MATHEMATICS OF COMPUTATION
VOLUME 55, NUMBER 191
JULY 1990, PAGES 277–287

LOWER BOUNDS FOR THE DISCREPANCY OF INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS

HARALD NIEDERREITER

ABSTRACT. The inversive congruential method is a uniform pseudorandom number generator which was introduced recently. For a prime modulus p the discrepancy $D_p^{(k)}$ of k-tuples of successive pseudorandom numbers generated by this method determines the statistical independence properties of these pseudorandom numbers. It was shown earlier by the author that

$$D_p^{(k)} = O(p^{-1/2}(\log p)^k) \quad \text{for } 2 \le k < p.$$

Here it is proved that this bound is essentially best possible. In fact, for a positive proportion of the admissible parameters in the inversive congruential method the discrepancy $D_p^{(k)}$ is at least of the order of magnitude $p^{-1/2}$ for all $k \ge 2$.

1. INTRODUCTION AND STATEMENT OF RESULTS

The well-known deficiencies of the linear congruential method for the generation of uniform pseudorandom numbers, such as the relatively coarse lattice structure of linear congruential pseudorandom numbers, have prompted recent efforts at devising methods with more favorable properties. One way of breaking up the lattice structure is to use a congruential method with a nonlinear recursion. A particularly attractive method of this type is based on achieving nonlinearity by employing the operation of multiplicative inversion with respect to a prime modulus. This *inversive congruential method* was introduced by Eichenauer and Lehn [2].

For an arbitrary finite field F_q with q elements, let F_q^* be the multiplicative group of nonzero elements of F_q. For $c \in F_q^*$ let $\bar{c}$ denote the inverse of c in the group F_q^*, and for $0 \in F_q$ put $\bar{0} = 0$. The group F_q^* is cyclic, and a generator of this group is called a *primitive element* of F_q. A monic polynomial over F_q of degree $d \ge 1$ is called a *primitive polynomial* over F_q if it has a primitive element of the extension field F_{q^d} as a root. We refer to [4, Chapter 3] for information on primitive polynomials. We note, in particular, that a primitive polynomial over F_q is always irreducible over F_q.

Received August 7, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 65C10; Secondary 11K38, 11K45, 11T21.

We can now describe the inversive congruential method. For a prime $p \geq 5$ we consider the finite field F_p which we can also identify with the set $F_p = \{0, 1, \ldots, p-1\}$ of integers. Choose a, $b \in F_p$ in such a way that $x^2 - bx + a$ is a primitive polynomial over F_p. Then we generate a sequence $y_0, y_1, \ldots$ of elements of F_p by the recursion

$$y_{n+1} \equiv -a\overline{y}_n + b \bmod p \quad \text{for } n = 0, 1, \ldots . \tag{1}$$

The numbers $x_n = y_n/p$, $n = 0, 1, \ldots$, in the interval $[0, 1)$ are called *inversive congruential pseudorandom numbers*. In practice, p is taken to be a large prime such as $p = 2^{31} - 1$.

It was shown in [2] that the sequence $y_0, y_1, \ldots$ (and thus the sequence $x_0, x_1, \ldots$) is purely periodic with period length p and that $\{y_0, y_1, \ldots, y_{p-1}\} = F_p$. From the work of Eichenauer, Grothe, and Lehn [1] and the author [7] it follows that inversive congruential pseudorandom numbers pass the *k-dimensional lattice test* for all dimensions $k \leq (p+1)/2$.

The behavior of these pseudorandom numbers under the k-dimensional serial test was investigated in [8]. We recall that this test amounts to considering the *discrepancy* of k-tuples of successive pseudorandom numbers. For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^k$, $k \geq 1$, we define the discrepancy

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) = \sup_J |F_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0, 1)^k$, $F_N(J)$ is N^{-1} times the number of terms among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and $V(J)$ denotes the k-dimensional volume of J. If $x_0, x_1, \ldots$ is a sequence of inversive congruential pseudorandom numbers with modulus p, then we consider the points

$$\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+k-1}) \in [0, 1)^k \quad \text{for } n = 0, 1, \ldots, p-1,$$

and we write

$$D_p^{(k)} = D_p(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p-1})$$

for their discrepancy. It was proved in [8] that $D_p^{(k)} = O(p^{-1/2}(\log p)^k)$ for $2 \leq k < p$, where the implied constant is absolute. In the following we establish lower bounds for $D_p^{(k)}$ which show that the upper bound is essentially best possible. We let ϕ be Euler's totient function and $\omega(m)$ be the number of different prime factors of a positive integer m.

