58. *Asymptotic Distribution* mod m *and Independence of Sequences of Integers.* II

By Lauwerens KUIPERS*) and Harald NIEDERREITER**)

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

This is the continuation of the paper on the preceding pages. For notation and terminology, we refer to the first part. The numbering of theorems, definitions, and equations is continued from the first part.

We remark that if (a_n) and (b_n) are independent mod m, then (a_n) and (a_n+b_n) need not be independent mod m. For, otherwise, since (a_n) and (0) are independent mod m by Theorem 4, (a_n) and (a_n) would be independent mod m, which happens only under special circumstances (see Theorem 3). However, the following result can be shown.

Theorem 7. *Let (a_n) and (b_n) be independent* mod m *with (b_n) u.d.* mod m. *Let $h, k, l \in \boldsymbol{Z}$ be such that* g.c.d. (l, m) *divides k. Then the sequences (ha_n), $n=1,2,\cdots$, and (ka_n+lb_n), $n=1,2,\cdots$, are independent* mod m.

Proof. Let $q \in \boldsymbol{Z}$ be a solution of the congruence $lx \equiv k \pmod{m}$. By a remark following Theorem 6, the sequence (qa_n+b_n), $n=1,2,\cdots$, is u.d. mod m. For $r, s \in \boldsymbol{Z}$ we have

$$\begin{aligned}\|A(a_n\equiv r, qa_n+b_n\equiv s)\| &= \|A(a_n\equiv r, b_n\equiv s-qr)\| \\ &= \|A(a_n\equiv r)\|\cdot\|A(b_n\equiv s-qr)\| = \|A(a_n\equiv r)\|\cdot\frac{1}{m} \\ &= \|A(a_n\equiv r)\|\cdot\|A(qa_n+b_n\equiv s)\|,\end{aligned}$$

and therefore the sequences (a_n) and (qa_n+b_n) are independent mod m. Thus, by Theorem 2, the sequences (ha_n) and (lqa_n+lb_n) are independent mod m. But the second sequence is mod m identical with (ka_n+lb_n), and so we are done.

Remark. Theorem 7 has the following partial converse. If (a_n) and (b_n) have α and β as their a.d.f. mod m, respectively, if $\alpha(j)>0$ and $\beta(j)>0$ for all j, and if (a_n) and (b_n) are independent mod m, then the independence mod m of (a_n) and (ka_n+lb_n) implies that g.c.d. (l, m) divides k. For if k were not divisible by g.c.d. (l, m), then we would have

$$\begin{aligned}\|A(a_n\equiv 0)\|\cdot\|A(ka_n+lb_n\equiv k)\| &= \|A(a_n\equiv 0, ka_n+lb_n\equiv k)\| \\ &= \|A(a_n\equiv 0, lb_n\equiv k)\| = 0.\end{aligned}$$

*) 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.

This would imply $\|A(ka_n+lb_n\equiv k)\|=0$. But by Theorem 1 we have

$$\|A(ka_n+lb_n\equiv k)\|=\sum_{\substack{r,s=0\\ kr+ls\equiv k(\mathrm{mod}\ m)}}^{m-1}\alpha(r)\beta(s)\geq\alpha(l)\beta(0)>0,$$

which results in a contradiction. As the above argument shows, the condition on α and β may even be relaxed.

We generalize now a result of Kuipers and Shiue [2].

Theorem 8. *Let (a_n) and (b_n) have α and β as their a.d.f.* mod m, *respectively, and let (a_n) and (b_n) be independent* mod m. *Let j be a fixed integer with $\alpha(j)>0$, and let (a_{k_n}) be the subsequence of (a_n) containing all elements a_{k_n} with the property $a_{k_n}\equiv j$* (mod m). *Then the sequence (c_n), where $c_n=b_{k_n}$ for $n=1,2,\cdots$, has β as its a.d.f.* mod m.

