BOLLETTINO
UNIONE MATEMATICA ITALIANA

A. De Matteis, B. Faleschini

Some arithmetical properties in connection with pseudo-random numbers.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **18** (1963), n.3, p. 171–184.
Zanichelli
<http://www.bdim.eu/item?id=BUMI_1963_3_18_3_171_0>

Bollettino dell'Unione Matematica Italiana, Zanichelli, 1963.

SEZIONE SCIENTIFICA

BREVI NOTE

Some arithmetical properties in connection with pseudo-random numbers.

Nota di A. De Matteis e B. Faleschini (a Bologna) (*) (**)

Sunto. - *Il periodo di una successione di numeri pseudo-casuali generata con un metodo congruenziale moltiplicativo é il gaussiano, per un assegnato modulo, del moltiplicatore fisso. La conoscenza del gaussiano del moltiplicatore è importante anche per il metodo moltiplicativo-additivo, in quanto l'esistenza di un sottoperiodo influenza la casualità della successione. Vengono qui messe in evidenza le proprietà dei numeri che hanno lo stesso gaussiano, grazie alle quali l'insieme di tali numeri viene individuato con semplici operazioni di congruenza partendo da una sottoclasse minima.*

1. - Introduction.

A new scheme for generating pseudo-random numbers has been proposed by Rotenberg [6]; namely, the linear congruence

$$x_{i+1} \equiv ax_i + k \pmod{m}, \tag{1}$$

completely defined by the choice of the integer parameters m, a, k, x_0. The case $k = 0$ is Lehmer's classical scheme [5], which in general differs from (1) for the length of period of the obtainable succession. In the Lehmer-scheme this period, for a and x_0 prime to m, is called the exponent to which a belongs modulo m, and following Lucas [1] it will be denoted by gss (m, a). Its value is less than m, while the period of the succession (1) may reach m.

Recently it has been pointed out [7-8] that some statistical properties, which these sequences of numbers must satisfy to be entitled to the (vague) qualification « random », may be inferred

(*) Pervenuta alla Segreteria dell'U. M. I. il 16 aprile 1963.

(**) Work executed at the Centro di Calcolo del C. N. E. N. (Bologna) and partially published in the C. N. E. N. report n. 88 « Pseudo-random sequences of equal length », (1960).

« a priori », on account of the arithmetical nature of the generating procedure. They depend on the values of the parameters entering (1). It is thus important to dispose of a large possibility of choice.

It is the purpose of this note to investigate some properties of the numbers belonging to the same exponent modulo m, by which the whole set of such numbers may be obtained by simple additions, starting from a minimal subset.

The study of gss (m, a) is emphasized also because of its remarkable influence on the randomness of the sequences (1), as may be seen in Figure 1 for the simple case $m = 3^3$. The values x_i are plotted versus i for a succession of period m.

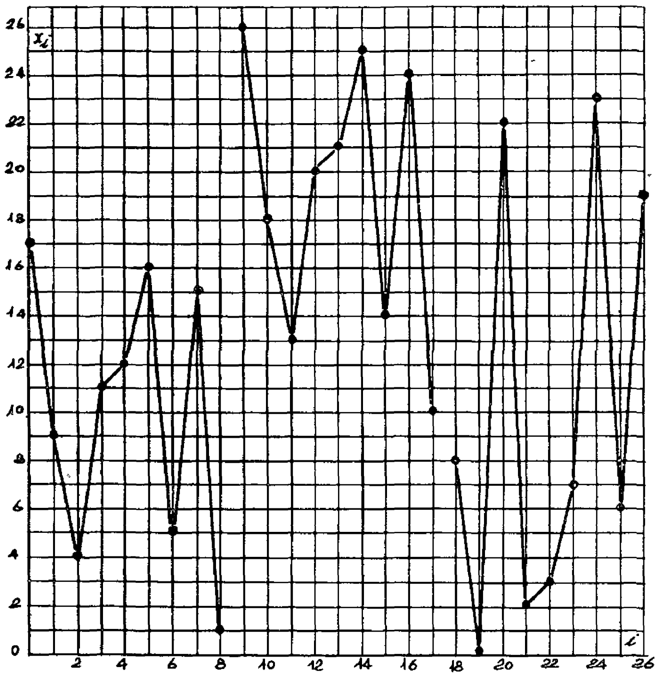

Fig. 1 - A full sequence with $m=27$, $a=4$, $k=22$, $x_0=17$; gss $(27, 4) = 9$.

