

COMPOSITIO MATHEMATICA

MIKLÓS AJTAI

Divisibility properties of recurring sequences

Compositio Mathematica, tome 21, n° 1 (1969), p. 43-51

http://www.numdam.org/item?id=CM_1969__21_1_43_0

© Foundation Compositio Mathematica, 1969, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Divisibility properties of recurring sequences

by

Miklós Ajtai

Let $v_0 = 0, v_1 = 0, \dots, v_{n-2} = 0, v_{n-1} = 1, v_n \dots$ be a sequence of rational integers, which satisfies the recursion

$$v_{i+n} = a_1 v_{i+n-1} + \dots + a_n v_i \quad i = 0, 1, 2, \dots$$

where a_1, a_2, \dots, a_n are rational integers and $n \geq 2$.

If in the sequence there exist $n-1$ consecutive elements with positive indices divisible by p , then let $j(p)$ be the smallest positive integer such that $v_{j(p)} \equiv v_{j(p)+1} \equiv \dots \equiv v_{j(p)+n-2} \equiv 0 \pmod{p}$.

H. J. A. Duparc proved in [1], that if the characteristic polynomial of the sequence

$$f(x) = x^n - a_1 x^{n-1} - a_2 x^{n-2} - \dots - a_n$$

mod p is irreducible then $j(p)$ exists and

$$j(p) \left| \frac{p^n - 1}{p - 1}, \right.$$

and he considered sequences with reducible characteristic polynomial, and he proved that every sequence which satisfies the recursion, is periodic mod p , in the following sense: there exists a rational integer c such that $u_{m+j(p)} \equiv cu_m \pmod{p}$ $m = 0, 1, 2, \dots$, where u_0, u_1, u_2, \dots is the sequence.

The assertions of theorem 2 and 3 are well-known results about the Fibonacci numbers to be found in [1].

THEOREM 1. Let K be a finite field with p^n elements (where p is a prime number and n is a positive integer) whose prime field is P . Let $f(x)$ be an irreducible polynomial of $P[x]$ of degree n . If $x_0 \in K$ and $f(x_0) = 0$, then there exists a smallest positive integer j such that $x_0^j \in P$, and if

$$k \left| \left(\frac{p^n - 1}{p - 1}, p - 1 \right), k > 0, \right.$$

then

$$j \mid \frac{1}{k} \frac{p^n - 1}{p - 1}$$

if and only if $(-1)^n j(0)$ is k -th power in P .

PROOF. Let $K^* = K - \{0\}$ and $P^* = P - \{0\}$. P^* is a normal subgroup of K^* since K^* is commutative. Let $q = (p^n - 1)/(p - 1)$. The order of $K_j^* \circ (K^*) = p^n - 1$ and that of $P_j; \circ (P^*) = p - 1$ then $o(K^*/P^*) = q$.

Let \bar{a} be the coset modulo P^* containing “ a ” where $a \in K^*$. For every $a \in K^*$, $\bar{a}^q = P^*$, since $o(K^*/P^*) = q$.

Suppose $a \in K^*$ and let $N(a) = a^q$. Obviously, $N(a) \in P^*$ and $N(ab) = N(a)N(b)$ if $a, b \in K^*$.

Let for $a \in K^* N(a)$ be k -th power in P , where $k \mid (q, p - 1)$.

$$\begin{aligned} q &= \frac{1}{p-1} [(p-1)+1]^{n-1} \\ &= \frac{1}{p-1} \left[(p-1)^n + \binom{n}{1}(p-1)^{n-1} + \dots + 1 - 1 \right] \\ &= (p-1) \left[(p-1)^{n-2} + \dots + \binom{n}{n-2} \right] + n. \end{aligned}$$

Therefore $(q, p - 1) = (n, p - 1)$, consequently $k \mid n$.

Let $b \in \bar{a}$. Since a and b are in the same coset, there exists an element c of P^* such that $b = ca$.

$$\begin{aligned} N(b) &= b^q = b \cdot b^p \cdot \dots \cdot b^{p^{n-1}} \\ &= c \cdot a \cdot c^p \cdot a^p \cdot \dots \cdot c^{p^{n-1}} a^{p^{n-1}} = c^n N(a), \end{aligned}$$

since $c^p = c$. $k \mid n$, hence c^n is k -th power in p , thus also $c^n N(a) = N(b)$ is also k -th power.

By this we proved the following:

(1) if $k \mid (q; p - 1)$, then $N(b)$ is k -th power in p either for every b in a coset \bar{a} of P^* or for none of the elements b of \bar{a} .

