MATHEMATICS OF COMPUTATION, VOLUME 25, NUMBER 116, OCTOBER, 1971

Pseudo-Random Numbers: The Exact Distribution of Pairs*

By U. Dieter

To the Memory of H. Rademacher
February 7, 1969

Abstract. Pseudo-random numbers are usually generated by linear congruential methods. Starting with an integer y_0, a sequence $\{y_i\}$ is constructed by $y_{i+1} \equiv ay_i + r \pmod m$, m, a, r being integers. The derived fractions $x_i \equiv y_i/m$ are taken as samples from the uniform distribution on $[0, 1)$. In this paper it is shown that the joint probability distribution of pairs x_i, x_{i+s} can be calculated exactly. Explicit calculations show that this distribution is surprisingly near to the uniform distribution for most 'reasonable' generators. The best approximation to the uniform distribution on the unit-square is achieved if the continued fraction for a^s and m (or a^s and m/f) is long.

1. Introduction. This paper deals with pseudo-random numbers generated by the well-known linear congruential method, originally due to D. H. Lehmer [20]: A sequence of integers is started with a value y_0 and continued by

$$y_{i+1} \equiv ay_i + r \pmod m, \qquad 0 \leqq y_i < m \quad \text{for all } i. \tag{1.1}$$

The fractions

$$x_i = y_i/m \tag{1.1'}$$

are the derived pseudo-random numbers in the interval $[0, 1)$. The 'modulus' m, the 'factor' a, and the 'increment' r are given integers.

The linear congruential method has considerable advantages:

(1) For an appropriate choice of a, r, and m, the fractions $x_i = y_i/m$ are uniformly distributed in the interval $[0, 1)$.

(2) Subsequences of most generators pass different statistical tests, i.e. frequency tests, run tests, poker tests.

(3) The method is fast and easy to program.

The fact (1) is well known and will be referred to in Section 2. The facts (2) and (3) will not be considered in this paper.

Relatively recently, some mathematicians have considered number-theoretic properties of the generator (1.1). Important for the randomness of the sequence x_i is the serial correlation ρ_s between x_i and x_{i+s}, taken over the whole period. In a 'good' random sequence, ρ_s should be extremely small for small s. Coveyou [2] and Greenberger [11] derived bounds for ρ_s; Jansson [16], [17] showed that ρ_s can be

Received February 5, 1971.

AMS 1969 *subject classifications*. Primary 6515; Secondary 1050.

Key words and phrases. Multiplicatively generated pseudo-random numbers.

* Research supported by DFG (Deutsche Forschungsgemeinschaft) and N. R. C. (National Research Council of Canada).

calculated exactly for some important generators. That fact was rediscovered by the author (see Dieter [7]) without knowing Jansson's results. For an extremely fast method of computation of the serial correlation, see the paper Dieter/Ahrens [8]; that paper covers all subcases of the generator (1.1). Computations showed that the serial correlation ρ_t is extremely small for most generators. Although this condition is necessary for the use of a generator (1.1), it is in no way sufficient. Even if a is equal to 1, the increment r can be determined in such a way that $\rho_1 \approx 0$, which shows that the serial correlation by itself is by no means a sufficient indicator of randomness.

In most applications of pseudo-random numbers, one assumes that x_i and x_{i+1} are independent. Hence, it would be interesting to know the exact value of

$$(1.2) \qquad \Delta P = P(x \leqq x_i < x + \Delta x, y \leqq x_{i+1} < y + \Delta y) - \Delta x \Delta y.$$

The main purpose of this paper is to show that (1.2) can be calculated exactly for any choice of x, Δx, y, Δy, and to give numerical results for some often used generators.

The main tool of this calculation is the theory of the so-called generalized Dedekind sums, which are defined as follows:

$$(1.3) \qquad s_{g,h}^{(f)}(a, c) = \sum_{\mu=0}^{c-1} \left(\left(\frac{\mu}{c} + \frac{g}{cf}\right)\right)\left(\left(\frac{a\mu}{c} + \frac{ag + ch}{cf}\right)\right),$$

where a, c, g, h, f are integers and

$$(1.4) \qquad ((x)) = \begin{cases} x - [x] - \frac{1}{2} & \text{if } x \not\equiv 0 \pmod 1, \\ 0 & \text{if } x \equiv 0 \pmod 1) \end{cases}$$

differs only for integers x from the first Bernoulli-polynomial $P_1(x) = x - [x] - \frac{1}{2}$. The explicit expressions for (1.2) are alternating sums of generalized Dedekind sums. In particular, for the important generators $y_{i+1} \equiv ay_i \pmod{2^e}$, $a \equiv 5 \pmod 8$, the exact value of (1.2) is an alternating sum of four generalized Dedekind sums.

The generalized Dedekind sums (1.3) may be calculated using the reciprocity formula derived in Dieter [6]. This reciprocity suggests a Euclidean algorithm for a and c:

$$(1.5) \qquad a = q_0 c - a_1, \quad c = q_1 a_1 - a_2, \quad a_1 = q_2 a_2 - a_3, \cdots, a_{n-1} = q_n a_n,$$

where $|c| > |a_1| > |a_2| > \cdots > |a_{n-1}| > |a_n| = 1$ and the a_i are minimal at each step. The quotients q_i lead to a bound for the generalized Dedekind sum

$$(1.6) \qquad D(a, c) = \frac{1}{12}\left(\sum_{i=0}^{n} |q_i| + 3n + 5\right) \geqq |s_{g,h}^{(f)}(a, c)|,$$

which is independent of the subscripts g, h. Thus, $D(a, c)$ yields a bound for the quantity (1.2). For example, if the generator is defined by $y_{i+1} \equiv ay_i \pmod{2^e}$, $a \equiv 5 \pmod 8$, then

$$(1.7) \qquad |\Delta N| = 2^{e-2} |\Delta P| \leqq 3\, D(a, 2^{e-2}).$$

ΔN is the deviation of the number N of pairs x_i, x_{i+1} in a given rectangle $[x, x + \Delta x) \times [y, y + \Delta y)$ from their expected value $2^{e-2}\Delta x\Delta y$. Hence, (1.7) is small if $D(a, 2^{e-2})$ is small. This means:

The factor a has to be chosen in such a way that the Euclidean algorithm for a and 2^{e-2} has small quotients q_i.

Similar statements are true for general $m \neq 2^e$ and for generators with $r \neq 0$.

Extensive numerical computations of ΔN have been carried out with the help of J. Ahrens, Halifax, Canada and A. Grube, Karlsruhe, Germany. These calculations showed a surprising result: if the unit-square is divided into $2^\alpha \times 2^\alpha$ subsquares, then ΔN is extremely small for most factors a. For example, if the generator is defined by $y_{i+1} \equiv 5^{15} y_i \pmod{2^{35}}$ and the unit-square is divided into $2^{10} \times 2^{10}$ equal subsquares, ΔN is equal to one of the values 0, ± 1, ± 2, ± 3, ± 4, ± 5, ± 6, ± 7, and -8. This means: each of the $2^{10} \times 2^{10}$ subsquares should contain $2^{33-20} = 8{,}192$ pairs x_i, x_{i+1}. The actual numbers lie between 8,184 and 8,200. The bound (1. 7) is $39.75 < 40$.

These theoretical and numerical considerations show:

The factor a can be chosen in such a way that x_i and its successor x_{i+1} are nearly independent.

This property is particularly important for the generation of transformed random variables. A typical example is the construction of a standard normal variable z from two uniformly distributed independent random variables x and y according to the formula $z = (-2\ln x)^{1/2} \cos \pi y$. The convenient method of taking two successive pseudo-random numbers for x and y is legal only if successors and predecessors are statistically independent. Another example is numerical integration by Monte-Carlo methods. Here, it is always assumed that pairs of successive pseudo-random numbers are statistically independent.

The generator $y_{i+1} \equiv 5^{15} y_i \pmod{2^{35}}$ has the property that all quotients q_i of the Euclidean algorithm for 5^{15} and 2^{33} are small. However, some often used generators have quotients q_i which are quite large. These generators do not produce pseudo-random numbers which are as uniformly distributed in the unit square. For these generators it will be shown that to each large q_i there corresponds a set of sloping strips of subsquares of the unit square with equal values of ΔN. Although the values of ΔN are small for most 'reasonable' choices of the factor a, such pseudo-random number generators cannot be recommended: The set of sloping strips of subsquares with equal $\Delta N \neq 0$ causes a systematic deviation from the uniform distribution of pairs x_i, x_{i+1} in the unit square.

The results of this paper also show that the mixed congruential generator ($r \neq 0$) has no advantage over the purely multiplicative congruential generator ($r = 0$). Any adjustment of r cannot improve the statistical independence of pairs of pseudo-random numbers.

The paper is self-contained except for some number-theoretical results in Section 2 (length of period) and Section 4 (reciprocity formula). The formulas for the exact distribution of pairs are derived in Section 3. They are discussed in Section 5. Section 6 contains numerical results. A comparison of different generators closes the paper.

2. Length of Period and Generated Residues. The linear congruential method (1.1) generates nonnegative integers y_i which are smaller than the modulus m. If $y_n \equiv y_0 \pmod{m}$, the whole sequence $\{y_i\}$ is repeated. The smallest integer n such that $y_n \equiv y_0 \pmod{m}$ is called the length of the period. For a good approximation to the continuous uniform distribution, the period should have maximum length for a given modulus m. Fortunately, the maximum periods of the linear congruential generators depend on relatively simple properties of a, r, and m. As the results are different in the two cases $r \not\equiv 0 \pmod{m}$ and $r \equiv 0 \pmod{m}$, they will be quoted separately.

Case a. $r \not\equiv 0$ (mod m)—*Mixed Congruential Method.* The result is stated as

Theorem 2.1. *A complete period of the sequence* (1.1) *contains all residues* mod m, *if and only if*

(i) *r and m are relatively prime*;

(ii) $a \equiv 1$ (mod p) *for all prime factors p of m*;

(iii) $a \equiv 1$ (mod 4) *if* 4 *is a factor of m.*

A proof of this theorem can be found in Hull/Dobell [14], Jansson [17], Knuth [19]. In the proof, the relationship

$$y_{i+s} \equiv \begin{cases} a^s y_i + (a^{s-1} + a^{s-2} + \cdots + a + 1)r \pmod{m}, & \\ a^s y_i + \dfrac{a^s - 1}{a - 1} r \pmod{m} & \text{if } a \not\equiv 1 \pmod{m}, \\ a^s y_i + sr \pmod{m} & \text{if } a \equiv 1 \pmod{m} \end{cases} \tag{2.1}$$

is prominent. (2.1) is a direct consequence of the defining recursion (1.1) and will be used later on. In the rest of this paper, it is assumed that the conditions of Theorem 2.1 are always fulfilled.

Case b. $r \equiv 0$ (mod m)—*Multiplicative Congruential Method.* If the increment r is zero, the relation (2.1) can be simplified as

$$y_{i+s} \equiv a^s y_i \pmod{m}. \tag{2.2}$$

For the statement of the final result which corresponds to Theorem 2.1, an arithmetic function $\lambda(m)$ has to be introduced.

Definition 2.2.

$$\lambda(p^e) = \begin{cases} (p-1)p^{e-1} & \textit{if } p \neq 2,\ p \textit{ prime}, \\ 2^{e-2} & \textit{if } p = 2, e \geqq 3, \\ 2^{e-1} & \textit{if } p = 2, e = 1 \textit{ or } 2, \end{cases} \tag{2.3}$$

and

$$\lambda(m) = \lambda(p_1^{e_1} \cdots p_r^{e_r}) = \mathrm{LCM}(\lambda(p_1^{e_1}), \cdots, \lambda(p_r^{e_r})). \tag{2.4}$$

(LCM = Least common multiple.)

Secondly, the concept of a *primitive element* mod m is needed.

Definition 2.3. *a is called a primitive element* mod *m if*

(i) *a is a primitive root* mod *p for all odd prime factors p of m*;

(ii) $a^{p-1} \not\equiv 1$ (mod p^2) *if $p^2 \neq 4$ is a factor of m*;

(iii) $a \equiv \pm 5$ (mod 8) *if* 8 *is a factor of m*;

(iv) $a \equiv -1$ (mod 4) *if m is even and $m \not\equiv 0$* (mod 8).

With these definitions, the final result for the Case b can be stated as follows.

THEOREM 2.4. *The sequence* (1.1) *with* $r \equiv 0 \pmod{m}$ *has maximal period of length* $\lambda(m)$ *provided that*

(i) y_0 *and* m *are relatively prime*;

(ii) a *is a primitive element* mod m.

In the proof of Theorem 2.4, the recursion (2.2) is prominent. From now on, it will be assumed that these conditions for y_0 and a are fulfilled.

The Generated Residues. The mixed congruential method ($r \not\equiv 0$) generates all residues mod m if the directions of Theorem 2.1 are taken. Therefore, the interval $[0, 1)$ is covered by the x_i in (1.1′) such that all fractions μ/m occur. This is obviously the best approximation to the continuous uniform distribution within the accuracy $1/m$.

In the case of the multiplicative congruential method ($r = 0$), the generated residues mod m are not always spread as evenly. Therefore, Theorem 2.4 has to be supplemented by a detailed study of the residues which are obtained within a full period.

For this and for later purposes, an integer f is defined which depends solely on the modulus m:

DEFINITION 2.5.

(2.5) *f is the smallest of the divisors n of m for which* $\lambda(n)/n = \lambda(m)/m$.

If m/f is denoted by c one has

$$m = cf \quad \text{and} \quad \lambda(m) = c\lambda(f). \tag{2.6}$$

If $m = 2^e$ and $e \geqq 3$ then $f = 8$. It is easy to see that each prime factor p of m divides f. Since the directions in Theorem 2.4 for the choice of the factor a and the starting value y_0 are conditions mod p for odd $p|m$ and mod 8 if $8|m$, they are, in fact, conditions mod f. Hence, the generated residue classes mod m may be classified in terms of a set of residue classes $r_1, r_2, \cdots, r_{\lambda(f)}$ mod f. From here, the generated pseudo-random numbers may be represented as

$$\frac{\mu}{c} + \frac{r_1}{cf}, \frac{\mu}{c} + \frac{r_2}{cf}, \cdots, \frac{\mu}{c} + \frac{r_{\lambda(f)}}{cf} \quad \text{where } \mu = 0, 1, \cdots, c - 1. \tag{2.7}$$

For applications of (2.7) to any given m, a, and y_0, one starts with the determination of f. Then the generated residues $r_\nu \pmod{f}$ are calculated. Obviously, they depend only on the choice of the factor a and the starting value y_0. Only half of the number of possible choices for y_0 have to be considered: if y_0 is changed into $-y_0$, the pseudo-random numbers $x_i = y_i/m$ are merely transformed into $-x_i = -y_i/m \equiv 1 - (y_i/m) \pmod{1}$. Therefore, only those y_0, for which $0 < y_0 < f/2$, will be considered in the following special cases.