Connecting lines are shown between 3 groups of exactly 9 points each, i.e. gss (m, a). The three curves my be obtained from each other by translations in the system of integers mod m as will subsequently be shown. For these features of the sequences (1) one must be cautious when using a number of terms greater than gss $(m$, a).

2. - **Definitions and basic properties.**

We give here some definitions and properties which are fundamental in the theory of binomial congruences — [1—4].

Henceforth all numbers considered are positive integers unless otherwise stated.

DEFINITION - The number of positive integers less than and relatively prime to m is called the indicator of m and is written $\varphi(m)$.

THEOREM 2.1 - If p is a prime, then $\varphi(p^s) = p^{s-1}(p-1)$, $\varphi(1) = 1$.

THEOREM 2.2 - If $m = p^s \cdot q^t \dots r^v$ is the canonical decomposition of m, then

$$\varphi(m) = \varphi(p^s) \cdot \varphi(q^t) \dots \varphi(r^v)$$

THEOREM 2.3 - If d_1, $d_2 \dots d_k$ are all the divisors of m, including m and unity, then

$$\varphi(d_1) + \varphi(d_2) + \dots + \varphi(d_k) = m.$$

DEFINITION - Reduced indicator of m is called the function $\psi(m)$ so defined:

$$\psi(m) = \varphi(m)$$

if $m = 1, 2, 4, p^s, 2p^s$ where p is an odd prime;

$$\psi(2^s) = 2^{s-2}$$

if $s > 2$; and finally

$$\psi(m) = \text{l.c.m. } [\psi(p^s), \psi(q^t), \dots, \psi(r^v)],$$

where l.c.m. is the least common multiple and $m = p^s q^t \dots r^v$ is the canonical decomposition of m.

THEOREM 2.4 (Lucas) - If a is relatively prime to m, then

$$a^{\psi(m)} \equiv 1 \pmod{m}.$$

DEFINITION - The smallest number $g > 0$ satisfying the congruence

$$a^g \equiv 1 \pmod{m} \tag{2}$$

where a is prime to m, is called the exponent to which a belongs modulo m, or gaussian of a modulo m and will be written gss(m,a).

THEOREM 2.5 - All numbers g satisfying (2) are multiples of gss(m, a).

THEOREM 2.6 - The sequence of the least positive remainders modulo m of the successive powers of a (prime to m) is periodic and the number of terms of the proper period is gss(m, a).

THEOREM 2.7 - If p is an odd prime, if a is prime to p and p^r is the largest power of p dividing $a^{\mathrm{gss}(p,a)} - 1$, then

$$\mathrm{gss}(p^s, a) = \begin{cases} \mathrm{gss}(p, a) & \text{if } s \leq r \\ \mathrm{gss}(p, a) p^{s-r} & \text{if } s > r \end{cases}$$

THEOREM 2.8 - (i) If $a \equiv 1 \pmod{4}$ and 2^v is the largest power of 2 dividing $a - 1$, then

$$\mathrm{gss}(2^t, a) = \begin{cases} 1 & \text{if } t \leq v \\ 2^{t-v} & \text{if } t > v \end{cases}$$

(ii) If $a \equiv 3 \pmod{4}$ and 2^v is the largest power of 2 dividing $a + 1$, then

$$\mathrm{gss}(2^t, a) = \begin{cases} 1 & \text{if } t = 1 \\ 2 & \text{if } 1 < t \leq v \\ 2^{t-v} & \text{if } t > v \end{cases}$$

THEOREM 2.9 - If m, n, a are relatively prime in pairs, then

$$\mathrm{gss}(mn, a) = \text{l.c.m.} [\mathrm{gss}(m, a), \mathrm{gss}(n, a)]$$

THEOREM 2.10 - If $m = p^s$, where p is an odd prime, and d is a divisor of $\varphi(m)$, there are $\varphi(d)$ numbers belonging to d modulo m.

