KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN – AMSTERDAM
Reprinted from Proceedings, Series A, **57**, No. 3 and Indag. Math., **16**, No. 3, 1954

MATHEMATICS

PERIODICITY PROPERTIES OF RECURRING SEQUENCES. I

BY

H. J. A. DUPARC

(Communicated by Prof. J. F. Koksma at the meeting of April 24, 1954)

Introduction

In his thesis "Divisibility properties of recurring sequences" (Amsterdam, 1953) the author considered recurring sequences the elements of which belong to a kind of sets which in some way are connected to sets which he called *ff*-sets. In this paper, however, which mnst be considered as an introduction to a further paper on periodicity properties of sets of recurring sequences, in view of this application only recurring sequences are treated the elements of which belong to *ff*-sets. For the more general kind of sequences the reader is referred to the thesis, in only the last section of which such sequences occur essentially.

Very simple proofs and arguments are omitted in this paper. They can be found in the thesis.

In deriving the properties which connect those of chapter I where the necessary algebraic properties are developed and those of the recurring sequences, in the first section of chapter II another much simpler method is followed than in the thesis. This method (using the well-known shift-operator E) will also be used in the above-mentioned paper on sets of recurring sequences.

Chapter 1. General algebraic properties

Section 1. On *ff*-sets

An *ff*-set is a set with the following properties:

I. The set is a unique factorization domain, i.e. a commutative ring with a unit element e in which every element possesses a canonical decomposition into prime elements;

II. If m is an element of the set the residue set mod m of the set is finite, i.e. that residue set has only a finite number of elements.

Since in a unique factorization domain R the ideal (p) generated by a prime element of the domain R is divisorless, the residue set $R/(p)$ is an integral domain and since a finite integral domain is a field, one has

Theorem 1. *If p is a prime-element of an ff-set R, then the residue set $R/(p)$ is a field.*

By a well-known property on finite fields the number M of elements of the field is a positive integral power P^Q of a prime number P, where both $P=P(R, p)$ and $Q=Q(R, p)$ depend on R and p.

Since $R/(p)$ is a field, to every element q of R, not divisible by p, an element q_1 corresponds such that $q_1 q \equiv e \pmod{p}$. It is not difficult to prove that there also exists an element q_n in R such that $q_n q \equiv e \pmod{p^n}$, where n is a positive integer.

Further one easily deduces that the residue set $R/(p^n)$ possesses M^n elements, hence in the above notation

$$P(R, p^n) = P(R, p);\; Q(R, p^n) = nQ(R, p).$$

Definition. If m is an element of an *ff*-set R, the set of those elements of $R/(m)$ which are relatively prime to m is called the reduced residue set mod m of R.

The reduced residue set mod m of R will be denoted by $R//(m)$. From the above remarks it follows that if p is a prime element of an *ff*-set R, then the set $R//(p^n)$ is a multiplicative group with

$$\Phi_R(p^n) = M^n - M^{n-1} = P^{(n-1)Q}(P^Q - 1)$$

elements.

Also in the case m is an arbitrary element of the *ff*-set R a similar result holds. This result of which the proof may be omitted is formulated by

Theorem 2. *If m is an element of an ff-set R, then the set $R//(m)$ is a finite multiplicative group with*

$$\Phi_R(m) = \prod_{\substack{p^n | m \\ p^{n+1} \nmid m}} P(R, p)^{(n-1)\,Q(R,p)}\,(P(R, p)^{Q(R,p)} - 1)$$

elements.

Finally it is not difficult to prove that one has

Theorem 3. (Chinese remainder theorem). *If $m_1, \ldots, m_s$ are pairwise coprime elements of an ff-set R, then for any set $u_1, \ldots, u_s$ of elements of R there exists an element u of R such that*

$$u \equiv u_\sigma \pmod{m_\sigma} \qquad (\sigma = 1, \ldots, s).$$

Section 2. Extensions of *ff*-sets

In this section R denotes an *ff*-set.

If m denotes an element $\neq 0$ of R, the sets

$$R[x],\; R_0 = R/(m) \text{ and } R_0[x] = R[x]/(m)$$

are considered. The homomorphism $R \sim R_0$ induces a homomorphism $R[x] \sim R_0[x]$, hence to every element (polynomial) $g(x)$ of $R[x]$ corresponds one polynomial $g_0(x)$ of $R_0[x]$.

Theorem 4. *If p is a prime element of R, then $R_0[x] = R[x]/(p)$ is an ff-set.*

Proof. By theorem 1 the set $R/(p)$ is a commutative field, thus by some well-known theorems $R[x]/(p)$ is a commutative euclidean ring, hence a principal ideal ring, hence a unique factorization ring.

Further let $f_0(x)$ denote an arbitrary prime element (i.e. irreducible polynomial) of $R_0[x]$, which is of a degree N in x. Then the elements of $R_1[x] = R_0[x]/(f_0(x))$ can be represented by the polynomials of a degree[1])

[1]) Here and in future for the sake of simplicity the degree of the polynomial 0 is taken $-\infty$.

$\leqq N-1$ of $R_0[x]$ (viz. by the uniquely defined remainders of a degree $\leqq N-1$ obtained after division of such a polynomial by $f_0(x)$). Since each of the N coefficients of these remainders can assume only

$$M(R, p) = P(R, p)^{Q(R,p)}$$

values, the set $R_1[x]$ has exactly M^N, i.e. a finite number of elements.

Corollary. By theorem 1, applied to the ff-set $R_0[x]$, one finds that the set $R_0[x]/(f_0(x))$, where $f_0(x)$ is irreducible in $R_0[x]$, is a field,

Definition. A polynomial of $R[x]$ is called monic if the coefficient of its highest power term in x is equal to the unit element e of R.

Definition. If m belongs to R and $f(x)$ to $R[x]$, but not to R, then one writes

$$g(x) \equiv h(x) \pmod{\text{d}\ f(x), m}$$

if and only if in $R[x]$ the polynomial $g(x)-h(x)$ belongs to the ideal $(f(x), m)$ generated by $f(x)$ and m.

Definition. If $f(x)$ (of degree N in x) and $g(x)$ belong to $R[x]$, then the residue mod $f(x)$ of $g(x)$ is the uniquely determined polynomial $r(x)$ of a degree $\leqq N-1$ such that

$$g(x) \equiv r(x) \pmod{f(x)}.$$

Theorem 5. *One has*

$$g(x) \equiv 0 \quad (\text{modd } f(x), m) \tag{1}$$

if and only if the residue $r(x)$ mod $f(x)$ of $g(x)$ is divisible by m (i.e. if each of the coefficients of this residue $r(x)$ is divisible by m).

Proof. If (1) holds there exist polynomials $q(x)$ and $s(x)$ in $R[x]$ such that

$$g(x) = q(x)f(x)+m\, s(x).$$

Let $t(x)$ denote the residue mod $f(x)$ of $s(x)$. Then one has

$$g(x) \equiv m\, s(x) \equiv m\, t(x) \pmod{f(x)},$$

and the residue $r(x) = m\, t(x)$ mod $f(x)$ of $g(x)$ is divisible by m.

Conversely if m divides the residue $r(x)$ the relation (1) follows immediately.

The following two theorems may be mentioned without their simple proofs.

Theorem 6. *If $m \in R$, $m_1 \in R_1$, $m_1|m$ and $f(x) \in R[x]$, then*

$$(f(x), m_1)|(f(x), m).$$

Theorem 7. *If $m \in R$, if $f(x), f_1(x), f_2(x)$ belong to $R[x]$ and if*

$$f(x) \equiv f_1(x)f_2(x) \pmod{m},$$

then

$$(f_1(x), m)|(f(x), m).$$

Theorem 8. *If $m = m_1m_2\ldots m_s$, where $m_1, \ldots, m_s$ are pairwise coprime elements of R and if $f(x)$ is a monic polynomial of $R[x]$, then*

$$(f(x), m) = \prod_{\sigma=1}^{s} (f(x), m_\sigma).$$

Proof. Any element of $(f(x), m)$ belongs by theorem 6 to each of the s ideals $(f(x), m_\sigma)$ $(\sigma=1, \ldots, s)$. Conversely for any element $g(x)$ which belongs to each of these s ideals all coefficients of its residue mod $f(x)$ are divisible by each of the s pairwise coprime elements $m_1, \ldots, m_s$ of R, hence by their product m, Then by theorem 5 the polynomial $g(x)$ belongs to $(f(x), m)$.