Proof. Let r be an integer. We observe that $A(k_N;j,a_n)=N$ and $A(k_N;j,a_n;r,b_n)=A(N;r,c_n)$ for all $N\geq 1$. From the assumptions of the theorem, we have

$$\lim_{N\to\infty}A(k_N;j,a_n;r,b_n)/k_N=\|A(a_n\equiv j,b_n\equiv r)\|=\alpha(j)\beta(r)$$

and $\lim_{N\to\infty}N/k_N=\lim_{N\to\infty}A(k_N;j,a_n)/k_N=\alpha(j)$. Now write

$$\frac{A(N;r,c_n)}{N}=\frac{A(k_N;j,a_n;r,b_n)}{k_N}\cdot\frac{k_N}{N},$$

and letting $N\to\infty$, we obtain the desired result.

Remark. The sequences (a_n) and (c_n) in Theorem 8 need not be independent mod m. Consider the following example. Let $m=2$, let (a_n) be the periodic sequence $0,1,0,1,\cdots$ of period 2, and let (b_n) be the periodic sequence $0,0,1,1,0,0,1,1,\cdots$ of period 4. Then (a_n) and (b_n) are independent mod 2 and u.d. mod 2. Choose $j=0$ in Theorem 8; then $(c_n)=(a_n)$, and (a_n) and (c_n) are not independent mod 2.

Most of our results on independent pairs of sequences can be extended to independent tuples. For $s\geq 3$, let $(a_n^{(1)}),\cdots,(a_n^{(s)})$ be s sequences of integers. For $N\geq 1$ and $j_1,\cdots,j_s\in\boldsymbol{Z}$, let $A(N;j_1,a_n^{(1)};\cdots;j_s,a_n^{(s)})$ be the number of n, $1\leq n\leq N$, such that simultaneously $a_n^{(i)}\equiv j_i$ (mod m) for $1\leq i\leq s$. We write

$$\|A(a_n^{(1)}\equiv j_1,\cdots,a_n^{(s)}\equiv j_s)\|=\lim_{N\to\infty}A(N;j_1,a_n^{(1)};\cdots;j_s,a_n^{(s)})/N$$

in case the limit exists.

Definition 3. The sequences $(a_n^{(1)}),\cdots,(a_n^{(s)})$ are called independent mod m if for all $j_1,\cdots,j_s\in\boldsymbol{Z}$ with $0\leq j_i<m$ for $1\leq i\leq s$ the limits $\|A(a_n^{(1)}\equiv j_1,\cdots,a_n^{(s)}\equiv j_s)\|$ exist and we have

$$\|A(a_n^{(1)}\equiv j_1,\cdots,a_n^{(s)}\equiv j_s)\|=\prod_{i=1}^{s}\|A(a_n^{(i)}\equiv j_i)\|.$$

Theorem 9. *If the sequences $(a_n^{(1)}),\cdots,(a_n^{(s)})$ are independent* mod m, *then for any integer t with $2\leq t<s$ the sequences $(a_n^{(1)}),\cdots,(a_n^{(t)})$ are independent* mod m.

Proof. We have

$$A(N;j_1,a_n^{(1)};\cdots;j_t,a_n^{(t)})=\sum_{j_{t+1},\cdots,j_s=0}^{m-1}A(N;j_1,a_n^{(1)};\cdots;j_s,a_n^{(s)}).$$

Divide by N and let $N\to\infty$. Then

$$\begin{aligned}\|A(a_n^{(1)}\equiv j_1,\cdots,a_n^{(t)}\equiv j_t)\|&=\sum_{j_{t+1},\cdots,j_s=0}^{m-1}\|A(a_n^{(1)}\equiv j_1)\|\cdots\|A(a_n^{(s)}\equiv j_s)\|\\&=\|A(a_n^{(1)}\equiv j_1)\|\cdots\|A(a_n^{(t)}\equiv j_t)\|\\&\quad\cdot\left(\sum_{j_{t+1}=0}^{m-1}\|A(a_n^{(t+1)}\equiv j_{t+1})\|\right)\cdots\left(\sum_{j_s=0}^{m-1}\|A(a_n^{(s)}\equiv j_s)\|\right)\\&=\|A(a_n^{(1)}\equiv j_1)\|\cdots\|A(a_n^{(t)}\equiv j_t)\|.\end{aligned}$$