Since K^* is a cyclic group, there exists an element g of K^* , such that $\{g\} = K^*$, that is the elements $1, g, g^2, \dots, g^{p^n - 2}$ are different. Thus the elements

$$1, g^q = N(g), g^{2q} = (N(g))^2, \dots, g^{(p-2)q} = (N(g))^{p-2}$$

are also different, consequently $\{N(g)\} = P^*$. Hence every $c \in P^*$ can be written in the form $c = (N(g))^m$, where m is uniquely determined mod $p - 1$. $k \mid p - 1$ implies that c is k -th power in P if and only if there exists an integer m_1 such that $m \equiv km_1$

(mod $p-1$). Obviously, $\{\bar{g}\} = (K^*/P^*)$ and it follows from (1) that for any $a \in \bar{g}^m$, $N(a)$ is k -th power in P if and only if $N(g^m) = (N(g))^m$ is also k -th power in P , that is $m \equiv km_1 \pmod{p-1}$.

$k|(q, p-1)$, thus there are exactly q/k numbers in the sequence $1, 2, \dots, q$ which can be m such that the above congruence with appropriate m_1 is satisfied. Thus P^* has exactly q/k cosets in which $N(a)$ is k -th power in P for every element "a", while the other cosets of P^* have no elements with this property.

Let H be the set of the former type cosets, then $P^* \in H$, since $1 \in P^*$ and $N(1) = 1$ is k -th power in P , thus H is non-vacuus.

If $m' \equiv m'_1 k$ and $m'' \equiv m''_1 k \pmod{p-1}$, then

$$m' + m'' \equiv (m'_1 + m''_1)k$$

(mod $p-1$) and so H is closed relative to multiplication. These two properties imply that H is a subgroup of (K^*/P^*) and that $o(H) = q/k$.

$f(x)$ is irreducible in $P(x)$, $f(x_0) = 0$, thus $x_0, x_0^p, \dots, x_0^{p^{n-1}}$ are different roots of $f(x)$ which has no other roots, hence $(-1)^n f(0) = x_0^n = N(x_0)$. Thus, if $(-1)^n f(0)$ is k -th power in P , then this holds also for $N(x_0)$ and consequently $\bar{x}_0 \in H$. Obviously $j = o(\bar{x}_0) | o(H) = (1/k)q$, and thus we proved the first part of the second assertion of the theorem.

Suppose $j|(1/k)q$, that is $o(x_0)|(1/k)q$. Since x_0 can be written in the form $\bar{x}_0 = \bar{g}^m$, then

$$\bar{1} = \bar{x}_0^{o(H)} = \bar{x}_0^{(1/k)q} = \bar{g}^{m(1/k)q},$$

consequently $(m/k)q \equiv 0 \pmod{q}$ and so m/k is an integer that is, $k|m$, hence $\bar{x}_0 \in H$, therefore $N(x_0) = (-1)^n f(0)$ is k -th power in P , thus we proved the theorem.

Let u_0, u_1, u_2, \dots be the Fibonacci sequence, that is $u_0 = 0$, $u_1 = 1$, and $u_{n+1} = u_n + u_{n-1}$ ($n = 1, 2, 3, \dots$). If there exists in the Fibonacci sequence any element different from u_0 and divisible by p , let $j(p)$ be the smallest positive integer such that $p | u_{j(p)}$.

THEOREM 2. Let p be a prime and $p \equiv 3$ or $-3 \pmod{5}$, then there exists in the Fibonacci sequence an element different from u_0 and divisible by p and

if $p \equiv 1 \pmod{4}$, then $j(p) | \frac{1}{2}(p+1)$

if $p \equiv -1 \pmod{4}$, then $j(p) | p+1$ but $j(p) \nmid \frac{1}{2}(p+1)$

PROOF. Let K_p be the field of the residue classes mod p , where p is an odd prime, and let R be the set of the matrices $\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}$ where $a, b \in K_p$. R is a ring relative to the matrix operations, since if $a, b, c, d \in K_p$

$$\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} + \begin{pmatrix} c & d \\ d & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ b+d & (a+c)+(b+d) \end{pmatrix} \in R$$

$$\begin{pmatrix} -a & -b \\ -b & -a-b \end{pmatrix} \in R$$

$$\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \begin{pmatrix} c & d \\ d & c+d \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bc+cd \\ ad+bc+bd & (ac+bd)+(ad+bc+bd) \end{pmatrix} \in R.$$

R is commutative, since its elements are symmetrical matrices and if the product of two symmetrical matrices is also symmetrical, then the two matrices are permutable.