Theorem 9. *If p is a prime element of R and if*

$$f(x) \equiv f_1(x) \ldots f_s(x) \quad (\mathrm{mod}\ p),$$

where $f_1(x), \ldots, f_s(x)$ are pairwise coprime elements of the ff-set

$$R_0[x] = R[x]/(p),$$

then

$$(f(x), p) = \prod_{\sigma=1}^{s} (f_\sigma(x), p).$$

Proof. By theorem 7 any polynomial which belongs to $(f(x), p)$ also belongs to each of the s ideals $(f_\sigma(x), p)$ $(\sigma=1, \ldots, s)$. Conversely let $g(x)$ belong to each of these s ideals. In the homomorphism $R[x] \sim R_0[x]$ let $g(x)$ correspond to $g_0(x)$, $f(x)$ to $f_0(x)$ and $f_\sigma(x)$ to $f_{\sigma 0}(x)$ $(\sigma=1, \ldots, s)$. Then one has

$$f_{\sigma 0}(x) | g_0(x) \quad (\sigma=1, \ldots, s).$$

By theorem 4 the set $R_0[x]$ is an ff-set, hence a unique factorization domain, thus $f_0(x) | g_0(x)$, i.e. $g(x) \in (f(x), p)$.

Section 3. Resultants

Let R be an integral domain. Then for any two elements $f(x)$ and $g(x)$ of $R[x]$ consider the resultant $T(f, g)$ of $f(x)$ and $g(x)$ with respect to x. This resultant belongs to R.

For resultants one has the following four well known properties which will be used later.

I. If f, g and h belong to $R[x]$, then

$$T(gh, f) = T(g, f)\, T(h, f).$$

II. If f, g and h belong to $R[x]$ and if m is an element of R, then from

$$g \equiv h \ (\mathrm{modd}\ f, m)$$

it follows that

$$T(g, f) \equiv T(h, f) \quad (\mathrm{mod}\ m).$$

III. For any f and g of $R[x]$ there exist elements q and s of $R[x]$ such that

$$T(f, g) = qf + sg.$$

Here without loss of generality it may be supposed that the degree of q is less than the degree of g and that the degree of s is less than the degree of f.

IV. If $r \in R$ and if $f(x)$ is a polynomial of degree N of $R[x]$, then

$$T(r, f) = r^N.$$

Definition. If m is an element of an ff-set R and if $f(x)$ is a monic polynomial of $R[x]$, then the set of elements $g(x)$ of $R[x]$ for which the resultant $T(f, g)$ and m are relatively prime, is called the reduced residue set modd $f(x), m$ of $R[x]$.

This reduced residue set will be denoted by

$$R[x]//(f(x), m).$$

Theorem 10. *If m is an element of an ff-set R and if $f(x)$ is monic in $R[x]$, then the set*

$$S=R[x]//(f(x), m)$$

is a multiplicative group.

Proof. Let g and h belong to S. Then by property II of resultants one has $T(gh, f)=T(g, f)\,T(h, f)$. Since both $T(g, f)$ and $T(h, f)$ are relatively prime to m, so is $T(gh, f)$, hence $gh \in S$.

Further if $g \in S$ then by property III of resultants an element q of $R[x]$ exists such that

$$t=T(g, f)=qg+sf,$$

and moreover t and m are relatively prime. Then for the element t_1 of R with $t_1 t \equiv e \pmod{m}$ one has

$$e \equiv t_1 t \equiv t_1 qg \;(\text{modd } f(x), m),$$

hence the inverse element $t_1 q$ of g in $R\,(f(x), m)$ is found and

$$T(t_1 q, f)\,T(g, f)=T(t_1 qg, f) \equiv T(e, f)=e \pmod{m}.$$

Thus $T(t_1 q, f)$ and m are relatively prime and $t_1 q \in S$,

Theorem 11. *For the set S introduced in the above theorem one has $x \in S$ if and only if $f(0)$ and m are relatively prime.*

Proof. From

$$f(x)=xq(x)+f(0),$$

where $q(x) \in R[x]$, one finds

$$T(x, f(x))=f(0),$$

whence follows the assertion.

Section 4. Periods

Theorem 12. *Every element r of an ff-set R which is not divisible by a prime element p of R satisfies*

$$r^{M-1} \equiv e \pmod{p};$$

here M denotes the integer $M(R, p)$ introduced in section 1.

Proof. By theorem 1 the elements $\neq 0$ of $R/(p)$ form a group with $M(R, p)-1$ elements, Then the assertion follows from a property of finite multiplicative groups.

Theorem 13. *If p is a prime element of an ff-set R, if $f(x)$ is a mod p irreducible polynomial of degree N of $R[x]$, then for any polynomial $g(x)$ not belonging to the ideal $(f(x), p)$ one has*

$$(g(x))^{M^N-1} \equiv e \quad (\text{modd } f(x), p).$$

Proof. In theorem 4 it was found that the set $R_1 = R_0[x]/(f(x))$ where $R_0 = R/(p)$ is a field with M^N elements. Since in the homomorphism $R[x] \sim R_1$ the element $g(x)$ of $R[x]$ does not correspond to the zero element of R_1, the assertion follows as before from a property of finite multiplicative groups.

Theorem 14. *Let p be a prime element of an ff-set R and k a positive integer. Then for polynomials $f(x)$, $g(x)$ and $h(x)$ of $R[x]$ satisfying*

$$g(x) \equiv h(x) \pmod{\text{d } f(x), p^k}$$

one has

$$(g(x))^P \equiv (h(x))^P \quad (\text{modd } f(x), p^{k+1});$$

here P denotes the integer $P(R, p)$, introduced in section 1.

Proof. By assumption there exists a polynomial $r(x)$ of $R[x]$ such that

$$g(x) \equiv h(x) + p^k r(x) \quad (\text{mod } f(x)).$$

Hence

$$(g(x))^P \equiv (h(x) + p^k r(x))^P \quad (\text{mod } f(x))$$

and by the binomial theorem the right hand side of the last relation can be written in the form

$$(h(x))^P + P(h(x))^{P-1} p^k r(x) + p^{2k} s(x),$$

where $s(x)$ is a suitably chosen element of $R[x]$. Since $R/(p)$ is an additive group with P elements one has in R

$$Pe \equiv 0 \quad (\text{mod } p),$$

hence on account of $2k \geqq k+1$

$$(g(x))^P \equiv (h(x))^P \quad (\text{modd } f(x), p^{k+1}).$$

In a similar way one can prove

Theorem 15. *Let p be a prime element of an ff-set R and k a positive integer. Then for polynomials $f(x)$, $g(x)$ and $h(x)$ of $R[x]$ satisfying*

$$g(x) \equiv h(x) \quad (\text{modd } (f(x))^k, p)$$

one has

$$(g(x))^P \equiv (h(x))^P \quad (\text{modd } (f(x))^{kP}, p).$$

Theorem 16. *If p is a prime element of an ff-set R, if $f(x)$ is an irreducible polynomial of degree N of $R[x]/(p)$, then for every polynomial $g(x)$ not belonging to the ideal $(f(x), p)$ one has*

$$(g(x))^{P^{k-1}(M^N-1)} \equiv e \quad (\text{modd } f(x), p^k).$$

Proof. This property immediately follows from the theorems 13 and 14.

Theorem 17, *If p is a prime element of an ff-set R and if $f(x)$ is an irreducible polynomial of degree N of $R[x]/(p)$, then*

$$x^{M^N-1} \equiv e \quad (\text{modd } f(x), p);$$

$$x^{M^n-1} \not\equiv e \quad (\text{modd } f(x), p) \quad (n = 1, 2, \ldots, N-1).$$

Proof. Since x does not belong to the ideal $(f(x), p)$ the first assertion holds by theorem 13.

Further suppose that for some positive $n<N$

$$x^{M^n-1} \equiv e \quad (\text{modd } f(x), p).$$

Using the relation

$$(a+b)^{P^n} \equiv a^{P^n}+b^{P^n} \quad (\text{mod } p)$$

(to be proved by induction on n) one finds for every polynomial

$$g(x) = \sum_{h=0}^{N-1} a_h x^h$$

of $R[x]$ the relation

$$(g(x))^{M^n} \equiv \sum_{h=0}^{N-1} a_h^{M^n} x^{hM^n} \quad (\text{mod } p).$$

By theorem 12 for $h=0, 1, \dots, N-1$ one has

$$a_h^{M^n} \equiv a_h \quad (\text{mod } p)$$

and from the assumption one gets

$$x^{hM^n} \equiv x^h \quad (\text{modd } f(x), p).$$

Consequently

$$(g(x))^{M^n} \equiv \sum_{h=0}^{N-1} a_h x^h = g(x) \quad (\text{modd } f(x), p)$$

and every element of $S=R[x]/(f(x), p)$ would be a root of the equation

$$X^{M^n}=X$$

in S. Then this equation of degree M^n would have M^N roots, which is impossible since $n<N$.

Theorem 18. *If p is a prime element of an ff-set R and if $f(x)$ is an irreducible polynomial of degree N of $R[x]/(p)$, then for every polynomial $g(x)$ not belonging to the ideal $(f(x), p)$ an element u of R exists such that*

$$(g(x))^n \equiv u \quad (\text{modd } f(x), p),$$

where $n=(M^N-1)/(M-1)$.

