LA-6667-MS

Informal Report

UC-32 & UC-34

Issued: January 1977

Number Theory of the Congruential Random Number Generators

by

C. J. Everett

los alamos
scientific laboratory
of the University of California
LOS ALAMOS, NEW MEXICO 87545

An Affirmative Action/Equal Opportunity Employer

UNITED STATES
ENERGY RESEARCH AND DEVELOPMENT ADMINISTRATION
CONTRACT W-7405-ENG. 36

Printed in the United States of America. Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161
Price: Printed Copy $4.00 Microfiche $3.00

NUMBER THEORY OF THE CONGRUENTIAL RANDOM NUMBER GENERATORS

by

C. J. Everett

ABSTRACT

The number theory underlying the "random number" generators $gx_n \equiv x_{n+1}$ and $gx_n + c \equiv x_{n+1}$ mod m is developed in greater detail than is customary, with the practical application to random number generation in mind. The arithmetic theory of the mixed generator does not appear in the standard texts, and the treatment here is believed to be new. In any case, it involves many features of interest which are not as well known as the classical theory of primitive roots required for the multiplicative generator. Even the latter theory, as presented below, displays some unorthodox aspects of importance for the construction of generators. An Appendix contains a summary of the classical theoretical background.

I. THE MULTIPLICATIVE GENERATOR

The recursion formula

$$gx_n \equiv x_{n+1} \text{ mod } m$$

defines a sequence of integers $X = \{x_0, x_1, x_2, \ldots\}$ which has the greatest possible period $\lambda(m)$ (cf. the Appendix) for properly chosen x_0 and g. This is the subject of the present section.

Lemma 1. If $k_i = pd(g_i \text{ mod } m)$, $i = 1,\ldots,\ell$, and if $k = pd(\Pi g_i \text{ mod } m)$, then

$$k = \Pi k_i \tag{2}$$

provided the k_i are co-prime.

Proof. Clearly $k \mid \Pi k_i$, since $(\Pi g_i)^{\Pi k_i} \equiv 1 \bmod m$. To prove $\Pi k_i \mid k$, it suffices to prove each $k_i \mid k$. For example, $k_1 \mid k$ since $1 \equiv (\Pi g_i)^{k\, k_2 \ldots k_\ell} \equiv g_1^{k\, k_2 \ldots k_\ell} \bmod m$ implies $k_1 \mid k\, k_2 \ldots k_\ell$, and hence $k_1 \mid k$.

Note 1. The relation $pd(\Pi g_i \bmod m) = [k_1, \ldots, k_\ell]$ need not hold. Thus for $m = 61$, one has $pd(2 \bmod 61) = 60$, and mod 61, $pd(2^6) = 60/(6,60) = 10$, $pd(2^{10}) = 60/(10,60) = 6$, but $pd(2^{16}) = 60/(16,60) = 15 \neq [10,6] = 30$.

Lemma 2. If p is an odd prime, the group G(p) of $\phi(p) = p-1$ integers $G(p) = \{1,2,\ldots,p-1\} \bmod p$ is cyclic, i.e., there exists an integer g of period $pd(g \bmod p) = p-1$, and hence $G(p) = \{g, g^2, \ldots, g^{p-1} \equiv 1\} \bmod p$. The set

$$H(p) = \{g_1, \ldots, g_{\phi(p-1)}\}$$

of residues of those $\phi(p-1)$ powers g^j with $(j,p-1) = 1$ consists of all integers g_i for which

$$pd(g_i \bmod p) = p-1, \quad 1 \leqslant g \leqslant p \ .$$

Proof. Writing $p-1 = \Pi q^b$ in standard form, it suffices by Lemma 1 to exhibit, for each prime $q \mid p-1$, an integer g_q of period q^b mod p, for then their product

$$g = \Pi g_q \bmod p$$

will have period $\Pi q^b = p-1 \bmod p$. For each such q, we may take

$$g_q = (x_q)^{(p-1)/q^b} \bmod p,$$

provided $(x_q)^{(p-1)/q} \not\equiv 1 \bmod p$, since this implies

$$\left(g_q\right)^{q^b} \equiv \left(x_q\right)^{p-1} \equiv 1 \bmod p,$$

whereas $\left(g_q\right)^{q^{b-1}} \equiv \left(x_q\right)^{(p-1)/q} \not\equiv 1 \bmod p$. Such an x_q exists, since the congruence $x^{(p-1)/q} \equiv 1 \bmod p$ has only $(p-1)/q < p-1$ roots.

Note 2. Following the above method for $p = 31$, $p-1 = 2 \cdot 3 \cdot 5$, we find that, mod 31,

$$3^{15} \equiv -1 \not\equiv 1 \qquad 3^{10} \equiv -6 \not\equiv 1 \qquad 2^6 \equiv 2 \not\equiv 1$$

$$x_2 \equiv 3 \qquad x_3 \equiv 3 \qquad x_5 \equiv 2$$

$$g_2 \equiv 3^{15} \equiv -1 \qquad g_3 \equiv 3^{10} \equiv -6 \qquad g_5 \equiv 2^6 \equiv 2$$

$$g \equiv g_2 g_3 g_5 \equiv 12, \ \mathrm{pd}(g \bmod 31) = 2 \cdot 3 \cdot 5 = 30.$$

Note 3. It is clear that $\mathrm{pd}(g \bmod m) = k$ iff $g^k \equiv 1 \bmod m$ and $g^{k/q} \not\equiv 1 \bmod m$ for every prime $q \mid k$. Thus the least $g \geq 1$ of period $p-1$ mod p is the first integer g for which $g^{(p-1)/q} \not\equiv 1 \bmod p$ for every $q \mid p-1$. (For $q = 2$, one knows $g^{(p-1)/2} \equiv \pm 1 \equiv (g/p) \bmod p$, and may use the short cut of quadratic residue theory.) For the prime $p = 31$ (Note 2) one finds the least such g is $g = 3$, since $3^{15} \equiv -1$, $3^{10} \equiv -6$, $3^6 \equiv 16 \bmod 31$, whereas $2^{15} \equiv 1 \bmod 31$. Using the generator $g = 3$, we find mod 31:

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^j	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30 ≡ -1

j	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3^j	28	22	4	12	5	15	14	11	2	6	18	23	7	21	1.

Note that $3^{15+j} \equiv -\left(3^j\right) \bmod 31$.

The integers ≤ 31 of period 30 are the $\phi(30) = 8$ residues of those powers 3^j with $(j, 30) = 1$, namely

j	1	7	11	13	17	19	23	29
3^j	3	17	13	24	22	12	11	21
$H(31)=$	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8.

Note that $12 \equiv 3^{19} \bmod 31$ in accord with Note 2.

In a similar way one may verify that $g = 2$ is the least integer of period 60 mod 61, since

$$2^{30} \equiv -1,\ 2^{20} \equiv 47,\ 2^{12} \equiv 9 \bmod 61.$$

(Cf. Note 1.)

Lemma 3. If p is an odd prime, then an integer g is a "universal generator" (for p), in the sense that

$$k \equiv \mathrm{pd}(g \bmod p^a) = p^{a-1}(p-1) = \phi(p^a)$$

for every $a \geqslant 1$, iff g has the two properties:

(i) $\mathrm{pd}(g \bmod p) = p-1$ and

(ii) $g^{p-1} \not\equiv 1 \bmod p^2$.

