GENERATING RANDOM WALKS IN GROUPS

J. SATTLER and C. P. SCHNORR

Fachbereich Mathematik, Goethe-Universität Frankfurt/Main, Robert-Mayer St. 6 – 10.

(Received July 30, 1984)

This research has been sponsored by BMFT-grant 08 3108.

Abstract. For randomly chosen $a_1, \ldots, a_r \in G$, $G \cong \mathbf{Z}/n\mathbf{Z}$ a finite abelian group, and a random function $g: G \to \{1, \ldots, r\}$ we analyse the recursion $x_{i+1} := x_i + a_{g(x_i)} \bmod n$. Let $m := \min \{j \in \mathbf{N} \mid \exists i < j: x_i = x_j\}$. Under some plausible assumption we prove the existence of constants $d_8 \geq d_9 \geq \ldots \geq \geq d_r \geq \ldots$ such as the expected value of m is bounded by $E(m) < d_r \cdot \sqrt{\frac{\pi}{2} n}$ for all sufficiently large n. Moreover $\lim\limits_{r \to \infty} d_r = 1$. This gives a practical way for evaluating $\mathrm{ord}(h)$ for $h \in G$ within $O(\sqrt{\mathrm{ord}(h)})$ group operations and a fixed number of registers, each storing a group element. So far, deterministic methods for computing $\mathrm{ord}(h)$ require in the worst case $O(\sqrt{\mathrm{ord}(h)})$ group operations and $O(\sqrt{\mathrm{ord}(h)})$ registers.

The proposed method is useful in connection with factoring algorithms of Schnorr and Lenstra [7] and the computation of indices, see Pollard [6].

1. Introduction

Let $n \in \mathbf{N}$, $\mathbf{Z}_n \cong \mathbf{Z}/n\mathbf{Z}$ and $f: \mathbf{Z}_n \to \mathbf{Z}_n$ a function. The sequence

$$(1.1) \qquad x_0 := 0, \quad x_{i+1} := f(x_i) \quad i = 0, 1, 2, \ldots$$

is ultimately periodic. Suppose that $x_0, x_1, \ldots, x_{m-1}$ are pairwise distinct and $x_m = x_\lambda$, $\lambda < m$. Then $\mu := m - \lambda$ is the *period length* of (1.1) and λ is the *length of the non periodic segment* of (1.1).

The mean values of λ, μ are known for random functions $f: \mathbf{Z}_n \to \mathbf{Z}_n$; see [4, exercise 3.1.12]:

$$1 + E(\mu) = E(\lambda) \approx \sqrt{\frac{\pi}{8} n} + 1/3.$$

An example of a pseudo-random fuction $f:\mathbf{Z}_n \to \mathbf{Z}_n$ is

$$f(x) = x^2+1 \bmod n.$$

This function has been used in the factoring algorithms of Pollard [6], Brent and Pollard [2] see also Guy [3]. The values of λ, μ for this f oscillate around $\sqrt{\frac{\pi}{8}n}$.

In this paper we study pseudo-random recursions of the type

$$(1.2) \qquad x_{i+1} := x_i + a_{g(x_i)} \bmod n \quad i = 0, 1, 2, \dots$$

with g: $\mathbf{Z}_n \to \{1, \dots, r\}$ a pseudo-random function and pairwise distinct $a_1, \dots, a_r \in \mathbf{Z}_n$. The corresponding sequence $(x_i)_{i\geq 0}$ is *additively generated.* This recursion has been proposed by H. W. Lenstra, Jr.

A main problem is: What is the minimal number r of distinct terms $a_1, \dots, a_r$ necessary to generate a sufficiently randomized sequence $(x_i)_{i\geq 0}$? We show that $r = 8$ is sufficient to generate a sequence $(x_i)_{i\geq 0}$ with $E(\mu)$, $E(\lambda) = O(\sqrt{n})$.

An important feature of the additive recursion (1.2) is, that such a recursion can be done in any finite group using the group operation instead of addition. The additive recursion (1.2) is computational efficient. $x_{i+1} \equiv x_i^2+1 \bmod n$ takes one multiplication and one addition in $\mathbf{Z}_n$ per iteration step. One recursion step of (1.2) merely requires one addition and one evaluation of g. We shall see that g can be chosen as a very simple function.

2. Analysis of $F_j = \text{prob}\,[\exists\, 1<j: x_1 \equiv x_j \bmod n \mid \#\{x_0, \dots, x_{j-1}\} = j]$

The critical point of the additive scheme (1.2) is the commutativity of the recursion steps. The commutativity implies that the number of distinct values

$$(2.1) \qquad x_j - x_i \bmod n, \ 0 \leq i < j \leq k$$

as a function of k increases less rapidly than without this commutativity.

This increases $m = \mu+\lambda$, since by definition

$$m = \mu+\lambda = \min\{j \in \mathrm{N} \mid \exists\, i<j: x_j - x_i \equiv 0 \bmod n\}.$$

The chance of 0 occuring as $x_j - x_i$ mod n certainly decreases with the number of distinct elements in (2.1). We like to measure this effect quantitatively. With the recursion (1.2) we associate the following vectors

$$S_i = (S_{i,1}, \dots, S_{i,r}) \quad i = 0, 1, 2, \dots$$

$$(2.2) \qquad S_{0,\nu} = 0$$

$$S_{i,\nu} = \begin{cases} S_{i-1,\nu}+1 & \text{if } g(x_i) = \nu \\ S_{i-1,\nu} & \text{otherwise.} \end{cases}$$

This implies $x_i = \sum_{1\leq\nu\leq r} S_{i,\nu}\, a_\nu$ mod n, i.e. $x_i = (S_i, a)$ mod n with $a = = (a_1, \dots, a_r)$ and (S_i, a) the scalar product of S_i and a.

