Difference Equations and Divisibility Properties of Sequences

TAMÁS LENGYEL

Mathematics Department, Occidental College, 1600 Campus Road, Los Angeles, CA 90041, USA

There are many different ways of defining a sequence in terms of solutions to difference equations. In fact, if a sequence satisfies one recurrence then it satisfies an infinite number of recurrences. Arithmetic properties of an integral sequence are often studied by direct methods based on the combinatorial or algebraic definition of the numbers or using their generating function. The rational generating function is the main tool in obtaining various difference equations with coefficients and initial values exhibiting divisibility patterns that can imply particular arithmetic properties of the solutions. In this process we face the challenging task of finding difference equations that are relevant to the divisibility properties by transforming the original rational generating function. As a matter of fact, it is not necessarily the simple difference equation which helps the most in proving the properties. We illustrate this process on several examples and a sequence involving a p-sected binomial sum of the form $y_n = y_n(p,a) = \sum_{k=0}^{\infty} \binom{n}{kp} a^k$ where p is an arbitrary prime. Let $\rho_p(m)$ denote the exponent of the highest power of a prime p which divides m. Recently, the author obtained lower bounds for $\rho_p(y_n)$ based on recurrence relations of order p and $p-1$. The cases with tight bounds have also been characterized.

In this paper we prove that $\rho_p(y_{np}(p,a)) = n$ for $\rho_p(a+1) = 1,\ p \geq 3$. We obtain alternative difference equations of order p^2 for y_n and order p for the p-sected sequence y_{np} by a generating function based method. We also extend general divisibility results relying on the arithmetic properties of the coefficients and initial values.

AMS No. 11B37, 39A10, 11B65, 11B50

KEYWORDS: difference equations, divisibility, binomial sums, p-section

(*received: October 2001)*

1. INTRODUCTION

We view a recurrent sequence as a solution to a linear difference equation with constant coefficients. The study of the various properties of recurrent sequences including arithmetic properties such as periodicity, congruences, and divisibility is often based on their generating functions. We illustrate this approach on different sequences and a specific integral sequence defined as a p-sected sum. A rather different aspect of p-secting a power series is that it may provide an important technical tool in focusing on particular arithmetic details of the original sequence. In addition, the p-section turns the original difference equation into another one without increasing its order. We focus on results related to the p-sected sum $y_n(p,a) = \sum_{k=0}^{\infty} \binom{n}{kp} a^k$ involving binomial coefficients. This sum is of independent interest. We note that it is not immediately obvious that $y_n(p,a)$ should satisfy a recurrence with constant coefficients. Basic and alternative difference equations will be derived in Section 5 that will make this fact clear. Section 2 is devoted to examples to highlight the inherent differences of recurrent sequences from the point of view of divisibility. The generating function method is illustrated and applied to congruences and periodicity in Section 3. In Section 4 we develop and discuss fairly general tools for proving divisibility properties. Section 5 contains the main and some related results. Their derivation is based on the development of basic and alternative difference equations for $y_n(p,a)$.

2. BASIC NOTATIONS AND EXAMPLES

Let the integral sequence y_n satisfy the recurrence relation of order d with integer coefficients c_i

$$y_n = \sum_{i=1}^{d} c_i y_{n-i}, \ n \geq d+1. \tag{1}$$

Let $\rho_p(m)$ denote the exponent of the highest power of a prime p which divides m. We set $\rho_p(0) = \infty$ and $\rho_p(u/v) = \rho_p(u) - \rho_p(v)$ if both u and v are integers. Let $d_p(k)$ be the sum of the digits in the base p representation of k. As it often turns out $\rho_p(y_d)$ and $\rho_p(c_d)$ play an important role in the analysis of $\rho_p(y_n)$. We illustrate the basic differences in results and treatments of difference equations by presenting some examples. These examples are similar in appearance but rather different in nature. They aim at divisibility by 3. In Examples 1 and 2 this choice is arbitrary. The other two examples can be easily modified to discuss divisibility by other primes.

Example 1 Consider the following difference equation $y_n = -y_{n-1} + y_{n-2} + y_{n-3}, \ n \geq 3$, with the initial conditions $y_0 = 0, y_1 = 1, y_2 = -1$. Our goal is to calculate $\rho_3(y_{720})$.