Proof. The necessity of these is obvious, if we consider the cases $a = 1,2$. For an integer g satisfying both, we first prove by induction that

$$g^{p^{b-1}(p-1)} = 1 + p^b u_b;\ p \nmid u_b,\ b \geqq 1. \tag{1}$$

This holds for $b = 1$ by property (ii). The induction step reads

$$g^{p^b(p-1)} = 1 + \binom{p}{1} p^b u_b + \binom{p}{2} p^{2b} u_b^2 + \dots + \binom{p}{p} p^{pb} u_b^p = 1 + p^{b+1} u_{b+1},$$

where

$$u_{b+1} = u_b + \binom{p}{2} p^{b-1} u_b^2 + \dots + \binom{p}{p} p^{(p-1)b-1} u_b^p \not\equiv 0 \bmod p$$

since $b \geqslant 1$, $p \geqslant 3$, and $p \nmid u_b$. Thus Eq. (1) is true for all $b \geqslant 1$, and hence for any fixed $a \geqq 1$,

$$g^{p^{a-1}(p-1)} \equiv 1 \bmod p^a.$$

Thus the period $k \mid p^{a-1}(p-1)$. Now $g^k \equiv 1 \bmod p^a$ implies $g^k \equiv 1 \bmod p$, and from relation (i) we see that $p-1 \mid k$. We may therefore write $k = p^{b-1}(p-1)$ where $1 \leqslant b \leqslant a$. By Eq. (1), we then have $1 + p^b u_b = g^{p^{b-1}(p-1)} = g^k = 1 + p^a Q$. Since $p \nmid u_b$, it follows that $p^a \mid p^b$, and hence $p^{a-1}(p-1) \mid p^{b-1}(p-1) = k$.

Lemma 4. If c is any integer for which $c^{p-1} \equiv 1 \bmod p^2$ (p prime $\geqslant 2$), then $(c+hp)^{p-1} \not\equiv 1 \bmod p^2$ for every h prime to p.

Proof. If $(c+hp)^{p-1} \equiv 1 \bmod p^2$ with $(h,p) = 1$, we should have the contradiction mod p^2

$$(c+hp) \equiv (c+hp)^p = c^p + \binom{p}{1} c^{p-1}hp + \ldots + \binom{p}{p} h^p p^p \equiv c^p \equiv c \bmod p^2.$$

Note 4. It follows from Lemmas 2, 3, and 4 that there exists a universal generator u for an odd prime p. In particular, if g_1 is the least integer of period p-1, then $g_1 (\leqslant p)$ or $g_1 + p (\leqslant 2p)$ is universal according as $g_1^{p-1} \not\equiv 1 \bmod p^2$ or $g_1^{p-1} \equiv 1 \bmod p^2$. The latter case does occur, e.g., when $p = 40487$ ($g_1 = 5$). See references [1,2].

While universality involves the properties (i), (ii) of a positive integer, the concept of group generator is a property of an integer mod p^a. It is easy to see directly that, for $a \geqslant 2$, p an odd prime, the set $U(p^a)$ of all integers $u \leqslant p^a$ which are universal coincides with the set $H(p^a)$ of generators $g \leqslant p^a$ of the group $G(p^a)$. For $U(p^a) \subset H(p^a)$ by definition, and the implication $\left(x \equiv 1 \bmod p^t \rightarrow x^{p^s} \equiv 1 \bmod p^{t+s}\right)$, proved by an easy induction, shows that $H(p^a) \subset U(p^a)$. For suppose g is a generator. If $g^{p-1} \equiv 1 \bmod p^2$, we should have

$$\left(g^{p-1}\right)^{p^{a-2}} \equiv 1 \bmod p^a, \text{ whereas } pd(g \bmod p^a) = p^{a-1}(p-1).$$

Moreover if $k = pd(g \bmod p)$, then $(g^k) \equiv 1 \bmod p$ implies $(g^k)^{p^{a-1}} \equiv 1 \bmod p^a$. Hence $p^{a-1}(p-1) \mid kp^{a-1}$, $p-1 \mid k \mid p-1$ and $k = p-1$. Thus g has the properties (i), (ii) of universality.

In Lemmas 5 and 6 the identity $U(p^a) = H(p^a)$, $a \geqslant 2$, will be proved in a quite different way, providing two essentially different methods for computing these generators. Note that $U(p) \neq H(p)$ for $p = 40487$.

Lemma 5. Let p be an odd prime, and $H(p) = \{g_1, \ldots, g_{\phi(p-1)}\}$ the complete set of integers $\leqslant p$ of period p-1 mod p, as in Lemma 2. Then the $p\phi(p-1)$ distinct integers

$$g_{ij} = g_i + jp;\ i = 1, \ldots, \phi(p-1),\ j = 0, 1, \ldots, p-1$$

are precisely the integers $\leqslant p^2$ of period p-1 mod p. Moreover, for each i there is exactly one j for which $g_{ij}^{p-1} \equiv 1 \bmod p^2$. If these $\phi(p-1)$ g_{ij} be deleted, the remaining ones comprise the complete set

$$U(p^2) = \{u_1, \ldots, u_{(p-1)\phi(p-1)}\}$$

of integers $\leqslant p^2$ which are universal generators. This set $U(p^2)$ is identical with the set $H(p^2)$ of $\phi[\phi(p^2)]$ generators mod p^2.

Proof.

(a) Obviously $g_{ij} \leqq p + (p-1)p = p^2$, and $g_i + jp = g_k + \ell p$ implies $g_i - g_k = (\ell - j)p$, $g_i = g_k$, $i = k$, $j = \ell$. The original set of g_{ij} therefore consists of $p\phi(p-1)$ distinct integers $\leqslant p^2$, and these are the integers $\leqslant p^2$ of period p-1 mod p.

(b) By Lemma 4, there is for each i <u>at most</u> one j for which $g_{ij}^{p-1} \equiv 1 \bmod p^2$. Deletion of these $d \leqslant \phi(p-1)$ integers g_{ij} leaves a set $U(p^2)$ of $p\phi(p-1)-d$ integers u which are <u>all</u> of the universal generators $\leqslant p^2$. Hence if $H(p^2)$ denotes the set of all $\phi[\phi(p^2)]$ generators mod p^2, we have by definition,

$$U(p^2) \subset H(p^2)$$

so that $p\phi(p-1) - d \leqslant \phi[\phi(p^2)] = \phi[p(p-1)] = (p-1)\phi(p-1)$. This implies $d \geqq \phi(p-1)$. Hence $d = \phi(p-1)$, and $U(p^2) = H(p^2)$.

Note 5. For $p = 5$, one has $pd(2 \bmod 5) = 4 = p-1$, with $G(5) = \{2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1\}$, and generator set $H(5) = \{2,3\}$. The g_{ij} table for 5^2 is therefore

$$g_{1j} = 2,7,12,17,22 \text{ with only } 7^4 \equiv 1 \bmod 5^2$$

$$g_{2j} = 3,8,13,18,23 \text{ with only } 18^4 \equiv 1 \bmod 5^2.$$

Deletion of 7,18 leaves the set

$$U(5^2) = \{2,12,17,22;3,8,13,23\}$$

of $4\ \phi(4) = 8$ integers $\leqslant 5^2$ which are universal (for $p = 5$).

