_{j \in \{1,\dots,k\} \setminus \{d_1,\dots,d_t\}} x_j \Big) \sum_{n=0}^{M-1} e_{n+d_1} \dots e_{n+d_t} \Big|
\end{aligned}$$

$$\leq \frac{1}{2^k} \sum_{\substack{D\subset\{1,2,\ldots,k\}\\ D\neq\emptyset}} |V(E_N, M, D)| \leq \frac{1}{2^k} \sum_{t=1}^{k} \binom{k}{t} C_t(E_N)$$

$$\leq \max_{1\leq t\leq k} |C_t(E_N)|,$$

which proves (2.9).

The connection between the well-distribution measure and the correlation measures is less direct. The smallness of the quantities $|C_k(E_N)|$ implies a "weak tendency" towards well-distribution, but $W(E_N)$ can be quite large; problems 28, 29 and 30 in [Kn, p. 168] show the difficulties.

In the opposite direction, nothing can be said; indeed, it may occur that both the normality measure and the well-distribution measure are very small, but the correlation measure is very large:

EXAMPLE 1. Consider a sequence $E_N = (e_1, \ldots, e_N) \in \{-1, 1\}^N$ such that both the normality measure and well-distribution measure of it are possibly small, and define $E'_{2N} = (e'_1, e'_2, \ldots, e'_{2N}) \in \{-1, 1\}^{2N}$ by

$$e'_n = \begin{cases} e_n & \text{for } 1 \leq n \leq N, \\ e_{n-N} & \text{for } N < n \leq 2N. \end{cases}$$

Then the normality measure and well-distribution measure of E'_{2N} are less than a constant times the corresponding measure of E_N, but

$$C_2(E'_N) \geq \Big| \sum_{n=1}^{N} e'_n e'_{n+N} \Big| = N.$$

These considerations lead to the conclusion that *in order to show that a finite binary sequence can be considered as a PR-sequence in the sense that it possesses each of the random properties* 1, 2 *and* 3, *it suffices to show that both the well-distribution measure and correlation measure are small*; moreover, both these measures must be checked. These two measures can be combined, and this way we end up with the "combined PR-measures" that we propose to use:

6. *Combined* (well-distribution-correlation) *PR-measure of order k*:

$$Q_k(E_N) = \max_{a,b,t,D} \Big| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \ldots e_{a+jb+d_k} \Big| \tag{2.10}$$

$$= \max_{a,b,t,D} |Z(a, b, t, D)|$$

where

$$|Z(a, b, t, D)| = \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \ldots e_{a+jb+d_k} \tag{2.11}$$

is defined for all a, b, t, $D = (d_1, d_2, \dots, d_k)$ such that all the subscripts $a + jb + d_l$ belong to $\{1, \dots, N\}$ (and the maximum in (2.10) is taken over D's of dimension k). (Roughly speaking: $Q_k(E_N)$ measures the "correlation of order k along arithmetic progressions".)

7. *Combined PR-measure*:

$$Q(E_N) = \max_{k \le (\log N)/\log 2} Q_k(E_N) \tag{2.12}$$

(another option: $Q^*(E_N) = \sum_{k=1}^{\infty} Q_k(E_N)/2^k$).

Finally, consider the following example:

EXAMPLE 2. Consider a sequence $E_N = (e_1, \dots, e_N) \in \{-1, 1\}^N$ such that both the correlation measure and well-distribution measure (or even the combined measure) of it are small, and define $E'_{2N} = (e'_1, \dots, e'_{2N}) \in \{-1, 1\}^{2N}$ by

$$e'_n = \begin{cases} e_n & \text{for } 1 \le n \le N, \\ e_{2N-n} & \text{for } N \le n \le 2N. \end{cases}$$

Then it is easy to see that the correlation measure and the well-distribution measure of E'_{2N} are less than a constant times the corresponding measure of E_N so that in terms of our PR-measures the sequence E'_{2N} must be considered as a PR-sequence, although a "truly random" sequence certainly cannot be as symmetric as E'_{2N}.

This example illustrates that there is no perfect universal measure of pseudorandomness; one may pose further and further criteria for pseudorandomness (and in certain applications, one can be forced to do this), and correspondingly, one may introduce further PR-measures. However, it would be more and more difficult to handle these measures; besides posing too many PR-requirements, it may occur that there is no PR-sequence of a given size at all. This difficulty is discussed in [Kn] in details and, indeed, it is well described in terms of the theory of Kolmogorov complexity. Thus one has to draw the limit somewhere and to focus on certain basic PR-criteria playing the most important role in applications and studied most intensively; we drew this limit by restricting ourselves to normality, well-distribution and correlation.