THEOREM 2.11 - If $m = 2^t$ where $t \geq 3$, there are

1 number belonging to 1 modulo m

3 numbers » » 2 » »,

and if $2 \leq v \leq t - 2$, there are

2^v numbers belonging to 2^v modulo m.

THEOREM 2.12 - If for a, prime to m, gss $(m, a) = g$, then

$$\text{gss}\,(m,\ a^n) = \frac{g}{\text{g.c.d. } [g,\ n]}$$

where g.c.d. is the greatest common divisor.

DEFINITION - If gss $(m, a) = \varphi(m)$, a is called a primitive root of m.

THEOREM 2.13 - A number m has primitive roots if and only if m is 2, 4, p^s or $2p^s$, where p is an odd prime.

3. - Numbers belonging to the same exponent.

We shall investigate in this Section some properties which will allow us to determine by simple relations of congruence the class of all numbers belonging to a given exponent.

Special attention will be given to the numbers belonging (modulo p^s) to the divisors of $\varphi(p)$. They will be denoted by c, and computed by means of the following rule.

RULE 3.1 - Let p be an odd prime and i an integer less than p. Then for every c such that

$$c \equiv i^{p^{s-1}} \pmod{p^s},$$

one has

$$\text{gss}\,(p^s,\ c) = \text{gss}\,(p,\ i).$$

Indeed, let gss $(p, i) = d$ where d is a divisor of $p - 1$. With the notation of theorem 2.7 it will be

$$\text{gss}\,(p^s,\ i) = \begin{cases} d & \text{if } s \leq r \\ dp^{s-r} & \text{if } s > r \end{cases}$$

If $\text{gss}(p^s, i) = d$, by theorem 2.12 the assertion holds since p^{s-1} is prime to d.

On the other hand, if $\text{gss}(p^s, i) = dp^{s-r}$ then

$$\text{gss}(p^s, i^{p^{s-1}}) = \frac{dp^{s-r}}{\text{g.c d.}[dp^{s-r}, p^{s-1}]}$$

proving 3.1.

THEOREM 3.2 - Let p be an odd prime, c prime to p and gss $(p^s, c) = d$, where d is a divisor of $p-1$. Then for every r, $1 \leq \leq r < s$, and for every x satisfying the conditions

$$(3) \qquad x \equiv c(\text{mod } p^r), \qquad x \not\equiv c(\text{mod } p^{r+1})$$

one has

$$\text{gss}(p^s, x) = dp^{s-r}.$$

Indeed if d is a divisor of $p-1$. then $\text{gss}(p^s, c) = d$ implies $\text{gss}(p, c) = d$. Hence $\text{gss}(p, x) = \text{gss}(p, c) = d$.

Furthermore the numbers x have the form $x = c + hp^r$ where h (positive or negative integer) is prime to p. By the binomial expansion of $(c + hp^r)^d$ we get

$$x^d - 1 \equiv 0 \ (\text{mod } p^r) \text{ and } x^d - 1 \equiv dc^{d-1}hp^r \ (\text{mod } p^{r+1})$$

But c, d, h, are prime to p. Therefore p^r is a divisor of $x^d - 1$, but not p^{r+1}. The theorem then follows from theorem 2.7.

THEOREM 3.3 - The numbers x obtained under assumptions (3) of the preceding theorem from the $\varphi(d)$ numbers c, exhaust all numbers belonging to dp^{s-r} modulo p.

Indeed by 3.2 for every c we find $\varphi(p) = p - 1$ numbers belonging to dp^{s-r}, in any set of p^{r+1} successive numbers. Thus for a given c there are

$$\frac{p^s}{p^{r+1}}(p-1) = \varphi(p^{s-r})$$

positive integers less than p^s belonging to the same exponent.