A repetition $x_j - x_i \equiv x_{j'} - x_{i'}$ mod n, $j' < j$ in (2.1) in enforced (enforced by the commutativity of the recursion steps in (1.2)), if $S_j - S_i = S_{j'} - S_{i'}$.

Note that $S_j - S_i = S_{j'} - S_{i'}$ implies $j - i = j' - i'$. One of our main tasks is to analyse the expected number of the enforced repetitions.

We introduce a randomized version of the recursion (1.2). Let Y_i, $i = 1, 2, \dots$ be random variables which are uniformly distributed over $\{1, \dots, r\}$ and mutually independent for $i = 1, 2, \dots$.

Let the random variable $a = (a_1, \dots, a_r)$ be uniformly distributed over $\mathbf{Z}_n^r$ and independent of the Y_i.

Then the *randomized version* of (1.2) is

$$x_{i+1} \equiv x_i + a_\nu \bmod n \quad i = 0, 1, 2, \dots \tag{2.3}$$

with

$$\nu = \begin{cases} Y_i & \text{if } \#\{x_0, \dots, x_i\} = i+1 \\ Y_j & \text{if } j = \min \{i' < | x_{i'} = x_i\}. \end{cases}$$

This randomized scheme can equivalently be defined by choosing the function $g: \mathbf{Z}_n \to \{1, \dots, r\}$ in (1.2) at random with equal probability n^{-r} for every g.

In order to bound $E(m) = E(\mu + \lambda)$ for the recursion (2.3) we compare the schemes (1.1) and (2.3). If $f: \mathbf{Z}_n \to \mathbf{Z}_n$ in (1.1) is chosen at random then (1.1) implies

$$\text{prob } [\neg\, \exists i < j : x_i \equiv x_j \bmod n \,|\, \#\{x_0, \dots, x_{j-1}\} = j] = \frac{n-j}{n}.$$

From this we obtain, see Knuth [4, exercise 3.1.12]:

$$E(m) = \sum_{1\leq j\leq n} j \left(\prod_{1\leq i\leq j-1} \frac{n-1}{n} \right) \frac{j}{n} \approx \sqrt{\frac{\pi}{2} n} - \frac{1}{3}. \tag{2.4}$$

Now consider the scheme (2.3). Let

$$F_j = \text{prob } [\exists\, 1 < j : x_1 \equiv x_j \bmod n \,|\, \#\{x_0, \dots, x_{j-1}\} = j].$$

The mean value of m for (2.3) is

$$E(m) = \sum_{1\leq j\leq n} j \left(\prod_{1\leq i\leq j-1} (1 - F_i) \right) F_j. \tag{2.5}$$

It follows that $E(m)$ is decreasing on each F_j. Hence

Lemma 2.1. *We obtain an upper bound on* $E(m)$ *if we replace in* (2.5) *each* F_j *by a lower bound on* F_j.

So we need a lower bound on F_j for $j \leq m$. We will exploit the fact that $a = (a_1, \ldots, a_r)$ in (2.3) is independent of the $S_h - S_i$, $0 \leq h < i \leq m$. a is uniformly distributed over $\mathbf{Z}_n^r$. Let

$$H_{h,i} := \{y \in \mathbf{Z}_n^r | (S_h - S_{i,}\ _y) \equiv 0 \bmod n\}$$
$$T_j := \{H_{h,i} | 0 \leq h < i < j\}$$
$$M_j(x) := \#\{(i, h) | 0 \leq h < i < j,\ x \in H_{h,i}\}.$$

If n is prime then $H_{h,i}$ is a random hyperplane, $\# H_{h,i} = n^{r-1}$. In genaral

$$\# H_{h,i} = n^{r-1} \gcd(b_1, \ldots, b_r, n),$$

where $S_h - S_i = (b_1, \ldots, b_r)$.

Lemma 2.2. $F_j = \frac{1}{n} \sum_{1<j} \text{prob}\ [H_{l,j} \notin T_j] \cdot \text{prob}\ [M_j(a) =$
$= 0 | a \in H_{l,j} \notin T_j] / \text{prob}\ [M_j(a) = 0]$.

Proof. $F_j = \text{prob}\ [\exists\, 1 < j : x_1 \equiv x_j \bmod n | \#\{x_0, \ldots, x_{j-1}\} = j] =$

$$= \text{prob}\ [a \in \bigcup_{l<j} H_{l,j} | a \notin \bigcup_{h<i<j} H_{h,i}]$$

$$= \text{prob}\ [a \in \bigcup_{l<j} H_{l,j} \setminus \bigcup_{h<i<j} H_{h,i}] / \text{prob}\ [a \in \mathbf{Z}_n^r \setminus \bigcup_{h<i<j} H_{h,i}].$$

Using $H_{l,j} \cap H_{k,j} \subset H_{1,k}$ which follows from $S_1 - S_k = (S_1 - S_j) - (S_k - S_j)$ we conclude

$$F_j = \sum_{l<j} \text{prob}\ [a \in H_{l,j} \setminus \bigcup_{h<i<j} H_{h,i}] / \text{prob}\ [a \in \mathbf{Z}_n^r \setminus \bigcup_{h<i<j} H_{h,i}].$$