Proof. The $M-1$ different elements $u_1, \dots, u_{M-1} \neq 0$ of $R/(p)$ satisfy by theorem 12 the relation

$$X^{M-1}=e,$$

hence by the ordinary theory of equations in the field $R/(p)$ one has

$$X^{M-1}-e=(X-u_1) \dots (X-u_{M-1}).$$

Then in $R[x]/(p)$ one obtains taking $X=(g(x))^n$ (where $g(x)$ is an arbitrary element of $R[x]$ not belonging to $(f(x), p)$)

$$g^{M^N-1}-e=(g^n-u_1) \dots (g^n-u_{M-1}).$$

By theorem 13 one finds

$$(g^n-u_1), \dots, g^n-u_{M-1}) \equiv 0 \quad (\text{modd } f(x), p),$$

whence follows the assertion.

Corollary. *In particular one has*

$$x^{(M^N-1)/(M-1)} \equiv u \quad (\text{modd } f(x), p),$$

where u is a suitably chosen element of R.

Section 5. Periods with respect to U-sets

Definition, Let m be an element of an $\mathfrak{f}$-set R and $f(x)$ an element of $R[x]$. Then any multiplicative subgroup of the group $R[x]//(f(x), m)$ is called a U-set with respect to $f(x)$ and m, or shortly a U_{fm}-set.

Examples.

1. The set $R[x]//(f(x), m)$ itself;
2. the set $R//(m)$;
3. the set of unities of R;
4. the set E only consisting of the unit element e of R.

Definition. Let m be an element of an $\mathfrak{f}$-set, $f(x)$ be an element of $R[x]$ and U a U_{fm}-set. Then a positive integer d is called a period modd $f(x)$, m of a polynomial $g(x)$ of $R[x]$ with respect to U, if an element u of U exists such that

$$(g(x))^d \equiv u \pmod{d\ f(x), m}.$$

Obviously if such a period d exists also the smallest of such a period exists. This smallest period will be called the primitive period of g modd f, m with respect to U and will be denoted by $c_g(f, m; U)$.

In particular we shall write

$$c_x(f, m; U) = c(f, m; U);$$
$$c_g(f, m; E) = C_g(f, m); \quad c_g(f, m; R//(m)) = c_g(f, m);$$
$$c_x(f, m; E) = C(f, m); \quad c_x(f, m; R//(m)) = c(f, m).$$

Theorem 19. *Let m be an element of an $\mathfrak{f}$-set R, $f(x)$ and $g(x)$ belong to $R[x]$ and U a U_{fm}-set. If the primitive period $c = c_g(f, m; U)$ exists, then any multiple of c is a period modd $f(x)$, m of $g(x)$ with respect to U; conversely any period d modd $f(x)$, m of $g(x)$ with respect to U is a multiple of the primitive period c.*

Proof. If c exists an element u of U can be found such that

$$g^c \equiv u \quad (\text{modd } f(x), m)$$

hence for any positive integer k one has

$$g^{kc} \equiv u^k \quad (\text{modd } f(x), m),$$

where also u^k belongs to the U-set U; then the first assertion follows.

Conversely suppose there exists an element $v \in U$ such that

$$g^d \equiv v \quad (\text{modd } f(x), m).$$

Then the primitive period c exists and an element $u \in U$ can be found with

$$g^c \equiv u \quad (\text{modd } f(x), m).$$

Putting $d = qc + r$ where $0 \leqq r < c$ and q integer, one has

$$v \equiv g^d = g^{qc} g^r \equiv u^q g^r \quad (\text{modd } f(x), m).$$

Since U is an U_{fm}-set an element w of U exists such that

$$wu \equiv e \quad (\text{modd } f(x), m),$$

hence

$$g^r \equiv v w^q \quad (\text{modd } f(x), m).$$

Since $vw^q \in U$, also r is a period modd f, m of g with respect to U. From the minimality of c one gets $r=0$, hence $c|d$.

Theorem 20. *Let m and m_1 belong to an ff-set R and $f(x)$ and $f_1(x)$ to $R[x]$; further let U be a U_{fm}-set and U_1 a $U_{f_1m_1}$-set. Finally suppose*

$$(f(x), m)|(f_1(x), m_1) \text{ and } U_1 \subset U.$$

Then if $c_1=c_g(f_1, m_1; U_1)$ exists, also $c=c_g(f, m; U)$ exists and $c|c_1$.

Proof. The assertion follows after a little argument from theorem 19.

Theorem 21. *If $C=C_g(f, m)$ exists, then $c=c_g(f, m)$ exists and $c|C$.*

Proof. The result follows from the preceding theorem using the fact that $E \subset U=R//(m)$.

Definition. $v_g(f, m)=C_g(f, m)/c_g(f, m)$.

By the preceding theorem $v_g(f, m)$ is a positive integer.

Theorem 22. *If p is a prime element of R, then*

$$c=c(f, p; U)|c(f, p^k; U)|P^{k-1}\, c(f, p; U).$$

Proof. For $k=1$ the assertion is obvious. Further assume the assertion proved for some integer $k \geqq 1$, i.e. there exists an element u of U such that

$$g^d_2 \equiv u \quad (\text{modd } f, p^k),$$

where $d=c(f, p^k; U)$ satisfies $d|P^{k-1}c$. Then by theorem 14 one deduces

$$g^{Pd} \equiv u^P \quad (\text{modd } f, p^{k+1}),$$

hence using theorem 19

$$c(f, p^{k+1}; U)|Pd|P^k c,$$

whence follows the assertion.

Theorem 23. *If p is a prime element of R and if $f(x)$ is irreducible mod p, then*

$$c=c(f, p; U)|c(f^k, p; U)|P^t c,$$

where t is the smallest integer $\geqq 0$ with $P^t \geqq k$.

Proof. For all k with $t=0$ the assertion is obvious. Now suppose $t \geqq 0$ and the theorem proved for all positive integers $\leqq P^t$. Let further k be an integer satisfying $P^t<k \leqq P^{t+1}$; then one has

$$g^d \equiv u \quad (\text{modd } f^{P^t}. p),$$

where u is a suitably chosen element of U and $c|d|P^t c$. By theorem 15 one concludes

$$g^{Pd} \equiv u^P \quad (\text{modd } f^{P^{t+1}}, p),$$

hence, also using theorem 19 and 20,

$$c|c(f^k, p; U)|c(f^{P^{t+1}}, p; U)|Pd|P^{t+1}c.$$

Theorem 24. *If $m=m_1 \dots m_s$, where $m_1, \dots, m_s$ are pairwise coprime elements of R, if further U is a U_{fm_σ} $(\sigma=1, \dots, s)$-set and if finally the periods*

$$c_\sigma=c_g(f, m_\sigma; U) \qquad (\sigma=1, \dots, s)$$

exist, then also the period $c=c_g(f, m; U)$ exists and c is equal to the least common multiple d of $c_1, \dots, c_s$.

Proof. From

$$g^{c_\sigma} \equiv u_\sigma \quad (\text{modd } f(x), m) \qquad (\sigma = 1, \ldots, s)$$

it follows for $\sigma = 1, \ldots, s$, putting $d_\sigma = d/c_\sigma$

$$g^d \equiv u_\sigma^{d_\sigma} \quad (\text{modd } f(x), m_\sigma).$$

Now by the chinese remainder theorem an element w of U exists with

$$w \equiv u_\sigma^{d_\sigma} \quad (\text{modd } m_\sigma) \qquad (\sigma = 1, \ldots, s),$$

hence

$$g^d \equiv w \quad (\text{modd } f(x), m_\sigma) \qquad (\sigma = 1, \ldots, s)$$

and by theorem 8

$$g^d \equiv w \quad (\text{modd } f(x), m).$$

Thus $c = c_g(f, m; U)$ exists and $c|d$.

Further from

$$g^c \equiv u \quad (\text{modd } f(x), m)$$

with theorem 20 one deduces $c_\sigma|c$ for $\sigma = 1, \ldots, s$, hence $d|c$. Consequently $c = d$.

Theorem 25. *Let p be a prime element of R and suppose*

$$f(x) \equiv f_1(x) \ldots f_s(x) \quad (\text{mod } p),$$

where $f_1(x), \ldots, f_s(x)$ are pairwise coprime elements of $R[x]/(p)$. Let for $\sigma = 1, \ldots, s$ the set U be a $U_{f_\sigma p}$-set and let the period $c_\sigma = c_g(f_\sigma, p; U)$ exist. Then also the period $c = c_g(f, p; U)$ exists and if d denotes the least common multiple of $c_1, \ldots, c_s$ one has

$$d|c|c_g(f, p; E)|bd;$$

here b denotes the number of elements of U.

Proof. For $\sigma = 1, \ldots, s$ from

$$g^{c_\sigma} \equiv u_\sigma \quad (\text{modd } f_\sigma(x), p) \qquad (u_\sigma \in U)$$

it follows putting $d_\sigma = d/c_\sigma$

$$g^d \equiv u_\sigma^{d_\sigma} \quad (\text{modd } f_\sigma(x), p).$$

hence since the group U has b elements

$$g^{bd} \equiv e \quad (\text{modd } f_\sigma(x), p)$$

and by theorem 9

$$g^{bd} \equiv e \quad (\text{modd } f(x), p).$$

Then $c = c_g(f, p; U)$ exists and by theorem 20 one deduces

$$c|c_g(f, p; E)|bd.$$

The further result $d|c$ follows in a similar way as in the proof of the preceding theorem.

