DIVISIBILITY PROPERTIES BY RECURRENCE RELATIONS

TAMÁS LENGYEL
Occidental College, Los Angeles, CA 90041-3314, USA

Abstract We present applications to a fairly general criterion to obtain divisibility properties of a sequence defined by a linear recurrence with coefficients satisfying some divisibility patterns. Let $\nu_p(m)$ denote the exponent of the highest power of a prime p which divides m. This number is often referred to as the p-adic order of m. We determine $\nu_p\left(\sum_{k=0}^{\infty}\binom{n}{k\,p}a^k\right)$ in terms of n for an integer a by the method which offers insight into the structure of the problem without explicitly calculating the coefficients of the related recurrence. We find that the p-adic order of these sums depends on $\nu_p(a+1)$ for a prime $p \geq 3$ and on $\nu_2(a-1)$ for $p = 2$.

1. INTRODUCTION

The motivation of this paper is to extend the use of a method to characterize divisibility properties of combinatorial quantities (see e.g., [1] and [2]). We find linear recurrences that are satisfied by the quantities regarded as sequences to prove divisibility properties.

Recurrences are most often used to calculate the successive terms of a sequence. The approach presented here, however, does not aim at the explicit calculation but at the determination of the recurrences.

There are many different ways of defining a sequence in terms of recurrence relations. Finding recurrences *relevant* to the divisibility properties might be referred to as "creative recursion." The interested reader can find examples for this approach in [5] as linear and nonlinear recurrences are applied to the Fibonacci numbers. We note that a power series based analysis is outlined in [3] to discuss various congruential properties of sequences defined by a linear recurrence.

We focus on linear recurrences with coefficients and set of initial values exhibiting characteristics that guarantee the observed divisibility property of the sequence. This method can be carried out without explicitly calculating the coefficients and initial values.

We deal with a particular class of sums of the form $\sum_{k=0}^{\infty}\binom{n}{k\,p}a^k$. Note that these sums are really finite since $\binom{n}{m} = 0$ for $m > n$. We set $\nu_p(m) = l$

if $p^l|m$ but $p^{l+1}\not|\, m$, $\nu_p(0)=\infty$, and $\nu_p(u/v)=\nu_p(u)-\nu_p(v)$ if both u and v are integers, and define

$$y_n = y_n(p,a) = \sum_{k=0}^{\lfloor n/p \rfloor} \binom{n}{k\,p} a^k. \tag{1}$$

If $a \equiv -1 \pmod p$ then $\nu_p(y_n)$ becomes arbitrarily large as n increases. Our goal is to study the rate of growth. One case in point is the study of some divisibility properties of the Stirling numbers of the second kind, $S(N,K)$. They are ultimately related to $y_K(p,-1)$ as it was showed in [2] where $\nu_p\big(S(N,K)\big)$ is studied for particular values N.

The main result of this paper is

Theorem. *Let p be an arbitrary prime and a be an integer such that $\nu_p(a+1)=1$ if $p \geq 3$, or $a \equiv 3 \pmod 4$ if $p=2$. Then $\nu_p\left(\sum_{k=0}^{\lfloor n/p \rfloor}\binom{n}{k\,p}a^k\right) \geq \left\lfloor \frac{n+1}{p} \right\rfloor - 1$, and equality holds if and only if p divides $n+1$.*

If $p \geq 3$ and $\nu_p(a+1) \geq 2$ then for $n \geq 1$, $\nu_p\left(\sum_{k=0}^{\lfloor n/p \rfloor}\binom{n}{k\,p}a^k\right) \geq \left\lfloor \frac{n}{p-1} \right\rfloor - 1$, and equality holds if and only if $p-1$ divides n.

If $p=2$ and $\nu_2(a-1)=2$ then $\nu_2\left(\sum_{k=0}^{\lfloor n/2 \rfloor}\binom{n}{2k}a^k\right) = n-1$ for $n \equiv 1$ or $2 \bmod 3$, and it is at least as large as n if n is a multiple of 3.

If $p=2$ and $\nu_2(a-1) \geq 3$ then $\nu_2\left(\sum_{k=0}^{\lfloor n/2 \rfloor}\binom{n}{2k}a^k\right) = n-1$.

The proof of the Theorem is based on the derivation and analysis of recurrence relations of orders $p-1$ and p for y_n. Examples 2, 3, and 4 illustrate different applications of the Theorem.

