MINIMUM PERIODS OF $S(n, k)$ MODULO M

Y. H. Harris Kwong
SUNY College at Fredonia, Fredonia, NY 14063
(Submitted May 1987)

1. Introduction

The Stirling number of the second kind, $S(n, k)$, is defined as the number of ways to partition a set of n elements into k nonempty subsets. Obviously, $S(n, k) = 0$ if $n < k$. The sequence $\{S(n, k) \pmod{p^N}\}_{n \geq k}$ is known to be periodic. That is, there exists $N_0 \geq k$ and $\pi \geq 1$ such that

$$S(n + \pi, k) \equiv S(n, k) \pmod{p^N}, \text{ for } n > N_0.$$

Note that any period is divisible by the minimum period. Carlitz [2] showed that if $k > p > 2$ and $p^{b-1} < k \leq p^b$, where $b \geq 2$, $(p - 1)p^{N+b-2}$ is a period for $\{S(n, k) \pmod{p^N}\}_{n \geq k}$.

In this paper, we will determine the minimum period of $\{S(n, k) \pmod{M}\}_{n \geq k}$ for $k \geq 1$ and $M \geq 1$. This extends the results given in [1] and [3], and confirms that the periods in [2] are indeed the minimum periods for odd p.

2. Preliminaries

Given any sequence $\{a_n\}_{n \geq 0}$ of integers, its generating function, $A(x)$, is defined as

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Certainly, $A(x)$ is a formal power series over the ring of integers. A period of $\{a_n \pmod{M}\}_{n \geq 0}$ will also be called a period of $A(x)$ modulo M. The next theorem is obvious.

Theorem 2.1: If $\{a_n\}_{n \geq 0}$ is generated by $A(x)$, then π is a period of $\{a_n \pmod{M}\}_{n \geq 0}$ if and only if $(1 - x^\pi)A(x)$ is a polynomial modulo M.

We will study generating functions in the forms of $1/f(x)$, where $f(x) \in \mathbb{Z}[x]$, and $f(0) = 1$. We have

Theorem 2.2: Given $f(x)$, $u(x) \in \mathbb{Z}[x]$, where $f(0) = u(0) = 1$, let μ and μ' be the minimum periods of $1/f(x)$ and $1/f(x)u(x)$ modulo M, respectively. Then μ divides μ'.

Proof: From the definition of μ', we have

$$\frac{1 - x^{\mu'}}{f(x)u(x)} \equiv h(x) \in \mathbb{Z}_M[x].$$

Therefore,

$$\frac{1 - x^{\mu'}}{f(x)} \equiv h(x)u(x) \in \mathbb{Z}_M[x].$$

This implies that μ' is a period of $1/f(x)$ modulo M. However, μ' may not be the minimum period. Thus, $\mu \mid \mu'$. □

The next theorem is again obvious. Yet, it allows us to assume that M is a prime power.

Theorem 2.3: Let $p_1^{e_1} \cdots p_s^{e_s}$ be the prime factorization of M, and let $\mu(p_i^{e_i})$ be the minimum period of $\{a_n \pmod{p_i^{e_i}}\}_{n \geq 0}$. Then the minimum period of $\{a_n \pmod{M}\}_{n \geq 0}$ is the least common multiple of $\mu(p_i^{e_i})$, where $1 \leq i \leq s$.

Let $\mu(k; p^N)$ be the minimum period of the sequence of Stirling numbers of the second kind $\{S(n, k) \pmod{p^N}\}_{n \geq k}$. It is well known that

$$\sum_{n=0}^{\infty} S(n + k, k)x^n = \frac{1}{(1 - x)(1 - 2x) \cdots (1 - kx)}.$$

It now follows from Theorem 2.2 that $\mu(k; p^N) \mid \mu(k + 1; p^N)$. We would like to know when $\mu(k; p^N) = \mu(k + 1; p^N)$.

Theorem 2.4: Let $A(x)$ be a formal power series over the ring of integers, and $r \in \mathbb{Z}$, where $r \geq 1$. Let π be a period of $A(x)$ modulo p^N. Then π is not a period of $A(x)/(1 - rx)$ iff $r \not\equiv 0 \pmod{p}$ and $h(r^{-1}) \not\equiv 0 \pmod{p^N}$, where $h(x)$ is the polynomial $(1 - x^{\pi})A(x)$ modulo p^N, and r^{-1} is the inverse of r modulo p^N.