The same set may be obtained as $H(5^2)$ as follows. Since $pd(2 \bmod 5) = 4$, and $2^4 \not\equiv 1 \bmod 5^2$, 2 is universal. In particular $pd(2 \bmod 5^2) = \phi(5^2) = 5 \cdot 4 = 20$, and its powers 2^j, $j = 1,\ldots,20$ give all the $\phi(5^2)$ integers prime to 5. Thus

j	1	2	3	4	5	6	7	8	9	10
2^j	2	4	8	16	7	14	3	6	12	$24 \equiv -1 \bmod 5^2$
j	11	12	13	14	15	16	17	18	19	20
2^j	23	21	17	9	18	11	22	19	13	1 $\bmod 5^2$.

The $\phi[\phi(5^2)] = 8$ generators of period $\phi(5^2) = 20$ are the residues of those 2^j with $(j,20) = 1$, namely

j	1	3	7	9	11	13	17	19
2^j	{2	8	3	12	23	17	22	13} $= H(5^2) = U(5^2)$.

This illustrates two different methods for obtaining the generators mod p^2. Similarly, the generators $H(p^a)$, $a \geqslant 3$ may be found in two ways, as indicated in Note 6.

Lemma 6. If p is an odd prime, and $U(p^2) = \{u_1,\ldots,u_{(p-1)\phi(p-1)}\}$ the set of universal generators $\leqslant p^2$ of Lemma 5, then for each $a \geqslant 3$, the set U_1 of integers

$$g_{ij} = u_i + jp^2;\ i = 1,\ldots,(p-1)\phi(p-1), j = 0,1,\ldots,p^{a-2}-1$$

satisfies the relation $U(p^a) = U_1 = G(p^a)$, i.e., the g_{ij} are at once the complete set $U(p^a)$ of universal generators $\leqslant p^a$, and the set $H(p^a)$ of all generators of the group $G(p^a)$.

Proof.

(a) $g_{ij} \leqslant p^2 + (p^{a-2} - 1)p^2 = p^a$, and $u_i + jp^2 = u_k + \ell p^2$ implies $u_i - u_k = (\ell-j)p^2$, $u_i = u_k$, $i = k$, $j = \ell$. Thus U_1 is a set of $p^{a-2}(p-1)\phi(p-1) = \phi(p^{a-1})\phi(p-1) = \phi[p^{a-1}(p-1)] = \phi[\phi(p^a)]$ distinct integers $\leqslant p^a$.

(b) Since $g_{ij} \equiv u_i \bmod p^2$, g_{ij} is a universal generator, so $U_1 \subset U(p^a) \subset H(p^a)$.

(c) But by part (a), $\#U_1 = \phi[\phi(p^a)] = \#H(p^a)$, so $U_1 = U(p^a) = H(p^a)$.

Note 6. Using the set $U(5^2)$ of Note 5 for $p = 5$, we obtain for the group $G(5^3)$ of $\phi(5^3) = 100$ integers prime to 5 mod 5^3, the set of $\phi(100) = 40$ integers $\leqslant 5^3$ which are universal for $p = 5$, namely the integers

g_{ij} =	2	27	52	77	102
	3	28	53	78	103
	8	33	58	83	108
	12	37	62	87	112
	13	38	63	88	113
	17	42	67	92	117
	22	47	72	97	122
	23	48	73	98	123

This is also the set of residues mod 5^3 of those 40 powers 2^j, $1 \leqslant j \leqslant 100$, for which $(j,100) = 1$, that is, the set $H(5^3)$ of generators of the group $G(5^3)$.

Lemma 7. If p is an odd prime, and $a \geqq 1$, then

(a) $x^{\lambda(p^a)} \equiv 1 \bmod p^a$ for all x prime to p, where by definition $\lambda(p^a) \equiv \phi(p^a) = p^{a-1}(p-1)$.

(b) There exists a g with $\text{pd}(g \bmod p^a) = \lambda(p^a)$. Specifically: if $a=1$, every $g \equiv g_i \bmod p$ has period $p-1 \bmod p$, where g_i belongs to the set $H(p)$ of Lemma 2; if $a \geqq 2$, every $g \equiv u_i \bmod p^2$ has period $p^{a-1}(p-1) \bmod p^a$, where u_i belongs to the set $U(p^2)$ of Lemma 5.

Proof.

(a) is a special case of Euler's theorem (Appendix) and also follows from (b).

(b) $g \equiv g_i \bmod p$ implies g has the same period $p-1 \bmod p$ as does g_i; $g \equiv u_i \bmod p^2$ implies g has the universal properties (i), (ii) of Lemma 3, and therefore g has period $p^{a-1}(p-1) \bmod p^a$.

Lemma 8. For the prime $p=2$ and $a \geqq 3$, one has

(a) $x^{\lambda(2^a)} \equiv 1 \bmod 2^a$ for all x prime to 2, where we define $\lambda(2^a) = (1/2)\phi(2^a) = 2^{a-2}$.

(b) There exists a g with $k \equiv \text{pd}(g \bmod 2^a) = \lambda(2^a)$. Specifically, this is true for every $g \equiv \pm 5 \bmod 8$. For $a \geqq 4$, the latter condition is necessary. However, for $a=3$, one also has $\text{pd}(7 \bmod 8) = \lambda(2^3) = 2$.

Proof.

(a) For every odd $x = 1 + 2h$, we see that $x^2 = 1 + 4h(1+h) \equiv 1 + 2^3 z_3$, and an easy induction shows that $x^{2^{a-2}} = 1 + 2^a z_a \equiv 1 \bmod 2^a$ for $a \geqq 3$.

(b) Every $g \equiv \pm 5 \bmod 8$ may be written in the form $g = \pm 1 + 2^2 u_2$, $2 \nmid u_2$, where obviously $g \not\equiv 1 \bmod 2^a$ for $a \geqq 3$. Hence the period $k = \text{pd}(g \bmod 2^a) \geqq 2$. We show by induction that

$$g^{2^{b-2}} = 1 + 2^b u_b;\ 2 \nmid u_b,\ b \geqq 3. \tag{2}$$

For $b = 3$, we have $g^2 = (\pm 1 + 2^2 u_2)^2 = 1 + 2^3(\pm u_2 + 2u_2^2) = 1 + 2^3 u_3$, where $2 \nmid u_3$. The induction step is

$$g^{2^{b-1}} = 1 + 2^{b+1}(u_b + 2^{b-1}u_b^2) = 1 + 2^{b+1}u_{b+1} \text{ where } 2 \nmid u_{b+1}.$$

From Eq. (2) we obtain $g^{2^{a-2}} \equiv 1 \bmod 2^a$ for given $a \geqq 3$, so the period $k \mid 2^{a-2}$. Let $k = 2^{b-2}$ where we know $3 \leqslant b \leqslant a$. If $a=3$, we already have $k = 2^{a-2}$. For an $a \geqslant 4$, we see from Eq. (2) that

$$1 + 2^b u_b = g^{2^{b-2}} = g^k = 1 + 2^a Q;\ 2 \nmid u_b.$$

Hence $2^a \mid 2^b$, $a \leqslant b \leqslant a$, $b = a$, and $k = 2^{a-2}$.

