57. *Asymptotic Distribution* mod *m and Independence of Sequences of Integers.* I

By Lauwerens KUIPERS*) and Harald NIEDERREITER**)

(Comm. by Kenjiro SHODA, M. J. A., April 18, 1974)

Let $m \geq 2$ be a fixed modulus. Let (a_n), $n=1,2,\cdots$, be a given sequence of integers. For integers $N \geq 1$ and j, let $A(N;j,a_n)$ be the number of n, $1 \leq n \leq N$, with $a_n \equiv j \pmod m$. If

$$\alpha(j) = \lim_{N\to\infty} A(N;j,a_n)/N$$

exists for each j, then (a_n) is said to have α as its asymptotic distribution function mod m (abbreviated a.d.f. mod m). We denote $\alpha(j)$ also by $\|A(a_n \equiv j)\|$. Of course, it suffices to restrict j to a complete residue system mod m. If $\alpha(j) = 1/m$ for $0 \leq j < m$, then (a_n) is uniformly distributed mod m (abbreviated u.d. mod m) in the sense of Niven [4]. The numbers in brackets refer to the bibliography at the end of the second part of this paper.

If (b_n) is another sequence of integers, then for $N \geq 1$ and $j,k \in \boldsymbol{Z}$ we define $A(N;j,a_n;k,b_n)$ as the number of n, $1 \leq n \leq N$, such that simultaneously $a_n \equiv j \pmod m$ and $b_n \equiv k \pmod m$. We write

$$\|A(a_n \equiv j, b_n \equiv k)\| = \lim_{N\to\infty} A(N;j,a_n;k,b_n)/N \tag{1}$$

in case the limit exists. We note that if the limits (1) exist for all j, $k=0,1,\cdots,m-1$, then both (a_n) and (b_n) have an a.d.f. mod m. The following notion was introduced by Kuipers and Shiue [2].

Definition 1. The sequences (a_n) and (b_n) are called independent mod m if for all $j,k=0,1,\cdots,m-1$ the limits $\|A(a_n \equiv j, b_n \equiv k)\|$ exist and we have

$$\|A(a_n \equiv j, b_n \equiv k)\| = \|(A(a_n \equiv j)\| \cdot \|A(b_n \equiv k)\|.$$

Example 1. Let (c_n) be a sequence of integers that is u.d. mod m^2. Then writing $c_n \equiv a_n + mb_n \pmod{m^2}$, where $0 \leq a_n < m$ and $0 \leq b_n < m$, we obtain two sequences (a_n) and (b_n) that are independent mod m and u.d. mod m. See [2] and [1, Ch. 5, Example 1.5].

Example 2. Let α_1, α_2 be two real numbers such that $1, \alpha_1, \alpha_2$ are linearly independent over the rationals; or, more generally, let α_1, α_2 be two real numbers satisfying the condition of Theorem A in [3]. Then, according to this theorem, the sequence $(([n\alpha_1],[n\alpha_2]))$, $n=1,2,\cdots$, of lattice points is u.d. in $\boldsymbol{Z}^2$ (here $[x]$ denotes the integral part of

---

*) Department of Mathematics, Southern Illinois University, Carbondale, Illinois, U. S. A.

**) The Institute for Advanced Study, Princeton, New Jersey, U. S. A. The research of the second author was supported by NSF grant GP-36418X1.

x). It follows easily that the sequences $([n\alpha_1])$ and $([n\alpha_2])$ are u.d. mod m and independent mod m for all $m \geq 2$.

A method of constructing for each given sequence (a_n) possessing an a.d.f. mod m a sequence (b_n) with prescribed a.d.f. mod m such that (a_n) and (b_n) are independent mod m was communicated to us by M. B. Nathanson. His paper will appear in due course.

A criterion for independence mod m in terms of exponential sums has already been established (see [2] and [1, Ch. 5, Sect. 1]). The following criterion is of a different type.

