of all of the X_i. Let E_k = the expected number of tosses to observe k heads in a row. Let $Z = X_1 + \cdots + X_Y$. Then,

$$\begin{aligned} E_k &= E(Y + Z) = E(Y) + E(Z) \\ &= E(Y) + E(Z \mid Y = 1)Pr(Y = 1) + E(Z \mid Y = 2)Pr(Y = 2) + \cdots \\ &= E(Y) + \sum_{n=1}^{\infty} E(Z \mid Y = n)Pr(Y = n) = E(Y) + \sum_{n=1}^{\infty} nE(X_1)Pr(Y = n) \\ &= E(Y) + E(X_1)E(Y). \end{aligned}$$

But $E(Y)$ = the expected number of tosses to observe a head $= 1/p$, and $E(X_1) = E_{k-1}$. Thus $E_k = 1/p + (1/p)E_{k-1}$, which yields (3).

REFERENCE

1. L. E. Dickson, *History of the Theory of Numbers*, Vol. I (1919; Chelsea reprint 1966).
2. W. Feller, *Introduction to Probability Theory and Its Applications*, Vol. I (New York: John Wiley & Sons, 1968).

*****

STRONG DIVISIBILITY SEQUENCES WITH NONZERO INITIAL TERM

CLARK KIMBERLING
University of Evansville, Evansville, IN 47702

In 1936, Marshall Hall [1] introduced the notion of a kth *order linear divisibility sequence* as a sequence of rational integers $u_0, u_1, \ldots, u_n, \ldots$ satisfying a linear recurrence relation

(1) $$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n,$$

where $a_1, a_2, \ldots, a_k$ are rational integers and $u_m | u_n$ whenever $m | n$. Some divisibility sequences satisfy a stronger divisibility property, expressible in terms of greatest common divisors as follows:

$$(u_m, u_n) = u_{(m,n)}$$

for all positive integers m and n. We call such a sequence a *strong divisibility sequence*. An example is the Fibonacci sequence $0, 1, 1, 2, 3, 5, 8, \ldots$.

It is well known that for any positive integer m, a linear recurrence sequence $\{u_n\}$ is periodic modulo m. That is, there exists a positive integer M depending on m and $a_1, a_2, \ldots, a_k$ such that

(2) $$u_{n+M} \equiv u_n \pmod{m}$$

for all $n \geq n_0[m, a_1, a_2, \ldots, a_k]$; in particular, $n_0 = 0$ if $(a_k, m) = 1$.

Hall [1] proved that a linear divisibility sequence $\{u_n\}$ with $u_0 \neq 0$ is *degenerate* in the sense that the totality of primes dividing the terms of $\{u_n\}$ is finite. One should expect a stronger conclusion for a linear strong divisibility sequence having $u_0 \neq 0$. The purpose of this note is to prove that such a sequence must be, in the strictest sense, periodic. That is, there must exist a positive integer M depending on $a_1, a_2, \ldots, a_k$ such that

$$u_{n+M} = u_n, \qquad n = 0, 1, \ldots .$$

Suppose $\{u_n\}$ is a kth order linear strong divisibility sequence. In terms of a generating function for $\{u_n\}$, we write

$$u_0 + u_1 t + u_2 t^2 + \cdots = \frac{H(t)}{K(t)} = \frac{H(t)}{(1 - x_1 t)(1 - x_2 t) \cdots (1 - x_k t)}, \tag{3}$$

where $H(t)$ and $K(t)$ are polynomials with integer coefficients. Let $q = x_1 x_2 \ldots x_k$ $(=a_k)$. We assume that $q \neq 0$.

Lemma 1: $u_m | q^m u_0$ for $m = 1, 2, \ldots$.

Proof: The 0th m-multisection of (3) (e.g., Riordan [2]) gives

$$u_{jm} = M_1 u_{(j-1)m} - M_2 u_{(j-2)m} + \cdots + (-1)^{k-1} M_k u_0,$$

where the M_i are integers. Since $u_m | u_{cm}$ for $c = 1, 2, \ldots$, we have

$$u_m | (-1)^{k+1} M_k u_0,$$

and this finishes the proof, because $M_k = q^m$.