Theorem 1. *For any prime $p \geq 5$ there are at least $\phi(p+1)$ primitive polynomials $x^2 - bx + a$ over F_p such that for the corresponding inversive congruential pseudorandom numbers we have*

$$D_p^{(k)} > \frac{1}{2\pi + 4}(p^{-1/2} - 2p^{-3/5}) \quad \textit{for all } k \geq 2.$$

Theorem 2. *Let $p \geq 5$ be a prime, and let $0 < t < 1$. Then there are more than $A_p(t)\phi(p^2-1)/2$ primitive polynomials $x^2 - bx + a$ over F_p such that for the corresponding inversive congruential pseudorandom numbers we have*

$$D_p^{(k)} > \frac{t}{2\pi+4} p^{-1/2} \quad \text{for all } k \geq 2,$$

where

$$A_p(t) = \frac{(1-t^2)p - (p^{1/2}+2)2^{\omega(p-1)}}{(4-t^2)p + 4p^{1/2} + 1}.$$

These results demonstrate that for any p there exist parameters in the inversive congruential method such that $D_p^{(k)}$ is at least of the order of magnitude $p^{-1/2}$ for all $k \geq 2$. Therefore, the upper bound $D_p^{(k)} = O(p^{-1/2}(\log p)^k)$ is in general best possible up to the logarithmic factor. The fact that $D_p^{(k)}$ can be as large as $p^{-1/2}$ in order of magnitude shows that there is a considerable amount of irregularity in the sequence of pseudorandom numbers, a feature which can be advantageous for various simulation purposes. In contrast, for the linear congruential method with prime modulus p, it is known by the results of [5, 6] that, on the average, the k-dimensional discrepancy over the full period is at most of the order of magnitude p^{-1} times a logarithmic factor, and so there is substantially less irregularity in this case.

Theorem 2 gives more precise information in the following sense. We note, first of all, that it follows from well-known results of number theory [3, pp. 260, 359] that $2^{\omega(m)} = O(m^{\varepsilon})$ for every $\varepsilon > 0$ (see also the proof of Lemma 5 for an elementary effective bound). Thus, for fixed t we have

$$\lim_{p\to\infty} A_p(t) = \frac{1-t^2}{4-t^2} > 0.$$

Furthermore, the total number of primitive polynomials over F_p of degree 2 is given by $\phi(p^2-1)/2$ according to [4, Theorems 3.5 and 3.16]. Therefore, Theorem 2 says that for large p there is a positive proportion of the admissible parameter sets in the inversive congruential method for which $D_p^{(k)}$ is at least of the order of magnitude $p^{-1/2}$ for all $k \geq 2$.

To understand the proofs of our theorems it may be helpful to remark that if $x^2 - bx + a$ is a primitive polynomial over F_q, then a must be a primitive element of F_q. To see this, note that this primitive quadratic polynomial has a primitive element α of F_{q^2} as a root, hence the polynomial has the factorization $x^2 - bx + a = (x-\alpha)(x-\alpha^q)$. This implies $a = \alpha^{q+1}$, and since α^{q+1} has order $q-1$ in the group $F_{q^2}^*$, this yields the desired conclusion. We note also that $b \neq 0$, for otherwise $\alpha + \alpha^q = 0$, hence $\alpha^{2(q-1)} = 1$, a contradiction to α being a primitive element of F_{q^2}.

In §2 we show several auxiliary results, some of which may be of independent interest. The proof of Theorems 1 and 2 is completed in §3.

2. Auxiliary results

We write $e(u) = e^{2\pi i u}$ for real u and $\mathbf{u}\cdot\mathbf{v}$ for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$.