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R$, consequently R is a commutative ring with a unit element. Let $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Obviously $A \in R$.

Let $\bar{u}_0, \bar{u}_1, \bar{u}_2, \dots$ be the residue classes mod p which contain the numbers u_0, u_1, u_2, \dots . First we prove that

$$A^s = \begin{pmatrix} \bar{u}_{s-1} & \bar{u}_s \\ \bar{u}_s & \bar{u}_{s+1} \end{pmatrix} \quad s = 1, 2, 3, \dots$$

For $s = 0$ the assertion is obvious. Suppose that

$$A^{s-1} = \begin{pmatrix} \bar{u}_{s-2} & \bar{u}_{s-1} \\ \bar{u}_{s-1} & \bar{u}_s \end{pmatrix}$$

then

$$\begin{aligned} A^s &= AA^{s-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \bar{u}_{s-2} & \bar{u}_{s-1} \\ \bar{u}_{s-1} & \bar{u}_s \end{pmatrix} \\ &= \begin{pmatrix} \bar{u}_{s-1} & \bar{u}_s \\ \bar{u}_{s-2} + \bar{u}_{s-1} & \bar{u}_{s-1} + \bar{u}_s \end{pmatrix} = \begin{pmatrix} \bar{u}_{s-1} & \bar{u}_s \\ \bar{u}_s & \bar{u}_{s+1} \end{pmatrix} \end{aligned}$$

thus the assertion is true.

If $p|u_s$, that is $\bar{u}_s = 0$, then $\bar{u}_{s+1} = \bar{u}_s + \bar{u}_{s-1} = \bar{u}_{s-1}$, hence $A^s = \bar{u}_{s-1}I$, and conversely, if there exists any $c \in K_p$ such that $A^s = cI$, then $\bar{u}_s = 0$, that is $p|u_s$.

(2) Thus $p|u_s$ if and only if there exists a $c \in K_p$ such that $A = cI$, hence if $j(p)$ exists it is the smallest positive integer satisfies the equation $A^{j(p)} = cI$ with appropriately chosen $c \in K_p$, and if there exists a positive integer t with $d \in K_p$ such that $A^t = dI$, then $j(p)$ exists.

Let $B = \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \in R$. If $|B| = d \neq 0$, then B^{-1} exists and

$$B^{-1} = \begin{pmatrix} (a+b)d^{-1} & -bd^{-1} \\ -bd^{-1} & ad^{-1} \end{pmatrix} \in R$$

Thus if $B \in R$, then $B^{-1} \in R$ exists if and only if $|B| \neq 0$. Now let $p \equiv \pm 3 \pmod{5}$ and let $B \in R$, with $|B| = 0$.

$$(3) \quad |B| = a^2 + ab - b^2 = 0$$

if $b \neq 0$; $(ab^{-1})^2 + ab^{-1} - 1 = 0$, that is $(2ab^{-1})^2 + 4ab^{-1} + 1 = 5$, hence $(2ab^{-1} + 1)^2 = 5$ and it is in contradiction with $p \equiv \pm 3 \pmod{5}$. Consequently, $b = 0$ and also $a = 0$. Thus $B = 0$ if and only if $|B| = 0$ and R is therefore a field. R has p^2 elements since the elements a and b of the matrix $\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}$ can be chosen in p^2 different ways.

$f(x) = x^2 - x - 1$ is the characteristic polynomial of A , hence $f(A) = 0$. $f(x)$ is irreducible in $K[x]$, since its discriminant 5 and $(5/p) = -1$. Thus the theorem 1 can be applied to the cases $K = R$, $A = x_0$, $k = 1, 2$. The prime field of R is the set of matrices cI , $c \in K_p$, hence it follows that if j is the smallest positive integer such that $A^j = cI$ with appropriately chosen $c \in K_p$ then $j | \frac{1}{2}(p+1)$ if and only if

$$\left(\frac{f(0)}{p} \right) = \left(\frac{-1}{p} \right) = 1,$$

while $j | p+1$ in every case, which by (2) proves the theorem.

THEOREM 3. Let p be prime and $p \equiv 1$ or $-1 \pmod{5}$. Then there exists in the Fibonacci sequence an element different from u_0 and divisible by p and

if $p \equiv 1 \pmod{4}$, then $j(p) | \frac{1}{2}(p-1)$

if $p \equiv -1 \pmod{4}$, then $j(p) \nmid \frac{1}{2}(p-1)$ but $j(p) | p-1$

PROOF. $(5/p) = 1$, hence there exists a $h \in K_p$ such that $h^2 = 5$. $g = (1+h)2^{-1}$ is a root of the polynomial $x^2 - x - 1$, therefore $\begin{pmatrix} 1 & g \\ g & g+1 \end{pmatrix} = 0$. $g^2 - g - 1 = 0$, thus $g^2 + 1 = g + 2$. For $g + 2 = 0$ it would follow that $g = -2$, that is $5 = 0$ which is impossible and therefore $g + 2 = g^2 + 1 \neq 0$.