Proof: If $r \equiv 0 \pmod{p}$, then $1 - rx$ is invertible (mod p^N). Thus,

$$(1 - x^{\pi})A(x)/(1 - rx)$$

is still a polynomial modulo p^N. Now assume that $r \not\equiv 0 \pmod{p}$, and let

$$h(x) = \sum_{n=0}^{D} a_n x^n.$$

Then we have

$$\frac{(1 - x^{\pi})A(x)}{1 - rx} \equiv \frac{h(x)}{1 - rx} \equiv \left(\sum_{n=0}^{D} a_n x^n\right)\left(\sum_{n=0}^{\infty} (rx)^n\right)$$

$$\equiv \sum_{m=0}^{D-1} \left(\sum_{n=0}^{m} a_n r^{m-n}\right)x^m + \sum_{m=D}^{\infty} \left(\sum_{n=0}^{D} a_n r^{-n}\right)(rx)^m \pmod{p^N}$$

is a polynomial modulo p^N if and only if

$$\sum_{n=0}^{D} a_n r^{-n} \equiv h(r^{-1}) \equiv 0 \pmod{p^N}. \quad \square$$

Therefore, to determine $\mu(k; p^N)$, it suffices to find the minimum period of $1/f_k(x)$ modulo p^N, where

$$f_k(x) = \prod_{\substack{i=1 \\ p \nmid i}}^{k} (1 - ix).$$

3. Stirling Numbers

First of all, we determine $\mu(k; p^N)$ for $1 < k \le p$. The following theorem is a routine exercise.

Theorem 3.1: For $1 < k \le p$, $\mu(k; p^N)$ is the least common multiple of the orders of i modulo p^N for $1 \le i \le k$.

For $k > p$, we use induction on N. The case of $N = 1$ is relatively simple.

Theorem 3.2: If $k > p$, $b \ge 2$, then $\mu(k; p) = (p - 1)p^{b-1}$, where $p^{b-1} < k \le p^b$.

Proof: If $k = p^b$, $b \ge 1$, then

$$f_{p^b}(x) = \prod_{\substack{i=1 \\ p \nmid i}}^{p^b} (1 - ix) \equiv \left\{ \prod_{i=1}^{p-1} (1 - ix) \right\}^{p^{b-1}}$$

$$\equiv (1 - x^{p-1})^{p^{b-1}} \equiv 1 - x^{(p-1)p^{b-1}} \pmod{p}.$$

So, $\mu(p^b; p) = (p - 1)p^{b-1}$. Therefore, $\mu(k; p) \mid (p - 1)p^{b-1}$ for $p^{b-1} < k \le p^b$, $b \ge 1$. In particular, for a fixed $b \ge 2$,

$$h(x) = \frac{1 - x^{(p-1)p^{b-2}}}{f_{p^{b-1}}(x)} \equiv 1 \pmod{p}.$$

From Theorems 2.2 and 2.4, we know that

$$(p - 1)p^{b-2} = \mu(p^{b-1}; p) \text{ divides } \mu(p^{b-1} + 1; p) \text{ properly.}$$

Consider $p^{b-1} < k \le p^b$, $b \ge 2$. On one hand,

$$\mu(p^{b-1} + 1; p) \text{ divides } \mu(k; p),$$

so $(p - 1)p^{b-2}$ is a *proper* divisor of $\mu(k; p)$. On the other hand,

$$\mu(k; p) \text{ divides } \mu(p^b; p) = (p - 1)p^{b-1}.$$

Therefore, $\mu(k; p) = (p - 1)p^{b-1}$. □

The next lemma can be easily verified. We leave the proof to the reader.

Lemma 3.3: Let $f(x) \in \mathbb{Z}[x]$ such that $f(0) = 1$, and let π be a period of $1/f(x)$ modulo p^N. Then $p\pi$ is a period of $1/f(x)$ modulo p^{N+1}.

Corollary 3.4: For $p^{b-1} < k \le p^b$, $b \ge 1$, $\mu(k; p^N)$ always divides $(p - 1)p^{N+b-2}$.

Now we are ready to prove

Theorem 3.5: For $k > p > 2$, and $p^{b-1} < k \le p$, where $b \ge 2$,

$$\mu(k; p^N) = (p - 1)p^{N+b-2}.$$

Proof: The case of $N = 1$ is proved in Theorem 3.2. Assume it is true for some $N \ge 1$; we want to show that it is also true for $N + 1$. Because of Lemma 3.3, if $p^{b-1} < k \le p^b$, $b \ge 2$, then $\mu(k; p^{N+1})$ is either

$$(p - 1)p^{N+b-2} \quad \text{or} \quad (p - 1)p^{N+b-1}.$$

In any case, for $k = p^{b-1}$, we always have

$$h(x) = \frac{1 - x^{(p-1)p^{N+b-2}}}{f_{p^{b-1}}(x)} \in \mathbb{Z}_{p^{N+1}}[x].$$

If we are able to show that $h((p^{b-1} + 1)^{-1}) \not\equiv 0 \pmod{p^{N+1}}$, then

$$(p - 1)p^{N+b-2} \text{ divides } \mu(p^{b-1} + 1; p^{N+1}) \text{ properly.}$$