Remark 1. We note that if $a \not\equiv -1 \pmod p$ then $\nu_p(y_n)=0$, $n \geq 0$. In fact, $\sum_{k=0}^{\lfloor n/p \rfloor}\binom{n}{k\,p}a^k \equiv (a+1)^{\lfloor n/p \rfloor} \bmod p$ easily follows from Lucas' Theorem yielding $\binom{n}{k\,p} \equiv \binom{\lfloor n/p \rfloor}{k} \bmod p$.

Previous results used in this paper are given in Section 2. We have included the proof of our basic tool for deriving divisibility properties (Lemma A) in Section 3 for easy reference. Some extensions (Remarks 2 and 3) of Lemma A are also included. Section 4 is devoted to the discussion of the Theorem.

2. TOOLS

We shall need the following general

Lemma A. (Lemma 7 in [2]) *Let p be an arbitrary prime. Assume that the integral sequence x_k satisfies the recurrence*

$$x_k = \sum_{i=1}^{d} c_i x_{k-i}, \quad k \geq d+1, \tag{2}$$

and for some nonnegative integer m, $\nu_p(x_d) = m \geq 0$ and the initial values $x_i, i = 1, 2, \ldots, d-1$, are all divisible by p^m. Let $\nu_p(c_d) = r \geq 1$ and suppose that the coefficients c_i $(i = 1, 2, \ldots, d-1)$ are all divisible by p^r. We write $x_d = \alpha p^m$ and $c_d = \beta p^r$, and set $f(k) = f_p(k, m, r) = m - r + \lfloor \frac{k}{d} \rfloor r$. Then $\nu_p(x_k) \geq f(k)$, and equality holds if and only if $d \mid k$. If the modulo p^r order of β is s then $x_k/p^{f(k)} \pmod{p^r}$ has period sd. In particular, for any integer $t \geq 1$, we have $x_{td} \equiv \alpha\beta^{t-1}p^{m+(t-1)r} \pmod{p^{m+tr}}$.

The lemma helps in obtaining divisibility properties of recurrent sequences when the coefficients follow some divisibility patterns (e.g., [1]). It complements previous results that can be found, for example, in [6] and [8]. The relation between the lower bound $f(k)$ on $\nu_p(x_k)$ is based on the parameters $\nu_p(x_d), \nu_p(c_d)$, and d provided $\nu_p(x_i) \geq \nu_p(x_d)$ and $\nu_p(c_i) \geq \nu_p(c_d)$ for $i = 1, 2, \ldots, d-1$. What is remarkable about this relation is that we do not need the coefficients c_is and initial values x_is explicitly but a proof of their divisibility properties. This fact is utilized in the proof of the Theorem. Some extensions of Lemma A are outlined in Remarks 2 and 3.

3. THE PROOF AND EXTENSIONS OF LEMMA A

Proof of Lemma A. Notice that $(\frac{x_1}{p^{m-r}}, \ldots, \frac{x_{d-1}}{p^{m-r}}, \frac{x_d}{p^m}) \equiv (0, \ldots, 0, \alpha) \pmod{p^r}$, where the congruence is coordinate by coordinate. We obtain $x_{d+1} = c_1 x_d + c_2 x_{d-1} + \cdots + c_d x_1 \equiv 0 \pmod{p^{m+r}}$. Similarly, $x_{d+2}, \ldots, x_{2d-1} \equiv 0 \pmod{p^{m+r}}$. On the other hand, $x_{2d} \equiv c_d x_d \equiv \alpha\beta p^{m+r} \pmod{p^{m+2r}}$. We find that $(\frac{x_{d+1}}{p^m}, \ldots, \frac{x_{2d-1}}{p^m}, \frac{x_{2d}}{p^{m+r}}) \equiv (0, \ldots, 0, \alpha\beta) \pmod{p^r}$. This pattern repeats itself; for instance, we have $(\frac{x_{2d+1}}{p^{m+r}}, \ldots, \frac{x_{3d-1}}{p^{m+r}}, \frac{x_{3d}}{p^{m+2r}}) \equiv (0, \ldots, 0, \alpha\beta^2) \pmod{p^r}$. The proof follows by induction on the index k of sequence x_k. ∎

Remark 2. Note that Lemma A can be extended for linear congruential sequences. For instance, if we replace the recurrence (2) by

$$x_k \equiv \sum_{i=1}^{d} c_i x_{k-i} \pmod{p^{m-r+\lfloor \frac{k}{d} \rfloor r+u}}, \quad k \geq d+1, \tag{3}$$

where u is a nonnegative integer then the lemma still holds. In the case in which $u = 0$ the modular pattern of d consecutive terms closely resembles to the one studied in the proof above. A relevant application is used in the proof of Theorem for $\nu_p(a+1) \geq 2$.