Corollary. In the case $U = E$ one has $b = 1$, hence $c = d$.

Theorem 26. *The integer $v = v_g(f, m)$ is equal to the exponent q mod m of the residue u modd $f(x)$, m of g^c, where $c = c_g(f, m)$.*

Proof. From

$$g^c \equiv u \quad (\text{modd } f(x), m)$$

it follows

$$g^{qc} \equiv u^q \equiv e \quad (\text{modd } f(x), m),$$

hence $C = C_g(f, m) | cq$ and $v | q$.

Further

$$e \equiv g^C = g^{vc} \equiv u^v \quad (\text{modd } f(x), m),$$

hence $q | v$. Consequently $q = v$.

Theorem 27. *Let R be an arbitrary commutative ring with a unit element and let $f(x)$ denote a monic polynomial of degree N in $R[x]$. Then if a positive integer c and an element u of R satisfy*

(1) $$x^c \equiv u \quad (\text{mod } f(x)),$$

one has

$$((-)^N f(0))^c = u^N.$$

Proof. For $N = 1$ one has $f(x) = x - r$ where $r \in R$. Then from (1) by taking $x = r$ the required result follows.

Now suppose the theorem holds for all monic polynomials of degree $\leqq N-1$, the coefficients of which belong to an arbitrary commutative ring with a unit element.

By assumption a polynomial $q(x)$ of $R[x]$ exists such that

$$x^c = u + q(x)\, f(x).$$

Consider the ring $S = R[x, y]/(f(y))$. Put

(2) $$f(x) - f(y) = (x-y)\, g(x, y) = (x-y)\, h(x),$$

where $h(x)$ is a monic polynomial of degree $N-1$ in x with coefficients in $R[y]$. Then

$$x^c = u + q(x)\, f(y) + (x-y)\, q(x)\, h(x)$$

and in S one has

$$x^c \equiv u \quad (\text{mod } h(x)).$$

By the above induction hypothesis one concludes in S

$$((-)^{N-1}\, h(0))^c = u^{N-1}.$$

Further by (1) one has in S the relation $y^c = u$, hence

$$((-)^{N-1} y\, h(0))^c = u^N.$$

Finally (2) gives for $x = 0$ in S the result $f(0) = -yh(0)$, hence

$$((-)^N f(0))^c = u^N.$$

Since neither of the sides of this relation depends on y, it holds not only in S, but also in R.

Theorem 28. *Let m be an element of an ff-set R and $f(x)$ denote a polynomial of degree N of $R[x]$. Then for $c = c(f, m)$ and $v = v(f, m)$ one has*

$$\frac{\varepsilon}{(\varepsilon, c)} \,\Big|\, v \,\Big|\, \frac{N\varepsilon}{(\varepsilon, c)},$$

where ε denotes the exponent mod m of $a = (-)^N f(0)$.

Proof. From

$$x^c \equiv u \quad (\text{modd } f(x), m)$$

by the preceding theorem one gets

$$a^c \equiv u^N \quad (\text{mod } m),$$

hence

$$u^{N\varepsilon/(\varepsilon,c)} \equiv a^{c\varepsilon/(\varepsilon,c)} \equiv e^{c/(\varepsilon,c)} = e \quad (\text{mod } m),$$

thus by theorem 26

$$v \,\Big|\, \frac{N\varepsilon}{(\varepsilon,c)}.$$

Further for $C = C(f, m)$ one has using theorem 26 and 27

$$a^C = a^{vc} \equiv u^{vN} \equiv e^N = e \quad (\text{mod } m),$$

hence $\varepsilon | C$. Also one has $c | C$, hence $\{\varepsilon, c\} | C$, i.e. $\frac{c\,\varepsilon}{(\varepsilon, c)} \Big| cv$, thus

$$\frac{\varepsilon}{(\varepsilon,c)} \,\Big|\, v.$$

For a further result the symbol $B_q(m)$ is introduced, denoting the number of prime factors q in the positive integer m.

Theorem 29. *If a prime factor q of the degree N of $f(x)$ satisfies $B_q(\varepsilon) > B_q(c)$, where ε, $c = c(f, m)$ and m have the same meaning as in the preceding theorem, then*

$$\frac{\varepsilon q}{(\varepsilon,c)} \,\Big|\, v \,\Big|\, \frac{\varepsilon N}{(\varepsilon,c)}.$$

Proof. Since $B_q(\varepsilon) > 0$ one may put $\varepsilon = qd$, where d is a positive integer. Further put $N = qn$. Then by theorem 26 and 27 one has

$$u^v \equiv 1 \ (\text{mod } m), \qquad u^N \equiv a^c \ (\text{mod } m).$$

By theorem 28 the number b defined by $v = \varepsilon b/(\varepsilon, c)$ is integer. In virtue of $B_q(\varepsilon) > B_q(c)$ also $d/(\varepsilon, c) = \varepsilon/q\,(\varepsilon, c)$ is integer. Hence

$$1 \equiv u^{vn} = u^{\frac{\varepsilon b}{(\varepsilon,c)}\frac{N}{q}} = u^{N\frac{db}{(\varepsilon,c)}} \equiv a^{c\frac{db}{(\varepsilon,c)}} \quad (\text{mod } m),$$

thus by definition of ε one has $\varepsilon \Big| \frac{cdb}{(\varepsilon, c)}$ hence $q \Big| \frac{cb}{(\varepsilon, c)}$. Since $B_q(c) = B_q(\varepsilon, c)$ the last result gives $q | b$, consequently

$$\frac{\varepsilon q}{(\varepsilon,c)} \,\Big|\, v.$$

Corollary. If $a = (-)^N f(0) = e$, then $\varepsilon = 1$ and one obtains $q | v | N$. If, however, $a = -e$, then $\varepsilon = 2$. If moreover c is odd, one obtains $2q | v | 2N$, if, however, c is even, then $q | v | N$.

Mathematical Centre, Amsterdam.

KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN - AMSTERDAM
Reprinted from Proceedings, Series A, **57**, No. 4 and Indag. Math., **16**, No. 4, 1954

MATHEMATICS

PERIODICITY PROPERTIES OF RECURRING SEQUENCES. II

BY

H. J. A. DUPARC

(Communicated by Prof. J. F. KOKSMA at the meeting of May 29, 1954)

Chapter II. Recurring sequences

SECTION 1. GENERAL PROPERTIES

Consider a sequence $w_0, w_1, \dots$ satisfying

$$w_{n+N} = \sum_{h=1}^{N} a_h\, w_{n+N-h} \qquad (n = 0, 1, \dots), \tag{1}$$

where $w_0, \dots, w_{N-1}, a_1, \dots, a_N$ are arbitrary elements of an $\mathfrak{ff}$-set R.

In order to investigate properties of the sequence introduce the polynomial

$$f(x) = x^N - \sum_{h=1}^{N} a_h\, x^{N-h},$$

which is called the characteristic polynomial of the sequence. Let E be the operator which transforms any element w_n of the considered sequence into w_{n+1} $(n=0, 1, \dots)$ i.e. $Ew_n = w_{n+1}$. Then (1) may be written in the form

$$f(E)\, w_n = 0 \qquad (n = 0, 1, \dots). \tag{2}$$

Unless stated otherwise the integer n may assume all values $n=0, 1, \dots$.

Further introduce the polynomial $A_n(x)$ of $R[x]$ by

$$A_n(x) = \frac{f(x)-f(E)}{x-E}\, w_n\, ;$$

here first the expression $(f(x)-f(E))/(x-E)$ has to be written as a polynomial in x and E and this polynomial (operator) has to be applied to w_n. Obviously the polynomial $A_n(x)$ is of a degree $\leqq N-1$ in x.

Theorem 30. *One has*

$$x^n A_0(x) \equiv A_n(x) \qquad (\text{mod } f(x)).$$

Proof. For $n=0$ the assertion is obvious. Now suppose it holds for some integer $n \geqq 0$. Then one has using (2)

$$\begin{aligned} x^{n+1} A_0(x) &= x \cdot x^n A_0(x) \equiv x\, A_n(x) = (x-E+E)\, \frac{f(x)-f(E)}{x-E}\, w_n \\ &= f(x)\, w_n - f(E)\, w_n + \frac{f(x)-f(E)}{x-E}\, E\, w_n \\ &\equiv \frac{f(x)-f(E)}{x-E}\, w_{n+1} = A_{n+1}(x) \quad (\text{mod } f(x)). \end{aligned}$$

Definition. If m is an element of R and U a U_{fm}-set, then any positive integer d for which an integer $n_m \geqq 0$ and an element u of U exist such that

$$w_{n+d} \equiv u w_n \pmod{m} \qquad (n = n_m, n_m + 1, \dots)$$

is called a period mod m with respect to U of the recurring sequence. The smallest such positive integer is called the (primitive) period mod m with respect to U of the sequence.