Case A. $m = 2^e$. These moduli are important since they are convenient on binary computers. One can, of course, assume that $e \geqq 3$. Depending on the choice of the factor a, two subcases arise:

A.1. $a \equiv 5 \pmod{8}$, $y_0 \equiv 1 \pmod{4}$. All residues

$$4\mu + 1 \qquad (\mu = 0, 1, \cdots, 2^{e-2} - 1) \tag{2.8}$$

are generated. The derived pseudo-random numbers $x_i = y_i/2^e$ are as uniformly distributed as possible within the accuracy $1/2^{e-2}$. Since a classification mod 4 is possible, $f = 8$ may be changed into $f = 4$ and therefore $\lambda(f) = 1$, deviating from Definition 2.5.

A.2. $a \equiv 3 \pmod 8$, $y_0 \equiv 1$ *or* $3 \pmod 8$. All residues

$$(2.9) \qquad 8\mu + 1,\ 8\mu + 3 \qquad (\mu = 0, 1, \cdots, 2^{e-3} - 1)$$

are generated. $f = 8$ and $\lambda(f) = 2$ remain in accordance with (2.5). The distribution is not quite as uniform as the last one.

Case B. $m = p^e$, $p \not\equiv 2$. This case covers the odd prime numbers and their powers. $p^e = 2^k \pm 1$ and $p^e = 10^k \pm 1$ are of practical interest. One has $f = p$, $\lambda(f) = p - 1$ and $c = m/p = p^{e-1}$. The residues

$$(2.10) \qquad p\mu + \nu \qquad (\mu = 0, 1, \cdots, p^{e-1} - 1, \nu = 1, 2, \cdots, p - 1)$$

are generated provided that the directions in Theorem 2. 4 are taken. If m is a prime number p, all residues except 0 are generated. For $e > 1$, additional gaps occur at all points μp.

3. Joint Probability Distribution of Pairs.

In this section, pseudo-random numbers will be related to their successors: the joint probability distribution of the pairs x_i, x_{i+1} will be determined. The main tool is the theory of the generalized Dedekind sums from which an accurate expression for

$$(3.1) \qquad \Delta P = P(x \leqq x_i < x + \Delta x, y \leqq x_{i+1} < y + \Delta y) - \Delta x \Delta y$$

will be calculated. The results can be generalized easily to arbitrary pairs x_i, x_{i+s}, since the probabilities

$$P(x \leqq x_i < x + \Delta x, y \leqq x_{i+s} < y + \Delta y) - \Delta x \Delta y$$

for $s > 1$ may be obtained from the formulas below if the factor a is changed to a^s, and r to $r(a^s - 1)/(a - 1)$ if $a \not\equiv 1 \pmod m$ and rs if $a \equiv 1 \pmod m$. This is readily seen from formula (2.1).

In an ideal random sequence, all ΔP should be very small signifying statistical independence of predecessors and successors.

The discussion of (3.1) is started with a few elementary remarks. If x_i and x are numbers between 0 and 1 (excluding 1), the following formula holds:

$$(3.2) \qquad [x_i - x] = \begin{cases} -1 & \text{if } 0 \leqq x_i < x, \\ 0 & \text{if } x \leqq x_i < 1. \end{cases}$$

Therefore,

$$(3.3) \qquad [x_i - x] - [x_i - x - \Delta x] = \begin{cases} 1 & \text{if } x \leqq x_i < x + \Delta x, \\ 0 & \text{otherwise.} \end{cases}$$

The left-hand side of (3.3) can be written in terms of the first Bernoulli polynomial

$$(3.4) \qquad P_1(x) = x - [x] - \tfrac{1}{2}$$

as

$$(3.5) \qquad [x_i - x] - [x_i - x - \Delta x] = P_1(x_i - x - \Delta x) - P_1(x_i - x) + \Delta x.$$

Now let n be the period length of the pseudo-random numbers x_i (i.e. $n = m$ or $n = \lambda(m)$). Then the following formula for ΔP is a consequence of (3.5):

$$\begin{aligned}\Delta P &= \frac{1}{n}\sum_{i=1}^{n} [P_1(x_i - x - \Delta x) - P_1(x_i - x) + \Delta x] \\ &\qquad \cdot [P_1(x_{i+1} - y - \Delta y) - P_1(x_{i+1} - y) + \Delta y] - \Delta x \Delta y \\ &= \frac{1}{n}\sum_{i=1}^{n} [P_1(x_i - x - \Delta x) - P_1(x_i - x)] \\ &\qquad \cdot [P_1(x_{i+1} - y - \Delta y) - P_1(x_{i+1} - y)] + R_1 + R_2,\end{aligned} \tag{3.6}$$

where

$$\begin{aligned}R_1 &= \frac{\Delta y}{n}\sum_{i=1}^{n} [P_1(x_i - x - \Delta x) - P_1(x_i - x)] \\ &= \Delta y\,[P(x \leqq x_i < x + \Delta x) - \Delta x], \\ R_2 &= \frac{\Delta x}{n}\sum_{i=1}^{n} [P_1(x_{i+1} - y - \Delta y) - P_1(x_{i+1} - y)] \\ &= \Delta x\,[P(y \leqq x_{i+1} < y + \Delta y) - \Delta y].\end{aligned} \tag{3.7}$$

According to the results of Section 2, the quantities $P(x \leqq x_i < x + \Delta x) - \Delta x$ must be small; otherwise the pseudo-random numbers are not uniformly distributed. For an exact calculation of (3.7), a lemma is needed. (For the definition of $((x))$, see (1.4).)

LEMMA 3.1.

$$\text{(i)} \quad \sum_{\mu=0}^{m-1} P_1\left(\frac{\mu + x}{m}\right) = P_1(x); \qquad \text{(ii)} \quad \sum_{\mu=0}^{m-1} \left(\left(\frac{\mu + x}{m}\right)\right) = ((x)).$$

Proof. Since the function $P_1(x)$ is periodic with period 1, one can assume $0 \leqq x < 1$. Therefore,

$$\begin{aligned}\sum_{\mu=0}^{m-1} P_1\left(\frac{\mu + x}{m}\right) &= \sum_{\mu=0}^{m-1} \left(\frac{\mu + x}{m} - \frac{1}{2}\right) \\ &= \frac{m-1}{2} + x - \frac{m}{2} = x - \frac{1}{2} = P_1(x),\end{aligned}$$

proving part (i) of the lemma. If $x \not\equiv 0 \pmod 1$, part (i) and (ii) of the lemma coincide; If $x \equiv 0 \pmod 1$, one has

$$\begin{aligned}\sum_{\mu=0}^{m-1} \left(\left(\frac{\mu}{m}\right)\right) = \sum_{\mu=1}^{m-1} \left(\left(\frac{\mu}{m}\right)\right) &= \sum_{\mu=1}^{m-1} \left(\frac{\mu}{m} - \frac{1}{2}\right) \\ &= \frac{m-1}{2} - \frac{m-1}{2} = 0 = ((x)),\end{aligned}$$

which proves the lemma.

From now on the two cases $r \not\equiv 0 \pmod m$ and $r \equiv 0 \pmod m$ have to be considered separately.

Case a. $r \not\equiv 0 \pmod m$. In this case, $x_i \equiv \mu/m$ and $x_{i+1} \equiv ((a\mu + r)/m) \pmod 1$, where μ runs from 0 to $m - 1$. Furthermore, the following notation will be used

$$x = \frac{I_1}{m}, \qquad x + \Delta x = \frac{I_2}{m}, \quad \text{and} \quad y = \frac{J_1}{m}, \qquad y + \Delta y = \frac{J_2}{m}. \tag{3.8}$$

With the help of Lemma 3.1, the residual terms R_1 and R_2 in (3.7) are calculated first:

$$\begin{aligned} R_1 &= \frac{J_2 - J_1}{m^2} \sum_{\mu=0}^{m-1} \left\{ P_1\left(\frac{\mu}{m} - \frac{I_2}{m}\right) - P_1\left(\frac{\mu}{m} - \frac{I_1}{m}\right) \right\} \\ &= \frac{J_2 - J_1}{m^2} [P_1(-I_2) - P_1(-I_1)], \\ R_2 &= \frac{I_2 - I_1}{m^2} \sum_{\mu=0}^{m-1} \left\{ P_1\left(\frac{a\mu + r}{m} - \frac{J_2}{m}\right) - P_1\left(\frac{a\mu + r}{m} - \frac{J_1}{m}\right) \right\} \\ &= \frac{I_2 - I_1}{m^2} [P_1(-J_2) - P_1(-J_1)]. \end{aligned}$$

Without loss of generality, it can be assumed that I_1, I_2, J_1, and J_2 are integers. Then R_1 and R_2 vanish.

Now, the main part of ΔP, the expression (3.6), is calculated. One has

$$\Delta P = \frac{1}{m} \sum_{\mu=0}^{m-1} \left\{ P_1\left(\frac{\mu - I_2}{m}\right) - P_1\left(\frac{\mu - I_1}{m}\right) \right\} \left\{ P_1\left(\frac{a\mu + r - J_2}{m}\right) - P_1\left(\frac{a\mu + r - J_1}{m}\right) \right\},$$

which becomes by the substitution $\mu \to \mu + I_2$ and $\mu \to \mu + I_1$,

$$\begin{aligned} \Delta P = \frac{1}{m} \sum_{\mu=0}^{m-1} \Bigg\{ & P_1\left(\frac{\mu}{m}\right) P_1\left(\frac{a\mu}{m} + \frac{aI_2 - J_2 + r}{m}\right) - P_1\left(\frac{\mu}{m}\right) P_1\left(\frac{a\mu}{m} + \frac{aI_2 - J_1 + r}{m}\right) \\ & - P_1\left(\frac{\mu}{m}\right) P_1\left(\frac{a\mu}{m} + \frac{aI_1 - J_2 + r}{m}\right) + P_1\left(\frac{\mu}{m}\right) P_1\left(\frac{a\mu}{m} + \frac{aI_1 - J_1 + r}{m}\right) \Bigg\}. \end{aligned} \tag{3.9}$$

Here the sums are almost generalized Dedekind sums, since the function $((x))$ differs from $P_1(x)$ only for integer values. As this concerns only the values $\mu \equiv 0$ and $\mu \equiv -I_\lambda + a^{-1}J_\nu - a^{-1}r \pmod m$, where the subscripts λ and ν stand for 1 or 2, (3.9) becomes

$$\begin{aligned} \Delta P = \frac{1}{m} \sum_{\mu=0}^{m-1} \Bigg\{ & \left(\left(\frac{\mu}{m}\right)\right) \left(\left(\frac{a\mu}{m} + \frac{aI_2 - J_2 + r}{m}\right)\right) \\ & - \left(\left(\frac{\mu}{m}\right)\right) \left(\left(\frac{a\mu}{m} + \frac{aI_2 - J_1 + r}{m}\right)\right) \\ & - \left(\left(\frac{\mu}{m}\right)\right) \left(\left(\frac{a\mu}{m} + \frac{aI_1 - J_2 + r}{m}\right)\right) \\ & + \left(\left(\frac{\mu}{m}\right)\right) \left(\left(\frac{a\mu}{m} + \frac{aI_1 - J_1 + r}{m}\right)\right) \Bigg\} + R_3 + R_4 \end{aligned} \tag{3.10}$$

where

$$\begin{aligned}(3.11)\quad 2mR_3 &= -P_1\left(\frac{aI_2 - J_2 + r}{m}\right) + P_1\left(\frac{aI_2 - J_1 + r}{m}\right)\\ &\quad + P_1\left(\frac{aI_1 - J_2 + r}{m}\right) - P_1\left(\frac{aI_1 - J_1 + r}{m}\right)\\ &= \left[\frac{aI_2 - J_2 + r}{m}\right] - \left[\frac{aI_2 - J_1 + r}{m}\right]\\ &\quad - \left[\frac{aI_1 - J_2 + r}{m}\right] + \left[\frac{aI_1 - J_1 + r}{m}\right],\\ 2mR_4 &= -P_1\left(\frac{a^{-1}(J_2 - r) - I_2}{m}\right) + P_1\left(\frac{a^{-1}(J_2 - r) - I_1}{m}\right)\\ &\quad + P_1\left(\frac{a^{-1}(J_1 - r) - I_2}{m}\right) - P_1\left(\frac{a^{-1}(J_1 - r) - I_1}{m}\right)\\ &= \left[\frac{a^{-1}(J_2 - r) - I_2}{m}\right] - \left[\frac{a^{-1}(J_2 - r) - I_1}{m}\right]\\ &\quad - \left[\frac{a^{-1}(J_1 - r) - I_2}{m}\right] + \left[\frac{a^{-1}(J_1 - r) - I_1}{m}\right].\end{aligned}$$

Both expressions are of the form $[a + b] + [c + d] - [a + c] - [b + d]$, which is either -1, 0, or $+1$. Consequently, R_3 and R_4 can only attain one of the values $-1/2m$, 0, $+1/2m$. This means that $R_3 + R_4$ is bounded by $1/m$.