Remark. If for all t with $2\le t<s$, all t-tuples that can be formed from a given s-tuple of sequences are independent mod m, then the s-tuple itself need not necessarily be independent mod m. We offer the following simple counter-example. Let (a_n) be the periodic sequence $0,1,0,1,\cdots$ of period 2, let (b_n) be the periodic sequence $0,1,1,0,0,1,1,0,\cdots$ of period 4, and let (c_n) be the periodic sequence $0,0,1,1,0,0,1,1,\cdots$ of period 4. Each of these sequences is u.d. mod 2, and it is easily seen that they are pairwise independent mod 2. However, the triple (a_n), (b_n), (c_n) is not independent mod 2 since $\|A(a_n\equiv 1, b_n\equiv 1, c_n\equiv 1)\|=0$.

The following three results are shown in exactly the same way as Theorems 1, 2 and 3, respectively.

Theorem 10. *The sequences* $(a_n^{(1)}),\cdots,(a_n^{(s)})$ *are independent* mod m *if and only if for all* $h_1,\cdots,h_s\in \boldsymbol{Z}$ *the sequence* $(h_1a_n^{(1)}+\cdots+h_sa_n^{(s)})$, $n=1,2,\cdots$, *has an a.d.f.* mod m *given by*

$$\|A(h_1a_n^{(1)}+\cdots+h_sa_n^{(s)}\equiv j)\| =\sum_{\substack{r_1,\cdots,r_s=0\\ h_1r_1+\cdots+h_sr_s\equiv j\,(\mathrm{mod}\ m)}}^{m-1}\|A(a_n^{(1)}\equiv r_1)\|\cdots\|A(a_n^{(s)}\equiv r_s)\| \tag{4}$$

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

Theorem 11. *Let* $(a_n^{(1)}),\cdots,(a_n^{(s)})$ *be independent* mod m, *and let* $h_1,\cdots,h_s\in\boldsymbol{Z}$. *Then* $(h_1a_n^{(1)}),\cdots,(h_sa_n^{(s)})$ *are independent* mod m.

Theorem 12. *Suppose* (a_n) *has* α *as its a.d.f.* mod m. *Then* (a_n), $\cdots,(a_n)$ *are independent* mod m *if and only if* $\alpha(j)=1$ *for some* j.

The following is an analogue of Theorem 4.

Theorem 13. *Suppose* (a_n) *has* α *as its a.d.f.* mod m. *Then* (a_n), $(b_n^{(1)}),\cdots,(b_n^{(s-1)})$ *are independent* mod m *for any sequences* $(b_n^{(1)}),\cdots,(b_n^{(s-1)})$ *independent* mod m *if and only if* $\alpha(j)=1$ *for some* j.

Proof. First we show the necessity. It is easily seen that the sequences $(a_n),(c_n^{(1)}),\cdots,(c_n^{(s-2)})$ are independent mod m, where $(c_n^{(i)})=(0)$ for $1\le i\le s-2$. Therefore, by the given property of (a_n), the sequences $(a_n),(a_n),(c_n^{(1)}),\cdots,(c_n^{(s-2)})$ are independent mod m. It follows from Theorem 9 that (a_n) and (a_n) are independent mod m, so that an application of Theorem 3 completes the argument.

Now suppose that $\alpha(j)=1$ for some $j=0,1,\cdots,m-1$, and let $(b_n^{(1)})$,

$\cdots, (b_n^{(s-1)})$ be independent mod m. For $r_1, \cdots, r_s \in \boldsymbol{Z}$ with $0 \leq r_i < m$ for $1 \leq i \leq s$ and $r_1 \neq j$ we have $A(N; r_1, a_n; r_2, b_n^{(1)}; \cdots; r_s, b_n^{(s-1)}) \leq A(N; r_1, a_n)$ for all $N \geq 1$, so that

$$0 = \|A(a_n \equiv r_1, b_n^{(1)} \equiv r_2, \cdots, b_n^{(s-1)} \equiv r_s)\| = \|A(a_n \equiv r_1)\| \cdot \prod_{i=2}^{s} \|A(b_n^{(i-1)} \equiv r_i)\|.$$