Finally, if $a \geqslant 4$, and $x \equiv \pm 1 \bmod 8$, induction shows that $x^{2^{a-3}} = 1 + 2^a u_a$, so $\mathrm{pd}(x \bmod 2^a) \mid 2^{a-3} < 2^{a-2}$. Thus for $a \geqslant 4$, an integer of period 2^{a-2} must be $\equiv \pm 5 \bmod 8$.

Lemma 9. For the prime $p = 2$, and $a \geqq 3$:

(1) The $\phi(2^a) = 2^{a-1}$ odd integers $\leqslant 2^a$ fall into two classes, the class C of 2^{a-2} integers $\equiv 1 \bmod 4$, half of which are $\equiv 1$ and half $\equiv 5 \bmod 8$, and the class D of 2^{a-2} integers $\equiv 3 \bmod 4$, half $\equiv 3$ and half $\equiv 7 \bmod 8$. The powers $5^j \bmod 2^a$, $j = 1, \ldots, 2^{a-2}$ have the set C as residues, while their negatives have the set D as residues. Thus

$$C = \left\{1, 5, \ldots, 2^a - 3\right\} \equiv \left\{5, 5^2, \ldots, 5^{2^{a-2}} \equiv 1\right\} \bmod 2^a$$

$$D = \left\{3, 7, \ldots, 2^a - 1\right\} \equiv \left\{-5, -\left(5^2\right), \ldots, -\left(5^{2^{a-2}}\right) \equiv -1\right\} \bmod 2^a .$$

(2) The residues of the powers of form 5^{2h+1}, 5^{2h+2}, $-(5^{2h+1})$, $-(5^{2h+2})$ are respectively all the integers $\leqslant 2^a$ which are congruent to 5, 1, 3, 7 mod 8.

(3) Thus the 2^{a-2} integers $\pm(5^{2h+1})$, equivalently the integers $\equiv 5$ or $3 \bmod 8$, all have period $\lambda(2^a) = 2^{a-2} \bmod 2^a$, and for $a \geqq 4$ there are no others.

(4) A number $\equiv 5^j$ for odd j, i.e., a number $\equiv 5 \bmod 8$, generates the group C, whereas a number $\equiv -(5^j)$ for odd j, i.e., a number $\equiv 3 \bmod 8$, has powers with residues lying alternately in D and C, and running over all integers $\equiv 3$ and $1 \bmod 8$.

Proof. Aside from some details left to the reader, the Lemma is an obvious consequence of Lemma 8, and the fact that $\mathrm{pd}(5^j \bmod 2^a) = 2^{a-2}/(j, 2^{a-2}) = 2^{a-2}$ iff j is odd.

Note 7. For $2^6 = 64$, one finds the residues mod 64:

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16 = 2^4
C 5^j	5	25	61	49	53	9	45	33	37	57	29	17	21	41	13	1
D-(5^j)	59	39	3	15	11	55	19	31	27	7	35	47	43	23	51	63.

5^j generates the group C for $j = 1,3,5,\ldots,15$, these are the integers 5, 61, 53,...,13 congruent to 5 mod 8.

<u>Lemma 10</u>. For the prime power 2^a, $a \geqq 1$, one has

(a) $x^{\lambda(2^a)} \equiv 1 \bmod 2^a$ for every x prime to 2, where by definition $\lambda(2) = \phi(2) = 1$, $\lambda(2^2) = \phi(2^2) = 2$, $\lambda(2^a) = (1/2)\phi(2^a) = 2^{a-2}$ for $a \geqq 3$.

(b) There exists a g with $\mathrm{pd}(g \bmod 2^a) = \lambda(2^a)$. Specifically: if $a = 1$, every $g \equiv 1 \bmod 2$ has $\mathrm{pd}(g \bmod 2^a) = \lambda(2)$; if $a = 2$, every $g \equiv 3 \bmod 2^2$ has $\mathrm{pd}(g \bmod 2^2) = \lambda(2^2)$; if $a \geqq 3$, every $g \equiv \pm 5 \bmod 8$, or equivalently, every $g \equiv \pm(5^j) \bmod 2^a$, with j odd, has $\mathrm{pd}(g \bmod 2^a) = \lambda(2^a)$.

Proof. The lemma is by way of summary, being obvious for $a = 1,2$, and a consequence of Lemmas 8, 9 for $a \geqq 3$.

<u>Lemma 11</u>. If $m = p_1^{a_1} \ldots p_\ell^{a_\ell}$ and for each i

$$k_i = \mathrm{pd}\left(g \bmod p_i^{a_i}\right),$$

then $k \equiv \mathrm{pd}(g \bmod m) = [k_1,\ldots,k_\ell] \equiv M$.

Proof. Since each $k_i \mid M$, we know $g^M \equiv 1 \bmod p_i^{a_i}$, hence $g^M \equiv 1 \bmod m$, and $k \mid M$. But $g^k \equiv 1 \bmod m$ implies $g^k \equiv 1 \bmod p_i^{a_i}$ and $k_i \mid k$ for each i. Hence $M \mid k$ and $k = M$.

<u>Lemma 12</u>. If $m = p_1^{a_1} \ldots p_\ell^{a_\ell}$, we have

(a) $x^{\lambda(m)} \equiv 1 \bmod m$ for every x prime to m, where $\lambda(m) = $ l.c.m. $[\lambda(p_1^{a_1}),\ldots,\lambda(p_\ell^{a_\ell})]$. Thus $\lambda(m)$ is the greatest possible period mod m.

(b) There exists a g with period $\mathrm{pd}(g \bmod m) = \lambda(m)$. Specifically, this is true for any g satisfying the system of congruences

$$g \equiv c_i \bmod p_i^{b_i} \qquad \text{(S)}$$

constructed as follows:

1. For each odd prime $p_i \mid m$ with $a_i = 1$, system (S) includes a congruence $g \equiv g_i \bmod p_i$, where g_i is an element of the set $H(p_i)$ of Lemma 2.

2. For each odd $p_i \mid m$ with $a_i \geqslant 2$, system (S) includes a congruence $g \equiv u_i \bmod p_i^2$, where u_i is any element of the set $U(p_i^2)$ of Lemma 5.

3. If $2 \mid m$ with exponent $a \geqslant 1$, the system (S) includes a congruence

$$g \equiv 1 \bmod 2 \text{ if } a = 1,$$
$$g \equiv 3 \bmod 4 \text{ if } a = 2,$$
$$g \equiv \pm 5 \bmod 8 \text{ if } a \geqslant 3.$$

For any particular choice of the c_i, one for each $p_i \mid m$, there exists a unique positive solution $g_o \leqslant$ the product P of the moduli in system (S), and all positive solutions are then of form $g = g_o + hP$, $h = 0,1,2,\ldots$

Proof.

(a) Since $\lambda(p_i^{a_i}) \mid \lambda(m)$ for each p_i in m, it follows from part (a) of Lemmas 7, 10 that $x^{\lambda(m)} \equiv 1 \bmod p_i^{a_i}$ and hence mod m, for every x prime to m.

(b) By part (b) of Lemmas 7 and 10, we see that any g satisfying the system (S) as constructed has $\mathrm{pd}(g \bmod p_i^{a_i}) = \lambda(p_i^{a_i})$ for all i. Hence by Lemma 11, $\mathrm{pd}(g \bmod m) = [\lambda(p_1^{a_1}),\ldots,\lambda(p_\ell^{a_\ell})] = \lambda(m)$. The final statement is a consequence of the Chinese Remainder Theorem (Appendix).