Another proof of Lemma 1, depending on the periodicities (2), may be found in Hall [1].

Henceforth, we assume $u_0 \neq 0$. Let $p_1, p_2, \ldots, p_v$ be all the prime divisors of qu_0, so that we may write

$$q = p_1^{s_1} p_2^{s_2} \ldots p_v^{s_v} \quad \text{and} \quad u_0 = p_1^{i_{1,0}} p_2^{i_{2,0}} \ldots p_v^{i_{v,0}}.$$

Then, since $u_m | q^m u_0$ for $m = 0, 1, 2, \ldots$, we can write

$$u_m = p_1^{i_{1,m}} p_2^{i_{2,m}} \ldots p_v^{i_{v,m}}, \quad m = 0, 1, 2, \ldots .$$

Consider the set $\sigma_\ell = \{i_{\ell,1}, i_{\ell,2}, \ldots\}$, $\ell = 1, 2, \ldots, v$. Let $|\sigma_\ell|$ be the number of elements in σ_ℓ, with $|\sigma_\ell| = \infty$ if σ_ℓ is an infinite set. Define $a_\ell(j)$ for $j = 1, 2, \ldots$ inductively as follows:

$$a_\ell(1) = 1$$

$$a_\ell(2) = \begin{cases} 1 \text{ if } |\sigma_\ell| = 1 \\ \text{least } w \text{ such that } i_{\ell,w} \neq i_{\ell,1}, \text{ if } |\sigma_\ell| > 1 \end{cases}$$

$$\vdots$$

$$a_\ell(j) = \begin{cases} a_\ell(j-1) \text{ if } |\sigma_\ell| \leq j - 1 \\ \text{least } w \text{ such that } i_{\ell,w} \notin \{i_{\ell,a_\ell(r)} : 1 \leq r < j - 1\} \\ \text{if } |\sigma_\ell| > j - 1. \end{cases}$$

Thus, either the sequence $a_\ell(1), a_\ell(2), a_\ell(3), \ldots$ is strictly increasing and unbounded, or else it is strictly increasing up to some point and constant thereafter, or else it is the constant sequence $1, 1, \ldots$.

Lemma 2: Suppose $1 \leq \ell < v$. Then $a_\ell(j) | a_\ell(j + 1)$ for $j = 1, 2, \ldots$.

Proof: To simplify notation, let $a = a_\ell(j)$, $b = a_\ell(j + 1)$, and $c = (a, b)$. Without loss we assume $a \neq b$. Clearly $c \leq a$. Suppose $1 \leq c < a$. Then $i_{\ell,c} = i_{\ell,a_\ell(r)}$ for some $r < j$, so that $i_{\ell,c} \neq i_{\ell,a}$ and $i_{\ell,c} \neq i_{\ell,b}$. From $u_c = (u_a, u_b)$ follows $i_{\ell,c} = \min\{i_{\ell,a}, i_{\ell,b}\}$. This contradiction shows that $c = a$, as required.

Lemma 3: Suppose $1 \leq \ell < v$ and $j \geq 1$. If $1 \leq w \leq a_\ell(j) = a$, then

$$i_{\ell,w} \leq i_{\ell,a}.$$

Proof: If $1 \leq w \leq a$, then $i_{\ell,w} = i_{\ell,a_\ell(r)}$ for some $r < j$. Since $a_\ell(r) | a$, by Lemma 2, we have $u_{a_\ell(r)} | u_a$, so that $i_{\ell,a_\ell(r)} \leq i_{\ell,a}$.

Lemma 4: Suppose $1 \leq \ell \leq v$ and $j \geq 1$. If $1 \leq w \leq a_\ell(j) = a$, then

$$i_{\ell,(w,a)} = i_{\ell,w}.$$

Proof: $(u_w, u_a) = u_{(w,a)}$, so $\min\{i_{\ell,w}, i_{\ell,a}\} = i_{\ell,(w,a)}$. Now $i_{\ell,w} \leq i_{\ell,a}$, by Lemma 3, so $i_{\ell,(w,a)} = i_{\ell,w}$.