For all the c we have

$$\varphi(d)\varphi(p^{s-r}) = \varphi(dp^{s-r}).$$

According to theorem 2.10 they are all the numbers belonging to dp^{s-r}, proving 3.3.

Moreover the summation over all possible values of d and r, yields

$$\Sigma\ \varphi(d)\cdot\varphi(p^{s-r}) = \varphi(p^s) - \varphi(p)$$

which, added to the $\varphi(p)$ values of c, exhaust all numbers less than and prime to p^s.

As an easy example consider the case $p^s = 3^3$. The two numbers c may be computed by means of 3.1, or more easily by observing that, for every p, the number belonging to the exponent 2 modulo p^s is p^{s-1}. Thus 1 and 26 belong respectively to the exponents 1,2. Letting h run through the set of values prime to 3 we obtain the Table I below.

TABLE I

Example

c	3^r	$x \equiv c + h3^r \pmod{3^3}$	gss $(3^3, x)$
1	3	4, 7, *, 13, 16, *, 22, 25	9
	9	10, 19,	3
26	3	2, 5, *, 11, 14, *, 20, 23	18
	9	8, 17,	6

For the construction of a table reduced to its characteristic elements we have the two following theorems:

THEOREM 3.4 - If for x, prime to p, gss $(p^s, x) = dp^{s-r} (1 \leq r < s)$, then for every $y \equiv x \pmod{p^{r+1}}$ one has gss$(p^s, y) =$ gss(p^s, x).

By the theorem 3.3 every such number x may be written in only one way, $x = c + hp^r$, where h is prime to p and gss$(p^s, c) = d$.

If k is an integer, the number $c + (h + kp)p^r = x + kp^{r+1}$ also belongs to the exponent of x, since $h + kp$ is prime to p. This proves the theorem.

THEOREM 3.5 - There are $[\varphi(p)\cdot\varphi(d)]$ numbers less than p^{r+1} belonging to the exponent dp^{s-r} modulo p^s.

This follows immediately from the above theorems.

We conclude that there is a minimal subset of numbers belonging to a given exponent from which all others may be obtained by simple additions. In the above example all primitive roots of 3^3 are obtained from 2 and 5 by adding successively 3^2.

For the case $p=2$, with the restrictions $2 \leq v \leq t-2$, it follows from the basic theorems that the numbers belonging to 2^{t-v} modulo 2^t, are the 2^{t-v} numbers of the form $x = \pm 1 + h2^v$, where h is an odd pasitive integer, i.e., $x \equiv \pm 1 \pmod{2^v}$ and $x \not\equiv \pm 1 \pmod{2^{v+1}}$.

If we denote with c these four numbers belonging to the divisors of $\psi(2^3)=2$, modulo 2^t:

1	belonging	to	1
$2^{t-1}-1$	»	»	2
$2^{t-1}+1$	»	»	2
$2^t\ -1$	»	»	2

(the last of which is equivalente to -1 modulo 2^t), we have the following theorems, which are formally analogous to 3.2 and 3.4 for the modulus p^s.

THEOREM 3.6 - If $2 \leq v \leq t-2$ and with c defined as above, for the numbers

$$x \equiv c \pmod{2^v}, \quad \text{and} \quad x \not\equiv c \pmod{2^{v+1}},$$

one has

$$\text{gss}\,(2^t,\ x) = 2^{t-v}.$$

THEOREM 3.7 - If $2 \leq v \leq t-2$ and the odd number x is such that $\text{gss}\,(2^t,\ x) = 2^{t-v}$, then for every $y \equiv x \pmod{2^{v+1}}$ one has $\text{gss}\,(2^t,\ y) = \text{gss}\,(2^t,\ x)$.