Furthermore, we have

$$\begin{aligned} \frac{A(N; r_2, b_n^{(1)}; \cdots; r_s, b_n^{(s-1)})}{N} - \sum_{\substack{k=0 \\ k \neq j}}^{m-1} \frac{A(N; k, a_n)}{N} &\leq \frac{A(N; j, a_n; r_2, b_n^{(1)}; \cdots; r_s, b_n^{(s-1)})}{N} \\ &\leq \frac{A(N; r_2, b_n^{(1)}; \cdots; r_s, b_n^{(s-1)})}{N} \end{aligned}$$

for all $N \geq 1$, hence

$$\begin{aligned} \|A(a_n \equiv j, b_n^{(1)} \equiv r_2, \cdots, b_n^{(s-1)} \equiv r_s)\| &= \|A(b_n^{(1)} \equiv r_2, \cdots, b_n^{(s-1)} \equiv r_s)\| \\ &= \|A(a_n \equiv j)\| \cdot \prod_{i=2}^{s} \|A(b_n^{(i-1)} \equiv r_i)\|. \end{aligned}$$

Thus $(a_n), (b_n^{(1)}), \cdots, (b_n^{(s-1)})$ are independent mod m.

With an admissible s-tuple mod m of sequences defined in obvious analogy with Definition 2, we have the following criterion.

Theorem 14. *The s-tuple $(c_n^{(1)}), \cdots, (c_n^{(s)})$ is admissible* mod m *if and only if each $(c_n^{(i)})$, $1 \leq i \leq s$, has an a.d.f.* mod m *(denoted by γ_i, say) and $\gamma_1(j_1) = \gamma_2(j_2) = \cdots = \gamma_s(j_s) = 1$ for some integers $j_1, \cdots, j_s$.*

Proof. To show necessity, let (a_n) and (b_n) be an arbitrary pair of independent sequences mod m. By repeated application of Theorem 13, it follows that $(a_n), (b_n), (0), \cdots, (0)$ are independent mod m, where we have added $s-2$ sequences (0). By hypothesis, the sequences $(a_n + c_n^{(1)}), (b_n + c_n^{(2)}), (c_n^{(3)}), \cdots, (c_n^{(s)})$ are independent mod m; in particular, the sequences $(a_n + c_n^{(1)})$ and $(b_n + c_n^{(2)})$ are independent mod m by Theorem 9. This shows that the pair $(c_n^{(1)}), (c_n^{(2)})$ is admissible mod m, so that Theorem 5 can be applied. As to the other sequences $(c_n^{(i)})$, one proceeds in a similar way.

In order to prove sufficiency, one shows that if $(a_n^{(1)}), \cdots, (a_n^{(s)})$ are independent mod m, then one can take the sequences $(c_n^{(i)})$, one at a time, and add them termwise to the corresponding $(a_n^{(i)})$ without affecting independence mod m. The method is completely similar to that in the sufficiency part of the proof of Theorem 5. One uses, of course, Theorem 10 instead of Theorem 1.

Theorem 6 has an obvious analogue, for one shows by the same method (replacing, of course, the application of (2) by the application of (4)) that if $(a_n^{(1)}), \cdots, (a_n^{(s)})$ are independent mod m and u.d. mod m and if $h_1, \cdots, h_s$ are integers with g.c.d. $(h_1, \cdots, h_s, m) = 1$, then the sequence $(h_1 a_n^{(1)} + \cdots + h_s a_n^{(s)})$, $n = 1, 2, \cdots$, is u.d. mod m.

The following is an analogue of Theorem 8.