Theorem 31. *If c is the primitive period mod m with respect to the U_{fm}-set U of the recurring sequence, then any multiple of c is a period mod m with respect to U of the sequence. Conversely any period d mod m with respect to U of the sequence is a multiple of the primitive period c.*

Proof. By the definition of c an element u of U exists such that

$$(3) \qquad E^c w_n \equiv u w_n \pmod{m} \qquad (n = n_m, n_m + 1, \dots),$$

hence if k is a positive integer one gets for these values of n

$$E^{kc} w_n \equiv u^k w_n \pmod{m}.$$

Since also $u^k \in U$ the number kc is a period mod m with respect to U of the sequence.

Conversely let d be such a period. Then an element u_1 of U exists such that

$$E^d w_n \equiv u_1 w_n \pmod{m} \qquad (n = n'_m, n'_m + 1, \dots).$$

Putting $d = qc + r$ where $0 \leqq r < c$ and q is integer one finds using (3) for $n = n''_m, n''_m + 1, \dots,$ where $n''_m = \max(n_m, n'_m)$

$$u_1 w_n \equiv E^d w_n = E^r E^{qc} w_n \equiv E^r u^q w_n = u^q E^r w_n \pmod{m}.$$

Since U is a group an element u_2 of U exists such that

$$u u_2 \equiv e \pmod{f(x), m},$$

hence

$$E^r w_n \equiv u_2^q u_1 w_n \pmod{m} \qquad (n = n''_m, n''_m + 1, \dots).$$

Since $u_2^q u_1 \in U$ from the minimum property of c it follows that $r = 0$, hence $c|d$.

Theorem 32. *Let t denote the resultant of $A_0(x)$ and $f(x)$. If $f(0)$ and m are relatively prime, the period d mod m with respect to the U_{fm}-set U of the recurring sequence satisfies $c'|d|c$, where $c = c(f, m; U)$ and $c' = c(f, m'; U)$ with $m' = m/(t, m)$.*

Proof. By a wellknown property of resultants there exist polynomials $q(x)$ and $r(x)$ in $R[x]$ *such that*

$$t = q(x)\, A_0(x) + r(x)\, f(x),$$

hence

$$t \equiv q(x)\, A_0(x) \pmod{f(x)}.$$

Now by the definition of d there exists an element u of U such that

$$(E^d-u)\,w_n \equiv 0 \pmod{m} \quad (n=n_m,\, n_m+1,\, \ldots),$$

hence

$$(E^d-u)\,\frac{f(x)-f(E)}{x-E}\,w_n \equiv 0 \pmod{m} \quad (n=n_m,\, n_m+1,\, \ldots\,).$$

Using theorem 30 and the relation (2) one deduces

$$(4)\quad \left\{\begin{aligned} &(x^d-u)\,x^n A_0(x) \equiv (x^d-u)\,A_n(x) = (x^d-u)\,\frac{f(x)-f(E)}{x-E}\,w_n \\ &\quad= \frac{x^d-E^d}{x-E}\,(f(x)-f(E))\,w_n = \frac{x^d-E^d}{x-E}\,f(x)\,w_n \equiv 0 \quad (\text{modd}\, f(x), m). \end{aligned}\right.$$

Further putting $f(x)=xh(x)+f(0)$, one has

$$xh(x) \equiv -f(0) \pmod{f(x)}$$

and after multiplication by $(h(x))^n q(x)$ the relation (4) becomes

$$tf(0)(x^d-u) \equiv 0 \quad (\text{modd}\ f(x),\, m).$$

Since $f(0)$ and m are relatively prime one finds

$$t(x^d-u) \equiv 0 \quad (\text{modd}\ f(x),\, m),$$

hence

$$x^d \equiv u \quad (\text{modd}\ f(x),\, m')$$

and consequently $c'|d$.

Further from the definition of c it follows that there exist polynomials $a(E)$ and $b(E)$ of $R[E]$ and an element u of U such that

$$E^c = u + a(E)f(E) + mb(E),$$

hence using (2)

$$E^c w_n = uw_n + mb(E)w_n \equiv uw_n \pmod{m},$$

consequently

$$w_{n+c} \equiv uw_n \pmod{m}$$

and $d|c$.

Corollary. In the case $(t, m)=1$ one has $m'=m$ and $c=d$.

Then the period mod m with respect to U of the sequence is equal to the exponent $c(f, m; U)$.

Definition. An element m of R is called exceptional for a recurring sequence with characteristic polynomial $f(x)$ if at least one of the following properties holds:

1°: $f(0)$ and m are not relatively prime;

2°: the resultant t of $f(x)$ and $A_0(x)$ and the element m are not relatively prime.

All other elements of R are called nonexceptional for the sequence.

The result of the corollary to the preceding theorem may now be formulated as follows:

If m is non-exceptional for a recurring sequence with characteristic poly-

nomial $f(x)$, then the period mod m of the sequence with respect to a U_{fm}-set U is equal to the exponent $c(f, m; U)$.

In particular taking moreover $U = E$ and $U = R//(m)$ one finds the results:

The period mod m of the sequence is equal to $C(f, m)$; the period mod m with respect to the set $R//(m)$ of the sequence is equal to $c(f, m)$.

Finally for linear $f(x)$ one derives easily the wellknown property: *The period mod m of the sequence is equal to $c(f, m')$, where $m' = m/(w_0, m)$.*

For $f(x)$ of a degree $\geqq 2$ no such simple result holds. Then one has to use theorem 32 and in order to find a further result on the periods of the sequence one has to consider the exceptional primes of m separately.

Section 2. Recurring sequences of rational integers

The above results are now applied to the case R is the ff-set of rational integers. Then one has

$$P = P(R, p) = p;\; Q = Q(R, p) = 1.$$

For a recurring sequence satisfying

$$f(E) w_n = 0 \quad (n = 0, 1, \ldots),$$

where

$$f(E) = x^N - \sum_{h=1}^{N} a_h\, x^{N-h},$$

as before the exceptional primes are either divisors of $f(0) = -a_N$ or divisors of the resultant t of $A_0(x)$ and $f(x)$; here $A_0(x)$ has the same meaning as in the preceding section. Unless stated otherwise it is supposed that the numbers m, modulo which the sequence will be considered, have no exceptional prime factors.

With respect to the U-sets E and $R//(m)$ by theorem 32 the periods mod m of the sequence are equal to $C(f, m)$ and $c(f, m)$ respectively.

For the numbers $C(f, m)$ and $c(f, m)$ by the theorems 18, 17, 23, 25, 22 and 24 one has

Theorem 33. *If $f(x)$ is irreducible mod p, where p is a prime number then*

$$c(f, p) | (p^N - 1)/(p - 1),\; C(f, p) | p^N - 1,\; C(f, p) \nmid p^n - 1 \quad (n = 1, \ldots, N-1)$$
$$c(f, p) | c(f^h, p) | p^t c(f, p),\; C(f, p) | C(f^h, p) | p^t C(f, p);$$

here t denotes the smallest integer $\geqq 0$ with $p^t \geqq h$.

If

$$f(x) \equiv (f_1(x))^{r_1} \ldots (f_s(x))^{r_s} \quad (\text{mod } p),$$

where $f_1(x), \ldots, f_s(x)$ are pairwise coprime polynomials of $R/(p)$, then for the lowest common multiples

$$c = \{c(g_1^{r_1}, p), \ldots, c(g_s^{r_s}, p)\} \textit{ and } C = \{C(g_1^{r_1}, p), \ldots, C(g_s^{r_s}, p)\}$$

one has

$$c|c(f,\, p)|(p-1)c;\ C=C(f,\, p).$$

Further

$$c(f,\, p)|c(f,\, p^h)|p^{h-1}\, c(f,\, p);\ C(f,\, p)|C(f,\, p^h)|p^{h-1}\, C(f,\, p).$$

Finally if $m=p_1^{r_1}\dots p_s^{r_s}$, *where* $p_1, \dots, p_s$ *are different prime numbers, then*

$$c(f,\, m)=\{c(f,\, p_1^{r_1}),\ \dots,\ c(f,\, p_s^{r_s})\}\ \textit{and}\ C(f,\, m)=\{C(f,\, p_1^{r_1}),\ \dots,\ C(f,\, p_s^{r_s})\}.$$

For the set R considered in this section the results on $c(f, p^h)$, $C(f, p^h)$, $c(f^h, p)$ and $C(f^h, p)$ can be ameliorated.

