MINIMUM PERIODS OF BINOMIAL COEFFICIENTS MODULO M

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

1. Introduction

The minimum period of the sequence

$$\left\{\binom{n}{k} \pmod{M}\right\}_{n \geq k}$$

was discovered by Zabek [6] by investigating the Pascal triangle. Applying Vandermonde's convolution to $\binom{n+N}{k}$, Trench [5] obtained identical periods. By studying the highest prime power dividing $q^n - 1$, Fray [2] extended the results to q-binomial coefficients. All these approaches depend directly on the properties of the binomial coefficients. It is difficult to apply these techniques to other infinite integer sequences. In this paper, we will look at the problem from another perspective. In particular, we will consider the generating function of

$$\left\{\binom{n}{k}\right\}_{n \geq k}: \quad \frac{1}{(1 - x)^{k+1}} = \sum_{n=0}^{\infty} \binom{n + k}{k} x^n.$$

The problem can then be solved by studying divisibility of polynomials over $\mathbb{Z}_M$. This approach relies on the generating functions only, so it can also be applied to other sequences with similar generating functions. Thus, in this paper, we will assume all sequences to be infinite integer sequences.

2. Preliminaries

A sequence $\{a_n\}_{n \geq 0}$ is said to be *periodic modulo* M, with *period* π, if there is an integer $n_0 \geq 0$ such that, for $n \geq n_0$,

$$a_{n+\pi} \equiv a_n \pmod{M}.$$

If $n_0 = 0$, $\{a_n\}_{n \geq 0}$ is said to be *purely periodic modulo* M. If

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

generates $\{a_n\}_{n \geq 0}$, we also call π a period of $A(x)$ modulo M. Clearly, any period always divides the *minimum period*, which is, by definition, the smallest period. The next two theorems are obvious.

Theorem 2.1: If $\{a_n\}_{n \geq 0}$ is generated by $A(x)$, then π is a period of $\{a_n \pmod{M}\}_{n \geq 0}$ iff

$$(1 - x^{\pi})A(x) \in \mathbb{Z}_M[x].$$

Theorem 2.2: If $\{a_n\}_{n \geq 0}$ is generated by $A(x)$ and periodic modulo M with period π, then it is purely periodic modulo M iff the degree of $(1 - x^{\pi})A(x)$ is at most $\pi - 1$ in $\mathbb{Z}_M[x]$.

We will study generating functions of the form $1/f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $f(0) = 1$. Under these conditions, π is a period of $1/f(x)$ modulo M iff $f(x)$ divides $1 - x^{\pi} \pmod{M}$.

Theorem 2.3: 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: It suffices to show that μ' is a period of $1/f(x)$ modulo M. Equivalently, it suffices to show that $f(x)$ divides $1 - x^{\mu'} \pmod{M}$, which follows from the fact that $f(x)u(x)$ divides $1 - x^{\mu'} \pmod{M}$. □

The next result, which is again obvious, allows us to assume, for the rest of this paper, that M is a prime power.

Theorem 2.4: Let $p_1^{e_1} \ldots p_s^{e_s}$ be the prime factorization of M, and $\mu(p_i^{e_i})$ 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 $1 \leq i \leq s$.

Finally, if we know a period of $\{a_n \pmod{p}\}_{n \geq 0}$, we have an upper bound for the period of $\{a_n \pmod{p^N}\}_{n \geq 0}$.

Theorem 2.5: If π is a period of $1/f(x)$ modulo p^N, then $p\pi$ is a period of $1/f(x)$ modulo p^{N+1}.

Proof: From Theorem 2.1,

$$x^{\pi} = 1 - f(x)h(x) + p^N g(x), \text{ for some } h(x), g(x) \in \mathbb{Z}[x].$$

Then, for some $H(x)$, $G(x) \in \mathbb{Z}[x]$,

$$x^{p\pi} = \{1 - f(x)h(x)\}^p + p^{N+1}G(x) = 1 - f(x)H(x) + p^{N+1}G(x).$$

Thus, $f(x)$ divides $1 - x^{p\pi} \pmod{p^{N+1}}$. □

Corollary 2.6: If π is a period of $1/f(x)$ modulo p, then πp^{N-1} is a period of $1/f(x)$ modulo p^N for $N \geq 1$.

3. Binomial Coefficients

Let $\mu(t; p^N)$ be the minimum period of $1/(1 - x)^t$ modulo p^N. Since $\mu(1; p^N) = 1$ for $N \geq 1$, we may assume that $t > 1$. From Theorem 2.3, $\mu(t; p^N)$ always divides $\mu(t + 1; p^N)$ for $N \geq 1$. What we would like to know is, when will

$$\mu(t; p^N) \neq \mu(t + 1; p^N);$$

which would imply that $\mu(t; p^N)$ divides $\mu(t + 1; p^N)$ *properly*. The following theorem provides one such criterion.

Theorem 3.1: Let π be a period of $1/(1 - x)^t$ modulo M. Then π is also a period of $1/(1 - x)^{t+1}$ modulo M iff $h(1) \equiv 0 \pmod{M}$, where $h(x)$ is the polynomial $(1 - x^{\pi})/(1 - x)^t$ in $\mathbb{Z}_M[x]$.