Example 2 We shall determine $\rho_3(y_n)$ and y_n for the solution to the difference equation $y_n = y_{n-1} + y_{n-2}, \ n \geq 2$, with the initial conditions $y_0 = 0, y_1 = 1$.

Example 3 Consider the following difference equation $y_n = 3y_{n-1} - 3y_{n-2}, \ n \geq 3$, with the initial conditions $y_0 = y_1 = y_2 = 1$. Determine or at least give some bounds on the values of $\rho_3(y_n)$ and $\rho_3(y_{3n})$, and calculate y_n.

Example 4 We ask the same questions as in Example 3 for the difference equation $y_n = 3y_{n-1} - 3y_{n-2} + 3y_{n-3}, \ n \geq 3$, with the initial conditions $y_0 = y_1 = y_2 = 1$.

To answer these questions we consider the *generating function* $f(x) = \sum_{k=0}^{\infty} y_k x^k$ of the sequence and try to derive the solution in a "closed form." We explore the properties of the generating function to study arithmetic properties. The generating function $f(x)$ can be written as a rational function $P(x)/Q(x)$. The denominator $Q(x)$ represents the difference equation while the numerator $P(x)$ carries information on the initial values. For a recurrent sequence defined by identity (1) the usual initial choice for $Q(x)$ is the *characteristic polynomial* $1 - c_1x - c_2x^2 - \ldots - c_dx^d$. We note that if the roots of $Q(x)$ are integers then this approach might offer a complete direct treatment of the questions. The generating function method provides the following answers to the examples.

Example 1: We use the *partial fraction expansion* of the generating function

$$f(x) = \frac{x}{(1-x)(1+x)^2} = \frac{1/4}{1-x} + \frac{1/4}{1+x} - \frac{1/2}{(1+x)^2}.$$

This implies $y_n = 1/4 + 1/4 \cdot (-1)^n + 1/2 \cdot (-1)^{n-1}(n+1) = 1/4\{(-1)^{n-1}(2n+1)+1\}$. We get $y_{720} = -360$, $\rho_3(y_{720}) = 2$, and in general,

$$\rho_p(y_n) = \begin{cases} \rho_p(n/2), & \text{if } n \text{ is even,} \\ \rho_p((n+1)/2), & \text{if } n \text{ is odd.} \end{cases}$$

This also follows by observing that the sequence runs through the positive and negative integers in a simple pattern: $0, 1, -1, 2, -2, 3, -3, \ldots$.

Example 2: The generating function is $f(x) = \frac{x}{1-x-x^2}$ and y_n is the familiar Fibonacci number, F_n. For any prime $p \neq 2$ and 5, we have (cf. [4] and [7])

$$\rho_p(y_n) = \begin{cases} \rho_p(n) + \rho_p(F_{n(p)}), & \text{if } n \equiv 0 \pmod{n(p)}, \\ 0, & \text{if } n \not\equiv 0 \pmod{n(p)} \end{cases}$$

where $n(p)$ is the rank of apparition or Fibonacci entry-point of p, i.e., the smallest positive index n such that p divides F_n. For example, $n(3) = 4$ and $\rho_3(F_4) = 1$. Also note that $\rho_5(F_n) = \rho_5(n)$.

Example 3: The generating function is $f(x) = \frac{(1-x)^2}{1-3x+3x^2}$ and $y_n = 2 \cdot 3^{\frac{n}{2}-1} \cos\frac{n\pi}{6}$ for $n \geq 1$ ([13]); therefore, $y_{6n+3} = 0$ and $\rho_3(y_n) = \lfloor \frac{n-1}{2} \rfloor$, $n \not\equiv 3 \bmod 6$.

Example 4: In this case $f(x) = \frac{(1-x)^2}{1-3x+3x^2-3x^3}$ which implies that $\rho_3(y_n) \geq \lfloor \frac{n+1}{3} \rfloor - 1$, and equality holds if and only if $n+1$ is a multiple of 3 (by Theorem C in Section 5). It follows that $\rho_3(y_{3n}) \geq n$. In Section 5 we prove that equality holds here.