Theorem 34. *Let* p *be an odd prime and* U *a* U_{fp}*-set. If the residue* u *belonging to* U *of* x^c *mod* $f(x)$ *satisfies*

$$x^c \equiv u \ (\text{modd } f,\, p^k);\ x^c \not\equiv u \ (\text{modd } f,\, p^{k+1}),$$

then

$$c(f, p^h; U) = \begin{cases} c \ \text{if } h=1,\dots,k; \\ p^{h-k}c \ \text{if } h=k+1, k+2, \dots \end{cases}$$

Proof. First the following auxiliary property is proved for $h=k$, $k+1, \dots$:

$$(1) \qquad x^{p^{h-k}c} \equiv u^{p^{h-k}} \ (\text{modd } f,\, p^h)\ ;\ x^{p^{h-k}c} \not\equiv w \ (\text{modd } f,\, p^{h+1})$$

for all $w \in U$.

In fact this property holds for $h=k$. Now if it holds for some integer $h \geqq k$, one has

$$x^{p^{h-k}c} \equiv u_1 + p^h r(x) \quad (\text{mod } f(x)),$$

where $u_1 = u^{p^{h-k}}$ and $r(x) \in R[x]$. By theorem 5 one has $p \nmid r(x)$. Using the binomial theorem one gets

$$x^{p^{h-k+1}c} \equiv (u_1 + p^h r(x))^p \equiv u_1^p + p^{h+1} u_1^{p-1} r(x) \quad (\text{modd } f(x),\, p^{h+2}).$$

Since $u_1 \in U = R//(p)$ one has $p \nmid u_1$; since also $p \nmid r$ one has

$$(2) \qquad p^{h+2} \nmid p^{h+1}\, u_1^{p-1} r(x).$$

Again using theorem 5 one finds the relations (1) for $h+1$ instead of h.

Further from (1) one deduces for $h=k+1, k+2, \dots$

$$c|c(f,\, p^h)|p^{h-k}c;\ c(f,\, p^h) \nmid p^{h-k-1}c,$$

hence

$$c(f,\, p^h) = p^{h-k}c.$$

Remark. If $p=2$ the relation ceases to hold in the case $h=1$. After a small change of the argument for $p=2$ one finds:

If U *is a* U_{f2}*-set and the residue* u, *belonging to* U *of* x^c *mod* $f(x)$ *with* $c=c(f, 4)$ *satisfies*

$$x^c \equiv u \ (\text{modd } f,\, 2^k),\ x^c \not\equiv u \ (\text{modd } f,\, 2^{k+1}),$$

then

$$c(f, 2^h) = \begin{cases} c(f,4) \ \text{if } h=2,\dots,k \\ 2^{h-k}c(f,4) \ \text{if } h=k+1, k+2, \dots \end{cases}$$

In a similar manner as in theorem 34 the proof can be given of the following

Theorem 35. *If $f(x)$ is irreducible mod p and if the residue u mod $f(x)$ of x^c (where $c=c(f, p; U)$) satisfies*

$$x^c \equiv u \text{ (modd } f^k, p); \; x^c \not\equiv u \text{ (modd } f^{k+1}, p),$$

then

$$c(f^h, p; U)=p^t c(f, p; U),$$

where t is the smallest integer $\geqq 0$ with $kp^t \geqq h$.

Section 3. Recurring sequences of integers of the second order

Consider the sequence defined by

$$w_0=0, \; w_1=1, \; w_{n+2}=a_1 w_{n+1}-a w_n \quad (n=0, 1, \ldots).$$

The discriminant a_1^2-4a of the characteristic polynomial

$$f(E)=E^2-a_1E+a$$

will be denoted by D.

If $\left(\frac{D}{p}\right)=-1$ this polynomial is irreducible mod p; if $\left(\frac{D}{p}\right)=1$ it is reducible into two mod p different linear polynomials; if $\left(\frac{D}{p}\right)=0$ it is reducible into two mod p equal linear factors.

These results follow from the relations

$$4f(E)=(2E-a_1)^2-D \text{ hence } (2E-a_1)^2 \equiv D \text{ (mod } f(x)).$$

Consequently one has

Theorem 36. *Let p be an odd prime.*

If $\left(\frac{D}{p}\right)=-1$, then $c(f, p)|p+1$, $C(f, p)\nmid p+1$, $C(f, p)|p^2-1$;

if $\left(\frac{D}{p}\right)=1$, then $c(f, p)|C(f, p)|p-1$;

if $\left(\frac{D}{p}\right)=0$, then $c(f, p)=p$; $C(f, p)|p(p-1)$.

Remark 1. For $p=2$ one has

if $\left(\frac{D}{2}\right)=1$, then $c(f, 2)=C(f, 2)=3$;

if $\left(\frac{D}{2}\right)=0$, then $c(f, 2)=C(f, 2)=2$.

Remark 2. For $m=4$ one easily deduces the following results

a_1 (mod 4)	a (mod 4)	c	C	v
0	-1	2	2	1
± 1	-1	6	6	1
2	± 1	4	4	1
0	1	2	4	2
1	1	3	6	2
-1	1	3	3	1

Theorem 37.

If $\left(\frac{D}{p}\right)=-1$, *one has* $x^{p+1}\equiv a$ (*modd* $f(x), p$);
if $\left(\frac{D}{p}\right)=0$ *and* $p\neq 2$, *one has* $x^p\equiv 2^{-1}a_1$ (*modd* $f(x), p$).

Proof. In the first case one has by Euler's criterium

$$D^{\frac{1}{2}(p-1)}\equiv -1 \pmod p,$$

hence using

$$(2x-a_1)^2\equiv D \pmod{f(x)}$$

one gets

$$(2x-a_1)^{p-1}\equiv -1 \quad (\text{modd } f(x), p),$$

hence

$$2x^p-a_1^p\equiv (2x-a_1)^p\equiv a_1-2x \quad (\text{modd } f(x), p),$$

consequently

$$x^p\equiv a_1-x \ (\text{modd } f(x), p),\ x^{p+1}\equiv a_1x-x^2\equiv a \ (\text{modd } f(x), p).$$

In the second case using $p|D$ one has successively

$$(2x-a_1)^2\equiv D\equiv 0 \quad (\text{modd } f(x), p),$$
$$2x^p-a_1\equiv (2x-a_1)^p\equiv 0 \ (\text{modd } f(x), p),\ x^p\equiv 2^{-1}a_1 \ (\text{modd } f(x), p).$$

Corollary. In the first case one has (where as before ε denotes the exponent of a mod p)

$$x^{\varepsilon(p+1)}\equiv a^\varepsilon\equiv 1 \quad (\text{modd } f(x), p),$$

hence

$$C(f, p)|\varepsilon(p+1);$$

in the second case one has

$$C(f, p)=hp,$$

where h denotes the exponent mod p of $2^{-1}a_1$.

Theorem 38.

If $\left(\frac{a}{p}\right)=1$, p *prime* $\neq 2$, $p\nmid a_1$, *then*

$$c(f, p)|\tfrac{1}{2}(p-1) \ \textit{if} \ \left(\frac{D}{p}\right)=1;$$
$$c(f, p)|\tfrac{1}{2}(p+1) \ \textit{if} \ \left(\frac{D}{p}\right)=-1.$$

Proof. By assumption there exists an integer b with $b^2\equiv a \pmod p$, hence

(1) $\quad (x+b)(x+a_1-b)\equiv x^2+a_1x-b^2+a_1b\equiv a_1b \quad (\text{modd } f(x), p).$

Further $p\nmid a_1+2b$ because $p\nmid D=a_1^2-4a$. Moreover

$$(x+b)^2\equiv x(a_1+2b) \quad (\text{modd } f(x), p),$$

hence

$$(x+b)^{p-1}\equiv x^{\frac{1}{2}(p-1)}(a_1+2b)^{\frac{1}{2}(p-1)} \quad (\text{modd } f(x), p).$$

If $\left(\frac{D}{p}\right)=1$ by theorem 36 one has $x^p \equiv x$ (modd $f(x), p$), hence

(2) $x+b \equiv x^p+b \equiv (x+b)^p \equiv x^{\frac{1}{2}(p-1)}(a_1+2b)^{\frac{1}{2}(p-1)}(x+b)$ (modd $f(x), p$).

Then after multiplication by $(x+a_1-b)(a_1+2b)^{\frac{1}{2}(p-1)}a_1^{p-2}b^{p-2}$ one obtains from (1) and (2)

$$x^{\frac{1}{2}(p-1)} \equiv (a_1+2b)^{\frac{1}{2}(p-1)} \quad (\text{modd } f(x), p),$$

hence

$$c(f, p)\,|\,\tfrac{1}{2}(p-1).$$

If $\left(\frac{D}{p}\right)=-1$ by theorem 37 one has $x^{p+1} \equiv a$ (modd $f(x), p$), hence

$$(3) \qquad \begin{aligned} b(b+x) &\equiv a+bx \equiv x^{p+1}+bx = x(x^p+b) \equiv x(x+b)^p \\ &\equiv x^{\frac{1}{2}(p+1)}(a_1+2b)^{\frac{1}{2}(p-1)}(x+b) \quad (\text{modd } f(x), p). \end{aligned}$$

Then after multiplication by $(a_1+2b)^{\frac{1}{2}(p-1)}(x+a_1-b)a_1^{p-2}b^{p-2}$ one obtains from (1) and (3)

$$x^{\frac{1}{2}(p+1)} \equiv b(a_1+2b)^{\frac{1}{2}(p-1)} \quad (\text{modd } f(x), p),$$

hence

$$c(f, p)\,|\,\tfrac{1}{2}(p+1).$$

Theorem 39. *If* $c(f, p)\,|\,\frac{1}{2}(p \pm 1)$ *then* $\left(\frac{a}{p}\right)=1$.