Proof: Let $h(x) = \sum_{n=0}^{D} a_n x^n \in \mathbb{Z}_M[x]$. Then

$$\frac{1 - x^{\pi}}{(1 - x)^{t+1}} \equiv \frac{h(x)}{1 - x} \pmod{M}$$

$$= \left(\sum_{m=0}^{\infty} x^m\right)\left(\sum_{n=0}^{D} a_n x^n\right)$$

$$= \sum_{m=0}^{D-1}\left(\sum_{n=0}^{m} a_n\right)x^m + h(1)\sum_{m=D}^{\infty} x^m$$

is a polynomial modulo M iff $h(1) \equiv 0 \pmod{M}$. □

For $b \geq 0$, $(1 - x)^{p^b} \equiv 1 - x^{p^b} \pmod{p}$; thus, $\mu(p^b; p) = p^b$. Consequently, Corollary 2.6 implies that $\mu(p^b; p^N) \mid p^{N+b-1}$. But, from Theorem 2.3,

$$\mu(t; p^N) \mid \mu(p^b; p^N) \quad \text{if } t \leq p^b.$$

Hence, for $p^{b-1} < t \leq p^b$, $b \geq 1$, we have

$$G(x) = \frac{1 - x^{N+b-1}}{(1 - x)^t} \in \mathbb{Z}_M[x].$$

Since the leading coefficient of $(1 - x)^t$ is ± 1, the degree of $G(x)$ is at most $p^{N+b-1} - 1$. We conclude from Theorem 2.2 that $1/(1 - x)^t$ is purely periodic modulo M. In other words,

Theorem 3.2: $\left\{\binom{n}{k} \pmod{M}\right\}_{n \geq k}$ is purely periodic, for $k \geq 0$.

In particular,

$$H(x) = (1 - x^{p^{N+b-2}})/(1 - x)^{b-1}$$

is a polynomial modulo p^N:

$$H(x) \equiv \sum_{j=0}^{p^{N+b-2}-1} \binom{p^{b-1} + j - 1}{j} x^j \pmod{p^N}.$$

We want to know if p^{N+b-2} is still a period of $1/(1 - x)^{p^{b-1}+1}$ modulo p^N. In order to apply Theorem 3.1, we evaluate

$$H(1) \equiv \sum_{j=0}^{p^{N+b-2}-1} \binom{p^{b-1} + j - 1}{j} = \binom{p^{N+b-2} + p^{b-1} - 1}{p^{N+b-2} - 1} \pmod{p^N}.$$

The highest power of p which divides $\binom{A+B}{A}$ is the number of carries in the p-ary addition of $A + B$. (See, for example, [1], pp. 270-271.) Thus,

$$p^{N-1} \| H(1) \quad \text{and} \quad H(1) \not\equiv 0 \pmod{p^N}.$$

It now follows from Theorem 3.1 that

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

So, p^{N+b-2} is a *proper divisor* of $\mu(t; p^N)$ for all $t > p^{b-1}$. On the other hand, for $t \leq p^b$,

$$\mu(t; p^N) \mid \mu(p^b; p^N) \quad \text{and} \quad \mu(p^b; p^N) \mid p^{N+b-1}.$$

Therefore, we have just proved

Theorem 3.3: The minimum period for $1/(1 - x)^t$ modulo p^N is 1 if $t = 1$, and p^{N+b-1} if $p^{b-1} < t \leq p^b$, $b \geq 1$.

Corollary 3.4: The minimum period of

$$\left\{\binom{n}{k} \pmod{p^N}\right\}_{n \geq k}$$

is 1 if $k = 0$, and p^{N+b-1} if $p^{b-1} \leq k < p^b$, $b \geq 1$.

Corollary 3.5: If $p_1^{e_1} \ldots p_s^{e_s}$ is the prime factorization of M, then the minimum period of

$$\left\{\binom{n}{k} \pmod{M}\right\}_{n \geq k}$$

is 1 if $k = 0$, and

$$\prod_{i=1}^{s} p_i^{e_i + b_i - 1}$$

if $p_i^{b_i - 1} \leq k < p_i^{b_i}$, $b_i \geq 1$ for $1 \leq i \leq s$.

4. Final Remarks

Our approach can be used to determine minimum periods of many other infinite integer sequences. For example, the minimum periods of the Stirling numbers of the second kind are determined in [3]. In particular, we found the minimum periods of $1/f(x)$ modulo M, where the factors of $f(x)$ are all linear (in the form of $1 - rx$), or are all binomials of the form $1 - x^r$. These allow us to extend the results in [4] to any prime power modulus, and hence to any modulus. These results will appear in a forthcoming article elsewhere.

References

1. L. E. Dickson. *History of the Theory of Numbers.* Vol. I. Washington, D.C.: Carnegie Inst., 1952.
2. R. D. Fray. "Congruence Properties of Ordinary and q-Binomial Coefficients." *Duke Math J. 34* (1967):467-480.
3. Y. H. Kwong. "Minimum Periods of $S(n, k)$ Modulo M." *Fibonacci Quarterly 27.3* (1989):217-221.
4. A. Nijenhuis & H. S. Wilf. "Periodicities of Partition Functions and Stirling Numbers Modulo p." *J. Number Theory 25* (1987):308-312.
5. W. F. Trench. "On the Periodicities of Certain Sequences of Residues." *Amer. Math. Monthly 67* (1960):652-656.
6. S. Zabek. "Sur la Périodicité Modulo m des Suites de Nombers $\binom{n}{k}$." *Ann. Univ. Mariae Curie-Sklodowska A10* (1956):37-37.

*****