Theorem 15. *For $1\leq i\leq s$, let $(a_n^{(i)})$ have α_i as its a.d.f.* mod m, *and suppose that $(a_n^{(1)}),\cdots,(a_n^{(s)})$ are independent* mod m. *For given $t\in \boldsymbol{Z}$ with $1\leq t<s$, let $j_1,\cdots,j_t$ be fixed integers such that $\alpha_i(j_i)>0$ for $1\leq i\leq t$. Let $k_1<k_2<\cdots<k_n<\cdots$ be the sequence of all subscripts for which $a_{k_n}^{(i)}\equiv j_i$ (mod m) for all i, $1\leq i\leq t$. Then for the sequences $(a_{k_n}^{(t+1)}),\cdots,(a_{k_n}^{(s)})$ we have*

$$\|A(a_{k_n}^{(t+1)}\equiv j_{t+1},\cdots,a_{k_n}^{(s)}\equiv j_s)\|=\|A(a_n^{(t+1)}\equiv j_{t+1},\cdots,a_n^{(s)}\equiv j_s)\|$$

for all $j_{t+1},\cdots,j_s\in \boldsymbol{Z}$. Furthermore, if $t\leq s-2$, then $(a_{k_n}^{(t+1)}),\cdots,(a_{k_n}^{(s)})$ are independent mod m.

Proof. Let $j_{t+1},\cdots,j_s$ be integers. We note that $A(k_N;j_1,a_n^{(1)};\cdots;j_t,a_n^{(t)})=N$ and $A(k_N;j_1,a_n^{(1)};\cdots;j_s,a_n^{(s)})=A(N;j_{t+1},a_{k_n}^{(t+1)};\cdots;j_s,a_{k_n}^{(s)})$ for all $N\geq 1$. From the assumptions of the theorem, we have

$$\begin{aligned}\lim_{N\to\infty} A(k_N;j_1,a_n^{(1)};\cdots;j_s,a_n^{(s)})/k_N&=\|A(a_n^{(1)}\equiv j_1,\cdots,a_n^{(s)}\equiv j_s)\|\\&=\alpha_1(j_1)\cdots\alpha_s(j_s)\end{aligned}$$

and

$$\begin{aligned}\lim_{N\to\infty} N/k_N&=\lim_{N\to\infty} A(k_N;j_1,a_n^{(1)};\cdots;j_t,a_n^{(t)})/k_N=\|A(a_n^{(1)}\equiv j_1,\cdots,a_n^{(t)}\equiv j_t)\|\\&=\alpha_1(j_1)\cdots\alpha_t(j_t).\end{aligned}$$

Now write

$$\frac{A(N;j_{t+1},a_{k_n}^{(t+1)};\cdots;j_s,a_{k_n}^{(s)})}{N}=\frac{A(k_N;j_1,a_n^{(1)};\cdots;j_s,a_n^{(s)})}{k_N}\cdot\frac{k_N}{N},$$

and letting $N\to\infty$, we arrive at

$$\begin{aligned}\|A(a_{k_n}^{(t+1)}\equiv j_{t+1},\cdots,a_{k_n}^{(s)}\equiv j_s)\|&=\alpha_{t+1}(j_{t+1})\cdots\alpha_s(j_s)\\&=\|A(a_n^{(t+1)}\equiv j_{t+1},\cdots,a_n^{(s)}\equiv j_s)\|.\end{aligned}\tag{5}$$

This proves the first result. By keeping one j_i, $t+1\leq i\leq s$, in (5) fixed and summing over all the other j_p, $t+1\leq p\leq s$, $p\neq i$, from 0 to $m-1$, we arrive at $\|A(a_{k_n}^{(i)}\equiv j_i)\|=\alpha_i(j_i)$ for $t+1\leq i\leq s$. Therefore (5) shows also that the sequences $(a_{k_n}^{(t+1)}),\cdots,(a_{k_n}^{(s)})$ are independent mod m.

References

[1] L. Kuipers and H. Niederreiter: Uniform Distribution of Sequences. John Wiley and Sons, New York (1974).

[2] L. Kuipers and J.-S. Shiue: Asymptotic distribution modulo m of sequences of integers and the notion of independence. Atti Accad. Naz. Lincei (to appear).

[3] H. Niederreiter: On a class of sequences of lattice points. J. Number Th., **4**, 477–502 (1972).

[4] I. Niven: Uniform distribution of sequences of integers. Trans. Amer. Math. Soc., **98**, 52–61 (1961).