NOTE ON DIVISIBILITY SEQUENCES

BY MORGAN WARD

1. Introduction. We call a sequence of rational integers
\[(u) : u_1, u_2, u_3, \ldots, u_n, \ldots\]
a divisibility sequence if \(u_r\) divides \(u_s\) whenever \(r\) divides \(s\). The divisibility sequences most frequently studied are the linear sequences which satisfy linear difference equations with constant, integral coefficients.* In particular, the divisibility sequence associated with a difference equation of order two is essentially one of the important functions of Lucas.† I propose here to deduce two striking properties of divisibility sequences which do not depend on the fact that the sequence is linear.

2. Preliminary Definitions. An integer \(m\) will be said to be a divisor of \((u)\) if it divides some term of \((u)\), and a prime divisor if it is a prime. The suffix of the first term of \((u)\) divisible by \(m\) is called the rank of apparition of \(m\). If \(p\) is a prime divisor of \((u)\), the rank of apparition of \(p^a\) if it exists, will be denoted by \(p_a\).

If we assume that no term of \((u)\) is zero, we can build up from \((u)\) a set of numbers \([n, r]\), the binomial coefficients belonging to \((u)\),‡ defined by
\[
[u, r] = 1, \quad (r = 0; n = 0, 1, 2, \ldots),
\]
\[
[n, r] = \frac{u_n \cdot u_{n-1} \cdot \ldots \cdot u_{n-r+1}}{u_1 \cdot u_2 \cdot \ldots \cdot u_r}, \quad (r = 1, \ldots, n; n = 1, 2, \ldots).
\]

They will not in general be rational integers.

If \(a\) and \(b\) are any rational integers, we shall write as usual \(a \mid b\) for \(a\) divides \(b\) and \((a, b)\) for the greatest common divisor of \(a\) and \(b\).

* See Marshall Hall, Divisibility sequences of the third order, American Journal of Mathematics, vol. 58 (1936), pp. 577-584, for an account of these sequences and references to the work of Pierce, Poulet, and Lehmer.

† \(u_n\) equals the function \((\alpha^n - \beta^n)/(\alpha - \beta)\) up to a constant factor.

‡ For a systematic account of the remarkable properties of these numbers formed from any sequence \((u)\) with no non-vanishing terms see Morgan Ward, A calculus of sequences, American Journal of Mathematics, vol. 58 (1936), pp. 255-266.
and $b$. If $a^r$ is the highest power of $a$ which divides $b$, we shall write $a^r \mid b$.

Finally, since $u_1$ must divide every term of $(u)$, we may assume that $u_1 = 1$.

3. Statement of Results. A divisibility sequence will be said to have property A provided that

A. If $c = (a, b)$, then $u_c = (u_a, u_b)$, for every pair of terms $u_a, u_b$ of $(u)$.

It will be said to have property B provided that

B. For every prime divisor $p$ and every positive integer $a$, $u_r \equiv 0 \pmod{p^a}$ when and only when $r \equiv 0 \pmod{\rho_a}$, where $\rho_a$ is the rank of apparition of $p^a$ in $(u)$.

The results of this note may now be stated as follows.

**Theorem 1.** Property A and property B are equivalent to one another.

**Theorem 2.** The binomial coefficients belonging to every divisibility sequence having property A or property B are all rational integers.

Theorem 2 was proved for the Lucas function by Lucas himself,* and for a more general type of linear divisibility sequence by T. A. Pierce.†

4. **Proof of First Theorem.** Assume that the divisibility sequence $(u)$ has property A, and let $\rho_a$ be the rank of apparition of $p^a$, where $p$ is any prime divisor of $(u)$. Suppose that $u_r \equiv 0 \pmod{p^a}$. Then if $c = (r, \rho_a)$, $(u_r, u_{\rho_a}) = u_c$ by property A. Therefore since $u_r \equiv u_{\rho_a} \equiv 0 \pmod{p^a}$, $u_c \equiv 0 \pmod{p^a}$. Therefore $c \geq \rho_a$. But $c$ divides $\rho_a$. Therefore $c = \rho_a$ so that $\rho_a$ divides $r$. Since $(u)$ is a divisibility sequence, if $\rho_a$ divides $r$, $u_r = 0 \pmod{p^a}$. Therefore the sequence has property B.

Conversely, assume that $(u)$ has property B. Let $u_a$ and $u_b$ be any two terms of $(u)$, and let $p$ be any common prime divisor of $u_a$ and $u_b$. Suppose that $p^m \mid u_a$ and $p^n \mid u_b$. Then if $l$ is the smallest of the integers $m$ and $n$, it suffices to show that $p^l \mid u_c$, where $c = (a, b)$. For since $c \mid a$ and $c \mid b$, $u_c \mid u_a$ and $u_c \mid u_b$, so that

---

But \( p \mid (u_a, u_b) \). Therefore if \( p \mid u_c \) for every common prime divisor \( p \) of \( u_a \) and \( u_b \), we have \((u_a, u_b) \mid u_c \), so that \((u_a, u_b) = u_c \), and property A follows.

Now let \( p_m, p_n \) be the ranks of apparition of \( p^m \) and \( p^n \), respectively. Without loss of generality we may assume that \( m \geq n \), so that \( l = n \). Since property B holds, \( p_m \mid a, p_n \mid b \) and \( p_n \mid p_m \). Hence \( p_n \mid a \) and \( p_n \mid b \), so that \( p_n \mid c = (a, b) \). But then \( u_{p_n} \mid u_c \), so that \( p^l = p^n \mid u_c \).

5. **Proof of Second Theorem.** It suffices to show that \([n, r]\) is an integer modulo \( p \) for every prime divisor \( p \) of \((u)\) when \((u)\) has property B. If we let \([0]! = 1\), then \([s]! = u_1 u_2 \cdots u_s\), \((s \geq 1)\), \([n, r] = [n]!/[n-r]! [r]!\).

Now the highest power of \( p \) dividing \([n]!\) is clearly \( \sum_{s=1}^{\infty} [n/p_s] \), where as usual \([a/b]\) denotes the greatest integer in \( a/b \). (If \( p^s \) does not divide \((u)\), then neither does \( p^t \), \((t \geq s)\), and we break off the sum after \( s - 1 \) terms. Since \( p_s \rightarrow \infty \) with \( s \) if every power of \( p \) divides the sequence, the sum is finite in every case.)

It therefore suffices to show that

\[
\sum_{s=1}^{\infty} \left[ \frac{n}{p_s} \right] \geq \sum_{s=1}^{\infty} \left[ \frac{n-r}{p_s} \right] + \sum_{s=1}^{\infty} \left[ \frac{r}{p_s} \right],
\]

and this follows as in the ordinary case when \( u_n = n \) from the elementary inequality

\[
\left[ \frac{n + m}{p} \right] \geq \left[ \frac{n}{p} \right] + \left[ \frac{m}{p} \right].
\]

**CALIFORNIA INSTITUTE OF TECHNOLOGY**