Theorem 1. *The sequences (a_n) and (b_n) are independent* mod m *if and only if for all $h, k \in \boldsymbol{Z}$ the sequence $(ha_n + kb_n)$, $n = 1, 2, \cdots$, has an a.d.f.* mod m *given by*

$$\|A(ha_n + kb_n \equiv j)\| = \sum_{\substack{r,s=0 \\ hr+ks\equiv j \pmod m}}^{m-1} \|A(a_n \equiv r)\| \cdot \|A(b_n \equiv s)\| \tag{2}$$

for all $j \in \boldsymbol{Z}$.

Proof. Suppose (a_n) and (b_n) are independent mod m. We have

$$A(N; j, ha_n + kb_n) = \sum_{\substack{r,s=0 \\ hr+ks\equiv j \pmod m}}^{m-1} A(N; r, a_n; s, b_n),$$

and so, by dividing by N and letting $N \to \infty$, we arrive at

$$\|A(ha_n + kb_n \equiv j)\| = \sum_{\substack{r,s=0 \\ hr+ks\equiv j \pmod m}}^{m-1} \|A(a_n \equiv r, b_n \equiv s)\|$$
$$= \sum_{\substack{r,s=0 \\ hr+ks\equiv j \pmod m}}^{m-1} \|A(a_n \equiv r)\| \cdot \|A(b_n \equiv s)\|.$$

Conversely, suppose that (2) is satisfied, and choose integers p, q with $0 \leq p,\ q < m$. We note that for $x, y \in \boldsymbol{Z}$ the expression

$$\frac{1}{m^2} \sum_{h,k=0}^{m-1} \exp\left(-\frac{2\pi i}{m}(hp + kq)\right) \exp\left(\frac{2\pi i}{m}(hx + ky)\right)$$

is 1 precisely if $x \equiv p \pmod m$ and $y \equiv q \pmod m$, and 0 otherwise. Therefore,

$$A(N; p, a_n; q, b_n)$$
$$= \frac{1}{m^2} \sum_{h,k=0}^{m-1} \exp\left(-\frac{2\pi i}{m}(hp + kq)\right) \sum_{n=1}^{N} \exp\left(\frac{2\pi i}{m}(ha_n + kb_n)\right)$$
$$= \frac{1}{m^2} \sum_{h,k=0}^{m-1} \exp\left(-\frac{2\pi i}{m}(hp + kq)\right) \sum_{j=0}^{m-1} \exp\left(\frac{2\pi i}{m} j\right) A(N; j, ha_n + kb_n)$$

for all $N \geq 1$. Dividing by N, letting $N \to \infty$, and using (2), we obtain

$$\|A(a_n \equiv p, b_n \equiv q)\|$$
$$= \frac{1}{m^2} \sum_{h,k=0}^{m-1} \exp\left(-\frac{2\pi i}{m}(hp + kq)\right) \sum_{j=0}^{m-1} \exp\left(\frac{2\pi i}{m} j\right) \|A(ha_n + kb_n \equiv j)\|$$
$$= \frac{1}{m^2} \sum_{h,k=0}^{m-1} \exp\left(-\frac{2\pi i}{m}(hp + kq)\right) \sum_{j=0}^{m-1} \exp\left(\frac{2\pi i}{m} j\right)$$
$$\times \sum_{\substack{r,s=0 \\ hr+ks\equiv j \pmod m}}^{m-1} \|A(a_n \equiv r)\| \cdot \|A(b_n \equiv s)\|$$

$$=\frac{1}{m^2}\sum_{r,s=0}^{m-1}\|A(a_n\equiv r)\|\cdot\|A(b_n\equiv s)\|\sum_{j=0}^{m-1}\exp\left(\frac{2\pi i}{m}j\right)$$
$$\times\sum_{\substack{h,k=0\\ hr+ks\equiv j\ (\mathrm{mod}\ m)}}^{m-1}\exp\left(-\frac{2\pi i}{m}(hp+kq)\right)\cdot$$