Since $M_j(a) = 0 \Leftrightarrow a \notin \bigcup_{h<i<j} H_{h,i}$:

$$F_j = \sum_{l<j} \text{prob}\ [M_j(a) = 0,\ a \in H_{l,j}] / \text{prob}\ [M_j(a) = 0] =$$

$$= \sum_{l<j} \text{prob}\ [H_{l,j} \notin T_j]\ \text{prob}\ [M_j(a) = 0,\ a \in H_{l,j} | H_{l,j} \notin T_j] / \text{prob}\ [M_j(a) = 0] =$$

$$= \sum_{l<j} \text{prob}\ [H_{l,j} \notin T_j]\ \text{prob}\ [M_j(a) = 0 | a \in H_{l,j} \notin T_j] =$$

$$= \text{prob}\ [a \in H_{l,j} | H_{l,j} \notin T_j] / \text{prob}\ [M_j(a) = 0] =$$

$$= \sum_{l<j} \text{prob}\ [H_{l,j} \notin T_j]\ \text{prob}\ [M_j(a) =$$

$$= 0 | a \in H_{l,j} \notin T_j] / \text{prob}\ [M_j(a) = 0]. \ \square$$

In the remaining part of this section we give support to the

Conjecture 2.3.

$$\text{prob}[M_j(a) = 0] \leq \text{prob}\ [M_j(a) = 0 | a \in H_{l,j} \notin T_j].$$

For the proof of the main theorem 3.9 a weaker statement than Conjecture 2.3 would be sufficient, namely the existence of constants e_r with $\lim_{r\to\infty} e_r = 1$ such that

$$\frac{\text{prob } [M_j(a) = 0]}{\text{prob } [M_j(a) = 0 | a \in H_{i,j} \notin T_j]} \le e_r. \tag{2.6}$$

Since $M_j(a)$ only depends on $S_h - S_i$ with $0 \le h < i < j$, and $H_{l,j}$ only depends on $S_1 - S_j$, Conjecture 2.3 would hold with equality provided that S_j is independent of $S_1, S_2, \ldots, S_{j-1}$. However since $\|S_j - S_{j-1}\| = 1$, S_j clearly depends on S_{j-1}. Conjecture 2.3 means that the condition $(S_1 - S_j, a) \equiv 0 \bmod n$ disfavours the existence of $h < i < j$ such that $(S_1 - S_j, a) \equiv 0 \bmod n$.

The difficulty in proving Conjecture 2.3 is due to the complicated nature of prob $[M_j(a) = 0]$ which is defined by the inclusion-exclusion principle:

$$\begin{aligned} \text{prob } [M_j(a) = 0] = E[1 - n^{-r}[\sum_{h<i<j} \# H_{h,i} - \sum H_{h_1, i_1} \cap H_{h_2, i_2} + \\ + \sum \# H_{h_1, i_1} \cap H_{h_2, i_2} \cap H_{h_3, i_3} - + \ldots]], \end{aligned} \tag{2.7}$$

where the ν-th sum ranges over all pairs $(h_1, i_1) < (h_2, i_2) < \ldots < (h_\nu, i_\nu)$ with $h_\mu < i_\mu < j$ for $\mu = 1, \ldots, \nu$, and the pairs (h_μ, i_μ) taken in some order "$<$". This expression has to be compared with

$$\begin{aligned} &\text{prob } [M_j(a) = 0 | a \in H_{l,j} \notin T_j] = \\ &= E\left[1 - \frac{1}{\# H_{l,j}}[\sum_{h<i<j} \# H_{h,i} \cap H_{l,j} - \sum \# H_{h_1, i_1} \cap H_{h_2, i_2} \cap H_{l,j} + - \ldots]\right]. \end{aligned} \tag{2.8}$$

In comparing (2.7) and (2.8) we restrict to the case that n is prime. In this case the first two terms of (2.7) and (2.8) coincide. Note that

$$\# H_{l,j} = \# H_{h,i} = n^{r-1} \text{ and } \# H_{h,i} \cap H_{l,j} = n^{r-2}.$$

We are able to prove

$$n^{-r} E[\sum \# H_{h_1, i_1} \cap H_{h_2, i_2}] < n^{-r+1} E[\sum \# H_{h_1, i_1} \cap H_{h_2, i_2} \cap H_{l,j}]. \tag{2.9}$$

We argue that this relation dominates the influence of the further terms of (2.7), (2.8) and consequently proves conjecture (2.3).

Lemma 2.4. *For n prime and $r \ge 2$:*

$$E[M_j(a)] = E[M_j(a) | H_{l,j} \notin T_j] = E[M_j(a) | a \in H_{i,j} \notin T_j].$$

Proof. The first equality holds since a is independent of the event $[H_{l,j} \notin T_j]$. For the second equality note that

$$\begin{aligned} E[M_j(a) | H_{l,j} \notin T_j] &= \sum_{h<i<j} E[\# H_{h,i} | H_{l,j} \notin T_j] n_{=}{}^{r} = \\ &= \sum_{h<i<j} E[\# H_{h,i} \cap H_{l,j} | H_{l,j} \notin T_j] n^{-r+1} = E[M_j(a) | a \in H_{l,j} \notin T_j]. \end{aligned} \tag{2.10}$$

In fact (2.10) holds since $\# H_{h,i} = n^{r-1}$ and

$$\# H_{l,j} \cap H_{h,i} = \begin{cases} n^{r-1} & \text{if } H_{l,j} = H_{h,i} \\ n^{r-2} & \text{otherwise.} \end{cases}$$

This also shows that the condition $H_{l,j} \notin T_j$ is necessary. □
We define

$$M_j^*(a) := \begin{cases} M_j(a) - 1 & \text{if } M_j(a) > 1 \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\begin{aligned} E[M_j(a)] &= \text{prob}\,[M_j(a) \geq 1] + E[M_j^*(a)] = \\ &= 1 - \text{prob}[M_j(a) = 0] + E[M_j^*(a)]. \end{aligned}$$

Lemma 2.5. *For n prime and $r \geq 2$:*

$$\begin{aligned} \text{prob}\,[M_j(a) = 0 \,|\, a \in H_{l,j} \notin T_j] &= \text{prob}\,[M_j(a) = 0] + \\ &+ E[M_j^*(a) \,|\, a \in H_{l,j} \notin T_j] - E = [M_j^*(a)]. \end{aligned}$$