Proof. If $c(f, p)\,|\,\frac{1}{2}(p-1)$ an integer u exists such that

$$(1) \qquad x^{\frac{1}{2}(p-1)} \equiv u \quad (\text{modd } f(x), p),$$

hence

$$1 \equiv x^{p-1} \equiv u^2 \quad (\text{modd } f(x), p).$$

Further $f(x)=f(a_1-x)$, hence (1) gives

$$(a_1-x)^{\frac{1}{2}(p-1)} \equiv u \quad (\text{modd } f(x), p)$$

and

$$a^{\frac{1}{2}(p-1)} \equiv (x(a_1-x))^{\frac{1}{2}(p-1)} \equiv u^2 \equiv 1 \quad (\text{modd } f(x), p),$$

thus $\left(\frac{a}{p}\right)=1$.

If $c(f, p)\,|\,\frac{1}{2}(p+1)$ theorem 37 can be applied. Since by assumption an integer w exists such that

$$x^{\frac{1}{2}(p+1)} \equiv w \quad (\text{modd } f(x), p),$$

one has

$$a \equiv x^{p+1} \equiv w^2 \quad (\text{modd } f(x), p),$$

hence again $\left(\frac{a}{p}\right)=1$.

In order to find further results on $v(f, m)$ it be remarked that by theorem 28 one has

$$\frac{\varepsilon}{(\varepsilon, c)}\,|\,v\,|'\,\frac{2\varepsilon}{(\varepsilon, c)}, \quad \text{hence} \quad v=\frac{\varepsilon}{(\varepsilon, c)} \quad \text{or} \quad \frac{2\varepsilon}{(\varepsilon, c)};$$

here $c=c(f, m)$. A further discussion is given by the following

Theorem 40. *Let p be an odd prime.*

If $B_2(c) = B_2(\varepsilon) > 0$, then $v = \varepsilon/(\varepsilon, c)$;

if $B_2(c) \neq B_2(\varepsilon)$, then $v = 2\varepsilon/(\varepsilon, c)$.

Proof. If $B_2(\varepsilon) > B_2(c)$ by theorem 29 one has $v = 2\varepsilon/(\varepsilon, c)$. In both other considered cases c is even, say $= 2d$. Then one has for $w = w_{c+1}$

$$w \equiv -a^d \pmod{p}. \tag{1}$$

In fact by theorem 30 it followed

$$x^c \equiv A_e(x) \equiv w \quad (\text{modd } f(x), p),$$

hence by theorem 27

$$a^c \equiv w^2 \pmod{p}.$$

If $a^d \equiv w \pmod{p}$ one would have

$$x^c \equiv a^d \quad (\text{modd } f(x), p),$$

hence from $x(a_1 - x) \equiv a \pmod{f(x)}$ it would follow

$$a^d x^d \equiv x^c(a_1 - x)^d \equiv a^d(a_1 - x)^d \quad (\text{modd } f(x), p), \tag{2}$$

thus

$$x^d \equiv (a_1 - x)^d \quad (\text{modd } f(x), p).$$

Now by theorem 30 one has

$$x^d = x^d A_0(x) \equiv A_d(x) = w_d(x - a_1) + w_{d+1} \pmod{f(x)},$$

hence

$$(a_1 - x)^d \equiv -w_d x + w_{d+1} \pmod{f(x)}$$

and after addition these relations combined with (2) would give

$$2x^d \equiv 2w_{d+1} - a_1 w_d \quad (\text{modd } f(x), p),$$

contrary to the minimum property of c. This proves (1).

Now in the case $B_2(c) = B_2(\varepsilon) > 0$ both $\varepsilon/(\varepsilon, c)$ and $c/(\varepsilon, c)$ are odd. From the minimum property of ε (as exponent of a mod p) one deduces

$$a^{\frac{1}{2}\varepsilon} \equiv -1 \pmod{p},$$

hence

$$w^{\varepsilon/(\varepsilon,c)} \equiv (-)^{\varepsilon/(\varepsilon,c)} a^{d\varepsilon/(\varepsilon,c)} = -(a^{\frac{1}{2}\varepsilon})^{c/(\varepsilon,c)} \equiv -(-)^{c/(\varepsilon,c)} = 1 \pmod{p}$$

and $v = \varepsilon/(\varepsilon, c)$.

In the case $B_2(c) > B_2(\varepsilon)$ however $\varepsilon/(\varepsilon, c)$ is odd and $c/(\varepsilon, c)$ is even. Then one obtains

$$w^{\varepsilon/(\varepsilon,c)} \equiv (-)^{\varepsilon/(\varepsilon,c)} a^{d\varepsilon/(\varepsilon,c)} = -(a^{\varepsilon})^{d/(\varepsilon,c)} \equiv -1 \pmod{p},$$

hence

$$v = 2\varepsilon/(\varepsilon, c).$$

Remark. It is not difficult to find examples that in the case $B_2(c) = B_2(\varepsilon) = 0$ the integer v can assume either of the values $\varepsilon/(\varepsilon, c)$ and $2\varepsilon/(\varepsilon, c)$.

Summarizing the above results one has for odd primes p the following table of cases (where as before ε and h denote the exponents of a and $2^{-1}a_1$ mod p respectively).

1.	$\left(\frac{D}{p}\right)=\left(\frac{a}{p}\right)=1$	$c\mid\frac{1}{2}(p-1)$	$C\mid p-1$
2.	$\left(\frac{D}{p}\right)=-\left(\frac{a}{p}\right)=1$	$c\nmid\frac{1}{2}(p-1)$	$c\mid C\mid p-1$
3.	$-\left(\frac{D}{p}\right)=\left(\frac{a}{p}\right)=1$	$c\mid\frac{1}{2}(p+1)$	$C\nmid p+1,\ C\mid\varepsilon(p+1)$
4.	$-\left(\frac{D}{p}\right)=-\left(\frac{a}{p}\right)=1$	$c\nmid\frac{1}{2}(p+1)$	$c\mid p+1\quad C\nmid p+1,\ C\mid\varepsilon(p+1)$
5.	$\left(\frac{D}{p}\right)=0$	$c=p$	$C=hp.$

A.	$B_2(c)=B_2(\varepsilon)>0$	$v=\varepsilon/(\varepsilon, c)$	$B_2(v)=0$
B.	$B_2(c)=B_2(\varepsilon)=0$	$v=\varepsilon/(\varepsilon, c)$ or $2\varepsilon/(\varepsilon, c)$	$B_2(v)=0$ or 1
C.	$B_2(c)>B_2(\varepsilon)$	$v=2\varepsilon/(\varepsilon, c)$	$B_2(v)=1$
D.	$B_2(c)<B_2(\varepsilon)$	$v=2\varepsilon/(\varepsilon, c)$	$B_2(v)\geqq 2.$

For $p=2$ one has only the cases

$\left(\frac{D}{p}\right)=\left(\frac{a}{p}\right)=1$	$c=C=1,\quad v=1.$
$\left(\frac{D}{p}\right)=0$	$c=C=2,\quad v=1.$

Combining the results 1—5 and A—D after a little discussion one gets the following table exhausting all possibilities:

Case	p (mod 4)	Case	v	c	C
1	1	A, B, C, D	$\varepsilon/(\varepsilon, c)$ or $2\varepsilon/(\varepsilon, c)$	$c\mid\frac{1}{2}(p-1)$	$C\mid p-1$
1	-1	B	$\varepsilon/(\varepsilon, c)$ or $2\varepsilon/(\varepsilon, c)$	$c\mid\frac{1}{2}(p-1)$	$C\mid p-1$
2	± 1	A	$\varepsilon/(\varepsilon, c)$	$c\mid p-1$	$C\mid p-1$
3	1	B, D	ε or 2ε	$c\mid\frac{1}{2}(p+1)$	$C\mid\varepsilon(p+1)$
3	-1	B, C	ε or 2ε	$c\mid\frac{1}{2}(p+1)$	$C\mid\varepsilon(p+1)$
4	1	D	ε	$c\mid p+1$	$C\mid\varepsilon(p+1)$
4	-1	C	ε	$c\mid p+1$	$C\mid\varepsilon(p+1)$
5	1	B, D	ε or 2ε	$c=p$	$C=hp$
5	-1	B	ε or 2ε	$c=p$	$C=hp.$

If moreover $a=\pm 1$ still more can be found.

In the case $a=1$ one has $\varepsilon=1$ and the cases 2, 4, A and D are obviously excluded.