Finally, in view of the further applications, theorems 3.4 and 3.7 may be so extended, by means of theorem 2.9, to the composite modulus $m = 2^t p^s$:

THEOREM 3.8 - If x, prime to $m = 2^t p^s$, is such that

$$\text{gss}\,(2^t,\ x) = 2^{t-v}, \quad \text{gss}\,(p^s,\ x) = dp^{s-r}$$

where d is a divisor of $\varphi(p)$, $2 \leq v \leq t-2$, $1 \leq r < s$, then for every $y \equiv x \pmod{2^{v+1}p^{r+1}}$, one has

$$\text{gss}\,(m,\ y) = \text{gss}\,(m,\ x).$$

4. - Applications.

a) As a first application of the preceding theorems, we shall find all numbers belonging to $\psi(10^{10}) = 5.10^8$ modulo 10^{10}.

Since (with the notation of Section 3.) $t = s = 10$, $v = 2$, $r = 1$, one has $2^{v+1}5^{r+1} = 200$. It will be sufficient to find the numbers less than 200 belonging to 5.10^8; they are the numbers a quoted in Table II. From the column « periodicity », where the zeros stand for 10, one may obtain gss $(10^n, a)$ by multiplying the last n numbers (see Appendix) Furthermore, every number congruent a modulo 200 will belong to the same exponent of a, modulo 10^n.

TABLE II

$$\text{gss}\,(10^{10},\ a) = 5.10^8$$

a	periodicity	a	periodicity
3	0000005554	109	0000000552
11	0000000501	117	0000005554
13	0000005554	123	0000005554
19	0000000552	131	0000000501
21	0000000051	133	0000005554
27	0000005554	139	0000000552
29	0000000552	141	0000000051
37	0000005554	147	0000005554
53	0000005554	163	0000005554
59	0000000552	171	0000000501
61	0000000051	173	0000005554
67	0000005554	179	0000000552
69	0000000552	181	0000000051
77	0000005554	187	0000005554
83	0000005554	189	0000000552
91	0000000501	197	0000005554

Example - gss $(10^{10}, 3) = 10^6 \cdot 5 \cdot 5 \cdot 5 \cdot 4 = 5 \cdot 10^8$, and the numbers

xxxxxxx003, xxxxxxx203, etc.

where x are arbitrary digits, belong to the same exponent of 3. Furthermore, in the sequence of pseudo-random numbers generated with one of these numbers as fixed multiplier in the Lehmer scheme, the period of, say, the last five digits will be $10 \cdot 5 \cdot 5 \cdot 5 \cdot 4 = 5000$.

b) In general the numbers belonging to a given exponent modulo 10^{10} may be found without attempts by a procedure like that shown in Table I.

Let $c_{2,s}$ be the numbers prime to 2 and belonging to the divisors of $\psi(2^3) = 2$, modulo 2^s and $c_{5,s}$ the numbers prime to 5 and belonging to the divisors of $\varphi(5) = 4$, modulo 5^s. Tables III and IV yield these values for progressive moduli.

TABLE III

Values of $c_{2,s}$

	$c_{2,3}$	$c_{2,4}$	$c_{2,5}$	$c_{2,6}$	$c_{2,7}$	$c_{2,8}$	$c_{2,9}$	$c_{2,10}$
gss = 1	1	1	1	1	1	1	1	1
gss = 2	2	7	15	31	63	127	255	511
gss = 2	5	9	17	33	65	129	257	513
gss = 2	7	15	31	63	127	255	511	1023

TABLE IV

Values of $c_{5,s}$

	$c_{5,1}$	$c_{5,2}$	$c_{5,3}$	$c_{5,4}$	$c_{5,5}$	$c_{5,6}$	$c_{5,7}$	$c_{5,8}$	$c_{5,9}$	$c_{5,10}$
gss = 1	1	1	1	1	1	1	1	1	1	1
gss = 4	2	7	57	182	2057	14557	45807	280182	280182	6139557
gss = 4	3	18	68	443	1068	1068	32318	110443	1672943	3626068
gss = 2	4	24	124	624	3124	15624	78124	390624	1953124	9765624

Taking the numbers *c* in the following way

$$\begin{cases} c \equiv c_{2,10} \pmod{2^{10}} \\ c \equiv c_{5,10} \pmod{5^{1}} \end{cases}$$

then gss$(10^{10}, c)$ will be 1, 2 or 4. Since the possible combinations are 16, we find 16 values for *c*, shown in Table V.