Proof. $$\begin{aligned} 1 - \text{prob}\,[M_j(a) = 0 \,|\, a \in H_{l,j} \notin T_j] + E[M_j^*(a) \,|\, a \in H_{l,j} \notin T_j] &= \\ = E[M_j(a) \,|\, a \in H_{l,j} \notin T_j] = E[M_j(a)] &= \\ = 1 - \text{prob}\,[M_j(a) = 0] + E[M_j^*(a)]. \end{aligned}$$

Lemma 2.5 means that the first two terms of (2.7) and (2.8) coincide, and it remains to compare the further terms. In order to prove (2.9) we show that the event $[a \in \bigcap_{1 \leq \nu \leq k} H_{h_\nu, i_\nu}]$ for $k \geq 2$ becomes more likely under the condition $a \in H_{l,i} \notin T_j$. This shows that for $k \geq 3$ the k-th term in (2.8) is absolutely greater than the k-th term in (2.7).

Lemma 2.6. *For n prime, $r \geq 2$, and $h_\nu < i_\nu < j$:*

$$\text{prob}\,[a \in \bigcap_{1 \leq \nu \leq k} H_{h_\nu, i_\nu} | a \in H_{l,j} \notin T_j] \begin{cases} = \text{prob}\,[a \in \bigcap_{1 \leq \nu \leq k} H_{h_\nu, i_\nu}] & \text{if } k = 1 \\ > \text{prob}\,[a \in \bigcap_{1 < \nu \leq k} H_{h_\nu, i_\nu}] & \text{otherwise.} \end{cases}$$

Proof. Consider fixed values $\bar{\mathcal{S}}_{i_\nu}, \bar{\mathcal{S}}_{h_\nu}, \bar{\mathcal{S}}_j, \bar{\mathcal{S}}_l$ for $\mathcal{S}_{i_\nu}, \mathcal{S}_{h_\nu}, \mathcal{S}_j, \mathcal{S}_l$, and

$\bar{H}_{h_\nu, i_\nu}, \bar{H}_{l,j}$ for $H_{h_\nu, i_\nu}, H_{l,j}$. Let $d = \dim \bigcap_{1 \leq \nu \leq k} \bar{H}_{h_\nu, i_\nu}$. Then

$$\text{prob}\,[a \in \bigcap_{1 \leq \nu \leq k} \bar{H}_{h_\nu, i_\nu} | a \in \bar{H}_{l,j} \notin T_j] = \begin{cases} n^{d-r} & \text{if } \bigcap_{1 \leq \nu \leq k} \bar{H}_{h_\nu, i_\nu} \not\subset \bar{H}_{l,j} \\ n^{1+d-r} & \text{otherwise.} \end{cases}$$

These equalities imply

$$\text{prob }[a \in \bigcap_{1 \leqq \nu \leqq k} H_{h_\nu, i_\nu} | a \in H_{l,j} \notin T_j] = \text{prob }[a \in \bigcap_{1 \leqq \nu \leqq k} H_{h_\nu, l_\nu}] \cdot$$
$$\cdot (1 + (n-1) \text{ prob }[\bigcap_{1 \leqq \nu \leqq k} H_{h_\nu, i_\nu} \subset H_{l,j}]).$$

For $k = 1$ the event $H_{h,i} \subset H_{l,j}$ is excluded by the condition $H_{l,j} \notin T_j$. For $k > 1$ the event $\bigcap_{1 \leqq \nu \leqq k} H_{h_\nu, i_\nu}$ is quite likely for particular indices h_ν, i_ν, $\nu = 1, \ldots, k$. Clearly

$$\bigcap_{1 \leqq \nu \leqq k} H_{h_\nu, i_\nu} \subset H_{l,j} \Leftrightarrow S_j - S_l \in \text{ span } \{S_{h_\nu} - S_{i_\nu},\ \nu = 1, \ldots, k\}.$$

For example for $k = 2$ we have

$$S_j - S_l = S_{j-\nu} - S_l + S_i - S_{i-\nu} \Leftrightarrow S_j - S_{j-\nu} = S_i - S_{l-\nu}.$$

This implies for $j \neq i$:

$$\text{prob }[H_{j-\nu, l} \cap H_{i,i-\nu} \subset H_{l,j} | H_{l,j} \notin T_j] \geq r^{-\nu}.$$

The main conclusion of Conjecture 2.3 is

Theorem 2.7. *Assuming Conjecture* 2.3 *we have for* $r \geq 2$:

$$F_j \geq \frac{1}{n} \cdot \sum_{l<j} \text{prob }[H_{l,j} \notin T_j].$$

Following Theorem 2.7 it remains to prove lower bounds on $\text{prob}[H_{l,j} \notin T_j]$.

3. Lower bounds on prob $[H_{l,j} \notin T_j]$

The definitions of $H_{l,j}$ and T_j imply

(3.1) $$H_{l,j} \in T_j \Leftrightarrow \exists \alpha \in \mathbf{Z}_n^*\colon \exists h < i < j\colon S_j - S_l \equiv \alpha(S_i - S_h) \bmod n,$$

where $\mathbf{Z}_n^*$ is the set of invertible elements in $\mathbf{Z}_n$.

The case $\alpha = 1$ will be treated in Lemma 3.5, and the remaining part of this section deals with the case $\alpha \neq 1$.