Let

$$C = \begin{pmatrix} (g+2)^{-1} & g(g+2)^{-1} \\ g(g+2)^{-1} & (g+1)(g+2)^{-1} \end{pmatrix} \neq 0$$

$$D = \begin{pmatrix} (g+1)(g+2)^{-1} & -g(g+2)^{-1} \\ -g(g+2)^{-1} & (g+2)^{-1} \end{pmatrix} \neq 0$$

Obviously $C, D \in R$ and since $g^2 - g - 1 = 0$, $|C| = 0$ and $|D| = 0$ and

$$CD = \begin{pmatrix} g+1-g^2 & -g+2 \\ g^2+g-g^2-g & -g^2+g+1 \end{pmatrix} = 0$$

$C+D = I$, that is $C^2+CD = C$, $C^2 = C$ and similarly $D^2 = D$. Suppose $B \in R$ and

$$B = c_1C + d_1D = c_2C + d_2D, \text{ where } c_1, c_2, d_1, d_2 \in K_p.$$

Then $(c_1 - c_2)C^2 = (c_1 - c_2)C = 0$, $C \neq 0$ so $c_1 - c_2 = 0$, hence $c_1 = c_2$ and $d_1 = d_2$. Thus the elements $cC + dD$ are different if c and d run over the elements of K_p independently of each other. Hence we get p^2 different elements and since R has p^2 elements, each element of R is uniquely written in the form $cC + dD$, where $c, d \in K_p$.

If $B_1 = c_1C + d_1D$ and $B_2 = c_2C + d_2D$, then it follows from $DC = 0$, $C^2 = C$, $D^2 = D$ that

$$(4) \quad B_1B_2 = c_1c_2C + d_1d_2D \text{ and } B_1 + B_2 = (c_1 + c_2)C + (d_1 + d_2)D$$

(that is R is the direct sum of the ideals generated by C and D).

Let $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = A = c'C + d'D$. " A " is a root of the polynomial $f(x) = x^2 - x - 1$, hence because of (4) c' and d' are also roots of $f(x)$. $c' \neq d'$, since $A \neq bI$ if $b \in K_p$, thus, c' and d' are two different roots of $f(x)$ and therefore $c'd' = -1$.

(5) Let s be the smallest positive integer such that there exists a $v \in K_p$ which satisfies the equation $A^s = vI$. Such s is sure to exist, since $A^{p-1} = c^{p-1}C^{p-1} + d^{p-1}D^{p-1} = C + D = I$. Obviously, if $A^t = vI$ with $v \in K_p$, then $s|t$.

Suppose $(-1/p) = 1$. Since $c'd' = -1$, $(c'/p) = (d'/p)$, so

$$A^{(p-1)/2} = c'^{(p-1)/2}C + d'^{(p-1)/2}D = C + D = I$$

or

$$A^{(p-1)/2} = c^{(p-1)/2}C + d^{(p-1)/2}D = -C - D = -I$$

thus by (5) $s|_{\frac{1}{2}}(p-1)$ and this is by (2) the first assertion of the theorem.

Suppose $(-1/p) = -1$. $A^{p-1} = c^{p-1}C + d^{p-1}D = C + D = I$, thus by (5) and (2) $j(p)|p-1$.

$cd = -1$, thus $(c'/p) = (d'/p)$ and because of uniqueness

$$A^{(p-1)/2} = c^{(p-1)/2}C + d^{(p-1)/2}D = \pm C \mp D \neq vC + vD = vI$$

for any $v \in K_p$, thus by (5) $s \nmid \frac{1}{2}(p-1)$ and by (2) $j(p) \nmid \frac{1}{2}(p-1)$ which is the second assertion of the theorem.