Now

$$\frac{1}{m^2}\sum_{j=0}^{m-1}\exp\left(\frac{2\pi i}{m}j\right)\sum_{\substack{h,k=0\\ hr+ks\equiv j\ (\mathrm{mod}\ m)}}^{m-1}\exp\left(-\frac{2\pi i}{m}(hp+kq)\right)$$
$$=\frac{1}{m^2}\sum_{j=0}^{m-1}\sum_{\substack{h,k=0\\ hr+ks\equiv j\ (\mathrm{mod}\ m)}}^{m-1}\exp\left(-\frac{2\pi i}{m}(hp+kq-hr-ks)\right)$$
$$=\frac{1}{m^2}\sum_{h,k=0}^{m-1}\exp\left(\frac{2\pi i}{m}h(r-p)\right)\exp\left(\frac{2\pi i}{m}h(s-q)\right),$$

and the last sum is 1 precisely if $r=p$ and $s=q$, and 0 otherwise. This completes the proof of Theorem 1.

The necessary part of Theorem 1 can be improved as follows. Let $f:\boldsymbol{Z}^2\to\boldsymbol{Z}$ be a congruence-preserving function mod m, i.e., $f(i_1,i_2)=f(j_1,j_2)$ whenever $i_1\equiv j_1\ (\mathrm{mod}\ m)$ and $i_2\equiv j_2\ (\mathrm{mod}\ m)$. Then, if (a_n) and (b_n) are independent mod m, the sequence $(f(a_n,b_n))$, $n=1,2,\cdots$, has an a.d.f. mod m. For the proof, one simply notes that

$$A(N;j,f(a_n,b_n))=\sum_{\substack{r,s=0\\ f(r,s)\equiv j\ (\mathrm{mod}\ m)}}^{m-1}A(N;r,a_n;s,b_n),$$

so that one obtains the desired conclusion by dividing by N and letting $N\to\infty$.

Theorem 2. *Let (a_n) and (b_n) be independent* mod m, *and let h, $k\in\boldsymbol{Z}$. Then the sequences (ha_n), $n=1,2,\cdots$, and (kb_n), $n=1,2,\cdots$, are independent* mod m.

Proof. Set $c=\mathrm{g.c.d.}\,(h,m)$ and $d=\mathrm{g.c.d.}\,(k,m)$. Choose two integers r and s. If $c\nmid r$ or $d\nmid s$, then $\|A(ha_n\equiv r, kb_n\equiv s)\|=\|A(ha_n\equiv r)\|\cdot\|A(kb_n\equiv s)\|$ holds since both sides are equal to zero. If both $c\mid r$ and $d\mid s$, let $r_1,\cdots,r_c$ and $s_1,\cdots,s_d$ be the solutions in the least residue system mod m of the congruences $hx\equiv r\ (\mathrm{mod}\ m)$ and $ky\equiv s\ (\mathrm{mod}\ m)$, respectively. Then,

$$\|A(ha_n\equiv r, kb_n\equiv s)\|=\sum_{i=1}^{c}\sum_{j=1}^{d}\|A(a_n\equiv r_i, b_n\equiv s_j)\|$$
$$=\sum_{i=1}^{c}\sum_{j=1}^{d}\|A(a_n\equiv r_i)\|\cdot\|A(b_n\equiv s_j)\|$$
$$=\left(\sum_{i=1}^{c}\|A(a_n\equiv r_i)\|\right)\left(\sum_{j=1}^{d}\|A(b_n\equiv s_j)\|\right)$$
$$=\|A(ha_n\equiv r)\|\cdot\|A(kb_n\equiv s)\|.$$

Theorem 3. *Suppose (a_n) has α as its a.d.f.* mod m. *Then (a_n) and (a_n) are independent* mod m *if and only if $\alpha(j)=1$ for some j.*

Proof. If $0<\alpha(j)<1$ for some j, then $\|A(a_n\equiv j, a_n\equiv j)\|=\alpha(j)\neq\alpha^2(j)=\|A(a_n\equiv j)\|\cdot\|A(a_n\equiv j)\|$. If $\alpha(j)=1$ for some j, then for $r,s,\in\boldsymbol{Z}$ with

$0\leq r,\ s<m$ and $r\neq s$ we have

$$\|A(a_n\equiv r, a_n\equiv s)\|=0=\|A(a_n\equiv r)\|\cdot\|A(a_n\equiv s)\|,$$

and also

$$\|A(a_n\equiv r, a_n\equiv r)\|=\alpha(r)=\alpha^2(r)=\|A(a_n\equiv r)\|\cdot\|A(a_n\equiv r)\|,$$

since $\alpha(r)=0$ or 1.