Remember that $S_j - S_l = S_i - S_h$ implies $j - l = i - h$. For $\sum_{1 \leqq \nu \leqq r} i_\nu = k$, $i \in \mathbf{N}$, we have:

$$\text{prob }[S_j - S_{j-k} = (i_1, \ldots, i_r)] = \frac{k! r^{-k}}{i_1! \ldots i_r!}.$$

Let $$P_k := \text{MAX}\left[\frac{k! r^{-k}}{i_1! \ldots i_r!} \,\middle|\, \sum_{1 \leqq \nu \leqq r} i_\nu = k\right].$$

Lemma 3.1. *For the randomized scheme* 2.3 *and for* $k < j$:

$$\text{prob }[\exists i < j\colon S_j - S_{j-k} = S_i - S_{i-k}] \leq \sum_{1 \leqq \nu \leqq k} p_\nu + j p_k.$$

Proof. For $i \leq j-k$: $\text{prob}[S_j - S_{j-k} = S_i - S_{i-k}] \leq p_k$. On the other hand

$$S_j - S_{j-k} = S_i - S_{i-k} \Leftrightarrow S_j - S_i = S_{j-k} - S_{i-k}$$

implies for $i < j-k$:

$$\text{prob}\ [S_j - S_{j-k} = S_i - S_{i-k}] = \text{prob}\,[S_j - S_i = S_{j-k} - S_{i-k}] \leq p|j-i|.$$

Lemma 3.1 is an immediate consequence of both bounds. □

We need bounds for the p_k. Note that the sequence $(p_k)_{k \geq 1}$ is monotonously decreasing and is bounded as $p_k \leq k!\ r^{-k}$. Moreover

$$(3.2) \qquad \forall\, \nu \in \mathbf{N}: p_{\nu \cdot r} = \frac{(\nu \cdot r)!}{(\nu!)^r} \cdot r^{-\nu r} \cdot$$

Stirling's formula implies

Fact 3.2.

$$\forall\, \nu \in \mathbf{N}: p_{\nu \cdot r} \leq r^{0,5} (2\pi\nu)^{(1-r)/2} e^{1/(12r\nu)}.$$

Fact 3.3. *For* $r \geq 5$:

$$\sum_{1 \leq k \leq \infty} p_k \leq r^{-1} + 2r^{-2} + 30r^{-3} - 96r^{-4} + 1.35 r^{1.5} (2\pi)^{(1-r)/2}.$$

Proof.

$$\sum_{1 \leq k \leq \infty} p_k = \sum_{1 \leq k \leq r-1} p_k + \sum_{r \leq k \leq \infty} p_k \leq$$

$$\leq r^{-1} + 2r^{-2} + 6r^{-3} + 24r^{-4} + 24(r-5)r^{-4} + \sum_{0 \leq k \leq \infty} r \cdot 2^k p_{2^k \cdot r} \leq$$

$$\leq r^{-1} + 2r^{-2} + 30r^{-3} - 96r^{-4} + 1.35 r^{1.5} (2\pi)^{(1-r)/2}. \ \square$$

Fact 3.4. *For* $r \geq 8$ *and* $k, j \geq 3r \cdot j^{6/(r-1)}$ *we have*

$$j \cdot p_k \leq r^{-1.5} \cdot (2\pi)^{(1-r)/2}.$$

Proof. By $k \geq 3r\, j^{6/(r-1)}$ Fact 3.2 implies

$$j p_k \leq j \cdot p_{[k/2r] \cdot r} \leq j \cdot r^{0.5} \cdot (2\pi)^{(1-r)/2} \cdot j^{-3} \cdot e^{1/(12r)} \leq r^{-1.5} \cdot (2\pi)^{(1-r)/2}.$$

The last inequality holds, since $j \geq 3r j^{6/(r-1)}$ implies $j \geq 3\, r$. □

Combining (3.1) to (3.4) we obtain

Lemma 3.5. *For* $r \geq 8$ *and* $k, j \geq 3r j^{6/(r-1)}$:

$$\text{prob}\ [\exists i < j: S_k - S_{j-k} = S_i - S_{i-k}] \leq$$

$$\leq r^{-1} + 2r^{-2} + 30r^{-3} + 96r^{-4} + 1.36 r^{1.5} (2\pi)^{(1-r)/2}.$$

Proof. We have by Lemma 3.1

$$\text{prob}\ [\exists i < j: S_j - S_{j-k} = S_i - S_{i-k}] \leq \sum_{1 \leq \nu \leq k} p_\nu + j p_k,$$

and by the Facts 3.3, 3.4 we obtain for the right-hand side of the above inequality

$$\leq r^{-1}+2r^{-2}+30r^{-3}-96r^{-4}+1.35r^{1.5}(2\pi)^{(1-r)/2}+r^{-1.5}(2\pi)^{(1-r)/2}\leq$$
$$\leq r^{-1}+2r^{-2}+30r^{-3}+96r^{-4}+1.36r^{1.5}(2\pi)^{(1-r)/2}. \quad \square$$

The case $\alpha\neq 1$ in (3.1) will be treated in Lemma 3.6.

Lemma 3.6. *For* $r\geq 8$, $j\geq(3r)^{(r-1)/(r-7)}$, *and* $l\leq j-3rj^{6/(r-1)}$:

$$\text{prob}\,[\exists\alpha\in\mathbf{Z}_n\backslash\{1\},\ \exists h<i<j\colon S_j-S_l=\alpha(S_i-S_h)\ \text{mod}\ n]\leq$$
$$\leq r^{0,5}(2\pi)^{(1-r)/2}\,e^{1/(12r)}.$$

Proof. Let $r\geq 8$, $j\geq(3r)^{(r-1)/(r-7)}$, and let $l\geq j-3rj^{6/(r-1)}$ be fixed.

$$\text{prob}\ [\exists\alpha\in\mathbf{N}_n\backslash\{1\}\exists h<i<j\colon S_j-S_l=\alpha(S_i-S_h)\ \text{mod}\ n]\leq$$
$$\leq r^{0.5}(2\pi)^{(1-r)/2}e^{1/(12r)}.$$

Hence

(3.3) $$j-l\subset 3t \text{ with } t:=r\,j^{6/(r-1)}.$$

We distinguish 4 cases for h, i, and in each case we prove for fixed h, i and $\alpha\geq 2$:

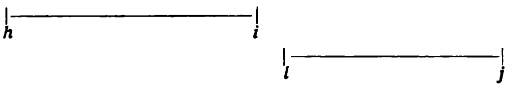
$$\text{prob}\ [S_j-S_l=\alpha(S_i-S_h)\ \text{mod}\ n]\leq p_t.$$

Let h, i range over the integers $\leq j$, and let α range over $\{(S_{j,1}-S_{l,1})/\beta\,|\,\beta\leq j\}$. We obtain

$$\text{prob}\ [\exists\alpha\in\mathbf{Z}_n\backslash\{1\},\ \exists h<i<j\colon S_j-S_l=\alpha(S_i-S_l)\ \text{mod}\ n]\leq$$
$$\leq p_t j^3\leq r^{0.5}(2\pi)^{(1-r)/2}e^{1/(12r)}.$$

The latter inequality follows from Fact 3.2 and $t=r\,j^{6/(r-1)}$. This proves the lemma. Here are the 4 cases for h, i:

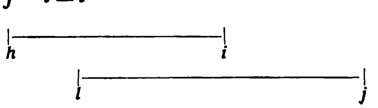
Case 1. $i\leq l$



Since $i\leq l$, S_j-S_l is independent of S_i-S_h. Hence for fixed h, i, α:

$$\text{prob}\ [S_j-S_l\equiv\alpha(S_i-S_h)\ \text{mod}\ n]\leq p_{j-1}\leq p_t.$$

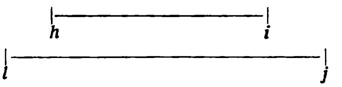
Case 2. $i>l$, $j-i\geq t$



Obviously,

$S_j - S_l \equiv \alpha(S_i - S_h) \bmod n \Leftrightarrow S_j - S_i \equiv \alpha(S_l - S_h) + (\alpha - 1)(S_i - S_l) \bmod n.$
Since $S_j - S_i$ is independent of $S_l - S_h$, $S_i - S_l$, it follows for fixed h, i, α:
prob $[S_j - S_l \equiv \alpha(S_i - S_h) \bmod n] \le p_{j-i} \le p_t$.

Case 3. $i > l$, $j - i < t \le h - l$

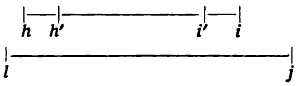


Obviously,

$S_j - S_l \equiv \alpha(S_i - S_h) \bmod n \Leftrightarrow S_h - S_l \equiv (\alpha - 1)(S_i - S_h) - (S_j - S_i) \bmod n.$
Since $S_h - S_l$ is independent of $S_i - S_h$, $S_j - S_i$ it follows for fixed h, i, α:

$$\text{prob } [S_j - S_1 \equiv \alpha(S_i - S_h) \bmod n] \le p_{h-l} \le p_t.$$

Case 4. $i < l$, $j - i < t$, $h - l < t$



Let $h' := 1 + t$ and $i' := j - t$. Then (3.3) implies

$$i' - h' \ge t.$$

Obviously,

$S_j - S_l \equiv \alpha(S_i - S_h) \bmod n \Leftrightarrow S_{i'} - S_{h'} \equiv$

$$\equiv \begin{cases} (\alpha - 1)^{-1}[(1 - \alpha)(S_i - S_{i'} + S_{h'} - S_h) + S_j - S_i + S_h - S_l \bmod n \text{ if } h \ge l \\ (\alpha - 1)^{-1}[(1 - \alpha)(S_i - S_{i'} + S_{h'} - S_l) + S_j - S_i - \alpha(S_l - S_h)] \bmod n \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{otherwise.} \end{cases}$$

Since $S_{i'} - S_{h'}$ is independent of $S_i - S_{i'}$, $S_{h'} - S_h$, $S_j - S_i$, and of $S_h - S_l$ (of $S_i - S_{i'}$, $S_{h'} - S_l$, $S_j - S_i$, and of $S_l - S_h$, respectively), it follows for fixed h, i, $\alpha \ge 2$:

$$\text{prob } [S_j - S_l \equiv \alpha(S_i - S_h) \bmod n] \le p_{i'-h'} \le p_t. \quad \square$$

We are now able to prove

Lemma 3.7 *For $r \ge 8$ and $j \le m$ we have*

$$\sum_{l<j} \text{prob } [\overline{H}_{l,j} \notin T_j] \ge (j - 3rj^{6/(r-1)}) \cdot$$

$$\cdot (1 - r^{-1} - 2r^{-2} - 30r^{-3} + 96r^{-4} - 1.5r^{1.5}(2\pi)^{(1-r)/2}).$$

Proof.

$$\sum_{l<j} \text{prob } H_{l,j} \notin T_j] \ge \sum_{l \le j - 3rj^{6/(r-1)}} (1 - \text{prob } [H_{l,j} \in T_j]) \ge$$

$$\ge (j - 3rj^{6/(r-1)})(1 - r^{-1} - 2r^{-2} - 30r^{-3} + 96r^{-4} - 1.36r^{1.5}(2\pi)^{(1-r)/2} -$$

$$- r^{0.5}(2\pi)^{(1-r)/2} e^{1/(12r)}) \ge$$

$$\ge (j - 3rj^{6/(r-1)})(1 - r^{-1} - 2r^{-2} - 30r^{-3} + 96^{-4} - 1.5r^{1.5}(2\pi)^{(1-r)/2}). \quad \square$$