We will see that the sequences in the last three examples are related to the sum $y_n(p, a)$.

3. CONGRUENCES AND PERIODICITY VIA GENERATING FUNCTIONS

The generating function carries lots of information on the sequence. However, it is far from being obvious how to recover information relevant to arithmetic properties. Sometimes the fine details of the integer sequence defined by formula (1) are obscured by the usual rational function representation. There are relatively prime polynomials $P(x)$ and $Q(x)$ with integer coefficients and $\deg Q(x) \leq d$ such that $f(x) = P(x)/Q(x)$. In fact, there are infinitely many pairs $(P(x), Q(x))$ of numerators and denominators yielding $f(x) = P(x)/Q(x)$. It might be beneficial to choose the pair with the *minimal polynomial*, $Q(x)$, i.e., the uniquely determined polynomial of least degree. The advantage is that we have to deal with the least number of roots after the rational fraction expansion. The potential drawback of this approach is that the arithmetic properties might get deemphasized. From a historical point of view, the various arithmetic properties of factorials and binomial coefficients were studied by Legendre, Kummer, Lucas, and Anton. They found some remarkable results concerning divisibility and congruential properties. New and related techniques were developed to study other combinatorial quantities and to include periodic properties. A generating function based method was popularized by Fine's proof of Lucas' Theorem on expanding the congruence $\binom{n}{k} \pmod p$ in 1947. A similar application (cf. [13]) shows that the Stirling number of the second kind, $S(n, k)$, satisfies the congruence $S(n, k) \equiv \binom{\lceil k/2 \rceil + n - k - 1}{n-k} \bmod 2$. The modulo p periodicity of a sequence is also often studied via its generating function. The sequence $\{y_n\}_{n \geq 0}$ is said to be *periodic modulo*

M with *period* π if there exists an $n_0 \geq 0$ such that $y_{n+\pi} \equiv y_n \pmod{M}$ for $n \geq n_0$. The smallest such π is called the *minimum period modulo* M. If $n_0 = 0$ then the sequence is said to be purely periodic. The following theorem describes an important situation.

Theorem A *Let $f(x) = 1/Q(x)$ be the generating function of the integer sequence y_n such that $Q(x)$ is a polynomial with integer coefficients. The minimum period modulo M is the smallest integer π such that $(1 - x^\pi)f(x)$ is a polynomial modulo M. If $Q(0) = 1$ and its leading coefficient is relatively prime to $M > 1$ then the sequence y_n is purely periodic modulo M.*

For example, the sequence $\{\binom{n}{k}\}_{n\geq k}$ is purely periodic for its generating function is $1/(1-x)^{k+1}$. The sequence in Example 2 and $\{y_{n+1}\}_{n\geq 0}$ of Example 1 are also purely periodic modulo any integer. Zabek [14] obtained the minimum period of the binomial coefficients modulo p^N in 1956, while Trench [12] extended this result for integer-valued polynomials in 1960. In 1987 Nijenhuis and Wilf [10] determined the modulo p periodicity of $S(n,k)$ in n, while Kwong [5] determined the period modulo $p^N, N > 1$, in 1989. Note that if $P(x)$ and $Q(x)$ are relatively prime modulo p then the *modulo p^N period length* of the sequence y_n depends on the denominator $Q(x)$ only ([4]).

4. DIVISIBILITY VIA GENERATING FUNCTIONS

Let the integral sequence y_n satisfy the recurrence (1) of order d. There are no general methods known to calculate $\rho_p(y_n)$ but ad hoc calculations based on the closed form of the sequence (cf. Examples 1 and 3) or modulo p^N periodicity. For example, the periodic property obtained by Kwong [5] lead to the divisibility properties described in

Theorem B [6, Theorem 2] *Let c be an odd and n be a non-negative integer. If $1 \leq k \leq n+2$ then $\rho_2(k!\, S(c\cdot 2^n, k)) = k-1$, i.e., $\rho_2(S(c\cdot 2^n, k)) = d_2(k) - 1$.*

We discuss three different sets of conditions on the divisibility of the coefficients and initial values that help in the systematic study of $\rho_p(y_n)$.