Theorem 4. *Suppose (a_n) has α as its a.d.f.* mod m. *Then (a_n) is independent* mod m *of any (b_n) having an a.d.f.* mod m *if and only if $\alpha(j)=1$ for some $j=0,1,\cdots,m-1$.*

Proof. If $0<\alpha(j)<1$ for some j, then (a_n) and (a_n) are not independent mod m by Theorem 3. Now suppose that $\alpha(j)=1$ for some $j=0,1,\cdots,m-1$, and let (b_n) have an a.d.f. mod m. Then for $r,s\in\boldsymbol{Z}$ with $0\leq r,\ s<m$ and $r\neq j$ we have $A(N;r,a_n;s,b_n)\leq A(N;r,a_n)$ for all $N\geq 1$, so that $0=\|A(a_n\equiv r, b_n\equiv s)\|=\|A(a_n\equiv r)\|\cdot\|A(b_n\equiv s)\|$. Furthermore, we have

$$\frac{A(N;s,b_n)}{N}-\sum_{\substack{k=0\\k\neq j}}^{m-1}\frac{A(N;k,a_n)}{N}\leq\frac{A(N;j,a_n;s,b_n)}{N}\leq\frac{A(N;s,b_n)}{N}$$

for all $N\geq 1$, hence

$$\|A(a_n\equiv j, b_n\equiv s)\|=\|A(b_n\equiv s)\|=\|A(a_n\equiv j)\|\cdot\|A(b_n\equiv s)\|.$$

Thus (a_n) and (b_n) are independent mod m.

Definition 2. A pair of sequences $(c_n),(d_n)$ of integers is called admissible mod m if for any sequences (a_n) and (b_n) that are independent mod m the sequences (a_n+c_n) and (b_n+d_n) are also independent mod m.

Theorem 5. *The pair of sequences $(c_n),(d_n)$ is admissible* mod m *if and only if each of (c_n) and (d_n) has an a.d.f.* mod m *(denoted, respectively, by γ and δ, say) and $\gamma(j_1)=\delta(j_2)=1$ for some integers j_1 and j_2.*

Proof. Let $(c_n),(d_n)$ be admissible mod m. Let (0) denote the constant sequence $0,0,\cdots$. Then, since (0) and (0) are independent mod m by Theorem 3, the sequences (c_n) and (d_n) are independent mod m. In particular, each of (c_n) and (d_n) has an a.d.f. mod m. Furthermore, by Theorem 1, (c_n-d_n) has an a.d.f. mod m, and by Theorem 4 the sequences (0) and (c_n-d_n) are independent mod m. Since $(c_n),(d_n)$ are admissible mod m, it follows that (c_n) and (c_n) are independent mod m, and so $\gamma(j_1)=1$ for some j_1 by Theorem 3. The corresponding property of δ follows in a similar way.

Now suppose that (d_n) has δ as its a.d.f. mod m and that $\delta(j)=1$ for some j. Let (a_n) and (b_n) be independent mod m with α and β as a.d.f. mod m, respectively. By Theorem 4, (b_n) and (d_n) are independent mod m, so that according to Theorem 1 the sequence (b_n+d_n) has an a.d.f. mod m given by $\varepsilon(i)=\beta(i-j)$ for all $i\in\boldsymbol{Z}$. We claim that (a_n) and (b_n+d_n) are independent mod m. We have to show by Theorem 1 that for all $h,k\in\boldsymbol{Z}$ the sequence $(ha_n+kb_n+kd_n)$ has an a.d.f. mod m

given by

$$(3)\quad \|A(ha_n+kb_n+kd_n\equiv p)\|=\sum_{\substack{r,s=0\\ hr+ks\equiv p\,(\mathrm{mod}\,m)}}^{m-1}\|A(a_n\equiv r)\|\cdot\|A(b_n+d_n\equiv s)\|$$