We conclude from Theorem 2.6 and Lemma 3.7

Proposition 3.8. Conjecture 2.3 implies the existence of c_r, $0<c_r<1$ of $d_r \in \mathbf{N}$ for $r \geq 8$ such that

$$(1) \qquad F_j \geq j(1-c_r)/n \qquad \text{for all } j \text{ with } d_r \leq j \leq m,$$

$$(2) \qquad \lim_{r\to\infty} c_r = 0.$$

Proof. Put $d_r := r^{14}$. Then, by Theorem 2.6 and Lemma 3.7, we have for all j, $d_r \leq j \leq m$:

$$F_j \geq j/n(1-3/r)(1-r^{-1}-2r^{-2}-30r^{-3}-1.5r^{1.5}(2\pi)^{(1-r)/2}).$$

This clearly proves the claim with c_r defined by

$$1-c_r = (1-3/r)(1-r^{-1}-2r^{-2}-30r^{-3}-1.5r^{1.5}(2\pi)^{(1-r)/2}). \qquad \square$$

By Lemma 2.1 Proposition 3.8 yields

$$(3.4) \qquad E[m] \leq \sum_{d_r \leq j \leq n} j \left[\prod_{d_r \leq i \leq j-1} \frac{i(1-c_r)}{n} \right] \frac{j}{n}(1-c_r).$$

A comparison of (2.4) and (3.4) yields the

Main Theorem 3.9. *Assuming Conjecture 2.3 we have for all* $r \geq 8$:

$$E[m] \leq \sqrt{\frac{1}{1-c_r} \frac{\pi}{2} n}(1+0(1)) + d_r^2.$$

Here $1+o(1)$ stands for $\prod_{1 \leq i \leq d_r - 1} \left(1 - \frac{i(1-c_r)}{n}\right)^{-1}$; for each $r \geq 8$ this term converges to 1 as $n \to \infty$.

Remarks. (1) $E[m]$ in Theorem 3.9 is a mean value for all choices of $(a_1, \ldots, a_r) \in \mathbf{Z}_n^r$ and g. So far Theorem 3.9 does not say anything about a particular choice of $a_1, \ldots, a_r$.

(2) Our experiments with the recursion (2.3) indicate that there must exist corresponding constants c_4, c_5, c_6, $c_7 < 1$, see Table 5.1. The existence of $c_3 < 1$ is open, and c_2 does not exist. It can be shown that $r = 2$ in (2.3) implies

$$E[m] = \Omega(n^{2/3}).$$

Thus, two additive terms a_1, a_2 are not enough for randomizing scheme (2.3).

4. Applications

4.1. Computing the order of group elements

Let $h \in G$ be an element of a finite group with an efficient multiplication procedure. Determine ord(h) as follows:

1. Choose $a_1, \ldots, a_r \in \mathbf{Z}_n$, $g: G \to \{1, \ldots, r\}$ and $h_0 \in G$ at random with $n \geq |G|$, $r \geq 8$.

Table 5.1

r \ 10^i	10^4	10^5	10^6	10^7	10^8	$\ldots/\sqrt{\frac{\pi}{8}10^8}$
2	397	1 989	8 992	61 705	268 149	42.79
3	146	424	r 515	5 411	18 602	3.02
3	146	424	1 515	5 411	18 602	3.02
4	94	276	892	2 479	9 448	1.50
5	76	242	846	2 287	8 459	1.23
6	75	242	719	1 983	8 682	1.27
7	72	217	712	2 609	7 494	1.20
8	71	221	692	2 178	6 239	1.02
9	70	219	707	1 952	6 169	1.01
10	64	206	721	2 203	7 944	1.27
11	68	253	639	2 436	7 608	1.02
12	66	206	746	2 086	7 171	1.14
13	63	215	696	2 962	6 962	1.12
14	71	208	657	2 091	7 377	1.15
15	66	240	594	1 811	5 944	0.95
16	56	209	685	1 811	6 577	1.04
$\left[\sqrt{\frac{\pi}{8}n}\right]$	62	198	626	1 981	6 266	

2. Recursively compute

$$h_{i+1} := h_i \cdot h^{a_{g(h_i)}} \text{ for } i = 0, 1, 2, \ldots$$

until some $i<j$ has been found with $h_i = h_j$.

(By Theorem 3.9 we can expect that there exist $i<j\leq\sqrt{\operatorname{ord}(h)}$ with $h_i = h_j$. By Brent's method such a pair can be found in keeping only one h_ν stored. Hence we find i, j with a *fixed number of registers* (each storing a group element) and with $O(\sqrt{\operatorname{ord}(h)})$ group operations.)

3. Compute $T = \sum_{i+1\leq\nu\leq j} a_{g(h_\nu)}$.

(Note that $h_i = h_j$ implies $\operatorname{ord}(h) | T$.)

4. $\operatorname{ord}(h)$ can be determined either as the gcd of several of such multiples T of $\operatorname{ord}(h)$ or by factoring T and by splitting off unnecessary factors of T.

Previous methods for computing $\operatorname{ord}(h)$ require $\sqrt{\operatorname{ord}(h)}$ registers, see e.g. baby-giant-step method of Shanks [8, p. 419].

4.2. Factoring integers by computing ambiguous classes of quadratic forms

In the recently published paper of Schnorr and Lenstra [7] one tries to factor $n\in\mathbf{N}$ as follows:

Choose a multiple $-n\cdot s$ of n which is a discriminant. Compute a nontrivial ambiguous class H (e.g. $H^2 = 1$, $H\neq 1$) in the class group of quadratic forms with discriminant $-ns$ (According to Gauss these ambiguous classes correspond to the factorizations $ns = s_1 s_2$ with $gcd(s_1, s_2) = 1$.) as follows:

Choose an arbitrary class F in the class group. Compute the order of F as in **4.1** If ord(F) is even, then $F^{\mathrm{ord}(F)/2}$ is a non-trivial ambiguous class. The method **4.1** has been successfully applied in this case.