Remark 3. Lemma A can be easily extended to the case in which x_i and c_i are not required to be integers but rationals. The proof is basically unaffected by this relaxation.

Example 1. For the recurrence $x_k \equiv 2x_{k-1}+6x_{k-2} \pmod{2^{\lfloor \frac{k}{2} \rfloor -1+u}}$, $k \geq 3$, with initial values $x_1 = x_2 = 1$ and $u \geq 0$ we obtain that $\nu_2(x_k) \geq \lfloor \frac{k}{2} \rfloor - 1$, and equality holds if and only if k is even. Notice that $d = 2$, $m = 0$, and $r = 1$ in this case. Similarly, by Remark 3 the recurrence $3x_k \equiv 2x_{k-1}+6x_{k-2} \pmod{2^{\lfloor \frac{k}{2} \rfloor -1+u}}$ has the characteristics of the previous sequence regarding divisibility by powers of 2.

4. OUTLINING THE PROOF OF THEOREM

We derive linear recurrence relations for y_{n+p} by an application of

Lemma. *For any $i \geq 1$, $\binom{n}{m-i}$ can be expressed as a linear combination of terms $\binom{n+j}{m}$, $0 \leq j \leq i$, such that the linear combination $\sum_{j=0}^{i} l_j \binom{n+j}{m}$ has integer coefficients $l_j = l_j(i)$ which depend on i and j only. In particular, the coefficient l_j of the term $\binom{n+j}{m}$ is $(-1)^{i-j}\binom{i}{j}$.*

The Lemma can be proved by induction on i or using the properties of the Pascal triangle. We apply Lemma in the

Sketch of the proof of Theorem. We focus on the coefficients of a^k as we express y_{n+p} by (1). It is well known that $\binom{n+p}{kp} = \sum_{i=0}^{p} \binom{n}{kp-i}\binom{p}{i}$, and $\binom{p}{i}$ is divisible by p for all $i: \ 1 \leq i \leq p-1$. Identity (1) yields

$$y_{n+p} = \sum_{k=0}^{\lfloor \frac{n+p}{p} \rfloor} \left\{ \binom{n}{kp}\binom{p}{0} + \cdots + \binom{n}{kp-p}\binom{p}{p} \right\} a^k. \tag{4}$$

We distinguish two cases.

Case 1. $p = 2$ and $\nu_2(a-1) \geq 1$. For $p = 2$ and $n \geq 0$ the summation in (4) reduces to

$$y_{n+2} = y_n + 2(y_{n+1} - y_n) + ay_n = 2y_{n+1} + (a-1)y_n. \tag{5}$$

The proof follows by applying Lemma A if $\nu_2(a-1)=1$, i.e., $a\equiv 3 \bmod 4$. We substitute $x_n=y_{n-1}, n\geq 1$, and observe that $x_1=x_2=1$, $c_1=2, c_2=a-1$, $d=2, m=0$, and $r=1$.

If $\nu_2(a-1)=2$ then we set $z_n=y_n/2^{n-1}$ for $n\geq 0$. The identity (5) can be rewritten as

$$z_n=z_{n-1}+\frac{a-1}{4}z_{n-2},\ n\geq 2, \text{ and } z_0=2, z_1=1. \tag{6}$$

In general, z_n is a Lucas sequence (see e.g., [7]) for any a provided $\nu_2(a-1)=2$. Thus it is periodic with period $(0,1,1)$ *modulo* 2. It follows that $\nu_2(y_n)=n-1$ if $n\equiv 1$ or $2 \bmod 3$, and $\nu_2(y_n)\geq n$ otherwise. On the other hand, if $\nu_2(a-1)\geq 3$ then by taking both sides of identity (6) *modulo* $\frac{a-1}{4}$, it follows that z_n is always an odd number for $n\geq 1$. This fact proves the remarkable pattern $\nu_2(y_n)=n-1$ for $n\geq 1$.

Case 2. $p\geq 3$ and $\nu_p(a+1)\geq 1$. A term-by-term summation in identity (4) results in

$$y_{n+p}=y_n+\sum_{k=0}^{\lfloor\frac{n+p}{p}\rfloor}\sum_{i=1}^{p-1}\binom{n}{kp-i}\binom{p}{i}a^k+ay_n. \tag{7}$$

By identities (1) and (7), Lemma, and simple calculations, it follows that

$$y_{n+p}=c_1y_{n+p-1}+c_2y_{n+p-2}+\ldots+c_{p-1}y_{n+1}+c_py_n \tag{8}$$

where all coefficients $c_1,c_2,\ldots c_p$ are divisible by p. In fact, by binomial coefficient identities we can deduce that

$$c_{p-j}=(-1)^j\binom{p}{j} \text{ for } 1\leq j\leq p-1 \text{ and } c_p=a+1. \tag{9}$$

Lemma A and Remark 2 complete the proof with $d=p$ if $\nu_p(a+1)=1$, and with $d=p-1$ if $\nu_p(a+1)\geq 2$, respectively. We omit the details.