Consequently, the final expression for ΔP becomes

$$(3.12)\qquad \Delta P = \frac{1}{m}\sum_{\lambda,\mu=1}^{2}(-1)^{\lambda+\mu}s^{(m)}_{0,aI_\lambda - J_\mu + r}(a, m) + R \quad \text{where } |R| \leqq \frac{1}{m}.$$

Case b, $r \equiv 0 \pmod{m}$—*General Considerations.* In this case, the pseudo-random numbers x_i and their successors x_{i+1} have the form (2.7):

$$x_i = \frac{\mu}{c} + \frac{r_\nu}{cf}, \qquad x_{i+1} \equiv \frac{a\mu}{c} + \frac{ar_\nu}{cf} \pmod{1}$$

where $\mu = 0, 1, \cdots, c - 1$, and the r_ν are residues mod f. Again, the notation (3.8) will be used. Then the residual terms R_1 and R_2 in (3.7) become by means of Lemma 3.1:

$$\begin{aligned}(3.13)\quad R_1 &= \frac{J_2 - J_1}{c^2 f\lambda(f)}\sum_{r_\nu}\sum_{\mu=0}^{c-1}\left\{P_1\left(\frac{\mu}{c} + \frac{r_\nu}{cf} - \frac{I_2}{cf}\right) - P_1\left(\frac{\mu}{c} + \frac{r_\nu}{cf} - \frac{I_1}{cf}\right)\right\}\\ &= \frac{J_2 - J_1}{c^2 f\lambda(f)}\sum_{r_\nu}\left\{P_1\left(\frac{r_\nu - I_2}{f}\right) - P_1\left(\frac{r_\nu - I_1}{f}\right)\right\}\end{aligned}$$

and similarly

$$(3.14)\qquad R_2 = \frac{I_2 - I_1}{c^2 f\lambda(f)}\sum_{r_\nu}\left\{P_1\left(\frac{r_\nu - J_2}{f}\right) - P_1\left(\frac{r_\nu - J_1}{f}\right)\right\}.$$

If f is small, it can be assumed that $I_1 \equiv I_2$ and $J_1 \equiv J_2 \pmod{f}$. Then (3.13) and (3.14) vanish. If $I_1 \not\equiv I_2$ or $J_1 \not\equiv J_2 \pmod{f}$, (3.13) and (3.14) have to be calculated exactly. A bound for $R_1 + R_2$ is given by

$$|R_1 + R_2| \leqq \frac{1}{c}\left(\frac{I_2 - I_1}{cf} + \frac{J_2 - J_1}{cf}\right) \leqq \frac{2}{c}. \tag{3.15}$$

Now the main part (3.6) of ΔP will be calculated.

$$\begin{aligned}\Delta P = \frac{1}{c\lambda(f)} \sum_{r_\nu} \sum_{\mu=0}^{c-1} &\left\{P_1\left(\frac{\mu}{c} + \frac{r_\nu - I_2}{cf}\right) - P_1\left(\frac{\mu}{c} + \frac{r_\nu - I_1}{cf}\right)\right\} \\ &\cdot\left\{P_1\left(\frac{a\mu}{c} + \frac{ar_\nu - J_2}{cf}\right) - P_1\left(\frac{a\mu}{c} + \frac{ar_\nu - J_1}{cf}\right)\right\} + R',\end{aligned} \tag{3.16}$$

where $R' = R_1 + R_2$. If

$$I_1 \not\equiv r_\nu, \qquad I_2 \not\equiv r_\nu, \qquad J_1 \not\equiv r_\nu, \qquad J_2 \not\equiv r_\nu \ (\mathrm{mod}\ f) \quad \text{for all } r_\nu \tag{3.17}$$

the function $P_1(\cdot)$ can always be changed into $((\cdot))$ and ΔP becomes again an alternating sum of generalized Dedekind sums. If one of the conditions (3.17) is not fulfilled, the change of $P_1(\cdot)$ to $((\cdot))$ produces the following terms

$$\begin{aligned}R_3 = \frac{1}{2c\lambda(f)} &\left\{\delta\left(\frac{r_\nu - I_2}{f}\right)\left(P_1\left(\frac{aI_2 - J_1}{cf}\right) - P_1\left(\frac{aI_2 - J_2}{cf}\right)\right)\right. \\ &\left. + \delta\left(\frac{r_\nu - I_1}{f}\right)\left(P_1\left(\frac{aI_1 - J_2}{cf}\right) - P_1\left(\frac{aI_1 - J_1}{cf}\right)\right)\right\},\end{aligned}$$

$$\begin{aligned}R_4 = \frac{1}{2c\lambda(f)} &\left\{\delta\left(\frac{ar_\nu - J_2}{f}\right)\left(P_1\left(\frac{a^{-1}J_2 - I_1}{cf}\right) - P_1\left(\frac{a^{-1}J_2 - I_2}{cf}\right)\right)\right. \\ &\left. + \delta\left(\frac{ar_\nu - J_1}{f}\right)\left(P_1\left(\frac{a^{-1}J_1 - I_2}{cf}\right) - P_1\left(\frac{a^{-1}J_1 - I_1}{cf}\right)\right)\right\},\end{aligned}$$

where

$$\delta(x) = \begin{cases}1 & \text{if } x \equiv 0 \ (\mathrm{mod}\ 1), \\ 0 & \text{if } x \not\equiv 0 \ (\mathrm{mod}\ 1).\end{cases}$$

A reasoning similar to that after (3.11) shows that R_3 and R_4 are bounded by $1/2c\lambda(f)$.

This gives the final answer

$$\Delta P = \frac{1}{c\lambda(f)} \sum_{r_\nu} \sum_{\lambda,\mu=1}^{2} (-1)^{\lambda+\mu} s^{(cf)}_{c(r_\nu - I_\lambda), aI_\lambda - J_\mu}(a, c) + R + R', \tag{3.18}$$

where R is bounded by $1/c\lambda(f)$. If $I_1 \equiv I_2$ and $J_1 \equiv J_2$ (mod f), R' is 0; otherwise, $R' = R_1 + R_2$, where $R_1 + R_2$ is bounded by (3.15) and has to be calculated according to (3.13) and (3.14).

The results (3.12) and (3.18) show that ΔP is essentially an alternating sum of generalized Dedekind sums with the same principal arguments a, m or a, c.

Case c. $r \equiv 0$ (mod m) –*Special Cases.* For later discussion, the results of the previous subsection will now be applied to some special m. The moduli $m = 2^e$ are most important as they are convenient on binary computers.

A.1. $m = 2^e$, $e \geqq 3$, $a \equiv 5$ (mod 8), $y_0 \equiv 1$ (mod 4). All residues of the form

$4\mu + 1$ ($\mu = 0, 1, \cdots, 2^{e-2} - 1$) are generated. Therefore, $c = 2^{e-2}$, $f = 4$, $r_\nu = 1$ and formally, $\lambda(f) = 1$. Without loss of generality, it can be assumed that $I_1 \equiv I_2$ and $J_1 \equiv J_2 \pmod 4$. (3.18) now becomes

$$\Delta P = \frac{1}{2^{e-2}} \sum_{\lambda,\mu=1}^{2} (-1)^{\lambda+\mu} s^{(2^e)}_{2^{e-2}(1-I_\lambda), aI_\lambda - J_\mu}(a, 2^{e-2}) + R, \qquad |R| \leqq \frac{1}{2^{e-2}}. \tag{3.19}$$

If $I_1 \equiv I_2 \not\equiv 1$ and $J_1 \equiv J_2 \not\equiv 1 \pmod 4$, the residual term R is 0. If $I_1 \equiv I_2 \equiv J_1 \equiv J_2 \equiv 1 \pmod 4$, (3.19) can be simplified a little

$$\Delta P = \frac{1}{2^{e-2}} \sum_{\lambda,\mu=1}^{2} (-1)^{\lambda+\mu} s^{(2^e)}_{0, aI_\lambda - J_\mu}(a, 2^{e-2}) + R \quad \text{where } |R| \leqq \frac{1}{2^{e-2}}. \tag{3.19$'$}$$

This expression is of the same form as (3.12) with $m = 2^{e-2}$. It will be discussed further in Section 7.

A.2. $m = 2^e$, $e \geqq 3$, $a \equiv 3 \pmod 8$, $y_0 \equiv 1$ *or* $3 \pmod 8$. All residues of the form $8\mu + 1$, $8\mu + 3$ ($\mu = 0, 1, \cdots, 2^{e-3} - 1$) are generated. Therefore, $c = 2^{e-3}$, $f = 8$, $\lambda(f) = 2$ and $r_\nu = 1$ or 3. Again, it can be assumed that $I_1 \equiv I_2$ and $J_1 \equiv J_2 \pmod 8$. (3.18) now becomes

$$\Delta P = \frac{1}{2^{e-2}} \sum_{\lambda,\mu=1}^{2} (-1)^{\lambda\cdot\mu} \left\{ s^{(2^e)}_{2^{e-3}(1-I_\lambda), aI_\lambda - J_\mu}(a, 2^{e-3}) + s^{(2^e)}_{2^{e-3}(3-I_\lambda), aI_\lambda - J_\mu}(a, 2^{e-3}) \right\} + R \tag{3.20}$$

$$\text{where } |R| \leqq \frac{1}{2^{e-2}}.$$

B.1. $m = p^e \neq 2^e$, p *prime*. All residues of the form $\mu p + \nu$ ($\mu = 0, 1, \cdots, p^{e-1} - 1$, $\nu = 1, \cdots, p - 1$) are generated. Therefore, $c = p^{e-1}$, $f = p$ and $r_\nu = \nu$. The residual terms R_1 (3.13) and R_2 (3.14) are calculated first by means of Lemma 3.1:

$$\begin{aligned} R_1 &= \frac{J_2 - J_1}{p^{2e-1}(p-1)} \sum_{\nu=1}^{p-1} \left\{ P_1\left(\frac{\nu - I_2}{p}\right) - P_1\left(\frac{\nu - I_1}{p}\right) \right\} \\ &= \frac{J_2 - J_1}{p^{2e-1}(p-1)} \left\{ \sum_{\nu=0}^{p-1} \left\{ P_1\left(\frac{\nu - I_2}{p}\right) - P_1\left(\frac{\nu - I_1}{p}\right) \right\} - P_1\left(-\frac{I_2}{p}\right) + P_1\left(-\frac{I_1}{p}\right) \right\} \\ &= \frac{J_2 - J_1}{p^{2e-1}(p-1)} \left\{ P_1(-I_2) - P_1(-I_1) - P_1\left(-\frac{I_2}{p}\right) + P_1\left(-\frac{I_1}{p}\right) \right\}, \end{aligned}$$

and hence, if I_1 and I_2 are integers,

$$|R_1| = \frac{J_2 - J_1}{p^{2e-1}(p-1)} \left\{ P_1\left(\frac{p - I_1}{p}\right) - P_1\left(\frac{p - I_2}{p}\right) \right\} \leqq \frac{J_2 - J_1}{p^{2e}} \leqq \frac{1}{p^e}. \tag{3.21}$$

For R_2 a similar value is obtained.

To simplify the expression (3.18) for ΔP, a lemma is needed.

Lemma 3.2.

$$\sum_{\nu=0}^{n-1} s^{(nf)}_{\nu f+g, h}(a, c) = s^{(nf)}_{ng, h}(a, n\,c).$$

Proof. If μ runs through the residue classes $0, 1, \cdots, c - 1$, and ν runs through the residue classes $0, 1, \cdots, n - 1$, then $\mu n + \nu$ runs through all residue classes $0, 1, \cdots, nc - 1$. Consequently:

$$\begin{aligned}\sum_{\nu=0}^{n-1} s_{\nu f+g,h}^{(nf)}(a, c) &= \sum_{\nu=0}^{n-1}\sum_{\mu=0}^{c-1}\left(\left(\frac{\mu}{c}+\frac{\nu f+g}{nfc}\right)\right)\left(\left(\frac{a\mu}{c}+\frac{a(\nu f+g)+ch}{nfc}\right)\right)\\ &= \sum_{\nu=0}^{n-1}\sum_{\mu=0}^{c-1}\left(\left(\frac{\mu n+\nu}{nc}+\frac{g}{nfc}\right)\right)\left(\left(\frac{a(\mu n+\nu)}{nc}+\frac{ag+ch}{nfc}\right)\right)\\ &= s_{ng,h}^{(nf)}(a, nc)\end{aligned}$$

which proves the lemma.

An application of the lemma yields for (3.18),

$$\begin{aligned}\sum_{\nu=1}^{p-1} s_{p^{e-1}(\nu-I),aI-J}^{(p^e)}(a, p^{e-1}) &= \sum_{\nu=0}^{p-1} s_{p^{e-1}(\nu-I),aI-J}^{(p^e)}(a, p^{e-1}) - s_{-p^{e-1}I,aI-J}^{(p^e)}(a, p^{e-1})\\ &= s_{-p^eI,aI-J}^{(p^e)}(a, p^e) - s_{-p^{e-1}I,aI-J}^{(p^e)}(a, p^{e-1})\\ &= s_{0,aI-J}^{(p^e)}(a, p^e) - s_{-p^{e-1}I,aI-J}^{(p^e)}(a, p^{e-1}).\end{aligned} \tag{3.22}$$

(3.21) and (3.22) give the final answer

$$\begin{aligned}\Delta P = \frac{1}{p^{e-1}(p-1)}\sum_{\lambda,\mu=1}^{2}(-1)^{\lambda+\mu}\\ \cdot\left\{s_{0,aI_\lambda-J_\mu}^{(p^e)}(a, p^e) - s_{-p^{e-1}I_\lambda,aI_\lambda-J_\mu}^{(p^e)}(a, p^{e-1})\right\} + R\end{aligned} \tag{3.23}$$

$$\text{where } |R| \leqq \frac{1}{p^{e-1}(p-1)} + \frac{2}{p^e} < \frac{4}{p^e}.$$

B.2. $m = p$, *p prime*. Then, $f = p$, $c = 1$ and $s_{-I,aI-J}^{(p)}(a, 1) = s_{-I,-J}^{(p)}(0, 1) = ((I/p))((J/p))$, according to Corollaries 1 and 2 of Section 4. Therefore, (3.23) can be simplified to

$$\Delta P = \frac{1}{p-1}\sum_{\lambda,\mu=1}^{2}(-1)^{\lambda+\mu}s_{0,aI_\lambda-J_\mu}^{(p)}(a, p) + R \quad \text{where } |R| \leqq \frac{4}{p-1}. \tag{3.24}$$

The significance of the present expressions will be discussed in Sections 5, 6, and 7. At the moment the results are merely summarized as

THEOREM 3.3. *The joint probability distribution of pairs of pseudo-random numbers is expressed in the following formulae: for* $r \not\equiv 0 \pmod m$ *in* (3.12), *for* $r \equiv 0 \pmod m$ *and arbitrary m the expression is found in* (3.18). *In particular, for* $m = 2^e$ *and* $a \equiv 5 \pmod 8$ *in* (3.19), *for* $m = 2^e$ *and* $a \equiv 3 \pmod 8$ *in* (3.20), *and for* $m = p^e \neq 2^e$ *in* (3.23) *and* (3.24).

4. The Computation of Generalized Dedekind Sums.

In the preceding section, it was shown that the determination of the exact number of pairs of pseudo-random numbers in a given rectangle can be reduced to the evaluation of generalized Dedekind sums.

The methods of computation which are presented here utilize a number of theorems on these sums which were proved in 1957 (cf. Dieter [6]). The corresponding theorems for ordinary Dedekind sums $s(a, c)$ have been known since Dedekind's Supplement to the Complete Works of Bernhard Riemann. They are the special cases $g \equiv h \equiv 0 \pmod f$ in all the subsequent identities.

Reciprocity Formula. Let $(a, c) = 1$. *Then*

$$\operatorname{sgn} c\, s_{g,h}^{(f)}(a, c) + \operatorname{sgn} a\, s_{h,g}^{(f)}(c, a) = \frac{a}{2c} P_2\left(\frac{g}{f}\right) + \frac{1}{2ac} P_2\left(\frac{ag + ch}{f}\right) + \frac{c}{2a} P_2\left(\frac{h}{f}\right)$$
$$+ \begin{cases} \left(\left(\frac{g}{f}\right)\right)\left(\left(\frac{h}{f}\right)\right) & \textit{if } (g, h) \not\equiv (0, 0) \pmod f \\ -\frac{1}{4} \operatorname{sgn}(ac) & \textit{if } g \equiv h \equiv 0 \pmod f). \end{cases}$$

Here

$$P_2(x) = (x - [x])^2 - (x - [x]) + \tfrac{1}{6}$$

is the second Bernoulli-polynomial.