3. The pseudorandomness of the Legendre symbol. It follows from the discussion above that the combined PR measures Q_k and Q have the desired properties 1–4 and 6. It remains to show that they also have property 5, i.e., they can be used for testing "nice" sequences for pseudorandomness. This can be shown by an example, and indeed, we will test the Legendre symbol, which seems to be the most natural candidate, for pseudorandomness:

THEOREM 1. *There is a number p_0 such that if $p > p_0$ is a prime number, $k \in \mathbb{N}$, $k < p$ and if we write*

$$E_{p-1} = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right)\right),$$

then

$$Q_k(E_{p-1}) \le 9kp^{1/2}\log p \tag{3.1}$$

so that, writing $N = p-1$,

$$Q(E_N) = \max_{k \le (\log N)/\log 2} Q_k(E_N) \le 27N^{1/2}(\log N)^2 \tag{3.2}$$

and also

$$Q^*(E_N) = \sum_{k=1}^{\infty} Q_k(E_N)/2^k \le 33N^{1/2}\log N. \tag{3.3}$$

(We will estimate the minimum of these PR-measures over $\{-1,1\}^N$ in a subsequent paper.)

The crucial tool in the proof of Theorem 1 will be the following result (which follows from A. Weil's theorem [We]):

THEOREM 2. *Suppose that p is a prime number, χ is a non-principal character modulo p of order d (so that $d \mid p-1$), $f(x) \in F_p[x]$ (F_p being the field of modulo p residue classes) has degree k and a factorization $f(x) = b(x-x_1)^{d_1}\ldots(x-x_s)^{d_s}$ (where $x_i \ne x_j$ for $i \ne j$) in $\overline{F}_p$ (the algebraic closure of F_p) with*

$$(d, d_1, \ldots, d_s) = 1. \tag{3.4}$$

Let X, Y be real numbers with $0 < Y \le p$. Then

$$\Big|\sum_{X < n \le X+Y} \chi(f(n))\Big| < 9kp^{1/2}\log p. \tag{3.5}$$

Note that similar results appear in [B] and [B-L]. However, in [B] no proof is given, while in [B-L] both the statement and proof are false due to the incorrect use of A. Weil's inequality (although the basic idea is right). Thus for the sake of completeness we shall present the proof here.

We shall need the following consequence of Theorem 2:

COROLLARY 1. *If p is a prime number, $f(x) \in F_p[x]$ is a polynomial of degree k such that it is not of the form $f(x) \in b(g(x))^2$ with $b \in F_p$, $g(x) \in F_p[x]$ (in other words, in the factorization of f in $\overline{F}_p$ as in Theorem 2, there is at least one odd exponent d_i), and X, Y are real numbers with $0 < Y \le p$, then writing*

$$\chi_p^*(n) = \begin{cases} \left(\frac{n}{p}\right) & \text{for } (n,p) = 1, \\ 0 & \text{for } p \mid n, \end{cases}$$

we have

$$\Big|\sum_{X<n\le X+Y}\chi_p^*(f(n))\Big| < 9kp^{1/2}\log p.$$

4. Four lemmas. To give an upper bound for the incomplete character sum in (3.5), first we need upper bound for complete hybrid character sums. (A hybrid character sum is one involving both multiplicative and additive characters.)

LEMMA 1. *If p, χ, d are defined as in Theorem* 2, *$a\in\mathbb{Z}$, $f(x)\in F_p[x]$ is a polynomial which has precisely s distinct ones among its roots, and the polynomials $y^d-f(x)$ and z^p-z-x are absolutely irreducible, then*

$$\Big|\sum_{x\in F_p}\chi(f(x))e\Big(\frac{ax}{p}\Big)\Big| \le sp^{1/2}. \tag{4.1}$$

P r o o f. This is a part of Theorem 2G in [Sch, p. 45] and, indeed, it is a consequence of Andre Weil's theorem on curves over finite fields [We] (while in [Sch] it is proved in a more elementary way).

LEMMA 2. *If $d\in\mathbb{N}$, K is a field, and $y^d-f(x)\in K[x,y]$, then the following two conditions are equivalent*:

(i) *$y^d-f(x)$ is absolutely irreducible*;

(ii) *if $f(x)=b(x-x_1)^{d_1}\dots(x-x_s)^{d_s}$ is the factorization of f in $\overline{K}$, with $x_i\ne x_j$ for $i\ne j$, then $(d,d_1,\dots,d_s)=1$.*

P r o o f. This is a part of Lemma 2C in [Sch].