Lemma 1. *Let* $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0,1)^k$, $k \geq 1$, *with discrepancy* $D_N = D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1})$. *Then for any nonzero* $\mathbf{h} = (h_1, \ldots, h_k) \in \mathbb{Z}^k$ *we have*

$$\left|\sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{t}_n)\right| \leq \frac{2}{\pi}\left(\left(\frac{\pi+1}{2}\right)^m - \frac{1}{2^m}\right) N D_N \prod_{j=1}^{k} \max(1, 2|h_j|),$$

where m *is the number of nonzero coordinates of* $\mathbf{h}$.

Proof. Like any complex number, the sum in question can be represented in the form

$$\sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{t}_n) = e(\theta)\left|\sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{t}_n)\right|$$

for some real θ. Therefore,

$$\left|\sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{t}_n)\right| = \sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{t}_n - \theta),$$

and taking real parts we get

$$\left|\sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{t}_n)\right| = \sum_{n=0}^{N-1} \cos 2\pi(\mathbf{h}\cdot\mathbf{t}_n - \theta).$$

The desired bound follows now from an inequality in [6, p. 64, last paragraph]. □

For a nontrivial additive character χ of F_q and for $a \in F_q^*$, we define the character sum

$$K(\chi, a) = \sum_{c\in F_q} \chi(c + a\bar{c}). \tag{2}$$

By changing c into $-c$ in the summation, we see that $K(\chi, a)$ is always real. Note that $\chi(c+d) = \chi(c)\chi(d)$ for all $c, d \in F_q$ by the definition of an additive character, and that $\sum_{c\in F_q} \chi(c) = 0$ by [4, p. 192].

Lemma 2. *For any nontrivial* χ *we have* $\sum_{a\in F_q^*} K(\chi, a)^2 = q^2$.

Proof. We have

$$\begin{aligned}\sum_{a\in F_q^*} K(\chi, a)^2 &= \sum_{a\in F_q^*}\sum_{c,d\in F_q} \chi(c + d + a(\bar{c} + \bar{d})) \\ &= \sum_{c,d\in F_q} \chi(c+d) \sum_{a\in F_q^*} \chi(a(\bar{c}+\bar{d})).\end{aligned}$$

The inner sum is equal to -1 if $\bar{c}+\bar{d}\neq 0$ and equal to $q-1$ if $\bar{c}+\bar{d}=0$, i.e., if $c+d=0$. Thus,

$$\sum_{a\in F_q^*} K(\chi, a)^2 = (q-1)q - \sum_{\substack{c,d\in F_q \\ c+d\neq 0}} \chi(c+d)$$
$$= (q-1)q - \sum_{c,d\in F_q} \chi(c+d) + q = q^2. \quad \square$$

For a nontrivial multiplicative character ψ of F_q we define the Gaussian sum

$$G(\psi, \chi) = \sum_{c\in F_q^*} \psi(c)\chi(c)$$

and the Jacobi sum

$$J(\psi) = \sum_{c\in F_q} \psi(c(1-c)),$$

where we use the convention $\psi(0)=0$. The conjugate character ψ^{-1} of ψ is defined by $\psi^{-1}(c)=\psi(\bar{c})$ for $c\in F_q$. Note that $\psi(cd)=\psi(c)\psi(d)$ for all c, $d\in F_q$ by the definition of a multiplicative character, and that $\sum_{c\in F_q}\psi(c)=0$ by [4, p. 205].

Lemma 3. *For any nontrivial χ and ψ we have*

$$\sum_{c,d\in F_q} \chi(c+d)\psi^{-1}(\bar{c}+\bar{d}) = G(\psi, \chi)(J(\psi)+2).$$

Proof. For $c, d\in F_q$ we have

$$\psi^{-1}(\bar{c}+\bar{d}) = \begin{cases} \psi^{-1}(c+d)\psi(cd) & \text{if } cd\neq 0, \\ \psi(c)+\psi(d) & \text{if } cd=0. \end{cases}$$

Therefore,

$$\sum_{c,d\in F_q} \chi(c+d)\psi^{-1}(\bar{c}+\bar{d})$$
$$= 2G(\psi, \chi) + \sum_{c,d\in F_q^*} \chi(c+d)\psi^{-1}(c+d)\psi(cd)$$
$$= 2G(\psi, \chi) + \sum_{c,d\in F_q} \chi(c+d)\psi^{-1}(c+d)\psi(cd).$$