COROLLARY 1. *$s_{g,h}^{(f)}(a + nc, c) = s_{g,ng+h}^{(f)}(a, c)$, n integral.*

COROLLARY 2. *$s_{g,h}^{(f)}(0, 1) = ((g/f))((h/f))$.*

COROLLARY 3. *$s_{g,h}^{(f)}(-a, c) = -s_{-g,h}^{(f)}(a, c) = -s_{g,-h}^{(f)}(a, c)$.*

The corollaries are simple consequences of the definition of the generalized Dedekind sums. The Reciprocity Formula is a deeper arithmetic law; for a proof see Dieter [6], Meyer [26], Rademacher [28], or a forthcoming paper of the author [10].

The stated identities are utilized for a computational procedure in the following way. Let $s = s_{g,h}^{(f)}(a, c)$ be the generalized Dedekind sum to be evaluated. If $|a| \geqq |c|$, change s into a sum for which $|a| < |c|$ by means of Corollary 1. Now, use the Reciprocity Formula for exchanging the numbers in the positions a, c and g, h. The new $|a|$ is no smaller than the new $|c|$ and can therefore be reduced by an application of Corollary 1.

Repeated steps of this kind will decrease the numbers in the positions a and c until, finally, Corollary 2 becomes applicable. Often the process can be shortened by applications of Corollary 3. The procedure suggests an Euclidean algorithm for a and c:

$$\begin{aligned} a &= q_0 c - a_1 \\ c &= q_1 a_1 - a_2 \\ &\;\vdots \\ a_{n-2} &= q_{n-1} a_{n-1} - a_n \\ a_{n-1} &= q_n a_n \quad \text{where } a_n = \pm 1. \end{aligned} \tag{4.1}$$

The $|a_\iota|$ must form a decreasing sequence if the process is to terminate. Since the signs of the q_ι and a_ι may be chosen freely, one can in fact ensure that

$$|a_{\iota+1}| \leqq \tfrac{1}{2} |a_\iota|. \tag{4.2}$$

This assumption causes all q_ι and a_ι to be uniquely determined. In Corollaries 1 and 3, the subscripts g and h are also transformed. This suggests the definitions:

$$(g_\nu, h_\nu) = (q_\nu g_{\nu-1} + h_{\nu-1}, -g_{\nu-1}), \qquad (g_{-1}, h_{-1}) = (g, h). \tag{4.3}$$

For the final expression, another integer, called d, is needed. d is the last number in a chain of numbers b_ι which is defined as follows:

$$\begin{aligned} &b_{n+1} = a_n, \qquad b_n = 0, \qquad b_{n-1} = -b_{n+1} = -a_n, \\ &b_k = q_{k+1} b_{k+1} - b_{k+2} \quad \text{for } k = n-1, n-2, \cdots, 0, -1. \end{aligned} \tag{4.4}$$

Now

$$b_0 = d \tag{4.5}$$

is used for the final expression of the Dedekind sums.

THEOREM 4.1. *Let the quotients* q_ν *be defined by the Euclidean algorithm* (4.1), (4.2), *the subscripts* g_ν, h_ν *by* (4.3) *and the integer* d *by* (4.4), (4.5). *If* $(g, h) \not\equiv 0 \pmod f$ *one has*

$$\begin{aligned} s^{(f)}_{g,h}(a, c) = {} & \frac{d}{2c} P_2\left(\frac{ag + ch}{f}\right) \\ & + \frac{a}{2c} P_2\left(\frac{g}{f}\right) - \frac{1}{2} \sum_{\nu=0}^{n} q_\nu P_2\left(\frac{h_\nu}{f}\right) - \sum_{\nu=0}^{n} \left(\left(\frac{g_\nu}{f}\right)\right)\left(\left(\frac{h_\nu}{f}\right)\right). \end{aligned} \tag{4.6}$$

If $g \equiv h \equiv 0 \pmod f$, *the ordinary Dedekind sums are obtained and the expression* (4.6) *changes to*

$$s^{(1)}_{0,0}(a, c) = s(a, c) = \frac{a + d}{12c} - \frac{1}{12} \sum_{\nu=0}^{n} q_\nu + \frac{1}{4} \sum_{\nu=1}^{n} \operatorname{sgn}(a_{\nu-1} a_\nu) \tag{4.7}$$

where $\operatorname{sgn}(x) = x/|x|$ *if* $x \neq 0$ *and* 0 *otherwise.*

Theorem 4.1 will be proved by induction. A different proof may be found in Rademacher [27] for the ordinary Dedekind sums and in Dieter [6] for the generalized Dedekind sums.

Proof of Theorem 4.1. The following identity will be considered first:

$$\begin{aligned} \operatorname{sgn}(c) s^{(f)}_{g,h}(a, c) = {} & \operatorname{sgn}(a_m) s^{(f)}_{g_{m-1}, h_{m-1}}(a_{m-1}, a_m) - \frac{b_m}{2a_m} P_2\left(\frac{ag + ch}{f}\right) \\ & - \frac{a_{m-1}}{2a_m} P_2\left(\frac{g_{m-1}}{f}\right) + \frac{d}{2c} P_2\left(\frac{ag + ch}{f}\right) + \frac{a}{2c} P_2\left(\frac{g}{f}\right) \\ & - \sum_{\nu=0}^{m-1} \left\{\left(\left(\frac{g_\nu}{f}\right)\right)\left(\left(\frac{h_\nu}{f}\right)\right) - \frac{1}{4} \operatorname{sgn}(a_\nu a_{\nu-1})\, \delta\left(\frac{g}{f}\right) \delta\left(\frac{h}{f}\right) + \frac{1}{2} q_\nu P_2\left(\frac{h_\nu}{f}\right)\right\}. \end{aligned} \tag{4.8}$$

The function

$$\delta(x) = \begin{cases} 1 & \text{if } x \equiv 0 \pmod 1, \\ 0 & \text{if } x \not\equiv 0 \pmod 1, \end{cases} \tag{4.9}$$

enables one to obtain (4.6) and (4.7) simultaneously from the special case $m = n$ in (4.8). The next two consequences of (4.1), (4.3), (4.6) and Corollary 2 show this:

$$\begin{aligned} \operatorname{sgn}(a_n) s^{(f)}_{g_{n-1}, h_{n-1}}(a_{n-1}, a_n) & = \operatorname{sgn}(a_n) s^{(f)}_{g_{n-1}, h_{n-1}}(q_n a_n, a_n) \\ & = \operatorname{sgn}(a_n) s^{(f)}_{g_{n-1},\, q_n g_{n-1} + h_{n-1}}(0, a_n) \\ & = s^{(f)}_{-h_n, g_n}(0, 1) = -\left(\left(\frac{g_n}{f}\right)\right)\left(\left(\frac{h_n}{f}\right)\right) \end{aligned}$$

and

$$\frac{a_{n-1}}{2a_n} P_2\left(\frac{g_{n-1}}{f}\right) = \frac{q_n}{2} P_2\left(\frac{h_n}{f}\right).$$

(4.8) will now be proved by induction. The case $m = 0$ is easily verified. The induction step from m to $m + 1$ uses Corollaries 1 and 3 and the reciprocity formula as follows:

$$\begin{aligned} \operatorname{sgn}(a_m)s^{(f)}_{g_{m-1},h_{m-1}}(a_{m-1}, a_m) &= \operatorname{sgn}(a_m)s_{g_{m-1},h_{m-1}}(q_m a_m - a_{m+1}, a_m) \\ &= \operatorname{sgn}(a_m)s^{(f)}_{g_{m-1},q_m g_{m-1}+h_{m-1}}(-a_{m+1}, a_m) = -\operatorname{sgn}(a_m)s^{(f)}_{h_m,g_m}(a_{m+i}, a_m) \\ &= \operatorname{sgn}(a_{m+1})s_{g_m,h_m}(a_m, a_{m+1}) + \frac{1}{4}\operatorname{sgn}(a_m a_{m+1})\,\delta\left(\frac{g}{f}\right)\delta\left(\frac{h}{f}\right) - \left(\left(\frac{g_m}{f}\right)\right)\left(\left(\frac{h_m}{f}\right)\right) \\ &\quad - \frac{a_m}{2a_{m+1}}P_2\left(\frac{g_m}{f}\right) - \frac{1}{2a_m a_{m+1}}P_2\left(\frac{a_m g_m + a_{m+1}h_m}{f}\right) - \frac{a_{m+1}}{2a_m}P_2\left(\frac{h_m}{f}\right). \end{aligned} \tag{4.10}$$

The last term is transformed using (4.1) and (4.3):

$$-\frac{a_{m+1}}{2a_m}P_2\left(\frac{h_m}{f}\right) = -\frac{q_m}{2}P_2\left(\frac{h_m}{f}\right) + \frac{a_{m-1}}{2a_m}P_2\left(\frac{g_{m-1}}{f}\right). \tag{4.11}$$

After a substitution of (4.10) and (4.11) into (4.8), it merely remains to show that

$$-\frac{b_m}{2a_m}P_2\left(\frac{ag + ch}{f}\right) - \frac{1}{2a_m a_{m+1}}P_2\left(\frac{a_m g_m + a_{m+1}h_m}{f}\right) = -\frac{b_{m+1}}{2a_{m+1}}P_2\left(\frac{ag + ch}{f}\right).$$

This identity follows from the relations

$$a_m b_{m+1} - a_{m+1}b_m = 1, \tag{4.12}$$

$$a_m g_m + a_{m+1}h_m = ag + ch. \tag{4.13}$$

Formula (4.12) will be proved by descending induction. It holds for $m = n$ since $a_n^2 = 1$. The induction step from $m + 1$ to m is carried out by means of an identity which follows from (4.1) and (4.4). Namely,

$$\begin{aligned} a_m b_{m+1} - a_{m+1}b_m &= (q_{m+1}a_{m+1} + a_{m+2})b_{m+1} - a_{m+1}(q_{m+1}b_{m+1} - b_{m+2}) \\ &= a_{m+1}b_{m+2} - a_{m+2}b_{m+1}. \end{aligned}$$

Formula (4.13) will be proved by ascending induction. It holds for $m = -1$, since $a_{-1}g_{-1} + a_0 h_{-1} = ag + ch$. The induction step from $m - 1$ to m is carried out by means of an identity which follows from (4.1) and (4.3).

$$\begin{aligned} a_m g_m + a_{m+1}h_m &= a_m(q_m g_{m-1} + h_{m-1}) + (q_m a_m - a_{m-1})(-g_{m-1}) \\ &= a_{m-1}g_{m-1} + a_m h_{m-1}. \end{aligned}$$

This completes the proof of formula (4.8) and therefore of (4.6) and (4.7).

5. Numerical Considerations. Further information on the joint distribution of pairs (x_i, x_{i+1}) can be extracted from Section 4 in which the precise calculation of generalized Dedekind sums was outlined. This will throw some light on cases in which the Euclidean algorithm for a and m or a and m/f has some large quotients.

The discussion will be based on generators

$$y_{i+1} \equiv ay_i \pmod{2^e}, \quad \text{where } a \equiv 5 \pmod 8, \tag{5.1}$$

since they are most important on binary computers. The unit-square is divided into $2^\alpha \times 2^\alpha$ subsquares of equal area $2^{-2\alpha}$. Hence, the following quantity has to be calculated

$$\Delta N(\lambda, \mu) = 2^{e-2} P\left(\frac{\lambda}{2^\alpha} \leqq x_i < \frac{\lambda + 1}{2^\alpha}, \frac{\mu}{2^\alpha} \leqq x_{i+1} < \frac{\mu + 1}{2^\alpha}\right) - 2^{e-2-2\alpha},$$

which becomes, by use of (3, 19),

$$\begin{aligned} \Delta N(\lambda, \mu) = {} & s^{(2^\alpha)}_{2^{\alpha-2}, a\lambda-\mu}(a, 2^{e-2}) - s^{(2^\alpha)}_{2^{\alpha-2}, a(\lambda+1)-\mu}(a, 2^{e-2}) \\ & - s^{(2^\alpha)}_{2^{\alpha-2}, a\lambda-\mu-1}(a, 2^{e-2}) + s^{(2^\alpha)}_{2^{\alpha-2}, a(\lambda+1)-\mu-1}(a, 2^{e-2}). \end{aligned} \tag{5.2}$$

The calculation of $s^{(f)}_{g,h}(a, c)$ in Section 4 starts with the Euclidean algorithm for a and c:

$$a = q_0 c - a_1, c = q_1 a_1 - a_2, \cdots, a_{n-2} = q_{n-1} a_{n-1} - a_n, a_{n-1} = q_n a_n. \tag{5.3}$$

Then, the integers (g_ν, h_ν) are constructed:

$$(g_{-1}, h_{-1}) = (g, h), \qquad (g_\nu, h_\nu) = (q_\nu g_{\nu-1} + h_{\nu-1}, -g_{\nu-1}). \tag{5.4}$$

To obtain a simple expression for g_ν, h_ν, the so-called νth convergent to the fraction a/c is defined as follows:

$$\frac{s_0}{t_0} = \frac{q_0}{1}, \quad \frac{s_1}{t_1} = q_0 - \frac{1}{q_1}, \quad \frac{s_2}{t_2} = q_0 - \frac{1}{q_1 - 1/q_2}$$

and, generally,

$$s_\nu = q_\nu s_{\nu-1} - s_{\nu-2}, \qquad t_\nu = q_\nu t_{\nu-1} - t_{\nu-2}. \tag{5.5}$$

That (5.5) defines the νth convergent to a/c follows from

$$\frac{\left(q_\nu - \dfrac{1}{q_{\nu+1}}\right)s_{\nu-1} - s_{\nu-2}}{\left(q_\nu - \dfrac{1}{q_{\nu+1}}\right)t_{\nu-1} - t_{\nu-2}} = \frac{q_{\nu+1}(q_\nu s_{\nu-1} - s_{\nu-2}) - s_{\nu-1}}{q_{\nu+1}(q_\nu t_{\nu-1} - t_{\nu-2}) - t_{\nu-1}} = \frac{q_{\nu+1}s_\nu - s_{\nu-1}}{q_{\nu+1}t_\nu - t_{\nu-1}} =: \frac{s_{\nu+1}}{t_{\nu+1}}.$$

(5.5) yields the following expression for (g_ν, h_ν):

$$(g_\nu, h_\nu) = (s_\nu g + t_\nu h, -s_{\nu-1} g - t_{\nu-1} h), \tag{5.6}$$

which can also be proved by induction:

$$\begin{aligned} (g_{\nu+1}, h_{\nu+1}) &= (q_{\nu+1} g_\nu + h_\nu, -g_\nu) = ((q_{\nu+1} s_\nu - s_{\nu-1})g + (q_{\nu+1} t_\nu - t_{\nu-1})h, -g_\nu) \\ &= (s_{\nu+1} g + t_{\nu+1} h, -s_\nu g - t_\nu h). \end{aligned}$$

With these definitions, formula (4.6) can now be applied to (5.2). However, the following terms in (4.6),

$$\frac{d}{2c} P_2\left(\frac{ag + ch}{f}\right) = \frac{d}{2^{e-1}} P_2\left(\frac{a}{4}\right), \frac{a}{2c} P_2\left(\frac{g}{f}\right) = \frac{a}{2^{e-1}} P_2\left(\frac{1}{4}\right), q_0 P_2\left(\frac{h_0}{f}\right) = q_0 P_2\left(\frac{1}{4}\right)$$

appear four times with alternating signs. Consequently, they cancel each other.