■

We note that if $a\not\equiv -1 \bmod p$ then identity (5) yields that y_n is odd for $p=2$. Similarly, for any prime $p\geq 3$, by (8) and (9) we can derive $y_n\equiv (a+1)y_{n-p} \bmod p$ yielding $y_n\equiv (a+1)^{\lfloor n/p\rfloor} \bmod p$ directly without using Lucas' Theorem.

Regarding the coefficient c_j, we note that only its divisibility by p and identity $l_0(i)=(-1)^i$ were used throughout the proof. The latter one is implicitly applied in transforming identity (7) into (8) with $c_p = a + 1$. Of the p coefficients, only c_p depends on a. We have included three examples to illustrate the use of Theorem.

Example 2. If $p = 2$ and $a = 3$ then $\nu_2(a-1) = 1$, and we obtain that $\nu_2(y_n(2,3)) = \frac{n-1}{2}$ for n odd, and it is at least $\frac{n}{2}$ for n even. This identity appeared in [1].

Example 3. The particular case in which $a = -1$ has been studied in [2], and the coefficients of recurrence (8) of order $p-1$ have also been indentified by the generating function method. For $a = 1$ we can directly deduce $y_n(2,1) = 2^{n-1}$ by carrying out the summation. For any odd prime p, we get $y_n(p,1) \equiv 2^{\lfloor n/p \rfloor} \bmod p$.

Example 4. The Fibonacci numbers $F_n = F_{n-1} + F_{n-2}$, $n \geq 2, F_0 = 0, F_1 = 1$, are related to the sequence $y_n(2,5)$ by the celebrated identity $2^{n-1}F_n = \sum_{k=0}^{\infty} \binom{n}{2k+1} 5^k$. It follows that $F_n = 2^{1-n}5^{-1}(y_{n+1} - y_n)$. Note that $\nu_2(a-1) = 2$ and the recurrence defined by (6) generates the Lucas numbers. The divisibility properties of the Lucas and Fibonacci numbers have been extensively studied (see [3], [5], and [7] for references). A close look at the sequence $\nu_2(y_n)$ for small values n reveals that $\nu_2(F_{3n+1}) = \nu_2(F_{3n+2}) = 0$, and $\nu_2(F_{3n}) \geq 1$. Note that the Theorem implies these relations, for $\nu_2(y_n) \geq n - 1$ and equality holds if and only if $n \equiv 1$ or $2 \bmod 3$. Numerical evidence suggests that $\nu_2(F_{6n+3}) = 1$ and $\nu_2(F_{6n}) \geq 2$. In fact, these patterns continue, and it can be showed (see e.g., [5]) that $\nu_2(F_{12n+6}) = 3$ while $\nu_2(F_{12n}) = \nu_2(n) + 2$.

ACKNOWLEDGMENT

The author wishes to thank the referee for suggestions which improved the presentation of this paper.

REFERENCES

[1] D. M. Bloom, Solution to Problem 428, *College Math. Journal* **22** (1991), 257-259.

[2] I. M. Gessel and T. Lengyel, On the order of Stirling numbers and alternating binomial coefficient sums, 1995, submitted

[3] D. E. Knuth, *The Art of Computer Programming,* vol. 2., Seminumerical Algorithms, Second Edition, Addison-Wesley, Reading, 1981.

[4] T. Lengyel, On the divisibility by 2 of the Stirling numbers of the second kind, *The Fibonacci Quarterly* **32** (1994), 194-201.

[5] T. Lengyel, The order of the Fibonacci and Lucas numbers, *The Fibonacci Quarterly* **33** (1995), 234-239.

[6] N. S. Mendelsohn, Congruence relationships for integral recurrences, *Can. Math. Bull.* **5** (1962), 281-284.

[7] P. Ribenboim, *The Little Book of Big Primes,* Springer-Verlag, New York–Berlin, 1990.

[8] D. W. Robinson, A note on linear recurrent sequences modulo m, *Amer. Math. Monthly* **73** (1966), 619-621.