This implies that $\mu(p^{b-1} + 1; p^{N+1})$ must be $(p - 1)p^{N+b-1}$. Then $\mu(k; p^{N+1})$, where $p^{b-1} < k \le p^b$, will also be $(p - 1)p^{N+b-1}$. Note that $h(x)$ can also be rewritten as

$$h(x) = \frac{1 - x^{(p-1)p^{N+b-3}}}{f_{p^{b-1}}(x)} \sum_{j=0}^{p-1} x^{j(p-1)p^{N+b-3}}.$$

From the inductive hypothesis on N, we have

$$\left.\frac{1 - x^{(p-1)p^{N+b-3}}}{f_{p^{b-1}}(x)}\right|_{x=(p^{b-1}+1)^{-1}} \not\equiv 0 \pmod{p^N}.$$

On the other hand, it is easy to check that the highest power of p that divides

$$\left. x^{j(p-1)p^{N+b-3}} \right|_{x=(p^{b-1}+1)^{-1}}$$

is exactly p. Hence, $h((p^{b-1} + 1)^{-1}) \not\equiv 0 \pmod{p^{N+1}}$. □

Theorem 3.6: If $p = 2$, then

(1) $\mu(1; 2^N) = \mu(2; 2^N) = 1$,

(2) $\mu(3; 2^N) = \mu(4; 2^N) = \begin{cases} 2 & \text{if } N = 1 \text{ or } 2 \\ 2^{N-1} & \text{if } N \ge 3 \end{cases}$,

(3) $\mu(k; 2^N) = 2^{N+b-2}$ for $2^{b-1} < k \le 2^b$, $b \ge 3$.

Proof: The proof is identical to that of Theorem 3.5 for $b \ge 3$. We have to determine $\mu(3; 2^N) = \mu(4; 2^N)$ separately. In this case, we study

$$\frac{1}{f_4(x)} = \frac{1}{(1 - x)(1 - 3x)} = \left(\sum_{i=0}^{\infty} x^i\right)\left(\sum_{j=0}^{\infty} 3^j x^j\right) = \sum_{n=0}^{\infty} b_n x^n,$$

where $b_n = (3^{n+1} - 1)/2$. Thus, $\mu(3; 2^N)$ is the smallest n such that

$$b_n \equiv b_0 = 1 \pmod{2^N}.$$

That is, it is the smallest n such that

$$3^n \equiv 1 \pmod{2^{N+1}}.$$

Therefore, $\mu(3; 2^N)$ satisfies (2) in the statement of the theorem. □

4. Final Remarks

It is possible to obtain the same results without invoking any induction. However, the computation is more involved. We were also able to extend the result to the generating function $1/f(x)$, where $f(x)$ is a product of linear factors of the forms $1 - rx$, $r \in \mathbb{Z}$. These approaches will appear in a forthcoming paper elsewhere.

References

1. H. W. Becker & J. Riordan. "The Arithmetic of Bell and Stirling Numbers." *Amer. J. Math.* *70* (1948):385-394.
2. L. Carlitz. "Congruences for Generalized Bell and Stirling Numbers." *Duke Math. J.* *22* (1955):193-205.
3. A. Nijenhuis & H. S. Wilf. "Periodicities of Partition Functions and Stirling Numbers Modulo p." *J. Number Theory* *25* (1987):308-312.

*****

ON r-GENERALIZED FIBONACCI NUMBERS

François Dubeau
Collège militaire royal de Saint-Jean
Saint-Jean-sur-Richelieu, Québec, Canada, J0J 1R0
(Submitted May 1987)

Introduction

Miles [5] defined the r-generalized Fibonacci numbers ($r \geq 2$) as follows:

$$u_{r,n} = 0 \quad (n = -1, -2, -3, \ldots), \tag{1a}$$

$$u_{r,0} = 1, \tag{1b}$$

$$u_{r,n} = \sum_{i=1}^{r} u_{r,n-i} \quad (n = 1, 2, 3, \ldots). \tag{1c}$$

In such a way, for $r = 2$, we get the ordinary Fibonacci numbers. The object of this paper is to present, in the first section, an elementary proof of the convergence of the sequences of ratios

$$\left\{ t_{r,n} = \frac{u_{r,n}}{u_{r,n-1}} \right\}_{n=1}^{\infty}$$

using neither the theory of difference equations nor the theory of continued fractions. In the second section, we consider a geometric interpretation of the r-generalized Fibonacci numbers that is a natural generalization of the golden rectangle. Finally, in the third section, we consider electrical schemes generating these numbers.

1. Convergence Results

For each $r \geq 2$, we consider the sequence of ratios

$$t_{r,n} = u_{r,n}/u_{r,n-1} \quad (n = 1, 2, 3, \ldots).$$

Rather than using the theory of difference equations to obtain a formula for $u_{r,n}$ and use it to prove the convergence of the sequence to the unique positive root of the polynomial

$$p_r(x) = x^r - \sum_{i=1}^{r} x^{r-i} \quad \text{(see [5])},$$