The last sum $\sum_{\nu=0}^{n}((g_\nu/f))((h_\nu/f))$ is bounded by $\frac{1}{4}(n+1)$ and will be denoted by R. Therefore, one obtains

$$\begin{aligned}\Delta N(\lambda,\mu) = -\frac{1}{2}\sum_{\nu=1}^{n} q_\nu \Big\{ & P_2\Big(\frac{S_{\nu-1}}{4}+\frac{t_{\nu-1}(a\lambda-\mu)}{2^\alpha}\Big) \\ & - P_2\Big(\frac{S_{\nu-1}}{4}+\frac{t_{\nu-1}(a\lambda-\mu-1)}{2^\alpha}\Big) \\ & - P_2\Big(\frac{S_{\nu-1}}{4}+\frac{t_{\nu-1}(a\lambda+a-\mu)}{2^\alpha}\Big) \\ & + P_2\Big(\frac{S_{\nu-1}}{4}+\frac{t_{\nu-1}(a\lambda+a-\mu-1)}{2^\alpha}\Big)\Big\} + R \end{aligned} \tag{5.7}$$

$$= -\frac{1}{2}\sum_{\nu=1}^{n} q_\nu S_{\nu-1} + R \quad \text{where } |R| \leqq n+1. \tag{5.8}$$

Formula (5.7) results in a global bound for $\Delta N(\lambda,\mu)$:

THEOREM 5.1. *If the generator is defined by* $y_{i+1} \equiv ay_i \pmod{2^e}$, $a \equiv 5 \pmod 8$, *the deviation* $\Delta N(\lambda,\mu)$ *is globally bounded by*

$$|\Delta N| \leqq \frac{1}{4}\sum_{i=0}^{n} |q_i| + n + 1. \tag{5.9}$$

Proof. The second Bernoulli polynomial is bounded by $-\frac{1}{12} \leqq P_2(x) \leqq \frac{1}{6}$. Hence, the curly bracket in (5. 7) is bounded by $\frac{1}{2}$, which proves Theorem 5.1.

It should be noted that similar theorems are true for generators $y_{i+1} \equiv ay_i + r \pmod m$ with $r \neq 0$ or $r = 0$.

To obtain stronger results, the term in the curly brackets in (5.7) has to be calculated exactly. For this, two lemmas are needed.

LEMMA 5.2. $P_2(x+\Delta x) - P_2(x) = 2\Delta x P_1(x) + (\Delta x)^2 - 2\,\Delta x R$, *where*

$$\begin{array}{lll} R = 0 & \text{if } n \leqq x,\ x+\Delta x < n+1 & \text{for some integer } n, \\ 0 < R \leqq 1 & \text{if } n-1 \leqq x < n \leqq x+\Delta x < n+1 & \text{for some integer } n, \\ -1 \leqq R < 0 & \text{if } n-1 \leqq x+\Delta x < n \leqq x < n+1 & \text{for some integer } n. \end{array}$$

LEMMA 5.3. $P_1(x+\Delta x) - P_1(x) = \Delta x - R$, *where*

$$\begin{array}{lll} R = 0 & \text{if } n \leqq x,\ x+\Delta x \leqq n+1 & \text{for some integer } n, \\ R = 1 & \text{if } n-1 \leqq x < n \leqq x+\Delta x < n+1 & \text{for some integer } n, \\ R = -1 & \text{if } n-1 \leqq x+\Delta x < n \leqq x < n+1 & \text{for some integer } n. \end{array}$$

Proof of Lemma 5.2. As the function $P_2(x)$ is periodic with period 1, one can assume $0 \leqq x < 1$. Hence,

$$\begin{aligned} P_2(x+\Delta x) - P_2(x) &= (x+\Delta x-[x+\Delta x])^2 - (x+\Delta x-[x+\Delta x]) - x^2 + x \\ &= 2\,\Delta x(x-\tfrac{1}{2}) + (\Delta x)^2 - [x+\Delta x][2(x+\Delta x) - [x+\Delta x] - 1] \\ &= 2\,\Delta x P_1(x) + (\Delta x)^2 - R'. \end{aligned}$$

If $[x + \Delta x] = 0$, then $R' = 0$. If $[x + \Delta x] = 1$, then $R' = 2(x + \Delta x) - 2 \leqq 2\Delta x$. If $[x + \Delta x] = -1$, then $R' = -2(x + \Delta x) = -2\Delta x - 2x \leqq 2\,|\Delta x|$ since $x \geqq 0$ and $\Delta x \leqq 0$ in this case. This proves Lemma 5.2.

Lemma 5.3 is obvious and will not be proved here.

The term in the curly brackets in (5.7) will be denoted by $S_{\nu-1}$ and $\frac{1}{4}s_\nu + (1/2^\alpha)t_\nu(a\lambda - \mu)$ by A_ν. Two applications of Lemma 5.2 and one of Lemma 5.3 result in

$$(5.10)\qquad S_\nu = P_2(A_\nu) - P_2\left(A_\nu - \frac{t_\nu}{2^\alpha}\right) - \left\{P_2\left(A_\nu + \frac{at_\nu}{2^\alpha}\right) - P_2\left(A_\nu + \frac{at_\nu}{2} - \frac{t_\nu}{2^\alpha}\right)\right\}$$

$$(5.11)\qquad = 2\frac{t_\nu}{2^\alpha}\left\{P_1\left(A_\nu - \frac{t_\nu}{2^\alpha}\right) - P_1\left(A_\nu - \frac{t_\nu}{2^\alpha} + \frac{at_\nu}{2^\alpha}\right) - R_1^{(\nu)} + R_2^{(\nu)}\right\}$$

$$(5.12)\qquad = -2\frac{t_\nu}{2^\alpha}\cdot\frac{at_\nu}{2^\alpha} + 2\frac{t_\nu}{2^\alpha}\{R_3^{(\nu)} - R_1^{(\nu)} + R_2^{(\nu)}\} \quad \text{where } |R_i^{(\nu)}| \leqq 1.$$

It can be assumed that t_ν and at_ν are reduced mod 2^α. Let the residue $\bar{x}$ for which

$$(5.13)\qquad \bar{x} \equiv x \pmod{2^\alpha}, \qquad |\bar{x}| \leqq 2^{\alpha-1},$$

be denoted by $\bar{x}$. Then (5.12) yields, for $\Delta N(\lambda, \mu)$,

$$(5.14)\qquad \Delta N(\lambda, \mu) = -\sum_{\nu=0}^{n-1} q_{\nu+1}\left(\frac{\bar{t}_\nu}{2^\alpha}(R_3^{(\nu)} - R_1^{(\nu)} + R_2^{(\nu)}) - \frac{\bar{t}_\nu}{2^\alpha}\cdot\frac{\overline{at}_\nu}{2^\alpha}\right) + R'$$

where $|R'| \leqq n + 1$ and the $R_i^{(\nu)}$ are bounded by 1.

To clarify the further discussion of (5.14), some additional notations are convenient.

Definition 5.4. *An index ν for which q_ν is large is called essential; all other indices are inessential. A subsquare $Q(\lambda, \mu) = [\lambda 2^{-\alpha}, (\lambda + 1)2^{-\alpha}) \times [\mu 2^{-\alpha}, (\mu + 1)2^{-\alpha})$ is called regular, if there are integers n_ν such that*

$$(5.15)\qquad n_\nu \leqq A_\nu - \frac{\bar{t}_\nu}{2^\alpha},\ A_\nu,\ A_\nu + \frac{\overline{at}_\nu}{2^\alpha} - \frac{\bar{t}_\nu}{2^\alpha},\ A_\nu + \frac{\overline{at}_\nu}{2^\alpha} < n_\nu + 1$$

is true for all essential ν, where $A_\nu = \frac{1}{4}s_\nu + (1/2^\alpha)t_\nu(a\lambda - \mu)$. Otherwise, it is called irregular.

In terms of these definitions, a theorem is formulated which is an elaboration of the expression (5.14).

Theorem 5.5. *If the subsquare $Q(\lambda, \mu)$ is regular, then*

$$(5.16)\qquad \Delta N(\lambda, \mu) = \sum_{\nu=1}^{n} q_\nu \frac{\bar{t}_{\nu-1}}{2^\alpha}\cdot\frac{\overline{at}_{\nu-1}}{2^\alpha} + R' \quad \textit{where } |R'| \leqq n + 1.$$

(5.16) is small in most cases and often zero. If $Q(\lambda, \mu)$ is irregular, then each essential index ν, for which (5.15) is not fulfilled, contributes to $\Delta N(\lambda, \mu)$ the amount

$$(5.17)\qquad -q_\nu \frac{|\bar{t}_{\nu-1}|}{2^\alpha} R^{(\nu)} \quad \textit{where } |R^{(\nu)}| \leqq 1.$$

$R^{(\nu)}$ is positive for pairs λ, μ, if $\bar{t}_{\nu-1} > 0$, $\overline{at}_{\nu-1} > 0$, or $\bar{t}_{\nu-1} < 0$, $\overline{at}_{\nu-1} < 0$ and if

there is an integer n_ν such that

$$(5.18)\qquad \frac{2^\alpha}{\bar t_{\nu-1}}(n_\nu + \tfrac{1}{4}s_{\nu-1}) - 1 < \mu - \bar a\lambda < \frac{2^\alpha}{\bar t_{\nu-1}}(n_\nu + \tfrac{1}{4}s_{\nu-1}) + \bar a.$$

$R^{(\nu)}$ is negative for pairs λ, μ, if $\bar t_{\nu-1} > 0$, $\overline{at}_{\nu-1} < 0$, or $\bar t_{\nu-1} < 0$, $\overline{at}_{\nu-1} > 0$ and if there is an integer n_ν such that

$$(5.19)\qquad \frac{2^\alpha}{\bar t_{\nu-1}}(n_\nu + \tfrac{1}{4}s_{\nu-1}) + \bar a - 1 < \mu - \bar a\lambda < \frac{2^\alpha}{\bar t_{\nu-1}}(n_\nu + \tfrac{1}{4}s_{\nu-1}).$$

Proof of Theorem 5.5. If a subsquare $Q(\lambda, \mu)$ is regular, all $R_i^{(\nu)}$ are zero. Hence (5.14) results in (5.16).

If a subsquare $Q(\lambda, \mu)$ is irregular, some of the $R_i^{(\nu)}$ are not zero. For the subsequent discussion, it will be assumed that $\bar t_{\nu-1} > 0$ and $\overline{at}_{\nu-1} > 0$. The discussion in the remaining three cases is similar and left to the reader.

According to (5.15), one of the following inequalities must hold for some integer n_ν:

$$(5.20)\qquad \frac{s_{\nu-1}}{4} + \frac{\bar t_{\nu-1}}{2^\alpha}(a\lambda - \mu) - \frac{\bar t_{\nu-1}}{2^\alpha} < -n_\nu \leqq \frac{s_{\nu-1}}{4} + \frac{\bar t_{\nu-1}}{2^\alpha}(a\lambda - \mu),$$

$$(5.21)\qquad \frac{s_{\nu-1}}{4} + \frac{\bar t_{\nu-1}}{2^\alpha}(a\lambda - \mu) < -n_\nu \leqq \frac{s_{\nu-1}}{4} + \frac{\bar t_{\nu-1}}{2^\alpha}(a\lambda - \mu) + \frac{\overline{at}_{\nu-1} - \bar t_{\nu-1}}{2^\alpha},$$

$$(5.22)\qquad \begin{aligned}&\frac{s_{\nu-1}}{4} + \frac{\bar t_{\nu-1}}{2^\alpha}(a\lambda - \mu) + \frac{\overline{at}_{\nu-1} - \bar t_{\nu-1}}{2^\alpha}\\ &\qquad < -n_\nu \leqq \frac{s_{\nu-1}}{4} + \frac{\bar t_{\nu-1}}{2^\alpha}(a\lambda - \mu) + \frac{\overline{at}_{\nu-1}}{2^\alpha}.\end{aligned}$$

If (5.20) is true, then $0 < R_1^{(\nu-1)} \leqq 1$, $R_2^{(\nu-1)} = 0$, $R_3^{(\nu-1)} = 1$. The term $R_1^{(\nu-1)}$ appears during the transition from (5.10) to (5.11). The term $R_3^{(\nu-1)}$ appears during the transition from (5.11) to (5.12). Hence, the contribution to $\Delta N(\lambda, \mu)$ is

$$-q_\nu \frac{\bar t_{\nu-1}}{2^\alpha}(R_3^{(\nu-1)} - R_1^{(\nu-1)}) = -q_\nu \frac{\bar t_{\nu-1}}{2^\alpha} R^{(\nu)}, \quad \text{where } 0 \leqq R^{(\nu)} \leqq 1.$$

If (5.21) is true, then $R_1^{(\nu-1)} = R_2^{(\nu-1)} = 0$, $R_3^{(\nu-1)} = +1$. There appear no terms $R_1^{(\nu-1)}$ and $R_2^{(\nu-1)}$ during the transition from (5.10) to (5.11), but there does appear the term $R_3^{(\nu-1)} = +1$ during the transition from (5.11) to (5.12). Hence, the contribution to $\Delta N(\lambda, \mu)$ is

$$-q_\nu \frac{\bar t_{\nu-1}}{2^\alpha} R_3^{(\nu-1)} = -q_\nu \frac{\bar t_{\nu-1}}{2^\alpha} R^{(\nu)} \quad \text{where } R^{(\nu)} = 1.$$

If (5.22) is true, then $R_1^{(\nu-1)} = 0$, $0 < R_2^{(\nu-1)} \leqq 1$, $R_3^{(\nu-1)} = 0$. Only the term $R_2^{(\nu-1)}$ appears during the transition from (5.10) to (5.11). Hence, the contribution to $\Delta N(\lambda, \mu)$ is

$$-q_\nu \frac{\bar t_{\nu-1}}{2^\alpha} R_2^{(\nu-1)} = -q_\nu \frac{\bar t_{\nu-1}}{2^\alpha} R^{(\nu)} \quad \text{where } 0 \leqq R^{(\nu)} \leqq 1.$$

$R_2^{(\nu-1)}$ is 0 if the right-hand side of inequality (5.22) is an integer and obtained by $-n_\nu$. Consequently, the $\leqq$ sign in (5.22) can be changed to a $<$ sign.