TABLE V

Values of c for 10^{10}

	gss $(5^{10},c)=1$	gss $(5^{10},c)=4$	gss $(5^{10},c)=4$	gss $(5^{10},c)=2$
gss $(2^{10},c)=1$	1	8092077057	8333704193	6425781249
gss $(2^{10},c)=2$	8574218751	6666295807	6907922943	4999999999
gss $(2^{10},c)=2$	5000000001	3092077057	3333704193	1425781249
ss $(2^{10},c)=2$	3574218751	1666295807	1907922943	9999999999

Taking now, with notation of Section 3, a number x such that $x \equiv c \pmod{2^v 5^r}$ but $x \not\equiv c \pmod{2^{v+1} 5^r}$ and $x \not\equiv c \pmod{2^v 5^{r+1}}$ one has

$$\text{gss}\,(2^{10},\ x) = 2^{10-v} \text{ and } \text{gss}\,(5^{10},\ x) = d5^{10-r},$$

where $d = 1$, 2 or 4. Hence

$$\text{gss}\,(10^{10},\ x) = \text{l.c.m. } [2^{10-v},\ d5^{10-r}].$$

For $v = 2$, $r = 1$, $2^v 5^r = 20$ and starting for instance from $c=1$ we find the numbers

$$1 + 20 = 21,\ 1 + 3 \cdot 20 = 61,\ 1 + 7 \cdot 20 = 141,\ 1 + 9 \cdot 20 = 181$$

less than 200 belonging to 5.10^8, given in Table II. This may be repeated for the other c.

By this procedure and by means of the IBM 650 Computer, a complete table of the minimal subset of numbers belonging to all divisors of $\psi(10^{10})$ has been prepared at the Computing Centre of the C. N. E. N. Bologna, Italy, We give here an abstract of this table, in Table VI, showing the smallest numbers a belonging to the exponent quoted in the first column. The third column, contains the moduli $2^{v+1}5^{r+1}$ such that the numbers $x \equiv a \pmod{2^{v+1} 5^{r+1}}$ belong to the same exponent of a.

TABLE VI

Smallest numbers belonging to the divisors of ψ (10^{10})

gss(10^{10}, a)	a	$2^{v+1} \cdot 5^{r+1}$
1	1	10^{10}
2	1425781249	10^{10}
4	592077057	5000000000
5	2000000001	10^{10}
8	175781249	2500000000
10	425781249	10^{10}
16	32922943	1250000000
20	74218751	5000000000
25	400000001	2000000000
32	103795807	625000000
40	83704193	2500000000
50	25781249	2000000000
64	19531249	312500000
80	41295807	1250000000
100	7922943	1000000000
125	80000001	400000000
128	25670807	156250000
160	11718751	625000000
200	16295807	500000000
250	14218751	400000000
256	6139557	78125000
320	1672943	312500000
400	781249	250000000
500	5781249	200000000
625	16000001	80000000
640	3906249	156250000
800	3795807	125000000
1000	2077057	100000000
1250	1781249	80000000
1280	2233307	78125000
1600	2454193	62500000
2000	1295807	50000000
2500	77057	40000000
3125	3200001	16000000
3200	670807	31250000
4000	422943	25000000
5000	218751	20000000
6250	181249	16000000
6400	110443	15625000
8000	45807	12500000
10000	704193	10000000
12500	104193	8000000
15625	640001	3200000
16000	156249	6250000
20000	204193	5000000
25000	322943	4000000
31250	138751	3200000
32000	156251	3125000
40000	31249	2500000
50000	18751	2000000
62500	21249	1600000
78125	128001	640000
80000	47943	1250000
100000	4193	1000000
125000	2943	800000
156250	10751	640000
160000	14557	625000
200000	27057	500000
250000	15807	400000
312500	8193	640000
390625	25601	128000
400000	2057	250000
500000	1249	200000
625000	5249	160000
781250	2049	128000
800000	6251	125000
1000000	5807	100000
1250000	193	80000
1562500	257	64000
1953125	5121	25600
2000000	807	50000
2500000	1057	40000
3125000	1151	32000
3906250	511	25600
4000000	443	25000
5000000	751	20000
6250000	449	16000
7812500	513	25600
10000000	57	10000
12500000	351	8000
15625000	127	6400
20000000	251	5000
25000000	49	4000
31250000	63	3200
50000000	7	2000
62500000	31	1600
100000000	43	1000
125100000	17	800
250000000	9	400
500000000	3	200