With the substitution $c+d=f$ we get

$$\begin{aligned}
&\sum_{c,d\in F_q}\chi(c+d)\psi^{-1}(c+d)\psi(cd)\\
&\quad=\sum_{c,f\in F_q}\chi(f)\psi^{-1}(f)\psi(c(f-c))\\
&\quad=\sum_{f\in F_q^*}\chi(f)\psi^{-1}(f)\sum_{c\in F_q}\psi(c(f-c))\\
&\quad=\sum_{f\in F_q^*}\chi(f)\psi^{-1}(f)\sum_{c\in F_q}\psi(cf(f-cf))\\
&\quad=\sum_{f\in F_q^*}\chi(f)\psi(f)\sum_{c\in F_q}\psi(c(1-c))=G(\psi,\chi)J(\psi).\quad\square
\end{aligned}$$

The group of multiplicative characters of F_q is isomorphic to F_q^*, and hence cyclic of order $q-1$. For a positive divisor m of $q-1$, let $H_q(m)$ be the set of characters of order m in this character group. Let P_q be the set of primitive elements of F_q. Furthermore, we write μ for the Moebius function and $\sum_{m|n}$ for a sum over the positive divisors m of a positive integer n.

Lemma 4. *For any nontrivial χ we have*

$$\begin{aligned}
\sum_{a\in P_q}K(\chi,a)^2=\frac{\phi(q-1)}{q-1}q^2+\frac{\phi(q-1)}{q-1}\sum_{\substack{m|(q-1)\\ m>1}}\frac{\mu(m)}{\phi(m)}\\
\cdot\sum_{\psi\in H_q(m)}G(\psi,\chi)^2(J(\psi)+2).
\end{aligned}$$

Proof. By a result in [4, p. 258] we have for $a\in F_q^*$

$$\frac{\phi(q-1)}{q-1}\sum_{m|(q-1)}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\psi(a)=\begin{cases}1 & \text{if } a\in P_q,\\ 0 & \text{if } a\notin P_q.\end{cases}$$

Therefore,

$$\begin{aligned}
\sum_{a\in P_q}K(\chi,a)^2&=\sum_{a\in F_q^*}\left(\frac{\phi(q-1)}{q-1}\sum_{m|(q-1)}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\psi(a)\right)K(\chi,a)^2\\
&=\frac{\phi(q-1)}{q-1}\sum_{m|(q-1)}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\sum_{a\in F_q^*}\psi(a)K(\chi,a)^2\\
&=\frac{\phi(q-1)}{q-1}q^2+\frac{\phi(q-1)}{q-1}\\
&\quad\cdot\sum_{\substack{m|(q-1)\\ m>1}}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\sum_{a\in F_q^*}\psi(a)K(\chi,a)^2,
\end{aligned}$$

where we have split off the contribution for $m = 1$ and used Lemma 2. Furthermore, for any nontrivial ψ we get

$$\begin{aligned}
\sum_{a\in F_q^*} \psi(a)K(\chi, a)^2 &= \sum_{a\in F_q^*} \psi(a) \sum_{c,d\in F_q} \chi(c+d+a(\bar{c}+\bar{d})) \\
&= \sum_{c,d\in F_q} \chi(c+d) \sum_{a\in F_q^*} \psi(a)\chi(a(\bar{c}+\bar{d})) \\
&= \sum_{\substack{c,d\in F_q \\ \bar{c}+\bar{d}=0}} \chi(c+d) \sum_{a\in F_q^*} \psi(a) + \sum_{\substack{c,d\in F_q \\ \bar{c}+\bar{d}\neq 0}} \chi(c+d) \sum_{a\in F_q^*} \psi(a)\chi(a(\bar{c}+\bar{d})) \\
&= \sum_{\substack{c,d\in F_q \\ \bar{c}+\bar{d}\neq 0}} \chi(c+d) \sum_{a\in F_q^*} \psi(a)\psi^{-1}(\bar{c}+\bar{d})\chi(a) \\
&= G(\psi, \chi) \sum_{c,d\in F_q} \chi(c+d)\psi^{-1}(\bar{c}+\bar{d}) = G(\psi, \chi)^2(J(\psi)+2),
\end{aligned}$$

where we used Lemma 3 in the last step. □

Lemma 5. *For any nontrivial χ there exists an $a \in P_q$ with $|K(\chi, a)| > q^{1/2} - 2q^{2/5}$.*