for all $p\in \boldsymbol{Z}$. Since (ha_n+kb_n) and (d_n) are independent mod m by Theorem 4, we obtain by applying Theorem 1 twice:

$$\|A(ha_n+kb_n+kd_n\equiv p)\|=\|A(ha_n+kb_n\equiv p-kj)\|=\sum_{\substack{r,s=0\\ hr+ks\equiv p-kj\,(\mathrm{mod}\,m)}}^{m-1}\alpha(r)\beta(s).$$

On the other hand, the right-hand side of (3) is equal to

$$\sum_{\substack{r,s=0\\ hr+ks\equiv p\,(\mathrm{mod}\,m)}}^{m-1}\alpha(r)\varepsilon(s)=\sum_{\substack{r,s=0\\ hr+ks\equiv p\,(\mathrm{mod}\,m)}}^{m-1}\alpha(r)\beta(s-j)=\sum_{\substack{r,s=0\\ hr+ks\equiv p-kj\,(\mathrm{mod}\,m)}}^{m-1}\alpha(r)\beta(s).$$

Thus (a_n) and (b_n+d_n) are independent mod m. Since (c_n) enjoys a property similar to that of (d_n), it follows by the same argument that (a_n+c_n) and (b_n+d_n) are independent mod m.

Theorem 6. *Let (a_n) and (b_n) be independent* mod m *and u.d.* mod m, *and let $h,k\in \boldsymbol{Z}$ with* g.c.d. $(h,k,m)=1$. *Then the sequence (ha_n+kb_n), $n=1,2,\cdots$, is u.d.* mod m.

Proof. By (2), it suffices to show that for each $j=0,1,\cdots,m-1$, the congruence $hr+ks\equiv j\ (\mathrm{mod}\ m)$ has exactly m ordered pairs (r,s), $0\le r,\ s<m$, as solutions. Since the condition g.c.d. $(h,k,m)=1$ implies that each of these congruences has a solution, and since each solution (r,s) of $hr+ks\equiv j\ (\mathrm{mod}\ m)$ is of the form $(r,s)=(r_0+r_1,s_0+s_1)$, where (r_0,s_0) is a specific solution of $hr+ks\equiv j\ (\mathrm{mod}\ m)$ and (r_1,s_1) is an arbitrary solution of $hr+ks\equiv 0\ (\mathrm{mod}\ m)$, it follows that all the congruences $hr+ks\equiv j\ (\mathrm{mod}\ m)$, $j=0,1,\cdots,m-1$, have the same number of solutions, and so each of them has m solutions.

Obviously, if g.c.d. $(h,k,m)>1$, then the sequence (ha_n+kb_n), $n=1,2,\cdots$, cannot be u.d. mod m, although it will still have an a.d.f. mod m, according to Theorem 1. We note that if (a_n) and (b_n) are independent mod m and (a_n) is u.d. mod m, then (ha_n+kb_n), $n=1,2,\cdots$, is u.d. mod m whenever g.c.d. $(h,m)=1$ (see [1, Ch. 5, Example 1.4]). The latter condition cannot be relaxed to g.c.d. $(h,k,m)=1$: choose $(b_n)=(0)$, and let $h,k\in \boldsymbol{Z}$ with g.c.d. $(h,m)>1$ and g.c.d. $(k,m)=1$; then (a_n) and (b_n) are independent mod m by Theorem 4, but $(ha_n+kb_n)=(ha_n)$, which is not u.d. mod m. One may also establish the following criterion. Suppose the sequence (a_n) has an a.d.f. mod m; then (a_n) is u.d. mod m if and only if the sequence (a_n+b_n) is u.d. mod m for all sequences (b_n) such that (a_n) and (b_n) are independent mod m. The necessity follows from a remark made above. As to the sufficiency, one chooses $(b_n)=(0)$, which is independent mod m of (a_n) by Theorem 4.

(References can be found at the end of the second Note.)