(a) Assume that the initial value condition $\rho_p(c_d) = 0$ holds. A basis of sequences is defined as a collection of d sequences for which any sequence can be described uniquely as a linear combination of the basis sequences. For any prime p such that $\rho_p(c_d) = 0$, there exist infinitely many integers k in a full arithmetic sequence with the property that a *block of d consecutive terms* of each basis sequence, starting with the kth term, has $d-1$ of these terms divisible by p while the remaining term is congruent to 1 mod p ([9]).

(b) Assume that for some nonnegative integer m and positive integer r, the initial values and coefficients satisfy the conditions

$$\min_{1\leq i\leq d-1} \rho_p(y_i) \geq \rho_p(y_d) = m \geq 0$$

and

$$\min_{1\leq i\leq d-1} \rho_p(c_i) \geq \rho_p(c_d) = r \geq 1,$$

respectively. The lower bound $\rho_p(y_n) \geq (\lfloor \frac{n}{d} \rfloor - 1)r + m$ is obtained in [2], and the cases where the bound is tight are also characterized. (Theorem C is a special case of this with $y_n = y_n(p,a)$.)

(c) If the initial values and coefficients satisfy the conditions

$$\rho_p(y_i) = i,\ 1 \le i \le d,$$

and

$$\rho_p(c_i) \ge i+1,\ 1 \le i \le d-1, \quad \text{and} \quad \rho_p(c_d) = d,$$

respectively, then $\rho_p(y_n) = n$ for $n \ge 1$. The proof follows by induction on n. We have not found any previous reference to this result. Case (c) is illustrated on the sum $y_n(p,a)$ in the Theorem provided $p \ge 3$ and $\rho_p(a+1) = 1$.

What is remarkable about these relations is that there is no need for calculating the coefficients c_is and initial values y_is explicitly but a proof of their divisibility properties. Conditions (b) and (c) imply that $\rho_p(y_n)$ increases as $n \to \infty$ while condition (a) shows that this is not always the case.

5. RESULTS: DIVISIBILITY PROPERTIES OF $y_n(p,a)$

The divisibility properties of $y_n(p,a)$ eventually depend on the divisibility by p of $a+1$ for any prime $p \ge 3$ and $a-1$ for $p=2$. The author recently proved

Theorem C [8] *Let p be an arbitrary prime and a be an integer such that $\rho_p(a+1) = 1$ if $p \ge 3$, or $a \equiv 3 \pmod 4$ if $p = 2$. Then $\rho_p\left(\sum_{k=0}^{\lfloor n/p \rfloor} \binom{n}{k\,p} a^k\right) \ge \left\lfloor \frac{n+1}{p} \right\rfloor - 1$, and equality holds if and only if p divides $n+1$.*
If $p \ge 3$ and $\rho_p(a+1) \ge 2$ then for $n \ge 1$: $\rho_p\left(\sum_{k=0}^{\lfloor n/p \rfloor} \binom{n}{k\,p} a^k\right) \ge \left\lfloor \frac{n}{p-1} \right\rfloor - 1$, and equality holds if and only if $p-1$ divides n.
If $p = 2$ and $\rho_2(a-1) = 2$ then $\rho_2\left(\sum_{k=0}^{\lfloor n/p \rfloor} \binom{n}{k\,p} a^k\right) = n-1$ 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 $\rho_2(a-1) \ge 3$ then $\rho_2\left(\sum_{k=0}^{\lfloor n/p \rfloor} \binom{n}{k\,p} a^k\right) = n-1$.
If $a \not\equiv -1 \bmod p$ then $\sum_{k=0}^{\lfloor n/p \rfloor} \binom{n}{k\,p} a^k \equiv (a+1)^{\lfloor n/p \rfloor} \bmod p$, hence $\rho_p\left(\sum_{k=0}^{\lfloor n/p \rfloor} \binom{n}{k\,p} a^k\right) = 0$.