It has to be shown, that the conditions (5.20) to (5.22) are equivalent to (5.18). A multiplication by $2^\alpha/\bar{t}_{\nu-1}$ changes (5.20) to (5.22) into

$$\frac{2^\alpha}{\bar{t}_{\nu-1}}\left(n_\nu + \frac{s_{\nu-1}}{4}\right) - 1 < \mu - a\lambda \leqq \frac{2^\alpha}{\bar{t}_{\nu-1}}\left(n_\nu + \frac{s_{\nu-1}}{4}\right), \tag{5.20'}$$

$$\frac{2^\alpha}{\bar{t}_{\nu-1}}\left(n_\nu + \frac{s_{\nu-1}}{4}\right) < \mu - a\lambda \leqq \frac{2^\alpha}{\bar{t}_{\nu-1}}\left(n_\nu + \frac{s_{\nu-1}}{4}\right) + \bar{a} - 1, \tag{5.21'}$$

$$\frac{2^\alpha}{\bar{t}_{\nu-1}}\left(n_\nu + \frac{s_{\nu-1}}{4}\right) + \bar{a} - 1 < \mu - a\lambda < \frac{2^\alpha}{\bar{t}_{\nu-1}}\left(n_\nu + \frac{s_{\nu-1}}{4}\right) + \bar{a}. \tag{5.22'}$$

As the contribution to $\Delta N(\lambda, \mu)$ is similar in the three cases (5.20) to (5.22), (5.20′) to (5.22′) can be taken together into (5.17). This completes the proof of Theorem 5.5.

Theorem 5.5 needs some further discussion.

If the number of subsquares $2^{2\alpha}$ is large compared with the quotients q_i, all the regular subsquares will have a value zero for ΔN. Hence, only the irregular subsquares are of interest. If $\bar{a} > 0$, (5.17) shows that the irregular subsquares for q_ν are situated at

$$\frac{2^\alpha}{\bar{t}_{\nu-1}}\left(n_\nu + \frac{s_{\nu-1}}{4}\right) - 1 < \mu - \bar{a}\lambda \leqq \frac{2^\alpha}{\bar{t}_{\nu-1}}\left(n_\nu + \frac{s_{\nu-1}}{4}\right) + \bar{a}. \tag{5.23}$$

If $\lambda = 0$, μ attains the values

$$\mu = \left[\frac{2^\alpha}{\bar{t}_{\nu-1}}\left(x + \frac{s_{\nu-1}}{4}\right)\right] + y, \quad \text{where } x = 0, 1, \cdots, \bar{t}_{\nu-1} - 1,\ y = 0, 1, \cdots, \bar{a}.$$

This means: Each row contains $(\bar{a} + 1)\bar{t}_{\nu-1}$ irregular subsquares corresponding to q_ν. They are cut in $\bar{t}_{\nu-1}$ subsets of subsquares; each subset consists of $\bar{a} + 1$ neighbouring irregular subsquares. Furthermore, the whole set of (λ, μ)-values subject to (5.23) is contained in $\bar{t}_{\nu-1}$ sloping strips. The slope of these parallel strips is $-1/\bar{a}$. Due to this slope, each strip is cut into $|\bar{a}|$ pieces. The $|\bar{a}|$ strips contained in (5.23) for fixed x will be called one strip for obvious reasons.

The situation is best explained with the help of a sketch which shows the strips of irregular subsquares of Example 1 of the next section. There, only q_1 and q_2 are significant. Furthermore, one has $\bar{a} \equiv -3$, $s_0 = 0$, $\bar{t}_0 \equiv 1$, $s_1 \equiv 1$, $\bar{t}_1 \equiv 3 \pmod{2^\alpha}$ for small $\alpha \leqq k$ (k is given). Hence, (5.19) is applicable and

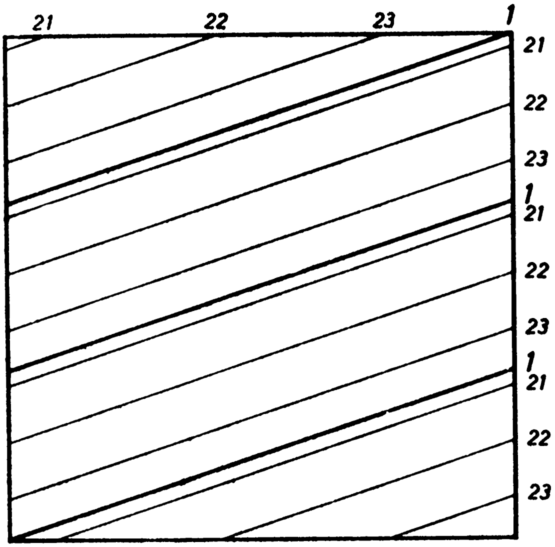
$$2^\alpha - 4 < \mu + 3\lambda < 2^\alpha, \tag{5.24}$$

$$\frac{2^\alpha}{3}(n + \tfrac{1}{4}) - 4 < \mu + 3\lambda < \frac{2^\alpha}{3}(n + \tfrac{1}{4}). \tag{5.25}$$

The strip which corresponds to (5.24) is denoted by 1. The strip which corresponds to (5.25) consists of three substrips; they are denoted by 21, 22, 23. The slope of all strips is $\frac{1}{3}$.

The situation is not so simple if more than two of the quotients q_i are significant. In such a situation, some of the strips can overlap and partially cancel each other.

The examples to follow will throw some further light on the situation.



6, **Numerical Results.** The formulas in Section 3 can easily be translated into computer programs, which allows rapid calculations of the value of ΔN for a given rectangle. Computations of this kind have been carried out with the help of J. Ahrens, Halifax, and A. Grube, Karlsruhe. The generators were of the type $y_{i+1} \equiv ay_i$ (mod 2^e) with $a \equiv 5$ (mod 8). The unit-square was divided into $2^\alpha \times 2^\alpha$ subsquares of equal size, Typical results for $\Delta N = 2^{e-2}\Delta P$ are given in the next tables.

TABLE 1. $y_{i+1} = 16381\, y_i$ (mod 2^{28}); *values of* $\Delta N = 2^{26}\Delta P$

$x_{i+1} \in$ / $x_i \in$	$(0,\frac{1}{8})$	$(\frac{1}{8},\frac{2}{8})$	$(\frac{2}{8},\frac{3}{8})$	$(\frac{3}{8},\frac{4}{8})$	$(\frac{4}{8},\frac{5}{8})$	$(\frac{5}{8},\frac{6}{8})$	$(\frac{6}{8},\frac{7}{8})$	$(\frac{7}{8},1)$
$(0,\frac{1}{8})$	171	171	228	170	171	-284	-341	-286
$(\frac{1}{8},\frac{2}{8})$	170	171	-284	-341	-286	171	171	228
$(\frac{2}{8},\frac{3}{8})$	-341	-286	171	171	228	170	171	-284
$(\frac{3}{8},\frac{4}{8})$	171	228	170	171	-284	-341	-286	171
$(\frac{4}{8},\frac{5}{8})$	171	-284	-341	-286	171	171	228	170
$(\frac{5}{8},\frac{6}{8})$	-286	171	171	228	170	171	-284	-341
$(\frac{6}{8},\frac{7}{8})$	228	170	171	-284	-341	-286	171	171
$(\frac{7}{8},1)$	-284	-341	-286	171	171	228	170	171

TABLE 2. $y_{i+1} = 41475557\, y_i \pmod{2^{28}}$; *values of* $\Delta N = 2^{26}\Delta P$.

$x_{i+1} \in$ / $x_i \in$	$(0,\frac{1}{8})$	$(\frac{1}{8},\frac{2}{8})$	$(\frac{2}{8},\frac{3}{8})$	$(\frac{3}{8},\frac{4}{8})$	$(\frac{4}{8},\frac{5}{8})$	$(\frac{5}{8},\frac{6}{8})$	$(\frac{6}{8},\frac{7}{8})$	$(\frac{7}{8},1)$
$(0,\frac{1}{8})$	-2	1	1	0	-1	0	-1	2
$(\frac{1}{8},\frac{2}{8})$	0	-1	0	-1	2	-2	1	1
$(\frac{2}{8},\frac{3}{8})$	-1	2	-2	1	1	0	-1	0
$(\frac{3}{8},\frac{4}{8})$	1	1	0	-1	0	-1	2	-2
$(\frac{4}{8},\frac{5}{8})$	-1	0	-1	2	-2	1	1	0
$(\frac{5}{8},\frac{6}{8})$	2	-2	1	1	0	-1	0	-1
$(\frac{6}{8},\frac{7}{8})$	1	0	-1	0	-1	2	-2	1
$(\frac{7}{8},1)$	0	-1	2	-2	1	1	0	-1

The tables show the following facts:

(i) The rows (columns) are cyclic permutations of the first one. A shift of tnree to the left changes a row into the next one.

(ii) The deviations ΔN are surprisingly small. The second generator is superior to the first one.

Fact (i) follows immediately from (5.2). This shows that only the first row has to be calculated.

It is no surprise that the second generator is better than the first one. The quotients of the continued fraction for 41475557 and $2^{26} = 67108864$ are given by 1, 3, 3, 3, 3, 3, 3, 3, 2, -2, 21, 4, -4, -5, -3, 3, whereas the quotients of the continued fraction of 16181 and 2^{26} are 0, -4097, -4, 455, 5, 2.

The next three examples treat some generators more systematically. The first two are generators which cannot be recommended. The third one, suggested by O. Taussky, generates pseudo-random numbers which are nearly independent on the unit-square.

Example 1. The generator is of the type $a \approx \sqrt{c}$:

$$m = 2^{2k+2}, \qquad c = 2^{2k}, \qquad a = 2^k - 3. \tag{6.1}$$

The Euclidean algorithm for a and c starts with

$$2^k - 3 = 0 \times 2^{2k} - (-2^k + 3), \qquad 2^{2k} = (-2^k - 3)(-2^k + 3) - (-9),$$
$$-2^k + 3 = q_2(-9) + \epsilon, \qquad |\epsilon| \leqq 4.$$

Hence,

$$q_0 = 0, \qquad q_1 = -2^k - 3, \qquad q_2 \approx \tfrac{1}{9}(2^k - 3), \qquad \mp q_3 = 1, 2, \text{ or } 4,$$

and

$$s_0 = 0, \qquad t_0 = 1; \qquad s_1 = 1, \qquad t_1 = 2^k + 3.$$

The only essential indices are $\nu = 1$ and $\nu = 2$. Formula (5.18) of Theorem 5.5 yields:

If $Q(\lambda, \mu)$ is irregular, then

$$\Delta N \approx -2^{k-\alpha} \quad \text{if } n \times 2^{\alpha} - 4 < \mu + 3\lambda < n \times 2^{\alpha}, \qquad 0 < n < 4, \tag{6.2}$$

$$\Delta N \approx \tfrac{1}{3}2^{k-\alpha} \quad \text{if } \tfrac{1}{3}(n + \tfrac{1}{4})2^{\alpha} - 4 < \mu + 3\lambda < \tfrac{1}{3}(n + \tfrac{1}{4})2^{\alpha},\ 0 < n < 12. \tag{6.3}$$

(6.2) is a sloping strip of width 3. (6.3) consists of three strips of width 4.

Actual calculations according to Section 3 were compared with the approximate values (6.2), (6.3). The case $k = 13$ was tested by dividing the unit-square into $2^9 \times 2^9$ subsquares. Hence, the values of (6.2) and (6.3) became

$$\Delta N \approx -16 \qquad \text{if } 512n - 4 < \mu + 3\lambda < 512n, \qquad n = 1, 2, 3,$$

$$\Delta N \approx \frac{16}{3} = 5,66 \quad \text{if } \frac{512}{3}n + \frac{128}{3} - 4 < \mu + 3\lambda < \frac{512}{3}n + \frac{128}{3},\ 0 < n < 12.$$

The actual values for ΔN are, for $\lambda = 0$,

$$\begin{array}{ll} -16, -16, -16 & \text{if } \mu = 509, 510, 511, \\ 1, 6, 5, 4 & \text{if } \mu = 39, 40, 41, 42, \\ 3, 6, 5, 2 & \text{if } \mu = 210, 211, 212, 213, \\ 6, 5, 5 & \text{if } \mu = 381, 382, 383. \end{array}$$

Note how accurate these values are.

Although the values of ΔN indicate reasonable uniformity of the distribution of pairs, the generator cannot be recommended: The strip (6.2) is deficient for general k and α, by $3 \times 2^{k-\alpha} \times 2^{\alpha} = 3 \times 2^k$ pairs. These missing pairs are contained in the other three strips of (6.3). In the example $k = 13$, this is a dislocation of 24576 out of 67,108,864 pairs, constituting a small but systematic deficiency of the generator.

Example 2. The generator is of the type $a \approx \sqrt{m}$:

$$m = 2^{2k+2}, \qquad c = 2^{2k}, \qquad a = 2^{k+1} - 3. \tag{6.4}$$

The Euclidean algorithm for a and c is

$$\begin{aligned} 2^{k+1} - 3 &= 0 \times 2^{2k} - (-2^{k+1} + 3), \\ 2^{2k} &= (-2^{k-1} - 1) \times (-2^{k+1} + 3) - (2^{k-1} - 3), \\ -2^{k+1} + 3 &= (-4) \times (2^{k-1} - 3) - 9, \\ 2^{k-1} - 3 &= q_3 \times 9 - \epsilon, \qquad |\epsilon| \leqq 4. \end{aligned}$$

Hence

$$q_1 = -2^{k-1} - 1, \qquad q_2 = -4, \qquad q_3 \approx \tfrac{1}{9}(2^{k-1} - 3), \qquad \mp q_4 = 1, 2 \text{ or } 4,$$

and

$$s_0 = 0, \quad t_0 = 1; \quad s_1 = 1, \quad t_1 = 2^{k-1} + 1; \quad s_2 = 4, \quad t_2 = 2^{k+1} - 3.$$

As q_2 may be neglected, formula (5.18) of Theorem 5.5 shows:

If $Q(\lambda, \mu)$ is regular, then

$$\Delta N \approx \frac{1}{2^{2\alpha}} [3(2^{k-1} - 1) - 3(2^{k-1} - 3)] = -\frac{6}{2^{2\alpha}} \approx 0;$$

if $Q(\lambda, \mu)$ is irregular, then

$$(6.5)\quad \Delta N \approx -\tfrac{2}{3}2^{k-1-\alpha} \quad \text{if } n2^\alpha - 4 < 3\lambda + \mu < n2^\alpha, \qquad 0 < n < 4,$$

$$(6.6)\quad \Delta N \approx \tfrac{1}{3}2^{k-1-\alpha} \quad \text{if } \frac{n}{3} \times 2^\alpha - 4 < 3\lambda + \mu < \frac{n}{3} \times 2^\alpha, \qquad 0 < n < 12, \quad n \not\equiv 0 \pmod 3.$$

(6.5) is again one sloping strip of width 3 and (6.6) consists of two strips of width 3.