Note 8. In contrast to the analogous result in Part II there is here no simple characterization of the integers of maximal period. According to Lemma 11, an integer g has maximal period $\lambda(m)$ mod $m = \Pi p_i^{a_i}$ iff $[k_1,\ldots,k_\ell] = [\lambda(p_1^{a_1}),\ldots,\lambda(p_\ell^{a_\ell})] \equiv \lambda(m)$, where $k_i = \mathrm{pd}(g \bmod p_i^{a_i})$. This may be obtained in a variety of ways. As an example, we note that for $m = 217 = 7 \cdot 31$, one has $k_1 = \mathrm{pd}(69 \bmod 7) = 2$, $k_2 = \mathrm{pd}(69 \bmod 31) = 15$, $[k_1,k_2] = 30 = \lambda(m)$, so $\mathrm{pd}(69 \bmod 217) = \lambda(m)$, although 69 does not have maximal period for either 7 or 31. Clearly the construction of Lemma 12 need not produce all integers of period $\lambda(m)$. The least g of period $\lambda(217)$ mod 217 is $g = 3$. This is indeed produced by the method of Lemma 12, since $\mathrm{pd}(3 \bmod 7) = 6$, $\mathrm{pd}(3 \bmod 31) = 30$.

A very simple instance of the above behavior is provided by the case $m = 12$. Here $G(12) = \{1,5,7,11\}$, the integers 5,7, and 11 all having maximal period $\lambda(12) = 2$. One finds that

pd(5 mod 4) = 1	pd(7 mod 4) = 2	pd(11 mod 4) = 2
pd(5 mod 3) = 2	pd(7 mod 3) = 1	pd(11 mod 3) = 2
[1,2] = 2	[2,1] = 2	[2,2] = 2

Solution of the system $g \equiv 3 \bmod 4$
$g \equiv 2 \bmod 3$
produces only $g \equiv 11 \bmod 12$.

Note 9. The least g of period $\lambda(m)$ mod m is the first g prime to m such that $g^{\lambda(m)/q} \not\equiv 1 \bmod m$ for every prime $q|\lambda(m)$. (Cf. Note 3.) It is of course possible to produce all g of period $\lambda(m)$ in such a way.

Theorem 1. If $m = p_1^{a_1} \ldots p_\ell^{a_\ell}$, and $(x_o,m) = 1$, then the sequence $X = \{x_o,x_1,\ldots\}$ of positive integers $\leqslant m$ defined recursively by

$$gx_n \equiv x_{n+1} \bmod m$$

is pure periodic of the greatest possible period $\lambda(m)$ iff $pd(g \bmod m) = \lambda(m)$. Such integers may be constructed as in Lemma 12, and all such g may be obtained by the method of Note 9.

Proof. The result is immediate, since the sequence $X = \{x_o, gx_o, g^2x_o, \ldots\}$ mod m, with $(x_o,m) = 1$, is obviously pure periodic with sequential period $k = pd(g \bmod m)$.

Note 10. $\lambda(m) \mid \phi(m)$, and $\lambda(m) = \phi(m)$ iff $m = 1,2,4,p^a$, or $2p^a$ (p odd prime) (Appendix).

Corollary 1. For $m = 2^a$, $a \geqq 4$, x_o odd, the sequence X defined by $gx_n \equiv x_{n+1} \bmod 2^a$ has maximal period 2^{a-2} iff $g \equiv \pm 5 \bmod 8$, or equivalently, $g \equiv \pm 5^j \bmod 2^a$ where j is odd.

Proof. See Lemma 9 and Theorem 1.

Corollary 2. For $m = p^a$, $a \geqq 1$, $p \nmid x_o$, p odd prime, the sequence X defined by $gx_n \equiv x_{n+1} \bmod p^a$ has maximal period $p^{a-1}(p-1)$ iff g is chosen as in Lemma 7.

Corollary 3. For $m = 10^a$, $a \geq 4$, $(x_o, 10) = 1$, the greatest possible period for the sequence X defined by $gx_n \equiv x_{n+1} \bmod 10^a$ is $\lambda(m) = 5 \cdot 10^{a-2}$, and is attained for any g of form $g = g_o + 200\,h$, $h = 0, 1, \ldots, 5 \cdot 10^{a-3} - 1$ where g_o is one of the integers $g_o = 3,13,27,37,53,67,77,83,117,123,133,147,163,173,187,197$.

Proof. Since $a \geq 4$, $\lambda(10^a) = [\lambda(2^a), \lambda(5^a)] = [2^{a-2}, 5^{a-1} \cdot 4] = 2^{a-2} \cdot 5^{a-1} = 5 \cdot 10^{a-2}$. The list of g_o values results from solving the 16 systems of form

$$g_o \equiv \pm 5 \bmod 8 \qquad (5)$$
$$g_o \equiv u_i \bmod 5^2,$$

where u_i runs through the set

$$U(5^2) = \{2,12,17,22;\ 3,8,13,23\}.$$

(See Lemma 12 and Note 5.)

We do not attempt to give a computer algorithm for solution of systems of form (S). It may be noted however that if $z_1, \ldots, z_\ell$ are solutions of the ℓ basic systems

$$\begin{array}{lcl} z_1 \equiv 1 \bmod p_1^{b_1} & \cdots & z_\ell \equiv 0 \bmod p_1^{b_1} \\ z_1 \equiv 0 \bmod p_2^{b_2} & & z_\ell \equiv 0 \bmod p_2^{b_2} \\ \vdots & & \vdots \\ z_1 \equiv 0 \bmod p_\ell^{b_\ell} & & z_\ell \equiv 1 \bmod p_\ell^{b_\ell} \end{array}$$

then $g \equiv c_1 z_1 + \ldots + c_\ell z_\ell \bmod \Pi p_i^{b_i}$ is obviously a solution of the system $g \equiv c_i \bmod p_i^{b_i}$; $i = 1, \ldots, \ell$. This method may be used to advantage in obtaining the 16 values of g_o listed above.

Note 11. In the case of Corollary 3, with $a = 4$, we find that

$$k_1 = \text{pd}(629 \bmod 2^4) = \text{pd}(5 \bmod 16) = 2^2 = \lambda(2^4)$$

$$k_2 = \text{pd}(629 \bmod 5^4) = \text{pd}(4 \bmod 5^4) = 2 \cdot 5^3 < \lambda(5^4).$$

Nevertheless, $pd(629 \bmod 2^4 \cdot 5^4) = [k_1,k_2] = 2^2 \cdot 5^3 = \lambda(2^4 \cdot 5^4)$. Thus 629 has maximal period, but is not obtainable from Corollary 3. (See Note 8.)

II. THE MIXED CONGRUENTIAL GENERATOR

The recursion formula

$$gx_n + c \equiv x_{n+1} \bmod m$$

defines a sequence of integers $X = \{x_0, x_1, x_2, \ldots\}$ which is pure periodic of full period m provided g and c are suitably chosen with respect to the modulus m. The present part establishes necessary and sufficient conditions, after a careful analysis of the underlying number theory, which does not appear in existing texts, and is of considerable interest in itself. The full statement of the final Theorem 2 is believed to be new.