Remark The last case easily follows from Lucas' Theorem. Actually, if $p|n$ then the congruence $\binom{n}{k\,p} \equiv \binom{n/p}{k} \bmod p$ can be improved to $\binom{n}{k\,p} \equiv \binom{n/p}{k} \bmod p^3$ for $p \ge 5$ (cf. [3]). Therefore, if $a \not\equiv -1 \bmod p$ and n is a multiple of p then the stronger statement $y_n(p,a) \equiv (a+1)^{n/p} \bmod p^3$ holds true for $p \ge 5$. The divisibility structures described in Theorem C are extended in the main result of this paper.

Theorem *Let p be an odd prime and a be an integer such that $\rho_p(a+1) = 1$. Then $\rho_p(y_{np}(p,a)) = n$ for $n \ge 0$. In particular,*

$$y_{(n+p)p} \equiv (a+1)^p y_{np} \pmod{p^{n+p+1}}. \tag{2}$$

For any prime $p \ge 3$ and $a = -1$ we have

$$y_{(n+p)(p-1)} \equiv -p^p y_{n(p-1)} \pmod{p^{n+p}}, \quad n \ge 1. \tag{3}$$

Some special cases with $a = -1, 1,$ and 5 are of considerable interest. The case with $a = -1$ has been studied in [2], and it is related to the divisibility properties of $S(n,k)$. If

$a=-1$ and $p=3$ as in Example 3, then the study of $y_n(3,-1)$ can be carried out by using the trigonometric formula $y_n(3,-1)=2\cdot 3^{\frac{n}{2}-1}\cos\frac{n\pi}{6}, n\geq 1$ [13, Example 4, in Section 2.4]. For $a=1$ direct summation yields $y_n(2,1)=2^{n-1}$ while for any odd prime p we get $y_n(p,1)\equiv 2^{\lfloor n/p\rfloor} \bmod p$. The Fibonacci numbers $F_n=F_{n-1}+F_{n-2}$, $n\geq 2, F_0=0, F_1=1$, are related to $y_n=y_n(2,5)$ by the celebrated identity $2^{n-1}F_n=\sum_{k=0}^{\infty}\binom{n}{2k+1}5^k$. It follows that $F_n=2^{1-n}5^{-1}(y_{n+1}-y_n)$. (For references on $\rho_p(F_n)$ see [4] or [7].) Theorem C also implies that $\rho_2(y_n(2,3))=\frac{n-1}{2}$ for n odd, and it is at least $\frac{n}{2}$ for n even. This identity appeared in [1].

Proof of the Theorem From now on p denotes an odd prime. We obtain a rational generating function for $y_k(p,a)$ with a numerator and denominator of the same degree

$$\sum_{k=1}^{\infty} y_k(p,a)x^k=\frac{x\{(1-x)^{p-1}+ax^{p-1}\}}{(1-x)^p-ax^p}=\frac{N_a(x)}{D_a(x)}. \tag{4}$$

Note that Theorem C can be proven by using this rational generating function. In fact,

$$\sum_{k=1}^{\infty} y_k(3,2)x^k=\frac{x-2x^2+3x^3}{1-3x+3x^2-3x^3} \tag{5}$$

yields the third order difference equation of Example 4: $y_{n+3}=3y_{n+2}-3y_{n+1}+3y_n$, $n\geq 0$. To prove the Theorem we form *alternative recurrence relations* for the original sequence y_n with properties that are more helpful in analyzing its p-sected subsequence y_{np}. For instance, we can switch from the original difference equation to $y_{n+4}=2y_{n+3}+3y_n$. This alternative difference equation can be obtained by substitutions or by realizing that $D_2(x)=1-3x+3x^2-3x^3$ multiplied by $1+x$ becomes $1-2x-3x^4$. The newly obtained difference equation of order 4 suggests an order 12 linear recurrence relation involving only terms with indices whose differences are *multiples* of 3. Unfortunately, this difference equation

$$y_{n+12}=8y_{n+9}+36y_{n+6}+54y_{n+3}+27y_n$$

is of little help in proving the particular divisibility properties as its coefficients did not follow any nice divisibility patterns.