Proof. We note that for nontrivial ψ and χ we have $|G(\psi, \chi)| = q^{1/2}$ by [4, Theorem 5.11] and $|J(\psi)| \le q^{1/2}$ by [4, Theorem 5.22]. Using also $\operatorname{card}(H_q(m)) = \phi(m)$, from Lemma 4 we obtain

$$\begin{aligned}
\sum_{a\in P_q} K(\chi, a)^2 &\ge \frac{\phi(q-1)}{q-1}q^2 - \frac{\phi(q-1)}{q-1} \sum_{\substack{m|(q-1) \\ m>1}} |\mu(m)|q(q^{1/2}+2) \\
&> \frac{\phi(q-1)}{q-1}q^2 - \frac{\phi(q-1)}{q-1}q(q^{1/2}+2) \sum_{m|(q-1)} |\mu(m)|.
\end{aligned}$$

The last sum is easily seen to be $2^{\omega(q-1)}$, hence

$$\sum_{a\in P_q} K(\chi, a)^2 > \frac{\phi(q-1)}{q-1}q^2 - \frac{\phi(q-1)}{q-1}q(q^{1/2}+2)2^{\omega(q-1)}. \tag{3}$$

We claim that for every positive integer m we have $2^{\omega(m)} < (2.4)m^{0.357}$. This is trivial for $m = 1$. For $m > 1$, let $m = p_1^{e_1} \cdots p_r^{e_r}$ be the canonical factorization of m. Then

$$2^{\omega(m)} = 2^r = m^{(\log 2)/\log 7} \prod_{j=1}^{r} \frac{2}{p_j^{e_j(\log 2)/\log 7}} < m^{0.357} \prod_{j=1}^{r} \frac{2}{p_j^{(\log 2)/\log 7}}.$$

In the last product the factors are ≤ 1 for primes $p_j \ge 7$, hence

$$2^{\omega(m)} < \frac{8}{30^{(\log 2)/\log 7}} m^{0.357} < (2.4)m^{0.357}.$$

Together with (3) we get

$$\sum_{a \in P_q} K(\chi, a)^2 > \frac{\phi(q-1)q}{q-1}(q - (2.4)q^{0.357}(q^{1/2}+2)).$$

If $q < 2^{10}$, then the result of Lemma 5 is trivial since the lower bound is negative. Thus, we can assume $q \geq 2^{10}$ in the rest of the proof. Then

$$\begin{aligned} 4q^{1/10} - (2.4)q^{0.057}(1 + 2q^{-1/2}) &\geq 4q^{1/10} - (2.55)q^{0.057} \\ &\geq 8 - (2.55)2^{0.57} > 4, \end{aligned}$$

hence

$$q - (2.4)q^{0.357}(q^{1/2}+2) > (q^{1/2} - 2q^{2/5})^2,$$

and so

$$\sum_{a \in P_q} K(\chi, a)^2 > \frac{\phi(q-1)q}{q-1}(q^{1/2} - 2q^{2/5})^2 > \phi(q-1)(q^{1/2} - 2q^{2/5})^2.$$

Since $\operatorname{card}(P_q) = \phi(q-1)$, the desired result follows. □

Lemma 6. *Let χ be nontrivial, and let $0 < t < 1$. Then there are more than $A_q(t)\phi(q-1)$ values of $a \in P_q$ for which $|K(\chi, a)| > tq^{1/2}$, where*

$$A_q(t) = \frac{(1-t^2)q - (q^{1/2}+2)2^{\omega(q-1)}}{(4-t^2)q + 4q^{1/2} + 1}.$$