Lemma 13. An integer $g \geqslant 2$ with $(g,2) = 1$ has period

$$k = pd[g \bmod 2(g-1)] = 2.$$

Proof. Writing $g = 1 + 2h$, we see that $(1+2h)^2 = 1 + 4h(1+h) \equiv 1 \bmod 4h$ whereas $(1+2h) \not\equiv 1 \bmod 4h$.

Lemma 14. If $g \geqq 2$, $(g,2^a) = 1$, $a \geqq 2$, and

$$k = pd[g \bmod 2^a(g-1)]$$

then $k = 2^a$ for $g \equiv 1 \bmod 4$, whereas $k \mid 2^{a-1}$ for $g \equiv -1 \bmod 4$.

Proof. If $g = 1 + 4h$, induction on b shows that

$$g^{2^b} = 1 + 2^b(g-1)u_b, \; 2 \nmid u_b, \; b \geqq 0. \qquad (3)$$

This is clear for $b = 0$ with $u_b = 1$, while the induction step reads

$$g^{2^{b+1}} = 1 + 2^{b+1}(g-1)u_{b+1},$$

where $u_{b+1} = u_b + 2^{b-1}(g-1)u_b^2 = u_b + 2^{b+1}hu_b^2$ is odd for $b \geqslant 0$. Setting $b = a$ in Eq. (3) shows that $k \mid 2^a$, and hence $k = 2^b$, $0 \leqslant b \leqslant a$. Then by Eq. (3),

$$1 + 2^b(g-1)u_b = g^{2^b} = g^k = 1 + 2^a(g-1)Q.$$

Since $2 \nmid u_b$, we have $2^a \mid 2^b = k$, so $k = 2^a$.

However, if $g = -1 + 4h$, a similar induction shows that

$$g^{2^{b-1}} = 1 + 2^b(g-1)hv_b, \; 2 \nmid v_b, \; b \geqq 2.$$

In fact, $g^2 = 1 + 4(4h-2)h = 1 + 2^2(g-1)hv_2$, with $v_2 = 1$, and by induction, $g^{2^b} = 1 + 2^{b+1}(g-1)hv_{b+1}$, where $v_{b+1} = v_b + 2^{b-1}(g-1)hv_b^2$ is odd since $b \geqslant 2$. Hence for $b = a \geqq 2$ we see that $k \mid 2^{a-1}$. (The parity of v_b is irrelevant for the lemma.)

Note 12. $\mathrm{pd}[7 \bmod 2^3(7-1)] = 2 \mid 2^2 \mid 2^3$, $\mathrm{pd}[11 \bmod 2^3(11-1)] = 2^2 \mid 2^3$.

Lemma 15. If p is an odd prime, $g \geqslant 2$, $(g,p^a) = 1$, $a \geqq 1$ and

$$k \equiv \mathrm{pd}[g \bmod p^a(g-1)]$$

then $k = p^a$ for $g \equiv 1 \bmod p$. Otherwise $k = \mathrm{pd}(g \bmod p^a) \mid \phi(p^a) < p^a$.

Proof. If $g = 1 + ph$, induction on b shows that

$$g^{p^b} = 1 + p^b(g-1)w_b, \; p \nmid w_b, \; b \geqslant 0, \tag{4}$$

the induction step being

$$g^{p^{b+1}} = 1 + \binom{p}{1} p^b(g-1)w_b + \binom{p}{2} p^{2b}(g-1)^2w_b^2 + \ldots + \binom{p}{p} p^{pb}(g-1)^pw_b^p$$

$$= 1 + p^{b+1}(g-1)w_{b+1}, \text{ where}$$

$$w_{b+1} = w_b + \binom{p}{2}p^{b-1}(g-1)w_b^2 + \ldots + \binom{p}{p} p^{(p-1)b-1}(g-1)^{p-1}w_b^p$$

$$= w_b + \binom{p}{2} p^bhw_b^2 + \ldots + \binom{p}{p}p^{(p-1)b+p-2}h^{p-1}w_b^p$$

is prime to p since $b \geq 0$, $p \geq 3$, and $p \nmid w_b$. With $b = a \geq 1$ in Eq. (4), we see that $k \mid p^a$, so $k = p^b$ for some $b \geq 0$. Thus by Eq. (4) we have

$$1 + p^b(g-1)w_b = g^{p^b} = g^k = 1 + p^a(g-1)Q.$$

Since $p \nmid w_b$, we infer that $p^a \mid p^b = k$, and $k = p^a$.

Now suppose $g \not\equiv 1 \bmod p$ has period $k = pd[g \bmod p^a(g-1)]$. Then $g^k \equiv 1 \bmod p^a(g-1)$, and hence also mod p^a. Consequently the period $\ell \equiv pd(g \bmod p^a)$ divides k. But then also

$$g^\ell \equiv 1 \bmod p^a$$
$$g^\ell \equiv 1 \bmod g-1.$$

Since $p \nmid g-1$ by assumption, we know $(p^a, g-1) = 1$, so that

$$g^\ell \equiv 1 \bmod p^a(g-1)$$

whence $k \mid \ell$. Thus $k = \ell = pd(g \bmod p^a) \mid \phi(p^a) = p^{a-1}(p-1) < p^a$.

Note 13. $pd[4 \bmod 3^2(4-1)] = 3^2$, $pd[5 \bmod 3^2(5-1)] = 6 = \phi(3^2) < 3^2$.

Lemma 16. If $m = p_1^{a_1} \ldots p_\ell^{a_\ell}$, $g \geqq 2$, $(g,m) = 1$, and

$$k_i \equiv pd[g \bmod p_i^{a_i}(g-1)]$$

then $k \equiv pd[g \bmod m(g-1)] = [k_1, \ldots, k_\ell] \equiv M$.

Proof. Since each $k_i \mid M$, we have $g^M \equiv 1 \bmod p_i^{a_i}(g-1)$. Thus each $p_i^{a_i} \mid (g^M-1)/(g-1)$, and so does m, whence

$$g^M \equiv 1 \bmod m(g-1)$$

and $k \mid M$. But $g^k \equiv 1 \bmod m(g-1)$ implies $g^k \equiv 1 \bmod p_i^{a_i}(g-1)$ for every i. Therefore each $k_i \mid k$ and so does their l.c.m. M. Hence $k = M$.

Note 14. $pd[5 \bmod 2^2(5-1)] = 2^2$, $pd[5 \bmod 3^2(5-1)] = 6$, $pd[5 \bmod 2^2 \cdot 3^2(5-1)] = 12 = [2^2, 6]$.

Lemma 17. If $m = p_1^{a_1} \dots p_\ell^{a_\ell}$, $g \geq 2$, $(g,m) = 1$, and

$$k \equiv pd[g \bmod m(g-1)]$$

then $k = m$ provided g satisfies condition

(C) $g \equiv 1 \bmod p_i$ for every odd prime $p_i \mid m$, and $g \equiv 1 \bmod 4$ if $4 \mid m$.

For any g not satisfying (C), one has a period $k < m$.