However, there is a general method providing us with a recurrence relation of order p^2 (for $\rho_p(a+1)=1$ and $p\geq 3$) such that all index differences are divisible by p, and the coefficients exhibit some divisibility patterns. We follow Gessel's idea [2] and multiply both $N_a(x)$ and $D_a(x)$ of (4) by $D_a(\omega x)D_a(\omega^2 x)\ldots D_a(\omega^{p-1}x)$, where ω is a primitive pth root of unity. Since $D_a^*(x)=D_a(x)D_a(\omega x)\ldots D_a(\omega^{p-1}x)$ is invariant under substituting ωx for x, it must be a polynomial in x^p. This allows us to p-sect the coefficients of the sequence y_k by multiplying its generating function by $D_a^*(x)$. We are able to write

$$\sum_{k=1}^{\infty} y_k(p,a)x^k=\frac{N_a^*(x)}{D_a^*(x)}, \tag{6}$$

where

$$N_a^*(x)=x\{(1-x)^{p-1}+ax^{p-1}\}\prod_{j=1}^{p-1}((1-\omega^j x)^p-a(\omega^j x)^p)=b_1x+b_2x^2+\ldots,$$

with $b_1 = 1$ and

$$D_a^*(x) = \prod_{j=0}^{p-1} ((1-\omega^j x)^p - a(\omega^j x)^p) = 1 + c_p x^p + c_{2p} x^{2p} + \ldots \tag{7}$$

are polynomials of degree p^2 if $\rho_p(a+1) = 1$ and $p(p-1)$ if $a = -1$, respectively. For example, we find an equivalent form of identity (5)

$$\sum_{k=1}^{\infty} y_k(3,2)x^k = \frac{x + x^2 + 3x^3 + 12x^5 + 18x^6 - 9x^7 + 9x^8 + 27x^9}{1 - 9x^3 - 27x^6 - 27x^9}. \tag{8}$$

If $\rho_p(a+1) = 1$ then by identities (6) and (7), and after determining $y_p, y_{2p}, \ldots y_{p^2}$, we can derive the recurrence relation $(n \geq 1)$

$$y_{(n+p)p} = -c_p y_{(n+p-1)p} - c_{2p} y_{(n+p-2)p} - \ldots - c_{p^2} y_{np}, \tag{9}$$

and that's all we need to evaluate y_{kp}, for $k > p$. For $a = -1$ and $n \geq 1$ we use

$$y_{(n+p)(p-1)} = -c_p y_{(n+p-1)(p-1)-1} - c_{2p} y_{(n+p-2)(p-1)-2} - \ldots - c_{(p-1)p} y_{n(p-1)} \tag{10}$$

to evaluate $y_{k(p-1)}$, for $k > p$. The degree of the denominator in identity (6) is the order of the difference equations in (9) and (10). However, the order can be reduced by a factor of p as we do p-section. To apply case (c) of Section 4 we need

Lemma 1 *If $\rho_p(a+1) = 1$ then $\rho_p(c_{kp}) \geq k+1$ for $k = 1, 2, \ldots, p-1$ and $\rho_p(c_{p^2}) = p$. If $a = -1$ then $\rho_p(c_{kp}) \geq k+1$ for $k = 1, 2, \ldots, p-2$ and $\rho_p(c_{(p-1)p}) = p$.*

This lemma is crucial in proving the Theorem both for small and large values of n. In the former case, for the initial values $k = 1, 2, \ldots, p$, we shall also need

Lemma 2 *For $\rho_p(a+1) = 1$ we have $\rho_p(b_{kp}) = k$ for $k = 1, 2, \ldots, p$.*

For example, multiplying both sides of (8) by $D_2^*(x)$ and equating the coefficients yields $\rho_3(b_{3k}) = k, 1 \leq k \leq 3$, by Lemma 2, and therefore, $\rho_3(y_{3k}) = k, 1 \leq k \leq 3$.