Proof. We can assume that $A_q(t) \geq 0$, for otherwise the result is trivial. We proceed by contradiction and suppose that $|K(\chi, a)| > tq^{1/2}$ holds for at most $A_q(t)\phi(q-1)$ values of $a \in P_q$. Then $|K(\chi, a)| \leq tq^{1/2}$ holds for at least $(1 - A_q(t))\phi(q-1)$ values of $a \in P_q$. Now we note that the sum $K(\chi, a)$ differs from a Kloosterman sum [4, Definition 5.42] only in one respect, namely that in (2) we also take into account the contribution from $c = 0 \in F_q$. Since this contribution is equal to 1, it follows from a classical bound for Kloosterman sums [4, Theorem 5.45] that

$$|K(\chi, a)| \leq 2q^{1/2} + 1 \quad \text{for all } a \in F_q^*.$$

Therefore, we obtain

$$\begin{aligned} \sum_{a \in P_q} K(\chi, a)^2 &\leq (1 - A_q(t))\phi(q-1)t^2 q + A_q(t)\phi(q-1)(2q^{1/2}+1)^2 \\ &= \phi(q-1)(q - (q^{1/2}+2)2^{\omega(q-1)}) \\ &\leq \frac{\phi(q-1)}{q-1}q^2 - \frac{\phi(q-1)}{q-1}q(q^{1/2}+2)2^{\omega(q-1)}, \end{aligned}$$

which is a contradiction to (3). □

3. Proof of Theorems 1 and 2

First we apply Lemma 1 with $k \geq 2$, $N = p$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n \leq p-1$, and $\mathbf{h} = (1, -1, 0, \ldots, 0) \in \mathbb{Z}^k$. This yields

$$pD_p^{(k)} \geq \frac{1}{2\pi + 4} \left| \sum_{n=0}^{p-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| .$$

Next we observe that from (1) we get

$$\begin{aligned} \left| \sum_{n=0}^{p-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| &= \left| \sum_{n=0}^{p-1} e(x_n - x_{n+1}) \right| = \left| \sum_{n=0}^{p-1} e\left(\frac{1}{p}(y_n - y_{n+1})\right) \right| \\ &= \left| \sum_{n=0}^{p-1} e\left(\frac{1}{p}(y_n + a\overline{y}_n - b)\right) \right| = \left| \sum_{n=0}^{p-1} e\left(\frac{1}{p}(y_n + a\overline{y}_n)\right) \right| . \end{aligned}$$

Let χ be the nontrivial additive character of F_p given by $\chi(c) = e(c/p)$ for $c \in F_p$. Then, since $y_0, y_1, \ldots, y_{p-1}$ run through F_p, a comparison with (2) shows that

$$\left| \sum_{n=0}^{p-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| = |K(\chi, a)| ,$$

and so

$$pD_p^{(k)} \geq \frac{1}{2\pi + 4} |K(\chi, a)| \quad \text{for all } k \geq 2 . \tag{4}$$

Therefore, if the primitive polynomial $x^2 - bx + a$ over F_p is chosen in such a way that for the primitive element $a \in F_p$ we have the lower bound for $|K(\chi, a)|$ in Lemma 5 (with $q = p$), then from (4) we obtain the lower bound for $D_p^{(k)}$ in Theorem 1. Similarly, the lower bound for $|K(\chi, a)|$ in Lemma 6 (with $q = p$) yields the lower bound for $D_p^{(k)}$ in Theorem 2. To prove Theorems 1 and 2 in their full extent, it remains to determine for each given primitive element $a \in F_p$ the number of primitive polynomials over F_p of the form $x^2 - bx + a$. This is done in the following lemma for any finite field F_q.

Lemma 7. *For any primitive element $a \in F_q$ there are exactly $\phi(q^2-1)/2\phi(q-1)$ primitive polynomials over F_q of the form $x^2 - bx + a$.*

Proof. As we noted in §1, if $x^2 - bx + a$ is primitive over F_q, then for some primitive element $\alpha \in F_{q^2}$ we have $x^2 - bx + a = (x - \alpha)(x - \alpha^q)$, hence $\alpha^{q+1} = a$. Since the primitive elements α and α^q determine the same primitive polynomial $x^2 - bx + a$, it follows that the desired number of primitive polynomials is given by $\frac{1}{2}S(a)$, where $S(a)$ is the number of primitive elements $\alpha \in F_{q^2}$ with $\alpha^{q+1} = a$. For any $\lambda \in F_{q^2}^*$ we write $\operatorname{ord}(\lambda)$ for the order of λ in the group $F_{q^2}^*$. Since $\operatorname{ord}(a) = q - 1$ and $F_{q^2}^*$ is cyclic, we have $a = \beta^{q+1}$