THEOREM 4. Let

$$v_0 = 0, v_1 = 0, \dots, v_{n-2} = 0, v_{n-1} = 1, v_n, v_{n+1}, \dots$$

be a sequence of integers which satisfies the recursion

$$v_{i+n} = a_i v_{i+n-1} + a_2 v_{i+n-2} + \dots + a_n v_i \quad i = 0, 1, 2, \dots$$

where a_1, a_2, \dots, a_n are integers and $n \geq 2$. If the characteristic polynomial of the sequence

$$f(x) = x^n - a_1 x^{n-1} - a_2 x^{n-2} - \dots - a_n \pmod p$$

irreducible where p is prime, then in the sequence there exist $n-1$ consecutive elements with positive indices which are divisible by p , and if $j(p)$ is the smallest positive integer such that

$$v_{j(p)} \equiv v_{j(p)+1} \equiv \dots \equiv v_{j(p)+n-2} \equiv 0 \pmod p,$$

then for

$$k \left| \left(\frac{p^n - 1}{p - 1}, p - 1 \right) k > 0; \quad j(p) \left| \frac{1}{k} \frac{p^n - 1}{p - 1} \right.$$

if and only if $(-1)^{n+1} a_n$ is k -th power mod p .

PROOF. Let

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ \vdots & & & \ddots & \vdots & \vdots \\ \vdots & & & & 1 & 0 \\ \vdots & & & & 0 & 1 \\ \vdots & & & & & \\ \bar{a}_n & \dots & \dots & \dots & \bar{a}_2 & \bar{a}_1 \end{bmatrix}$$

where $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n$ are the residue classes mod p which contain the numbers a_1, a_2, \dots, a_n .

Let K be the set of matrices $g(A)$, where $g \in K_p[x]$. The characteristic polynomial of A is $x^n - a_1 x^{n-1} - \dots - a_n = f(x)$. $f(x)$ is irreducible in $K_p[x]$ and since $f(A) = 0$, $g_1(A) = g_2(A)$ if and only if $g_1(x) \equiv g_2(x) \pmod{f(x)}$, hence K is a finite field with p^n elements.

Let

$$\underline{a} = \begin{bmatrix} \bar{v}_0 \\ \bar{v}_1 \\ \vdots \\ \bar{v}_{n-1} \end{bmatrix}$$

where $\bar{v}_0, \bar{v}_1, \bar{v}_2, \dots$ are the residue classes mod p which contain

the numbers $\bar{v}_0, \bar{v}_1, \bar{v}_2, \dots$ and prove that:

(6) if $B, C \in K$, then $B = C$ if and only if $Ba = Ca$.

With immediate calculation we have

$$(7) \quad A \begin{bmatrix} \bar{v}_s \\ \bar{v}_{s+1} \\ \vdots \\ \bar{v}_{s+n-1} \end{bmatrix} = \begin{bmatrix} \bar{v}_{s+1} \\ \bar{v}_{s+2} \\ \vdots \\ \bar{v}_{s+n} \end{bmatrix} \quad s = 0, 1, 2, \dots$$

The vectors

$$\underline{a} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 1 \end{bmatrix}, A\underline{a} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \cdot \end{bmatrix}, \dots, A^{n-1}\underline{a} = \begin{bmatrix} 1 \\ \cdot \\ \vdots \\ \cdot \\ \cdot \end{bmatrix}$$

are obviously linearly independent over K , since the determinant constructed these vectors is $-1 \neq 0$. Thus every n dimensional vectors over K_p can be written in the form

$$\sum_{j=0}^{n-1} c_j A^j \underline{a} = \left(\sum_{j=0}^{n-1} c_j A^j \right) \underline{a},$$

where $c_j \in K_p$.

There exist over K_p exactly p^n n -dimensional vectors, K has p^n elements and $\sum_{j=0}^{n-1} c_j A^j \in K$, thus if $B, C \in K$, then $B \neq C$ implies $Ba \neq Ca$, and (6) is true.

Since (7)

$$A^s \underline{a} = \begin{bmatrix} \bar{v}_s \\ \bar{v}_{s+1} \\ \vdots \\ \bar{v}_{s+n-1} \end{bmatrix}.$$

The prime field P of K is the set of matrices cI , $c \in K_p$. If $A^s \in P$ obviously

$$\bar{v}_s = \bar{v}_{s+1} = \dots = \bar{v}_{s+n-2} = 0$$

and conversely, if,

$$\bar{v}_s = \bar{v}_{s+1} = \dots = \bar{v}_{s+n-2} = 0$$

then by (6) $A^s = \bar{v}_{s+n-1} I \in P$. Consequently if j is the smallest

positive integer such that $A^j \in P$, then $j = j(p)$. (Such j is sure to exist since $A^{p^n-1} = I \in P$.)

By applying the first theorem to the case of $x_0 = A$ we get the assertion of theorem 4.

REFERENCE

H. J. A. DUPARC

- [1] Divisibility properties of recurring sequences, Dissertation Amsterdam 1963.
p. 1–96.

(Oblatum 7–11–67)

Budapest