4.3. Computing the index mod p

Let b be a primitive root of $\mathbf{Z}_p$. For every $a \in \mathbf{Z}_p^*$ there exists a unique i, $0 < i < p$, such that $a \equiv b^i \bmod p$, i is the *index* of a with respect to b. We propose a Monte Carlo method according to Pollard:

1. Choose random integers $a_1, \ldots, a_r, b_1, \ldots, b_s \in \mathbf{Z}_{p-1}$ and pseudo-random functions $f: \mathbf{Z}_p \to \{1, \ldots, r\}$, $g: \mathbf{Z}_p \to \{1, \ldots, s\}$, $s \geq 7$.
2. Recursively compute

$$h_{i+1} : \equiv h_i \cdot a^{a_{f(h_i)}} \cdot b^{b_{g(h_i)}} \bmod p \quad i = 0, 1, 2, \ldots$$

until some $i < j$ has been found with $h_i = h_j$.

(By Theorem 3.9 we can expect that there exist $i < j \leq \sqrt{p}$ with $h_i = h_j$. By Brent's method such a pair can be found in keeping only one h_ν stored. Hence we most likely find i, j with a fixed number of registers, each storing a group element, and with $O(\sqrt{p})$ group operations.)

3. Compute $T_a = \sum_{i+1 \leqq \nu \leqq j} a_{f(h_\nu)}$, $T_b = \sum_{i+1 \leqq \nu \leqq j} b_{g(h_\nu)}$.

(Note that $h_i = h_j$ implies $a^{-T_a} = b^{T_b}$)

4. Most likely we have $T_a \not\equiv 0 \bmod p-1$. In this case

$$a = b^{-T_b T_a^{-1} \bmod (p-1)}$$

Hence $-T_b T_a^{-1} \bmod (p-1)$ is the index of a with respect to b.

4.4. Suitable pseudo-random functions $n: G \to \{1, \ldots, r\}$

For $G = \mathbf{Z}/n\mathbf{Z}$ we successfully applied functions of the following type. Choose a small prime p with $r < p < n$ and let

$$g(b) = [(b^2 \bmod p) \cdot r/p] + 1.$$

Also by our experience it is not nenessary to choose $a_1, \ldots, a_r \in \mathbf{Z}_n$ at random. Even reqular sequences like $a_i \equiv c^{\nu+i} \bmod n$, $i = 1: \ldots$, with fixed c and ν work well.

However, it is necessary that the size of the $a_i \bmod n$ is well distributed over $\{1, \ldots, n-1\}$. If all residues $a_i \bmod n$ are small, then the method cannot work.

5. Some experimental results

Our experimental results with the recursion (1.2), see Table 5.1, show that the main Theorem 3.9 already holds provided that at least four additive terms are used, e.g. $r \geq 4$. The table shows the average behaviour of the period length μ. We obtained mean values for μ which are $\leq \bar{c}_r \sqrt{\frac{\pi}{8} n}$ with $\bar{c}_4 \leq 1.5$ and $\bar{c}_{16} \leq 1.05$.

For $r = 2$ the average μ roughly increases as $n^{2/3}$. The table is not conclusive for $r = 3$, $\bar{c}_3$ may be a function which slightly increases with n.

The additive terms

$a_1 =$	151 313 669	$a_9 =$	989 209 282
$a_2 =$	1 167 832 084	$a_{10} =$	903 322 227
$a_3 =$	218 048 340	$a_{11} =$	2 113 687 555
$a_4 =$	1 613 921 385	$a_{12} =$	475 347 718
$a_5 =$	584 867 687	$a_{13} =$	522 890 323
$a_6 =$	532 455 900	$a_{14} =$	2 092 819 987
$a_7 =$	963 669 779	$a_{15} =$	328 337 024
$a_8 =$	930 011 267	$a_{16} =$	880 150 971

have been generated by an ordinary Pollard-Brent recursion. The recursion (1.2) was done with the function

$$g\colon \mathbf{Z}_n \to \{1, \ldots, r\}, \quad b \to [(b^2 \bmod p\}r/p] + 1$$

with $p = 104\,879$ a prime.

The entry in column 10^i and row r of Table 5.1 records the average period length μ over the hundred values $n = 10^i + 1, \ldots, 10^i + 100$. For comparison the last row gives the wxpected values of μ for a pure random recursion $E[\mu] \approx \sqrt{\frac{\pi}{8} n}$. The last column records approximations for $\bar{c}_r$: the entry of the 10^8-column is divided by $\sqrt{\frac{\pi}{8} n}$.

Acknowledgement We thank H. W. Lenstra Jr. and A. Odlydzko for critical and helpful comments on a previous version of this paper.

REFERENCES

[1] *Brent R. P.:* Analysis of some new cycle finding and factorization algorithms. *BIT* **20** (1980), 176–184.

[2] *Brent R. P.* and *Pollard J. M.:* Factorization of the eighth Fermat number. *Mathematics of Computation* **36** (154) (1981), 627–630.

[3] *Guy R. K.:* How to factor a number. In: Proc. Fifth Manitoba Conference on Numerical Math. (1975), 49–89.

[4] *Knuth D. E.:* The Art of Computer Programming. Vol. II. Addison–Wesley, New York, 1981.

[5] *Pollard J. M.:* A Monte Carlo method for factorization. *BIT* **15** (1975), 331–334.

[6] *Pollard J. M.:* Monte Carlo methods for index computation (mod p). *Mathematics of Computation* **32** (1978), 918–924.

[7] *Schnorr C. P.* and *Lenstra H. W.:* A Monte Carlo factoring algorithm with finite storage. Preprint, University Frankfurt, 1982.

[8] *Shanks P.:* Class Number, a Theory of Factorization and Genera. In: Proc. Symp. Pure Math., Amer. Math. Soc. **20** (1971), 415–440.