STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1954- 19.2

Periodicity pfoperties of some recurring sets of integers

H.J.A. Duparc

Abstract from the Proceedings of the International Mathematical Congress, Amsterdam, Sept. 1954

1954

Abstract from the Proceedings of the International Mathematical Congress Amsterdam, Sept. 1954.

PERIODICITY PROPERTIES OF SOME RECURRING SETS OF INTEGERS

H. J. A. Duparc

Consider sets of integers (u_n, v_n) $(n = 0, 1, \ldots)$ satisfying the relations

$$(1) \qquad Uu_n = Vv_n, \quad 0 \leqq u_n < m \quad (n = 0, 1, \ldots),$$

where m is a fixed given positive integer and where

$$U = U(E) = \sum_{h=0}^{s} c_h E^h \quad \text{and} \quad V = V(E) = \sum_{k=0}^{t} d_k E^k$$

are polynomials with integer coefficients in the operator E which transforms any u_n into u_{n+1} and any v_n into v_{n+1}.

Let the operators U and V satisfy the following conditions:

I. $c_s = \pm 1$; $d_t = m$;

II. U and V are relatively prime;

III. $V(X)$ has no roots with absolute value $\geqq 1$.

The condition I assures the possibility of determining u_n (for $n \geqq s$) and v_n (for $n \geqq t$) uniquely, once the preceding elements of the sequences (u_n) and (v_n) are known.

Since Uu_n is bounded, by (1) and by condition III also the sequence (v_n) is bounded. Consequently each of the sequences (u_n), (v_n) and (u_n, v_n) is periodic.

By condition III it follows after a little argument that (u_n) and (u_n, v_n) have the same period C. In case U is relatively prime to every cyclotomic polynomial in E, the sequence (v_n) also has the period C.

By condition II there exists an integer $M \neq 0$ (the resultant of U and V) and polynomials P and Q in E with integer coefficients such that

$$M = PU + QV.$$

Putting

$$(2) \qquad a_n = Pv_n + Qu_n \quad (n = 0, 1, \ldots)$$

one finds for $n = 0, 1, \ldots$

$$(3) \qquad Ua_n = UPv_n + QUu_n = UPv_n + QVv_n = Mv_n$$

and similarly

$$(4) \qquad Va_n = Mu_n.$$

From (2) and (4) it follows that the sequence (a_n) also has the period C. Further from (3) and (4) it follows that C is a common multiple of the periods mod M of the recurring sequences of which the characteristic polynomials are U and V respectively. Under some restrictions these periods are equal to the periods $C(U, M)$ and $C(V, M)$ of E modd $U(E)$, M and modd $V(E), M$ respectively. [1]

In some cases more can be said about C.

A. If $V = m$, then $M = m$ and one obtains again wellknown results on the period mod m of the recurring sequence $Uu_n = 0$. If moreover $U = -E + g$ one obtains the wellknown result that the repeated fraction found by conversion of u_0/m (with $(u_0, m) = 1$) into the number system of the base g is equal to the exponent of g mod m.

B. If $V = mE - d$, where $0 < d < m$, then it can be proved that under the above restrictions (which here require $(m, M) = (d, M) = 1$) the period C is equal to the exponent of md^{-1} mod M', where $M' = M/(a_0, M)$.

C. Many interesting further applications can be given to other cases which can be realised by some simple cyclic shifting circuits.

---

[1] Cf. e.g. H. J. A. Duparc, Divisibility properties of recurring sequences, p. 48, thesis Amsterdam, 1953.

MATHEMATISCH CENTRUM,
2E BOERHAAVESTRAAT 49,
AMSTERDAM.