After some discussion one finds the following only possible cases:

Case	p (mod 4)	case	v	c	C
1	1	B, C	1 or 2	$c\mid\frac{1}{2}(p-1)$	$C\mid p-1$
1	-1	B	1 or 2	$c\mid\frac{1}{2}(p-1)$	$C\mid p-1$
3	1	B	2	$c\mid\frac{1}{2}(p+1)$	$C\mid p+1$
3	-1	B, C	1 or 2	$c\mid\frac{1}{2}(p+1)$	$C\mid p+1$
5	± 1	B	1 or 2	p	$C=p$ (if $a_1\equiv 2 \pmod{p}$) $C=2p$ (if $a_1\equiv -2 \pmod{p}$)

In the case $a=-1$ one has $\varepsilon=2$ and case B is excluded. Here after some discussion the only possible cases appear to be

Case	p (mod 4)	case	v	c	C
1	1	A, C, D	1, 2, 4	$c\mid\frac{1}{2}(p-1)$	$C\mid p-1$
2	-1	A	1	$c=C\nmid\frac{1}{2}(p-1)$	$c=C\mid p-1$
3	1	D	4	$4c=C\nmid(p+1)$	$4c=C\mid 2(p+1)$
4	-1	C	2	$2c=C\nmid p+1$	$2c=C\mid 2(p+1)$
5	±1	D	4	p	$4p$

As an application of the last case one may consider the sequence of Fibonacci defined by

$$w_0=0,\ w_1=1,\ w_{n+2}=w_{n+1}+w_n \quad (n=0,\ 1,\ \ldots)$$

with $f(E)=E^2-E-1$ and discriminant $D=5$. Here $\left(\frac{D}{p}\right)=1$ for $p\equiv\pm1$ (mod 10), $\left(\frac{D}{p}\right)=-1$ for $p\equiv\pm3$ (mod 10) and $\left(\frac{D}{p}\right)=0$ for $p=5$. One easily deduces the following table

p mod 20	Case	v	c	C
1 or 9	1A, 1C, 1D	1, 2, 4	$c\mid\frac{1}{2}(p-1)$	$C\mid p-1$
11 or 19	2A	1	$c=C\nmid\frac{1}{2}(p-1)$	$C\mid p-1$
13 or 17	3D	4	$c\mid\frac{1}{2}(p+1)$	$C\nmid p+1,\ C\mid 2(p+1)$
3 or 7	4C	2	$2c=C\nmid p+1$	$2c=C\mid 2(p+1)$
5	5D	4	5	20
2	—	1	3	3

Section 4.

Recurring sequences of rational integers of order $\geqq 3$

For a sequence of order 3 defined by

$$w_{n+3}=a_1w_{n+2}+a_2w_{n+1}+aw_n \quad (n=0,\ 1,\ \ldots)$$

the characteristic polynomial is

$$f(E)=E^3-a_1E^2-a_2E-a.$$

Let p denote an arbitrary prime number. Then one has by theorem 33 the following cases and results which contrary to the preceding section cannot all be distinguished by a criterium on the discriminant D of $f(E)$:

I. $f(x)$ is irreducible mod p. Then

$$c(f,\ p)\mid p^2+p+1,\ C(f,\ p)\nmid p^2-1,\ C(f,\ p)\mid p^3-1.$$

II. $f(x)$ is mod p reducible into a linear and an irreducible quadratic factor. Then

$$c(f,\ p)\mid C(f,\ p)\nmid p-1 \quad c(f,\ p)\mid C(f,\ p)\mid p^2-1.$$

III. $f(x)$ is mod p reducible into three mod p different linear factors. Then

$$c(f,\ p)\mid C(f,\ p)\mid p-1.$$

IV. $f(x)$ is reducible mod p into a product of three linear factors exactly two of which are equal mod p. Then

$$p\,|\,c(f,\,p)\,|\,C(f,\,p)\,|\,p(p-1).$$

V. $f(x)$ is reducible mod p into a product of three linear factors which are all equal mod p. Then

$$\begin{array}{ll} p=c(f,\,p)\,|\,C(f,\,p)\,|\,p(p-1) & \quad\text{if } p\neq 2; \\ c(f,\,2)=C(f,\,2)=4. & \end{array}$$

The cases IV and V only occur for primes p which divide D. By theorem 33 the values of the periods mod m where m is composite can be found easily from those of the periods modulo the prime numbers.

By theorem 28 one has

$$\frac{\varepsilon}{(\varepsilon,c)}\,\Big|\,v\,\Big|\,\frac{3\varepsilon}{(\varepsilon,c)},\quad\text{i.e. } v=\frac{\varepsilon}{(\varepsilon,c)}\ \text{ or }\ \frac{3\varepsilon}{(\varepsilon,c)},$$

where as before ε denotes the exponent mod m of a. By theorem 29 one has further $v=3\varepsilon/(\varepsilon,\,c)$ in the case $B_3(\varepsilon)>B_3(c)$. In the case $B_3(\varepsilon)<B_3(c)$ however no result exists similar to that of theorem 40. Still, combining these results with those of the cases I—V, sometimes more can be said about the integers c, C and v.

Also in the special case $a=\pm 1$ one can deduce more. Then obviously by theorem 29 one has $v=1$, 2, 3 or 6. For these results the reader is referred to the author's thesis.

Finally the main results are mentioned for a recurring sequence of the fourth order

$$w_{n+4}=a_1w_{n+3}+a_2w_{n+2}+a_3w_{n+1}-a\,w_n \quad (n=0,\,1,\,\ldots)$$

with characteristic polynomial

$$f(E)=E^4-a_1E^3-a_2E^2-a_3E+a.$$

Denoting by q_i, r_i, s_i, t_i $(i=1,\,2,\,3,\,4)$ mod p different and irreducible polynomials of degree i, by theorem 33 one has the following results

$$\begin{array}{rlll}
\text{I.} & f(x)\equiv q_4 \pmod p & c\,|\,(p+1)(p^2+1) & C\nmid p^2-1\ \ C\nmid p^3-1\ \ C\,|\,p^4-1 \\
\text{II.} & f(x)\equiv q_1q_3 \pmod p & C\nmid p^2-1 & c\,|\,C\,|\,p^3-1 \\
\text{III.} & f(x)\equiv q_2r_2 \pmod p & C\nmid p-1 & c\,|\,C\,|\,p^2-1 \\
\text{IV.} & f(x)\equiv q_1r_1q_2 \pmod p & C\nmid p-1 & c\,|\,C\,|\,p^2-1 \\
\text{V.} & f(x)\equiv q_1r_1s_1t_1 \pmod p & & c\,|\,C\,|\,p-1 \\
\text{VI.} & f(x)\equiv q_1^2q_2 \pmod p & C\nmid p-1 & p\,|\,c\,|\,C\,|\,p(p^2-1) \\
\text{VII.} & f(x)\equiv q_1^2r_1s_1 \pmod p & & p\,|\,c\,|\,C\,|\,p(p-1) \\
\text{VIII.} & f(x)\equiv q_1^2r_1^2 \pmod p & & p\,|\,c\,|\,C\,|\,p(p-1) \\
\text{IX.} & f(x)\equiv q_1^3r_1 \pmod p & & \left\{\begin{array}{l} p\,|\,c\,|\,C\,|\,p(p-1)\ \text{ if } p\neq 2 \\ p^2\,|\,c\,|\,C\,|\,p^2(p-1)\ \text{ if } p=2 \end{array}\right. \\
\text{X.} & f(x)\equiv q_1^4 \pmod p & & \left\{\begin{array}{l} p=c\,|\,C\,|\,p(p-1)\ \text{ if } p\neq 2,\,3 \\ p^2=c\,|\,C\,|\,p^2(p-1)\ \text{ if } p=2,\,3. \end{array}\right.
\end{array}$$

Further by theorem 28 one has

$$v=\frac{\varepsilon}{(\varepsilon,c)},\ \frac{2\varepsilon}{(\varepsilon,c)}\ \text{ or }\ \frac{4\varepsilon}{(\varepsilon,c)}$$

In the case $B_2(\varepsilon) > B_2(c)$ the value $v = \varepsilon/(\varepsilon, c)$ is excluded. It is not difficult to show that in this case also $v = 2\varepsilon/(\varepsilon, c)$ is excluded. In fact putting $\varepsilon = 2d$ from $a^\varepsilon \equiv 1 \pmod p$ on account of the minimum property of ε one deduces $a^d \equiv -1 \pmod p$. By theorem 27 one has $a^c \equiv u^4 \pmod p$, hence

$$u^{2\varepsilon/(\varepsilon,c)} = (u^4)^{d/(\varepsilon,c)} \equiv a^{cd/(\varepsilon,c)} = (a^d)^{c/(\varepsilon\, c)} \equiv (-)^{c/(\varepsilon,c)} = -1 \pmod p,$$

consequently $v = 4\varepsilon/(\varepsilon, c)$.

Since moreover $v(p) | p-1$ this can only occur if $p \equiv 1 \pmod 8$.

For a further discussion the reader is again referred to the author's thesis.

Mathematical Centre, Amsterdam