Lemma 5: Suppose $1 \leq \ell \leq v$ and $j \geq 2$. Suppose $a = a_\ell(j) \geq 2$ and b is a positive integer. Then

$$(i_{\ell,ba+1}, i_{\ell,ba+2}, \ldots, i_{\ell,ba+a-1}) = (i_{\ell,1}, i_{\ell,2}, \ldots, i_{\ell,a-1}).$$

Proof: Suppose $1 \leq w \leq a - 1$. Then $(u_{ba+w}, u_a) = u_{(ba+w,a)} = u_{(w,a)}$, so $\min\{i_{\ell,ba+w}, i_{\ell,a}\} = i_{\ell,(w,a)} = i_{\ell,w}$ by Lemma 4. Since $i_{\ell,w} < i_{\ell,a}$ by definition of a, we conclude $i_{\ell,ba+w} = i_{\ell,w}$.

Lemma 6: Suppose $1 \leq \ell \leq v$ and $2 \leq |\sigma_\ell| < \infty$. Let $L = a_\ell(|\sigma_\ell|)$, and let b be a positive integer. Then

$$(i_{\ell,bL+1}, i_{\ell,bL+2} \ldots, i_{\ell,2bL-1}) = (i_{\ell,1}, i_{\ell,2}, \ldots, i_{\ell,bL-1}).$$

Proof: By Lemma 5, we already know

$$\begin{aligned}(i_{\ell,1}, \ldots, i_{\ell,L-1}) &= (i_{\ell,L+1}, \ldots, i_{\ell,2L-1}) \\ &= (i_{\ell,2L+1}, \ldots, i_{\ell,3L-1}) \\ &\vdots \\ &= (i_{\ell,(b-1)L+1}, \ldots, i_{\ell,bL-1}),\end{aligned}$$

so it remains only to see that $i_{\ell,L} = i_{\ell,2L} = \cdots = i_{\ell,(b-1)L}$. For $1 \leq c \leq b - 1$, we have $(u_{cL}, u_L) = u_L$, so that $\min\{i_{\ell,cL}, i_{\ell,L}\} = i_{\ell,L}$. Since $i_{\ell,cL} < i_{\ell,L}$, we conclude $i_{\ell,cL} = i_{\ell,L}$.

Lemma 7: There exists a positive integer M such that $u_{M+j} = u_j$ for $j = 1, 2, \ldots, k$.

Proof: For $1 \leq \ell \leq v$, if $|\sigma_\ell| = \infty$, choose j_ℓ so large that $a_\ell(j_\ell) > k$, and if $|\sigma_\ell| < \infty$, let $a_\ell(j_\ell) = a_\ell(|\sigma_\ell|)$. Let M be the least common multiple of the numbers $a_1(j_1), a_2(j_2), \ldots, a_v(j_v), 2k$. (We include $2k$ to ensure that $M > k$ in case $|\sigma_\ell| < \infty$ for all ℓ.)

Now, by Lemma 5, for each ℓ with $|\sigma_\ell| = \infty$, we have

$$(i_{\ell,M+1}, \ldots, i_{\ell,M+k}) = (i_{\ell,1}, \ldots, i_{\ell,k}).$$

This same equation holds, by Lemma 6, for each ℓ with $2 \leq |\sigma_\ell| < \infty$, and clearly holds also for $\sigma_\ell = 1$. Therefore, for $1 \leq j \leq k$, we have $i_{\ell,M+j} = i_{\ell,j}$ for $1 \leq \ell \leq v$, so that $u_{M+j} = u_j$ for $1 \leq j \leq k$.

