A sequence \( \{ u_n \} \), \( n = 0, 1, 2, 3, \ldots \) is said to be an integral recurrence of order \( r \) if the terms satisfy the equation

\[
\begin{align*}
u_n &= a_1 u_{n-1} + a_2 u_{n-2} + \ldots + a_r u_{n-r} \\
& \quad \text{for } n = r+1, r+2, \ldots , \text{and } a_1, a_2, \ldots, a_r \text{ are integers, } a_r \neq 0.
\end{align*}
\]

In this case we will say that \( \{ u_n \} \) satisfies the relation \( [a_1, a_2, \ldots, a_r] \). The sequence \( \{ u_n \} \) is uniquely determined when \( u_1, u_2, \ldots, u_r \) are given specified values. If \( u_1, u_2, \ldots, u_r \) are integers all the terms of \( \{ u_n \} \) are integers. The generating function \( f(t) = u_1 t + u_2 t^2 + \ldots \) takes on the form

\[
f(t) = \frac{Q(t)}{R(t)}
\]

where \( Q(t) \) depends on the values of \( u_1, u_2, \ldots, u_r \) and

\[
R(t) = t^r - a_1 t^{r-1} - a_2 t^{r-2} - \ldots - a_r.
\]

We will refer to \( R(t) \) as the characteristic polynomial of the recurrence. The matrix

\[
A = \begin{pmatrix}
0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 1 & \ldots & 0 \\
& \ddots & \ddots & \ddots & \ddots \\
& & \ddots & \ddots & \ddots \\
& & & 0 & 0 & 0 & \ldots & 1 \\
& & & & a_r & \ldots & a_3, a_2, a_1
\end{pmatrix}
\]

of order $r$, is the companion matrix of the polynomial $R(t)$.

The determinant of $A$ is $(-1)^{r+1}a$. Also, a set of $r$
sequences $\{u_n^{(1)}\}, \{u_n^{(2)}\}, \ldots, \{u_n^{(r)}\}$ satisfying the relation
$[a_1, a_2, \ldots, a_r]$, is said to be a basis, if for any sequence $\{w_n\}$
which satisfies the given relation, there exist uniquely determined
constants $b_1, b_2, \ldots, b_r$ such that

$$w_n = b_1u_n^{(1)} + b_2u_n^{(2)} + \ldots + b_r u_n^{(r)}$$

for $n = 1, 2, 3, \ldots$.

Essentially, we prove the following congruence property
for sequences satisfying the relation $[a_1, a_2, \ldots, a_r]$. There
exists a basis of sequences $\{u_n^{(1)}\}, \{u_n^{(2)}\}, \ldots, \{u_n^{(r)}\}$,
such that for any prime $p$ which does not divide $a_r$, there
exist infinitely many integers $k$ with the property that a block
of $r$ consecutive terms of each sequence of the basis starting
with the $k$th term, has $(r-1)$ of these terms divisible by $p$
while the remaining term is congruent to $1 \mod p$. A bound
for the smallest $k$ is determined.

The proof of the theorem is the same for all $r$ so we will
state and prove it in the case $r = 3$.

**THEOREM.** Let $u_n, v_n, w_n$ be three sequences satisfying
the relation $[a, b, c]$ where $a, b, c$ are integers, $c \neq 0$, with
the following initial conditions: $u_1 = 0, u_2 = 0, u_3 = c; v_1 = 1,$
v_2 = 0, v_3 = b; w_1 = 0, w_2 = 1, w_3 = a$. Then for any prime $p$
such that $p \nmid c$, there exists infinitely many integers $k$ such
that $u_k \equiv v_{k+1} \equiv w_{k+2} \equiv 1 \mod p$ and $u_{k+1} \equiv u_{k+2} \equiv v_k \equiv v_{k+2}$
$\equiv w_k \equiv w_{k+1} \equiv 0 \mod p$. Also, if $k_1$ is the smallest value of $k$ then

$$k_1 \mid (p^2 + p + 1) (p^2 + p) p^2 (p-1)^3.$$
Proof: First note that the sequences \{u_n\}, \{v_n\}, \{w_n\} form a basis for sequences satisfying the relation \([a, b, c]\). It is easy to verify by induction that for \(k = 1, 2, 3, \ldots\),

\[
A^k = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c & b & a \end{pmatrix}^k = \begin{pmatrix} u_k & v_k & w_k \\ u_{k+1} & v_{k+1} & w_{k+1} \\ u_{k+2} & v_{k+2} & w_{k+2} \end{pmatrix}
\]

The matrix \(A\) is non-singular and we consider its entries to lie in the field of integers mod \(p\). The set of all such matrices form a group of order \((p^2 + p + 1)(p^2 + p)p^2(p-1)^3\). Hence \(A\) has order \(k_1\), where \(k_1 \mid (p^2 + p + 1)(p^2 + p)p^2(p-1)^3\), from which the result follows.

We make the following remarks.

(1) If \(a, b, c\) be rationals rather than integers the result still holds if we avoid those values of \(p\) which divide any of the denominators of \(a, b, c\) when these are expressed in their lowest terms.

(2) The congruences of our theorem hold if \(k_1\) is replaced by any multiple \(k_1t\). Now if \(p_1, p_2, \ldots, p_m\) are distinct primes, and the corresponding values of \(k\) are \(k_1, k_2, \ldots, k_m\), then for \(k\) equal to the l.c.m. of \(k_1, k_2, \ldots, k_m\), the congruences of our theorem hold simultaneously for each of the primes \(p_1, p_2, \ldots, p_m\).

(3) If we merely require of \(u_k, v_{k+1}, w_{k+2}\) that they be congruent to each other (but not necessarily congruent to 1) then the value of \(k_1\) is usually lowered and is always a divisor of \((p^2 + p + 1)(p^2 + p)p^2(p-1)^2\). This follows by considering the group of matrices modulo the scalar matrices.

283
(4) In the case \( r = 2 \) for a relation \([a, 1]\), the second basis sequence is merely the first sequence shifted a term. The theorem then reads. Let \( \{u_n\} \) be a sequence such that
\[
u_1 = 0, \quad u_2 = 1, \quad u_n = au_{n-1} + u_{n-2}.
\]
For any prime \( p \), there exists an integer \( k \), such that \( k | (p+1) \) \( p (p-1)^2 \) and such that \( u_k \equiv u_{k+2} \equiv 1 \mod p \), \( u_{k+1} \equiv 0 \mod p \).

In particular, by taking \( a = 1 \), the theorem holds for the famous Fibonacci sequence.

This paper was written at the Summer Research Institute of the Canadian Mathematical Congress.

University of Manitoba