Proof. By Lemma 16 we know that

$$k = [k_1, \dots, k_\ell],$$

where $k_i = pd[g \bmod p_i^{a_i}(g-1)]$. If condition (C) holds, then by Lemmas 13, 14, 15, we have $k_i = p_i^{a_i}$ for every $i = 1,\dots,\ell$, and $k = [p_1^{a_1},\dots,p_\ell^{a_\ell}] = p_1^{a_1} \dots p_\ell^{a_\ell} = m$. However, if condition (C) fails, we know from the same Lemmas that $k_i \leqslant p_i^{a_i}$ for all i, with $k_i < p_i^{a_i}$ for at least one i. In such a case, $k = [k_1, \dots k_\ell] \mid k_1, \dots, k_\ell < p_1^{a_1} \dots p_\ell^{a_\ell} = m$.

Lemma 18. For a given $m \geq 2$, the integers $g \geq 2$, and prime to m, for which $pd[g \bmod m(g-1)] = m$ are given by the following forms, where the p_i are odd primes, and $h \geq 1$ is arbitrary:

$m = 2$	$g = 1 + 2h$
$m = 2^a$, $a \geq 2$	$g = 1 + 4h$
$m = \Pi\, p_i^{a_i}$	$g = 1 + (\Pi\, p_i)h$
$m = 2\Pi\, p_i^{a_i}$	$g = 1 + (2\,\Pi\, p_i)h$
$m = 2^a\,\Pi\, p_i^{a_i}$, $a \geqslant 2$	$g = 1 + (4\,\Pi\, p_i)h$

Proof. This is an immediate consequence of Lemma 17.

Note 15. For $m = 10 = 2 \cdot 5$ and $g = 1 + 2 \cdot 5 = 11$, one has pd(11 mod 100) = 10; indeed we find for the powers of 11 mod 100 the residues

11,21,31,41,51,61,71,81,91,1 .

Theorem 2. Let $m = p_1^{a_1} \ldots p_\ell^{a_\ell} \geqslant 2$, $(g,m) = 1$, and $1 \leqslant g,c,x_o \leqslant m$. Then

(1) the sequence $X = \{x_o, x_1, \ldots\}$ of positive integers $\leqslant m$ defined recursively by $gx_n + c \equiv x_{n+1} \bmod m$ is pure periodic of sequential period $K \leqslant m$;

(2) for $g = 1$, $K = m/(c,m)$, and $K = m$ iff $(c,m) = 1$;

(3) for $g \geqslant 2$, $K = \text{pd}[g \bmod m_1(g-1)]$, where $m_1 = m/d$, and d is the g.c.d. of $(g-1)x_o + c$ and m;

(4) for $g \geqq 2$, regardless of x_o, $K = m$ iff g and c satisfy the two conditions

(C) $g \equiv 1 \bmod p_i$ for every odd prime $p_i \mid m$, and $g \equiv 1 \bmod 4$ if $4 \mid m$,

(D) $(c,m) = 1$.

In such a case, the sequence $\{x_o, \ldots, x_{m-1}\}$ is a permutation of the integers $\{1,2,\ldots,m\}$.

Proof.

(1) The sequence $\{x_o, x_1, \ldots, x_m\}$ of $m+1$ positive integers $\leqslant m$ must contain a repetition, and hence a first $x_k = x_i$ with $i < k$. Since $(g,m) = 1$, we must have $i = 0$, otherwise the recursion implies $x_{k-1} = x_{i-1}$. But then $x_o = x_k$ implies $x_n = x_{k+n}$ for all $n = 0,1,2,\ldots$ and X is pure periodic of sequential period

$$K = \min\{k;\ x_k = x_o\} \leqslant m.$$

(2) If $g = 1$, then $X \equiv \{x_o, x_o+c, x_o+2c, \ldots\} \bmod m$, its period K being the first $k \geqq 1$ for which $x_o + kc \equiv x_o \bmod m$, or equivalently $k \equiv 0 \bmod m/(c,m)$, i.e., $K = m/(c,m)$.

(3) If $g \geqq 2$, the recursion shows that, for every $k \geqslant 1$,

$$x_1 \equiv gx_o + c$$

$$x_2 \equiv g^2x_o + gc + c$$

$$\vdots$$

$$x_k \equiv g^kx_o + g^{k-1}c + \ldots + gc + c$$

$$\equiv g^kx_o + \left(\frac{g^k-1}{g-1}\right) c \qquad \text{mod } m .$$

Hence the sequential period K of X is the first $k \geqslant 1$ for which

$$\left(\frac{g^k-1}{g-1}\right)[(g-1)x_o+c] \equiv 0 \text{ mod } m,$$

this being equivalent to the equality $x_k = x_o$. Now if d is the g.c.d. of $[(g-1)x_o+c]$ and m, we infer that K is the first integer $k \geqslant 1$ for which $(g^k-1)/(g-1) \equiv 0 \text{ mod } m_1 = m/d$, i.e., $g^k \equiv 1 \text{ mod } m_1(g-1)$. Hence the sequential period is

$$K = \text{pd}[g \text{ mod } m_1(g-1)]. \tag{5}$$

(4) Now suppose conditions (C) and (D) both hold. Then $(g-1)x_o+c$ must be prime to m. For, if $2 \mid m$, then g is odd since $(g,m) = 1$, and $2 \mid g-1$ whereas $2 \nmid c$, which is prime to m. Also, any odd prime in m divides g-1 by condition (C), but not c which is prime to m. Hence m has no prime in common with $(g-1)x_o+c$, and $d = 1$, $m_1 = m$, $K = \text{pd}[g \text{ mod } m(g-1)]$ in Eq. (5) and the latter is m by Lemma 17.

Finally, suppose condition (C) or (D) fails. If (C) fails, we know from Lemma 17 that $g^k \equiv 1 \text{ mod } m(g-1)$ for a $k < m$, and hence also

$$g^k \equiv 1 \text{ mod } m_1(g-1); \; k < m.$$

It then follows from Eq. (5) that $K \mid k$, and $K \leqslant k < m$. If condition (C) holds but (D) fails, then there is a prime $p \geqq 2$ common to c and m. If this p is odd, it divides g-1 by condition (C), and hence $(g-1)x_o + c$ also. If $p = 2$, then m and c are even, while $(g,m) = 1$ implies $g-1$ even, and $p = 2$ divides $(g-1)x_0+c$. In either case we must have the g.c.d. $d > 1$ and $m_1 < m$. Now if $m_1 = 1$, then by relation (5), $K = pd[g \bmod (g-1)] = 1 < m$. If $m_1 \geq 2$, then by relation (5) and Lemma 17 (with m_1 for m), we have $K \leq m_1 < m$ (actually $K = m_1$).

Note 16. For $m = 10$, $g = 3$, $c = 2$, $x_0 = 1$, one obtains the sequence $X = \{1,5,7,3; 1,5,7,3;\ldots\}$ of period $K = 4$. Here, $(g-1)x_0 + c = 4$, $d = (4,10) = 2$, $m_1 = 5$, and $K = pd[3 \bmod 5(3-1)] = 4$, as in Eq. (5). Note that $K \nmid m$.

Note 17. Since the recursion is defined mod m, the only relevant values of g are $< m$. Reference to Lemma 18 shows that moduli of form $m = 2, 4, \Pi p_i$, $2\Pi p_i$, $4\Pi p_i$, with their associated $g = 1 + mh$, admit no recursive sequences X of period m other than the trivial one with $g = 1$, namely $X = \{x_0, x_0+c, x_0+2c, \ldots\}$.