Theorem: Suppose $\{u_n\}$, $n = 0, 1, \ldots,$ is a kth order strong divisibility sequence with $u_0 \neq 0$. Then the sequence $\{u_n\}$ is periodic and has a generating function of the form $H(t)/(1 - t^\rho)$, where ρ is the fundamental period of $\{u_n\}$. If $H(t)$ has no linear factor of the form $1 - rt$, where $r^\rho = 1$, then ρ is the least possible recurrence order of $\{u_n\}$. If

$$\rho = \rho_1^{e_1} \rho_2^{e_2} \ldots \rho_t^{e_t}$$

if the prime factorization of ρ, then

$$u_\rho = U u_{\rho_1^{e_1}} u_{\rho_2^{e_2}} \ldots u_{\rho_t^{e_t}}$$

for some nonzero integer U. Finally, $u_0 = u_\rho$, and $u_n | u_0$ for $n = 0, 1, \ldots$.

Proof: By Lemma 7 and the fact that $\{u_n\}$ is a kth order recurrent sequence, the sequence $\{u_n\}$ is periodic with period M. Letting ρ be the fundamental period, we now show that the denominator of the generating function $H(t)/K(t)$ must be of the form $1 - t^\rho$:

$$\begin{aligned}\frac{H(t)}{K(t)} &= u_0 + u_1 t + \cdots + u_{\rho-1}t^{\rho-1} + u_0 t^\rho + u_1 t^{\rho+1} + \cdots \\ &= u_0(1 + t^\rho + t^{2\rho} + \ldots) + u_1 t(1 + t^\rho + t^{2\rho} + \cdots) + \cdots \\ &= (u_0 + u_1 t + \cdots + u_{\rho-1}t^{\rho-1})(1 + t^\rho + t^{2\rho} + \cdots) \\ &= (u_0 + u_1 t + \cdots + u_{\rho-1}t^{\rho-1})\frac{1}{1 - t^\rho}.\end{aligned}$$

If $H(t)$ has no linear factors $1 - rt$ with $r^\rho = 1$, then $H(t)$ has no linear factors in common with $K(t)$. This means that no recurrence order for $\{u_n\}$ can be less than ρ.

We see that $\rho_i^{e_i} | \rho$ and $(\rho_i^{e_i}, \rho_j^{e_j}) = 1$ for $1 \le i < j \le t$, so that

$$u_\rho = U u_{\rho_1^{e_1}} u_{\rho_2^{e_2}} \cdots u_{\rho_t^{e_t}}$$

for some integer U. For $n \ge 1$, we have $u_{n\rho} = u_\rho$ and $u_n | u_{n\rho}$, so that $u_n | u_\rho$. That $u_0 = u_\rho$, so that $u_n | u_0$ for all n, follows from

$$\begin{aligned}a_k u_0 &= u_k - a_2 u_{k-1} - \cdots - a_k u_1 \\ &= u_{\rho+k} - a_2 u_{\rho+k-1} - \cdots - a_k u_{\rho+1} \\ &= a_k u_\rho.\end{aligned}$$

REFERENCES

1. Marshall Hall, "Divisibility Sequences of Third Order," *Amer. J. Math.*, Vol. 58 (1936), pp. 577-584.
2. John Riordan, *Combinatorial Identities* (New York: John Wiley & Sons, 1968).

*****

MINIMUM PERIODS MODULO *n* FOR BERNOULLI NUMBERS

W. HERGET
Technische Universitat, Braunschweig, Fed. Rep. Germany

The Bernoulli numbers B_m may be defined by

$$B_0 = 1 \tag{1}$$
$$B_m = \frac{1}{m+1}\sum_{i=0}^{m-1}\binom{m+1}{i}B_i \quad (m > 0).$$

By the Kummer congruence, we have [2, p. 78 (3.3)],

$$\sum_{i=0}^{r}(-1)^i\binom{r}{i}\frac{B_{m+iw}}{m+iw} \equiv 0 \bmod p^{re}, \tag{2}$$

with $w := p^{e-1}(p-1)$, where $r \ge 1$, $e \ge 1$, $m > re$, p prime such that $p - 1 \nmid m$. With $r = 1$ we get, in particular