5. - Sequences of full period.

An mentioned in the Introduction, for particular choices of the parameters, the sequences (1) may have m distinct numbers, i.e. a full period.

In Appendix I of ref. [8] it is shown that for $m = 2^t$, k odd and for every x_0, the full period is gss $(2^{t+v}, a)$ for any $a \equiv 1 \pmod 4$, where v is the highest power of 2 dividing $a - 1$.

Analogously the period of (1), for $m = p^s$ (p odd prime), k prime to p and for every x_0, is gss (p^{s+r}, a) for any $a \equiv 1 \pmod p$, where r is the highest power of p dividing $a - 1$. By theorem 3.2 where now $c = d = 1$ and s is replaced by $s + r$, follows

$$\text{gss}\,(p^{s+r},\ a) = p^s.$$

Finally for the composite modulus $m = 2^t p^s$ the full period is obtained for $a \equiv 1 \pmod{4p}$ and k prime to m.

The presence of subsequences with a number of terms $g =$ gss $(m, a) < m$ and translated among them in the system of integers mod m may be put in evidence by observing that, since

$$x_{i+n} \equiv a^n x_i + k(1 + a + \ldots + a^{n-1}) \pmod m,$$

for $n = g$ one obtains

$$x_{i+g} - x_i \equiv k(1 + a + \ldots + a^{g-1}) \pmod m$$

which does not depend on i.

APPENDIX

Computation of gss (m, a)

When the modulus is of the form $m = b^n$, the number gss (b^n, a) may be computed on an electronic machine as follows. Once one has found $g_1 =$ gss (b, a) by successive multiplications, then the first integer k_2 such that

$$(a^{g_1})^{k_2} \equiv 1 \pmod{b^2}$$

yields

$$g_2 = \mathrm{gss}\,(b^2,\ a) = k_2 g_1 .$$

If in general $g_i = \mathrm{gss}\,(b^i,\ a)$, it will be

$$g_i = k_i g_{i-1} \qquad (i > 1)$$

and

$$\mathrm{gss}\,(b^n,\ a) = k_n k_{n-1} \dots k_2 g_1 .$$

Since $g_1 \leq \varphi(b)$ and, as may easily be shown, $k_i \leq b$, the number of multiplications to perform is surely less than nb.

REFERENCES

[1] E. LUCAS, *Théorie des nombres*, Paris 1891.

[2] M. CIPOLLA, « *Teoria dei numeri, Analisi indeterminata* », in Enciclopedia delle Matematiche Elementari. Vol. I, Parte I, ULRICO HOEPLI, Milano, 1930.

[3] L. E. DICKSON, *History of the theory of numbers*, Vol. I, « Stechert & Co », New York, 1934.

[4] I. M. VINOGRADOV, *Elements of number theory*. Dover Publications, 1954.

[5] D. H. LEHMER, « *Mathematical methods in large-scale computing units* », *in Symposium on Large Scale Calculating Machinery*, pp. 141-146, « Harvard University », 1949.

[6] A. ROTENBERG, *A new pseudo-random number generator*, « J. Assoc. Comp. Mach. », 7 (1960), 75-77.

[7] R. R. COVEYOU, *Serial corrrelation in generation of pseudo-random numbers*, « J. Assoc. Comp. Mach. », 7 (1960), 72-74.

[8] M. GREENBERGER, *Notes on a new pseudo-random number generator*, « J. Assoc. Comp. Mach. », 8 (1961), 163-167.