Corollary 4. The sequence $X = \{x_0, x_1, \ldots\}$ defined by $gx_n + c \equiv x_{n+1} \bmod 2^a$, $a \geq 3$, g odd $\geqq 3$, x_0 arbitrary, has period 2^a iff c is odd and $g \equiv 1 \bmod 4$.

Note 18. The recursion $5x_n + 3 \equiv x_{n+1} \bmod 16$, $x_0 = 1$, gives $X = \{1,8,11,10,5,12,15,14,9,16,3,2,13,4,7,6; 1,\ldots\}$.

Corollary 5. The sequence $X = \{x_0, x_1, \ldots\}$ defined by $gx_n + c \equiv x_{n+1} \bmod p^a$, p prime ≥ 3, $a \geq 2$, $g \geq 2$, $(g,p) = 1$, x_0 arbitrary, has period p^a iff $p \nmid c$ and $g \equiv 1 \bmod p$.

Note 19. The recursion $6x_n + 1 \equiv x_{n+1} \bmod 25$, $x_0 = 5$, gives $X = \{5,6,12,23,14,10,11,17,3,19,15,16,22,8,24,20,21,2,13,4,25,1,7,18,9;5,\ldots\}$.

Corollary 6. The sequence $X = \{x_0, x_1, \ldots\}$ defined by $gx_n + c \equiv x_{n+1} \bmod 10^a$, $a \geqq 2$, $g \geq 2$, $(g,10) = 1$, x_0 arbitrary, has period 10^a iff $(c,10) = 1$, and $g = 1 + 20h$.

Note 20. The recursion $81x_n + 11 \equiv x_{n+1} \bmod 100$ generates a permutation of the integers $1,2,\ldots,100$.

APPENDIX

SUMMARY OF THE CLASSICAL THEORETICAL BACKGROUND

I. EULER'S ϕ-FUNCTION AND THE GROUP G(m)

The function $\phi(m)$ counts the number of integers x, $1 \leq x \leq m$, which are prime to m, i.e., with g.c.d. $(x,m) = 1$. The set of all such x forms a group G(m) of order $\phi(m)$ under multiplication mod m, and Euler's theorem asserts that $x^{\phi(m)} \equiv 1 \bmod m$ for $(x,m) = 1$. It can be shown that $\phi(1) = 1$, $\phi(p^a) = p^{a-1}(p-1)$, and $\phi(\Pi\, p^a) = \Pi\, \phi(p^a)$, p prime ≥ 2.

II. THE PERIOD k OF x mod m

The period $k = \text{pd}(x \bmod m)$ is the <u>least</u> $k \geq 1$ for which $x^k \equiv 1 \bmod m$. Important properties of k are:

A. $x, x^2, \ldots, x^k \equiv 1$ are distinct mod m, and form a cyclic subgroup $\{x\}$ of G(m).

B. $x^\ell \equiv 1 \bmod m$ iff $k \mid \ell$.

C. $\text{pd}(x^j \bmod m) = k/(j,k)$.

D. $\text{pd}(x^j \bmod m) = k$ iff $(j,k) = 1$. Thus there are $\phi(k)$ of the x^j which generate the group $\{x\}$ mod m.

III. THE GROUPS $G(p^a)$

In the special case $m = p^a$, p an odd prime, $G(p^a)$ is itself a cyclic group, i.e., there exists an integer g such that

$$G(p^a) = \{g, g^2, \ldots, g^{\phi(p^a)} \equiv 1\} \bmod p^a.$$

The set $H(p^a)$ of all its generators therefore contains $\phi[\phi(p^a)]$ elements.

This is also true for $m = 2^0, 2^1$, and 2^2. However, for $m = 2^a$, $a \geqq 3$, $G(2^a)$ is not cyclic, but consists of a cyclic subgroup C of order $(1/2)\phi(2^a) = 2^{a-2}$, and a single coset $D \equiv -C \bmod 2^a$.

IV. THE λ-FUNCTION

Motivated by this anomaly, a function $\lambda(m)$ is defined by $\lambda(1) = 1$, and

$$\lambda(p_1^{a_1} \ldots p_\ell^{a_\ell}) = \text{l.c.m.}[\lambda(p_1^{a_1}), \ldots, \lambda(p_\ell^{a_\ell})],$$

where $\lambda(p^a) = \phi(p^a) = p^{a-1}(p-1)$, p odd prime;

$$\lambda(2) = \phi(2) = 1;\ \lambda(2^2) = \phi(2^2) = 2;\ \lambda(2^a) = (1/2)\phi(2^a) = 2^{a-2},$$

$a \geqslant 3$. The λ-function has the properties:

A. $x^{\lambda(m)} \equiv 1 \bmod m$ for all x of G(m).

B. There exists a g with pd(g mod m) = λ(m). Thus λ(m) is the greatest period possessed by any element of the group G(m), and all such periods divide λ(m).

C. G(m) is itself cyclic iff $\lambda(m) = \phi(m)$, i.e., m has one of the simple forms $m = 1, 2, 2^2, p^a$, or $2p^a$, p odd prime. This is easily inferred from the relations $\lambda(\Pi\, p^a) = \text{l.c.m.}[\lambda(p^a)]\ |\Pi\, \lambda(p^a)\ |\Pi\, \phi(p^a) = \phi(\Pi\, p^a)$.

V. THE CHINESE REMAINDER THEOREM

This is a very general theorem which implies that a system of congruences

$$g \equiv c_i \bmod p_i^{b_i};\ i = 1, \ldots, \ell$$

(p_i distinct primes $\geqslant 2$) has a unique solution $g_o \bmod \Pi\, p_i^{b_i}$, all solutions being of form $g = g_o + h\, \Pi\, p_i^{b_i}$.

VI. STRUCTURE OF THE GROUP G(m)

For a composite modulus $m = \Pi\, p_i^{a_i}$, the system of congruences

$$x \equiv x_i \bmod p_i^{a_i};\ i = 1,\ldots,\ell$$

induces a multiplicative isomorphism

$$x \longleftrightarrow (x_1,\ldots,x_\ell)$$

between the group G(m) of $\phi(m)$ integers x prime to m, and the direct product of ℓ groups, the i'th being the group $G(p_i^{a_i})$ of the $\phi(p_i^{a_i})$ integers prime to p_i. Hence one has the relations

$$G(m) \cong G(p_1^{a_1}) \times \ldots \times G(p_\ell^{a_\ell}),$$

$$\phi(m) = \phi(p_1^{a_1}) \ldots \phi(p_\ell^{a_\ell}).$$

For odd p_i, $G(p_i^{a_i})$ is cyclic. If $2 \mid m$, the corresponding group $G(2^a)$ of $\phi(2^a) = 2^{a-1}$ odd integers is cyclic iff a = 1 or 2. Otherwise it has the structure $C \cup D$ referred to in part (III) above. Thus $\lambda(m)$ is the l.c.m. of the maximal periods obtaining in the groups $G(p_i^{a_i})$.

REFERENCES

1. H. Riesel, "Note on the congruence $a^{p-1} \equiv 1(p^2)$," Mathematics of Computation 18, 149-150 (1964).

2. J. C. P. Miller and A. E. Western, Tables of Indices of Primitive Roots, (Cambridge University Press, New York, 1968).

☆ U.S. GOVERNMENT PRINTING OFFICE 1977—777-018/3