Again, actual calculations according to Section 3 were carried out for comparison: $k = 13$ and $2^9 \times 2^9$ subsquares lead to values for (6.5) and (6.6) of -5.66 and 2.66, respectively. The actual values were -5, -5, -6 for (6.5) and 3, 3, 2 and 2, 2, 3, 1 for (6.6). The strip (6.5) had a deficiency of $3 \times \frac{2}{3} \times 2^{k-1-\alpha} \times 2^\alpha = 2^k$ pairs. The generator is better than the previous one but it is not really recommended because it still suffers from systematic deficiencies of the distribution of pairs.

Example 3. This generator, suggested by O. Taussky [30], is widely used:

$$m = 2^{35}, \qquad a = 5^{15} \equiv 4\,747\,774\,349 \pmod{2^{33}}.$$

The Euclidean algorithm (4.1) for 4 747 774 349 and 2^{33} yields the quotients:

$$q_i = 1, 2, -4, 4, -8, 5, -23, -5, 4, 13, 3, 6, 2, -4, -2, 3.$$

The bound (5.9) of Theorem 5.1 for ΔN is equal to $38\frac{1}{4}$. The actual values of ΔN are given in Table 3. The unit-square was divided into $2^{10} \times 2^{10}$ subsquares of equal area. The maximal values of ΔN are -8 and $+7$. Only the values for $\Delta N(0, \mu)$, $0 \leqq \mu \leqq 1023$ are given; the other values $\Delta N(\lambda, \mu)$ for $\lambda \neq 0$ are cyclic permutations of these values.

7. Final Conclusions. The question has been raised whether any particular value of r in the mixed congruential generator $y_{i+1} \equiv ay_i + r \pmod m$ offers special advantages. From the behaviour of pairs (x_i, x_{i+1}), a negative answer seems to be indicated.

Obviously, the probability $P(I_1 \leqq y_i < I_2, J_1 \leqq y_{i+1} < J_2)$ is equal to $P(I_1 \leqq y_i < I_2, J_1 \leqq ay_i + r < J_2)$. If r is changed into $r + r'$, one has

$$(7.1)\quad \begin{aligned} &P(I_1 \leqq y_i < I_2,\ J_1 \leqq ay_i + r + r' < J_2) \\ &\qquad = P(I_1 \leqq y_i < I_2,\ J_1 - r' \leqq ay_i + r < J_2 - r'). \end{aligned}$$

Hence, a shift $r \to r + r'$ simply moves the rectangle $[I_1, I_2) \times [J_1, J_2)$ to $[I_1, I_2) \times [J_1 - r', J_2 - r')$. The same can be deduced from formula (3.12)

$$(7.2)\qquad \Delta P = \frac{1}{m} \sum_{\lambda,\mu=1}^{2} (-1)^{\lambda+\mu} s_{0,aI_\lambda - J_\mu + r}^{(m)}(a, m).$$

Changing r into $r + r'$ merely moves J_1 to $J_1 - r'$ and J_2 to $J_2 - r'$.

For the total square $[0, 1) \times [0, 1)$, the consequences are as follows: If this square is split into n^2 equal subsquares of length $1/n$, the integers I_λ and J_μ are of the form $\nu m/n$, where $\nu = 0, 1, \cdots, n - 1$. Thus, as long as r' is a multiple of m/n, the change $r \to r + r'$ effects the same cyclic permutation on all subsquares of each strip parallel to the J-axis. In other words, it merely permutes the "rows" $[0, 1) \times [J_1, J_2)$ of subsquares cyclically.

TABLE 3

Values of $\Delta N(0, \mu)$, $0 \leqq \mu < 1024$, *for the generator* $y_{i+1} \equiv 5^{15} y_i \pmod{2^{35}}$

$\mu = \mu' + \mu''$	$\mu''=0$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\mu' =$ 0	-2	+3	-4	+4	-3	+2	-1	+1	+1	-3	+4	-4	+3	-3	+2	+1	-4	+4	-5	+5
20	-5	+3	0	-1	+2	-4	+5	-4	+2	0	0	+1	-3	+5	-5	+3	-2	+2	+1	-3
40	+3	-5	+5	-5	+2	0	-1	+2	-4	+5	-3	+1	0	0	+2	-4	+5	-5	+4	-3
60	+2	+1	-3	+4	-5	+6	-5	+2	+1	-2	+2	-4	+4	-3	+1	+1	-1	+2	-3	+4
80	-5	+5	-4	+2	+2	-4	+4	-4	+4	-4	+2	+2	-2	+2	-3	+3	-3	+2	-1	-1
100	+3	-4	+4	-4	+4	-4	+2	+3	-5	+4	-3	+3	-4	+3	+1	-2	+3	-4	+4	-3
120	+2	-2	0	+3	-5	+4	-4	+4	-5	+2	+3	-4	+3	-3	+3	-3	+2	+1	-2	+3
140	-4	+4	-2	+1	-2	+1	+4	-6	+4	-3	+3	-5	+3	+1	-4	+4	-4	+3	-2	+1
160	+1	-2	+4	-5	+4	-2	+1	-2	+2	+3	-6	+6	-4	+3	-3	+2	+1	-4	+5	-6
180	+3	-1	0	+1	-1	+3	-5	+5	-3	+1	-1	+1	+3	-6	+6	-4	+3	-2	0	+2
200	-3	+5	-6	+3	0	-1	0	-1	+4	-6	+5	-3	+2	-2	+1	+3	-6	+6	-4	+3
220	-2	0	+2	-2	+4	-6	+5	-1	-1	+1	-2	+4	-7	+5	-3	+1	-1	0	+3	-5
240	+5	-4	+3	-2	0	+3	-3	+4	-5	+4	-1	-1	+2	-2	+4	-6	+4	-3	+2	-2
260	0	+3	-6	+5	-3	+2	-2	0	+4	-4	+4	-4	+3	-1	0	0	-1	+4	-6	+5
280	-3	+3	-3	0	+3	-5	+4	-4	+2	-1	-1	+4	-4	+4	-4	+3	-1	0	0	-1
300	+5	-7	+5	-2	+2	-2	0	+4	-5	+4	-3	+1	-1	0	+2	-4	+5	-5	+3	-1
320	0	0	-1	+6	-8	+5	-7	+1	-2	+1	+3	-5	+5	-4	+2	0	-1	+2	-4	+5
340	-6	+3	0	-2	0	0	+5	-8	+6	-2	+1	-1	-1	+4	-5	+5	-4	+2	+1	-2
360	+2	-3	+6	-7	+3	0	-1	-1	0	+4	-8	+6	-2	+1	-1	-1	+4	-5	+5	-4
380	+2	+2	-3	+2	-2	+5	-7	+5	-1	-1	0	-1	+4	-7	+5	-3	0	+1	-2	+4
400	-4	+4	-4	+3	+1	-3	+3	-3	+5	-6	+4	-1	-1	+2	-2	+4	-5	+4	-3	+1
420	0	-2	+4	-5	+4	-3	+2	+1	-3	+3	-3	+5	-5	+3	-1	0	+1	-2	+4	-4
440	+3	-3	+2	+1	-3	+4	-5	+4	-4	+2	+1	-3	+3	-3	+5	-5	+3	-1	+1	0
460	-2	+5	-5	+3	-2	+1	+1	-3	+5	-5	+4	-3	+1	0	-2	+2	-3	+5	-6	+3
480	0	0	0	-2	+5	-5	+3	-1	0	+1	-2	+4	-5	+5	-4	+2	+1	-3	+2	-3
500	+5	-6	+3	0	-1	0	-2	+5	-5	+4	-2	0	+2	-3	+4	-5	+6	-5	+2	+1
520	-2	+2	-3	+5	-5	+3	0	-1	0	-2	+4	-5	+4	-2	0	+3	-4	+4	-4	+5
540	-5	+2	+2	-3	+2	-2	+4	-5	+4	-1	-1	+2	-3	+4	-4	+3	-3	0	+4	-5
560	+4	-3	+4	-5	+3	+1	-3	+3	-3	+4	-4	+3	-1	-1	+3	-4	+5	-3	+2	-3
580	+1	+3	-6	+4	-3	+3	-4	+2	+1	-3	+4	-4	+4	-3	+2	-1	-1	+4	-5	+5
600	-3	+2	-3	+2	+3	-6	+4	-3	+3	-4	+2	0	-2	+3	-4	+4	-2	+1	-1	0
620	+3	-5	+6	-4	+2	-2	+1	+2	-5	+6	-4	+3	-2	+1	0	-1	+2	-4	+4	-3
640	+1	0	-1	+3	-5	+6	-4	+2	-1	0	+2	-4	+5	-4	+4	-3	+1	+1	-1	+2
660	-4	+4	-3	+1	0	-2	+3	-4	+5	-4	+3	-2	0	+2	-3	+4	-4	+4	-3	+1
680	+1	-1	+2	-5	+6	-3	+1	0	-2	+4	-6	+5	-4	+3	-3	0	+3	-4	+4	-3
700	+3	-3	+1	+2	-3	+3	-4	+5	-3	+2	-1	-1	+5	-7	+5	-3	+2	-3	0	+3
720	-5	+4	-2	+2	-3	+2	+1	-3	+4	-5	+5	-2	+1	-1	-1	+6	-8	+6	-2	+1
740	-2	+1	+2	-5	+5	-4	+2	-2	+1	+1	-3	+5	-6	+5	-2	+1	-1	-1	+6	-8
760	+5	-1	+1	-2	+1	+2	-3	+4	-4	+2	-1	0	0	-3	+6	-7	+5	-1	0	-1
780	0	+4	-7	+6	-2	+1	-1	0	+2	-3	+4	-4	+3	0	-1	0	-2	+5	-8	+6
800	-2	-1	0	-1	+4	-7	+6	-2	+1	0	-1	+2	-2	+3	-4	+4	-1	-1	+1	-2
820	+5	-7	+5	-2	-1	+1	-2	+3	-6	+5	-2	+1	0	-1	+2	-2	+3	-5	+5	-1
840	-1	+1	-2	+6	-8	+6	-2	0	0	-2	+3	-5	+4	-3	+2	-1	-1	+3	-4	+4
860	-4	+4	-1	-1	+2	-3	+6	-7	+5	-2	+1	0	-2	+4	-5	+4	-2	+1	-1	-1
880	+3	-5	+4	-3	+3	-1	0	+1	-3	+7	-8	+5	-1	0	0	-2	+5	-6	+4	-1
900	+1	-1	0	+2	-5	+5	-5	+3	-1	0	+1	-3	+7	-8	+4	0	0	0	-2	+5
920	-5	+3	-1	+1	0	-1	+2	-4	+6	-6	+3	0	-2	+1	-3	+5	-7	+4	+1	-1
940	0	-1	+4	-5	+4	-2	+1	+1	-2	+2	-4	+6	-6	+4	+1	-3	+1	-2	+4	-7
960	+5	-1	-1	+1	-2	+4	-4	+3	-2	+1	+2	-3	+2	-3	+5	-6	+5	0	-3	+3
980	-3	+4	-5	+4	-1	-1	+2	-3	+3	-4	+3	-3	+2	+2	-3	+2	-3	+6	-7	+5
1000	0	-2	+2	-3	+4	-4	+3	-1	0	+2	-3	+3	-3	+2	-4	+3	+1	-3	+3	-4
1020	+6	-6	+4	0																

This leaves the question whether the mixed congruential generators $y_{i+1} \equiv ay_i + r \pmod{m}$ have any advantage over the purely multiplicative generator $y_{i+1} \equiv ay_i \pmod{m}$. Undoubtedly, the mixed generators provide a larger period fo the same modulus.

In the following comparison, purely multiplicative and mixed generators with the same period 2^{e-2} and the same factor a are taken:

$$(7.3)\qquad y_{i+1} \equiv ay_i + r \pmod{2^{e-2}}, \qquad a \equiv 5 \pmod 8, \qquad r \equiv 1 \pmod 2,$$

$$(7.4)\qquad y_{i+1} \equiv ay_i \qquad \pmod{2^e}\ , \qquad a \equiv 5 \pmod 8, \qquad y_0 \equiv 1 \pmod 2.$$

For both generators the probability that

$$(7.5)\qquad (x_i, x_{i+1}) = \left(\frac{y_i}{2^{e-2}}, \frac{y_{i+1}}{2^{e-2}}\right) \in \left[\frac{I_1}{2^{e-2}}, \frac{I_2}{2^{e-2}}\right) \times \left[\frac{J_1}{2^{e-2}}, \frac{J_2}{2^{e-2}}\right)$$

will be calculated. For the generator (7.3), one has

$$(7.6)\qquad \begin{aligned} &P\left(\frac{I_1}{2^{e-2}} \leqq \frac{y_i}{2^{e-2}} < \frac{I_2}{2^{e-2}}, \frac{J_1}{2^{e-2}} \leqq \frac{ay_i + r}{2^{e-2}} < \frac{J_2}{2^{e-2}}\right) \\ &= P\left(\frac{I_1}{2^{e-2}} \leqq \frac{\mu}{2^{e-2}} < \frac{I_2}{2^{e-2}}, \frac{J_1 - r}{2^{e-2}} \leqq \frac{a\mu}{2^{e-2}} < \frac{J_2 - r}{2^{e-2}}\right) \qquad (0 \leqq \mu < 2^{e-2}). \end{aligned}$$

This expression was determined in (3.12) as

$$(7.7)\qquad \frac{I_2 - I_1}{2^{e-2}} \times \frac{J_2 - J_1}{2^{e-2}} + \frac{1}{2^{e-2}} \sum_{\lambda,\mu=1}^{2} (-1)^{\lambda+\mu} s^{(2^{e-2})}_{0,aI_\lambda - J_\mu + r}(a, 2^{e-2}).$$

For the generator (7.4), one can use that y_i is of the form $4\mu' + 1$ where $0 \leqq \mu' < 2^{e-2}$. Hence, the subsquare in (7.5) may be changed according to

$$\left[\frac{I_1}{2^{e-2}}, \frac{I_2}{2^{e-2}}\right) \times \left[\frac{J_1}{2^{e-2}}, \frac{J_2}{2^{e-2}}\right) \to \left[\frac{4I_1 + 1}{2^e}, \frac{4I_2 + 1}{2^e}\right) \times \left[\frac{4J_1 + 1}{2^e}, \frac{4J_2 + 1}{2^e}\right).$$

This yields, for the probability of (7.5),

$$P\left(\frac{I_1}{2^{e-2}} \leqq \frac{y_i}{2^e} < \frac{I_2}{2^{e-2}}, \frac{J_1}{2^{e-2}} \leqq \frac{ay_i}{2^e} < \frac{J_2}{2^{e-2}}\right)$$

$$(7.8)\qquad \begin{aligned} &= P\left(\frac{4I_1 + 1}{2^e} \leqq \frac{y_i}{2^e} < \frac{4I_2 + 1}{2^e}, \frac{4J_1 + 1}{2^e} \leqq \frac{ay_i}{2^e} < \frac{4J_2 + 1}{2^e}\right) \\ &= P\left(\frac{4I_1 + 1}{2^e} \leqq \frac{4\mu' + 1}{2^e} < \frac{4I_2 + 1}{2^e}, \frac{4J_1 + 1}{2^e} \leqq \frac{4a\mu' + a}{2^e} < \frac{4J_2 + 1}{2^e}\right) \end{aligned}$$

$$(7.9)\qquad = P\left[\frac{I_1}{2^{e-2}} \leqq \frac{\mu'}{2^{e-2}} < \frac{I_2}{2^{e-2}}, \frac{J_1 - \frac{a-1}{4}}{2^{e-2}} \leqq \frac{a\mu'}{2^{e-2}} < \frac{J_2 - \frac{a-1}{4}}{2^{e-2}}\right].$$

(7.8) was calculated in (3.19); for the application of (3.19), I_λ and J_μ have to be substituted by $4I_\lambda + 1$ and $4J_\mu + 1$ and a factor 4 has to be cancelled in the subscripts. This yields

$$(7.10)\qquad \frac{I_2 - I_1}{2^{e-2}} \times \frac{J_2 - J_1}{2^{e-2}} + \frac{1}{2^{e-2}} \sum_{\lambda,\mu=1}^{2} (-1)^{\lambda+\mu} s^{(2^{e-2})}_{0,aI_\lambda - J_\mu + (a-1)/4}(a, 2^{e-2}).$$

If one compares (7.6) and (7.9) or the equivalent expressions (7.7) and (7.10), one realizes immediately:

The multiplicative congruential generator (7.4) *is equivalent to the mixed congruential generator* (7.3) *with* $r = (a - 1)/4$. *As the mixed congruential generators* *are equivalent for different increments r, they are all equivalent to the purely multiplicative congruential generator* (7.4).