for some $\beta \in F_{q^2}^*$. Let γ be a fixed primitive element of F_{q^2}; then $\beta = \gamma^h$ for some integer h. Now

$$q - 1 = \operatorname{ord}(a) = \operatorname{ord}(\gamma^{(q+1)h}) = \frac{q^2 - 1}{\gcd(q^2 - 1, (q+1)h)},$$

thus $\gcd(q^2 - 1, (q+1)h) = q + 1$, and so $\gcd(q - 1, h) = 1$. For $\lambda \in F_{q^2}^*$ we have $\lambda^{q+1} = a$ if and only if $(\lambda\overline{\beta})^{q+1} = 1$, which holds precisely if $\lambda\overline{\beta} = \gamma^{(q-1)j}$ for some integer j. Thus the elements $\lambda \in F_{q^2}^*$ with $\lambda^{q+1} = a$ are exactly those of the form $\lambda = \gamma^{h+(q-1)j}$, where h is fixed and j varies. Consequently, $S(a)$ is equal to the number of integers $j \bmod (q+1)$ with $\gcd(q^2-1, h+(q-1)j) = 1$. Since $\gcd(q - 1, h) = 1$, we have $\gcd(q^2 - 1, h + (q - 1)j) = 1$ if and only if $\gcd(q + 1, h + (q - 1)j) = 1$.

First let q be even. Then $\gcd(q + 1, q - 1) = 1$, and so for every integer $m \bmod (q + 1)$ with $\gcd(q + 1, m) = 1$ we can solve the congruence $h + (q - 1)j \equiv m \bmod (q + 1)$ uniquely for $j \bmod (q + 1)$. Therefore, $S(a) = \phi(q + 1) = \phi(q^2 - 1)/\phi(q - 1)$.

Now let q be odd, hence $\gcd(q + 1, q - 1) = 2$. For every integer $m \bmod (q + 1)$ with $\gcd(q + 1, m) = 1$ consider the congruence $h + (q - 1)j \equiv m \bmod (q + 1)$, or equivalently $(q - 1)j \equiv m - h \bmod (q + 1)$. Since $\gcd(q + 1, m) = \gcd(q - 1, h) = 1$, both m and h are odd, and so the last congruence has exactly two solutions $j \bmod (q + 1)$ for every choice of m. Therefore $S(a) = 2\phi(q + 1) = \phi(q^2 - 1)/\phi(q - 1)$. □

It follows from Lemma 7 and the preceding discussion that in Theorem 1 we get at least $\phi(p^2 - 1)/2\phi(p - 1) = \phi(p + 1)$ suitable primitive polynomials. Similarly, together with Lemma 6, we see that in Theorem 2 we get more than

$$A_p(t)\phi(p - 1)\frac{\phi(p^2 - 1)}{2\phi(p - 1)} = A_p(t)\frac{\phi(p^2 - 1)}{2}$$

suitable primitive polynomials.

Bibliography

1. J. Eichenauer, H. Grothe, and J. Lehn, *Marsaglia's lattice test and nonlinear congruential pseudo random number generators*, Metrika **35** (1988), 241–250.
2. J. Eichenauer and J. Lehn, *A non-linear congruential pseudo random number generator*, Statist. Hefte **27** (1986), 315–326.
3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Clarendon Press, Oxford, 1960.
4. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, Mass., 1983.
5. H. Niederreiter, *Pseudo-random numbers and optimal coefficients*, Adv. in Math. **26** (1977), 99–181.
6. ——, *The serial test for pseudo-random numbers generated by the linear congruential method*, Numer. Math. **46** (1985), 51–68.

7. H. Niederreiter, *Remarks on nonlinear congruential pseudorandom numbers*, Metrika **35** (1988), 321–328.
8. ____, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144.

INSTITUTE FOR INFORMATION PROCESSING, AUSTRIAN ACADEMY OF SCIENCES, DR.-IGNAZ-SEIPEL-PLATZ 2, A-1010 VIENNA, AUSTRIA