LEMMA 3. *If p, χ, d, $f(x)$ and k are defined as in Theorem* 2 *and $a\in\mathbb{Z}$, then*

$$\Big|\sum_{x\in F_p}\chi(f(x))e(ax/p)\Big| \le kp^{1/2}. \tag{4.2}$$

P r o o f. Since (3.4) is assumed, (ii) of Lemma 2 holds with F_p in place of K, so that by Lemma 2, $y^d-f(x)$ is absolutely irreducible.

Next, we apply Lemma 2 with F_p, x and z^p-z in place of K, y^d and $f(x)$, respectively. Since now $d=1$ we find that (ii) of Lemma 2 holds so that by Lemma 2 the polynomial $x-(z^p-z)$ (and thus also its negative) is absolutely irreducible.

Thus Lemma 1 can be applied. Since clearly we have $s\le k$, (4.2) follows from (4.1) and this completes the proof of Lemma 3.

To switch from complete character sums to incomplete character sums, one may use the Vinogradov [Vin] principle extended and generalized in the form of the Erdős–Turán inequality. Here we use this inequality in the following form:

LEMMA 4. *If $m \in \mathbb{N}$, the function $g(x) : \mathbb{Z} \to \mathbb{C}$ is periodic with period m, and X, Y are real numbers with $Y > 0$ then*

$$\Big|\sum_{X<n\le X+Y} g(n)\Big| \le \frac{Y+1}{m}\Big|\sum_{n=1}^{m} g(n)\Big| + \sum_{1\le|h|\le m/2} |h|^{-1}\Big|\sum_{n=1}^{m} g(n)e\Big(\frac{hn}{m}\Big)\Big|. \tag{4.3}$$

Proof. This form of the Erdős–Turán inequality is presented in a preprint written by Friedlander and Iwaniec [F-I] where the authors write: "In this form (4.3) follows for instance from two applications of (3.4) of [Iw]".

5. Completion of the proof of Theorem 2. Applying first Lemma 4 with p and $\chi(f(n))$ in place of m and $g(n)$, respectively, and then using Lemma 3 we obtain

$$\begin{aligned}\Big|\sum_{X<n\le X+Y} \chi(f(n))\Big| &\le \frac{Y+1}{p}\Big|\sum_{n=1}^{p}\chi(f(n))\Big| \\ &\quad + \sum_{1\le|h|\le p/2}|h|^{-1}\Big|\sum_{n=1}^{p}\chi(f(n))e(hn/p)\Big| \\ &< 2kp^{1/2} + 2\sum_{1\le h\le p/2} h^{-1}kp^{1/2} \\ &< 2kp^{1/2}(1+(1+\log(p/2))) < 2kp^{1/2}(2+\log p) \\ &\le 2kp^{1/2}\Big(2\frac{\log p}{\log 2}+\log p\Big) < 9kp^{1/2}\log p.\end{aligned}$$

Proof of Corollary 1. Choosing $\chi(n) = \chi_p^*(n)$ in Theorem 2, we have $d = 2$ so that (3.4) in Theorem 2 holds if (and only if) one of the exponents $d_1, \dots, d_s$ is odd, i.e., $f(x)$ is not of the form $f(x) = b(g(x))^2$.

6. Proof of Theorem 1. Defining $Z(a,b,t,D)$ by (2.11) (with $e_n = \big(\frac{n}{p}\big)$), for $k < p$ we have

$$|Z(a,b,t,D)| = \Big|\sum_{n=0}^{t}\Big(\frac{a+nb+d_1}{p}\Big)\Big(\frac{a+nb+d_2}{p}\Big)\dots\Big(\frac{a+nb+d_k}{p}\Big)\Big| \tag{6.1}$$

for all a, b, t, $D = (d_1, \dots, d_k)$ such that

$$a + nb + d_l \in \{1, \dots, p-1\} \quad \text{for } n = 0, 1, \dots, t \text{ and } l = 1, \dots, k. \tag{6.2}$$

Clearly, we may assume that $(b,p) = 1$. Then let $\bar{b}$ be an integer with $b\bar{b} \equiv 1 \pmod p$ and for $j = 1, \dots, k$, let h_j denote an integer with

$$h_j \equiv (a+d_j)\bar{b} \pmod{p}$$

so that

$$h_i \not\equiv h_j \pmod{p} \quad \text{for } 1 \le i < j \le k. \tag{6.3}$$

Write $f(n) = (n+h_1)(n+h_2)\dots(n+h_k)$. Then it follows from (6.1) that

$$\begin{aligned}|Z(a,b,t,D)| &= \left|\sum_{n=0}^{t}\left(\frac{a\bar{b}+n+d_1\bar{b}}{p}\right)\left(\frac{a\bar{b}+n+d_2\bar{b}}{p}\right)\dots\left(\frac{a\bar{b}+n+d_k\bar{b}}{p}\right)\right| \\ &= \left|\sum_{n=0}^{t}\left(\frac{n+h_1}{p}\right)\left(\frac{n+h_2}{p}\right)\dots\left(\frac{n+h_k}{p}\right)\right| \\ &= \left|\sum_{n=0}^{t}\left(\frac{f(n)}{p}\right)\right| = \left|\sum_{n=0}^{t}\chi_p^*(f(n))\right|\end{aligned}$$

with the character χ_p^* defined in Corollary 1.