It should be mentioned that a similar argument is true for triplets, quadruplets, and any number of pseudo-random numbers. Hence, the above material indicates:

A special choice of the increment r has no advantage with respect to the joint probability distribution of two, three, four, or more successive pseudo-random numbers. If the modulus is of the form $m = 2^e$, $r = 0$ *seems to be as good a choice as any. For random-number transformations, it has the advantage that a precise* 0 *is never generated.*

This shows that the properties of the linear congruential generator are merely determined by the factor a. The results of this paper suggest the following rule for the choice of the factor:

The factor a should be chosen in such a way that the Euclidean algorithm for a and $c = m/f$ *(in the multiplicative case) or a and m (in the mixed congruential case) has small quotients. In particular, for the generator* $y_{i+1} \equiv ay_i \pmod{2^e}$, $a \equiv 5 \pmod 8$, *the quotients of the Euclidean algorithm for a and* 2^{e-2} *should be small.*

A measure for the quality of the generator is the global bound

$$\frac{1}{4}\sum_{i=0}^{n}|q_i| + n + 1 \geqq |\Delta N| \tag{7.11}$$

for the deviation ΔN of pairs x_i, x_{i+1} in any subsquare of the unit-square. It was derived in Theorem 5.1.

It should be noted that such a choice of the factor a results also in a small value for the serial correlation ρ_1 between x_i and x_{i+1}. The explicit expressions for ρ_1 can be found in Dieter/Ahrens [8]. They are again sums of generalized Dedekind sums. For example, for the generator $y_{i+1} \equiv ay_i \pmod{2^e}$, $a \equiv 5 \pmod 8$, one has

$$\rho_1 = \frac{\dfrac{48}{2^e}\left(s_{1,0}^{(4)}(a, 2^{e-2}) - \dfrac{1}{4 \times 2^e}\right)}{1 - \dfrac{16}{2^{2e}}} \approx \frac{48}{2^e}\, s_{1,0}^{(4)}(a, 2^{e-2}). \tag{7.12}$$

In a subsequent paper, it will be shown that the frequency of permutations of triplets can also be expressed as sums of generalized Dedekind sums. For example, for the generator $y_{i+1} \equiv ay_i \pmod{2^e}$, $a \equiv 5 \pmod 8$, one has the following expressions where a^{-1} stands for an integer for which $aa^{-1} \equiv 1 \pmod{2^e}$

$$\begin{aligned} &P(x_{i-1} < x_i < x_{i+1}) - \frac{1}{6} \\ &= \frac{1}{2^{e-2}}\Big\{s_{1,0}^{(4)}(a, 2^{e-2}) - s_{1,0}^{(4)}(a^2, 2^{e-2}) + s_{1,0}^{(4)}(a^2 - a, 2^{e-2}) \\ &\qquad + s_{1,0}^{(4)}(a^{-2} - a^{-1}, 2^{e-2}) + 4s_{1,0}^{(4)}(a, 2^{e-4})\Big\} + R_1, \end{aligned}$$

$$\begin{aligned} &P(x_i < x_{i+1} < x_{i-1}) - \frac{1}{6} \\ &= \frac{1}{2^{e-2}}\Big\{-s_{1,0}^{(4)}(a^{-1} - 1, 2^{e-2}) + s_{1,0}^{(4)}(a^2 - 1, 2^{e-2}) \\ &\qquad + s_{1,0}^{(4)}(a - a^2, 2^{e-2}) + s_{1,0}^{(4)}(a^{-1} - a, 2^{e-2}) - 4s_{1,0}^{(4)}(1 + a^{-1}, 2^{e-4})\Big\} + R_2, \end{aligned}$$

$$P(x_i < x_{i-1} < x_{i+1}) - \frac{1}{6}$$

$$= \frac{1}{2^{e-2}} \Big\{ -s^{(4)}_{1,0}(a - 1, 2^{e-2}) + s^{(4)}_{1,0}(a^{-2} - 1, 2^{e-2})$$

$$+ s^{(4)}_{1,0}(a^{-1} - a^{-2}, 2^{e-2}) + s^{(4)}_{1,0}(a - a^{-1}, 2^{e-2}) - 4s^{(4)}_{1,0}(1 + a, 2^{e-4}) \Big\} + R_3,$$

where

$$R_1 = \frac{4}{2^e} - \frac{8}{3 \times 2^{2e}}, \qquad R_2 = \frac{6}{2^e} - \frac{32}{3 \times 2^{2e}}, \qquad R_3 = -\frac{6}{2^e} - \frac{32}{3 \times 2^{2e}}$$

if $a \equiv 5 \pmod{16}$,

$$R_1 = -\frac{4}{2^e} - \frac{8}{3 \times 2^{2e}}, \qquad R_2 = -\frac{6}{2^e} - \frac{32}{3 \times 2^{2e}}, \qquad R_3 = \frac{6}{2^e} - \frac{32}{3 \times 2^{2e}}$$

if $a \equiv 13 \pmod{16}$.

The residual terms R_1, R_2, R_3 are extremely small for any choice of the factor a. The exact values of $P(x_{i-1} < x_i < x_{i+1})$, $P(x_i < x_{i+1} < x_{i-1})$, $P(x_i < x_{i-1} < x_{i+1})$ can be calculated using the results of Section 4. For most 'reasonable' factors a, these values are rather small. For example, for the generator

$$y_{i+1} \equiv 41475557\, y_i \pmod{2^{28}}$$

only 3, 2, or 1 triplets are dislocated. More details will be given in the forthcoming paper [9].

Often, bounds for $P(x_{i-1} < x_i < x_{i+1}) - \frac{1}{6}$ are sufficient. For this purpose, the function $D(a, c)$ defined in (1.6) may be used. If the factor a is chosen in such a way that

$$D(a, 2^{e-2}),\ D(a - 1, 2^{e-2}),\ D(a + 1, 2^{e-4}),\ D(a^{-1} - 1, 2^{e-2}),\ D(a^{-1} + 1, 2^{e-4}),$$

$$D(a, 2^{e-4}),\ D(a^2, 2^{e-2}),\ D(a^2 - 1, 2^{e-2}),\ D(a^{-2} - 1, 2^{e-2}),$$

$$D(a^2 - a, 2^{e-2}),\ D(a^{-2} - a^{-1}, 2^{e-2}),\ D(a - a^{-1}, 2^{e-2})$$

are generally bounded by K, then

$$2^{e-2}(P(x_{i-1} < x_i < x_{i+1}) - \tfrac{1}{6}),$$

$$2^{e-2}(P(x_i < x_{i+1} < x_{i-1}) - \tfrac{1}{6}),$$

$$2^{e-2}(P(x_i < x_{i-1} < x_{i+1}) - \tfrac{1}{6})$$

are bounded by $8K + \frac{3}{2}$. This means: At most $8K + 2$ triplets are dislocated with respect to their order.

This shows again the high quality of some linear congruential generators.

8. **Acknowledgement.** The paper was much improved by the help of J. Ahrens, Halifax, Canada. His discussions, his computer programs, and his knowledge of English were of considerable help for the final version of the paper.

Institut für Mathematische Statistik
Universität Karlsruhe
Karlsruhe, Germany

1. J. Ahrens, U. Dieter & A. Grube, "Pseudo-random numbers: A new proposal for the choice of multiplicators," *Computing*, v. 6, 1970, pp. 121–138.

2. R. R. Coveyou, "Serial correlation in the generation of pseudo-random numbers," *J. Assoc. Comput. Mach.*, v. 7, 1960, pp. 72–74. MR **22** #8643.

3. R. R. Coveyou & R. D. MacPherson, "Fourier analysis of uniform random numbers," *J. Assoc. Comput. Mach.*, v. 14, 1967, pp. 100–119. MR **36** #4779.

4. R. R. Coveyou, "Random number generation is too important to be left to chance," *Studies in Appl. Math.*, v. 3, 1969, pp. 70–111.

5. R. Dedekind, "Erläuterungen zu den Fragmenten XXVIII," in *Riemanns Gesammelten Werken*, Leipzig, 1892, pp. 466–478.

6. U. Dieter, "Das Verhalten der Kleinschen Funktionen log $\sigma_{g,h}(\omega_1, \omega_2)$ gegenüber Modultransformationen und verallgemeinerte Dedekindsche Summen," *J. Reine Angew. Math.*, v. 201, 1959, pp. 37–70. MR **21** #3397.

7. U. Dieter, "Autokorrelation multiplikativ-erzeugter Pseudo-Zufallszahlen," *Operations Research Verfahren*, v. 6, 1969, pp. 69–85.

8. U. Dieter & J. Ahrens, "An exact determination of serial correlation of pseudo-random numbers," *Numer. Math.*, v. 16, 1970, pp. 101–123.

9. U. Dieter, "Pseudo-random numbers: Permutations of triplets." (To appear.)

10. U. Dieter, "Simple proofs for some identities for generalized Dedekind sums." (To appear.)

11. M. Greenberger, "An a priori determination of serial correlation in computer generated random numbers," *Math. Comp.*, v. 15, 1961, pp. 383–389. MR **26** #2033.

12. M. Greenberger, "Method in randomness," *Comm. ACM*, v. 8, 1965, pp. 177–179.

13. J. H. Halton, "A retrospective and prospective survey of the Monte Carlo method," *SIAM Rev.*, v. 12, 1970, pp. 1–63. MR **41** #2878.

14. T. E. Hull & A. R. Dobell, "Random number generators," *SIAM Rev*, v. 4, 1962, pp. 230–254. MR **26** #5710.

15. D. L. Jagerman, "The autocorrelation and joint distribution functions of sequences $\{aj^2/m\}$, $\{a(j + \tau)^2/m\}$," *Math. Comp.*, v. 18, 1964, pp. 211–232. MR **31** #1762.

16. B. Jansson, "Autocorrelations between pseudo-random numbers," *Nordisk Tidskr. Informations-Behandling*, v. 4, 1964, pp. 6–27. MR **29** #2934.

17. B. Jansson, *Random Number Generators*, Almqvist & Wiksell, Stockholm, 1966. MR **36** #7297.

18. M. L. Juncosa, *Random Number Generation on the BRL High-Speed Computing Machines*, Report #855, Ballistic Research Laboratories, Aberdeen Proving Ground, Md., 1953. MR **15**, 559.

19. D. E. Knuth, *The Art of Computer Programming*. Vol. 2: *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969.

20. D. H. Lehmer, *Mathematical Method in Large-Scale Computing Units*, Proc. Second Sympos. Large-Scale Digital Calculating Machinery, Harvard Univ. Press, Cambridge, Mass., 1949, pp. 114–146. MR **13**, 495.

21. M. D. MacLaren & G. Marsaglia, "Uniform random number generators," *J. Assoc. Comput. Mach.*, v. 12, 1965, pp. 83–89. MR **30** #687.

22. G. Marsaglia, *Random Variables and Computers*, Trans. Third Prague Conf. Information Theory, Statist. Decision Functions, Random Processes (Lidice, 1962), Publ. House Czech. Acad. Sci., Prague, 1964, pp. 499–512. MR **29** #1721.

2→ G. Marsaglia, "Random numbers fall mainly in the planes," *Proc. Nat. Acad. Sci. U.S.A.*, v. 61, 1968, pp. 25–28. MR **38** #3998.

24. G. Marsaglia, "Regularities in congruential random number generators," *Numer. Math.*, v. 16, 1970, pp. 8–10.

25. C. Meyer, "Über einige Anwendungen Dedekindscher Summen," *J. Reine Angew. Math.*, v. 198, 1957, pp. 143–203. MR **21** #3396.

26. C. Meyer, "Bemerkungen zu den allgemeinen Dedekindschen Summen," *J. Reine Angew. Math.*, v. 205, 1960/61, pp. 186–196. MR **23** #A1624.

27. H. Rademacher, "Zur Theorie der Modulfunktionen," *J. Reine Angew. Math.*, v. 167, 1932, pp. 312–336.

28. H. Rademacher, "Some remarks on certain generalized Dedekind sums," *Acta Arith.*, v. 9, 1964, pp. 97–105. MR **29** #1172.

29. A. Rotenberg, "A new pseudo-random number generator," *J. Assoc. Comput. Mach.*, v. 7, 1960, pp. 75–77. MR **22** #8642.

30. O. Taussky & J. Todd, *Generation and Testing of Pseudo-Random Numbers*, Sympos. on Monte Carlo Methods (University of Florida, 1954), Wiley, New York; Chapman & Hall, London, 1956, pp. 15–28. MR **18**, 239.

31. P. H. Verdier, "Relations within sequences of congruential pseudo-random numbers," *J. Res. Nat. Bur. Standards Sect. B*, v. 73, 1969, pp. 41–44. MR **39** #1081.