Proof of Lemma 1 Binomial expansion yields $D_a(x) = (\sum_{j=0}^{p-1} \binom{p}{j}(-1)^j x^j) - (a+1)x^p$. We expand the denominator $D_a^*(x)$ symbolically by counting the ways its factors contribute to $x^{kp}, k = 0, 1, \ldots, p$. We observed that $D_a^*(x)$ is actually a polynomial in x^p; therefore, we need only these terms. Any combination of p factors contributing x^{kp} to the expansion can be characterized by the number, i_j, of polynomial factors in (7) in which the term with x^j is selected. For $\rho_p(a+1) = 1$ we get $\sum_{j=0}^{p} j i_j = kp$ and $\sum_{j=0}^{p} i_j = p$ since each of the p factors has exactly one contributing term. By binomial expansion and ignoring the factors of ω, the contribution of any term with the characterization $(i_0, i_1, \ldots, i_p)$ is a multiple of

$$\binom{p}{0}^{i_0} \binom{p}{1}^{i_1} \cdots \binom{p}{p-1}^{i_{p-1}} (-a-1)^{i_p}. \tag{11}$$

We determine the exponent in the power of p which divides this quantity in terms of $(i_0, i_1, \ldots, i_p)$. The exponent is at least $p - i_0 \geq k$ and equality holds if and only if

$(i_0, i_1, \ldots i_p) = (p-k, 0, 0, \ldots, 0, k)$. In this latter case there are $\binom{p}{k}$ ways of choosing the k factors with x^p. It follows that $\rho_p(c_{kp}) \geq k+1$ for $1 \leq k \leq p-1$ and $\rho_p(c_{p^2}) = p$. In fact, $c_{p^2} = -(a+1)^p$.

If $a = -1$ then none of the p factors in (7) have a term involving x^p; therefore, we can remove the last factor of (11). In this case $p - i_0 \geq k+1$ holds yielding $\rho_p(c_{kp}) \geq k+1$ for $1 \leq k \leq p-2$, while $c_{(p-1)p} = p^p$. Note that $c_{kp} = 0$ is also true for k odd ([2]). ■

Proof of Lemma 2 We leave out the details but note that although $N_a^*(x)$ looks less structured than $D_a^*(x)$ it is easier to describe the relevant coefficients $b_{kp}, 1 \leq k \leq p$. Actually, we are able to determine $b_{kp} \pmod{p^{k+1}}$ as calculations similar to those in the proof of Lemma 1 lead to $b_{kp} \equiv (-1)^{k-1}\binom{p-1}{k-1}((a+1)^k + \binom{p}{k}^{p-1}(-1)^k) \pmod{p^{k+1}}$ for $k \leq p-1$ and $b_{p^2} = (a+1)^p$. The condition $\rho_p(a+1) = 1$ guarantees that $\rho_p(b_{kp}) = k$. ■

The proof of the Theorem is now complete by the p-sections $y'_n = y_{np}$ and $c'_i = c_{ip}$, and transforming identity (9) to identity (1) with $d = p$. In fact, Lemmas 1 and 2 guarantee the conditions in part (c) of Section 4. By the lemmas, identities (9) and (10) also imply (2) and (3). ■

Note that the p-secting steps of the proof can be easily extended to polynomial denominators different from $D_a^*(x)$ with the original orders preserved.

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, *Fibonacci Quarterly* **39**(2001), 444–454.

[3] A. Granville, Binomial coefficients modulo prime powers, in preparation at http: //www.math.uga.edu:80/~andrew in Binomial/index.html or Postscript/binomial.ps

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

[5] Y. H. Kwong, Minimum periods of $S(n,k)$ modulo M, *Fibonacci Quarterly* **27**(1989), 217–221.

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

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

[8] T. Lengyel, Divisibility properties by recurrence relations, in: *Advances in Difference Equations*, Proceedings of the Second International Conference on Difference Equations and Its Applications, (S. Elaydi, I. Győri, and G. Ladas, Eds.), Gordon and Breach Science Publishers, London, 1997, pp. 391–397.

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

[10] A. Nijenhuis and H. S. Wilf, Periodicities of partition functions and Stirling numbers modulo p, *J. Number Theory* **25**(1987), 308–312.

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

[12] W. F. Trench, On periodicities of certain sequences of residues, *Amer. Math. Monthly* **67**(1960), 652–656.

[13] H. S. Wilf, *generatingfunctionology*, Academic Press, Boston, 1990.

[14] S. Zabek, Sur la periodicite modulo m des suites de nombres $\binom{n}{k}$, *Ann. Univ. Mariae Curie-Sklodowska*, Sect. A **10**(1956), 37–47.