Writing $X=-1$, $Y=t+1$, clearly we may assume that $0<Y=t+1\le N+1=p$. Moreover, since $f(x)$ has no multiple zero by (6.3), Corollary 1 can be applied. We obtain

$$|Z(a,b,t,D)| < 9kp^{1/2}\log p,$$

which proves (3.1). Now, (3.2) and (3.3) follow from (3.1) and this completes the proof of Theorem 1.

Acknowledgements. We would like to thank Professors H. Iwaniec and F. Rodier for the valuable discussions.

References

[B] A. Barg, *Exponential sums and constrained error-correcting codes*, in: Algebraic Coding (Paris, 1991), Lecture Notes in Comput. Sci. 573, Springer, 1992, 16–22.

[B-L] A. Barg and S. N. Lytsin, *DC-constrained codes from Hadamard matrices*, IEEE Trans. Inform. Theory 37 (1991), 801–807.

[C] J. W. S. Cassels, *On a paper of Niven and Zuckerman*, Pacific J. Math. 2 (1952), 555–557.

[C-T] F. R. K. Chung and P. Tetali, *Communication complexity and quasirandomness*, SIAM J. Discrete Math. 6 (1993), 110–123.

[E-L-T] J. Eichenauer, J. Lehn and A. Topuzoğlu, *A nonlinear congruential pseudorandom generator with power of two modulus*, Math. Comp. 51 (1988), 757–759.

[EH-N1] J. Eichenauer-Herrmann and H. Niederreiter, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus*, ibid. 58 (1992), 775–779.

[EH-N2] —, —, *Kloosterman-type sums and the discrepancy of nonoverlapping pairs of inversive congruential pseudorandom numbers*, Acta Arith. 65 (1993), 185–194.

[EH-N3] J. Eichenauer-Herrmann and H. Niederreiter, *Bounds for exponential sums and their applications to pseudorandom numbers*, ibid. 67 (1994), 269–281.

[F-I] J. Friedlander and H. Iwaniec, preprint.

[F-M1] E. Fouvry et C. Mauduit, *Sommes des chiffres et nombres presque premiers*, Math. Ann. 305 (1996), 571–599.

[F-M2] —, —, *Méthodes de crible et fonctions sommes des chiffres*, Acta Arith. 77 (1996), 339–351.

[Ge] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, ibid. 13 (1968), 259–265.

[Iw] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. 87 (1987), 385–401.

[Kn] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

[Ko] A. N. Kolmogorov, *On table of random numbers*, Sankhya A 25 (1963), 369–376.

[MW-S] F. J. MacWilliams and N. J. A. Sloane, *Pseudo-random sequences and arrays*, Proc. IEEE 64 (1976), 1715–1729.

[ML] P. Martin-Löf, *The definition of random sequences*, Inform. and Control (Shenyang) 6 (1966), 602–619.

[M-S1] C. Mauduit and A. Sárközy, *On the arithmetic structure of sets characterized by sum of digits properties*, J. Number Theory 61 (1996), 25–38.

[M-S2] —, —, *On the arithmetic structure of the integers whose sum of digits is fixed*, Acta Arith. 81 (1997), 145–173.

[Ni1] H. Niederreiter, *Recent trends in random number and random vector generation*, Ann. Oper. Res. 31 (1991), 323–345.

[Ni2] —, *New methods for pseudorandom number and pseudorandom vector generation*, in: Proc. 1992 Winter Simulation Conference, J. J. Swain *et al.* (eds.), IEEE Press, Piscataway, N.J., 1992, 264–269.

[Ni3] —, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[N-Z] I. Niven and H. S. Zuckerman, *On the definition of normal numbers*, Pacific J. Math. 1 (1951), 103–109.

[Sch] W. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math. 536, Springer, New York, 1976.

[Vin] I. M. Vinogradov, *Elements of Number Theory*, Dover, 1954.

[We] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.

Institut de Mathématiques de Luminy
CNRS-UPR 9016
163 av. de Luminy, Case 930
F-13288 Marseille Cédex 9, France

Department of Algebra and Number Theory
Eötvös Loránd University
Muzeum krt. 6-8
H-1088 Budapest, Hungary
E-mail: sarkozy@cs.elte.hu

Received on 4.2.1997 (3126)