The Periodic Property of Binomial Coefficients Modulo m and Its Applications

Chi-Jen Lu*   Shi-Chun Tsai†

Abstract

We show the periodic property of binomial coefficient modulo m, where m is a composite number. It is shown that the cycle is much longer than that of modulo a prime power. We illustrate two applications of this interesting property. First we prove a degree lower bound on representing the boolean function $OR(x_1, \cdots, x_n)$ with a polynomial modulo m. It is surprising that the degree is lower when m is composite. Secondly, we prove the number of distinct m-ary codes generated by repeatedly applying a specific m-ary Gray code mapping.

1 Preliminary

Let j be a non-negative integer, and let k and m be any positive integers. Fix k and m, then the integer function $f(j) = \binom{j}{k} \bmod m$ is a cyclic function of j. This property has been proved by several other authors by using different methods [2, 6, 8]. It is interesting that the cycle is much longer when m is a compsite integer. We exploit this periodic property to study computational problems. We first prove a degree lower bound for representing the boolean function $OR(x_1, \cdots, x_n)$ with a polynomial modulo m. This is used to study the computational power of MOD_m gate [7] (the boolean function $\mathrm{MOD}_m(x_1, ..., x_n)$ is defined to be 0 if $\sum_{i=0}^{n} x_i$ is a multiple of m and 1 otherwise). For completeness, we prove the property in the following.

Lemma 1 *[6] Let p be any prime number, and let a and k be any positive integers. Then $\binom{j}{k}$ mod p^a has the cycle length p^{a+e}, where $e = \lfloor \log_p k \rfloor$.*

Proof.

*Institute of Information Science, Academia Sinica, Nankang 11529, Taipei, Taiwan, Email: cjlu@iis.sinica.edu.tw

†Dept of Information Management, National Chi-Nan University, 1 University Road, Pu-Li, Nan-Tou 545, Taiwan, Email: tsai@im.ncnu.edu.tw. The work was supported in part by the National Science Council of Taiwan under contract NSC 89-2213-E-260-009.

Define $L_k = p^{a+\lfloor \log_p k \rfloor}$. We want to prove $\binom{sL_k+j}{k} \equiv \binom{j}{k} \pmod{p^a}$ for any non-negative integer s and any positive integer k by induction on j. For the base case $j = 0$, since $\binom{sL_k}{k} = \frac{sL_k}{sL_k-k}\binom{sL_k-1}{k}$ is an integer and the largest power of p that divides $sL_k - k$ is at most $p^{\lfloor \log_p k \rfloor}$, we know $\binom{sL_k}{k}$ is divisible by p^a. Thus $\binom{sL_k}{k} \equiv 0 \pmod{p^a}$ for all non-negative integer s and any positive integer k. Suppose $\binom{sL_k+j}{k} \equiv \binom{j}{k} \pmod{p^a}$ for any non-negative integer s and any positive integer k, for $0 \le j \le i$. Now consider the case when $j = i + 1$.

$$\begin{aligned}
\binom{sL_k+i+1}{k} &= \binom{sL_k+i}{k} + \binom{sL_k+i}{k-1} \\
&\equiv \binom{i}{k} + \binom{i}{k-1} \pmod{p^a}, \quad \text{because } L_{k-1}|L_k. \\
&\equiv \binom{i+1}{k} \pmod{p^a}.
\end{aligned}$$

Next we need to prove that L_k is the smallest cycle. To show L_k is the smallest cycle of $\binom{j}{k}$ mod p^a, we prove that there exists an i, $0 \le i < k$, such that $\binom{\frac{L_k}{p}+i}{k} \not\equiv \binom{i}{k} \equiv 0 \pmod{p^a}$. WLOG let $k = p^l + i$, where l is any positive integer and $0 \le i < p^{l+1} - p^l$. With this assumption we have $\lfloor \log_p k \rfloor = l$. By induction on i, we will prove $p^a \not| \binom{p^{l+a-1}+i}{p^l+i}$. This is clear for the base case $i = 0$. Suppose it holds for the case up to i, i.e. $p^a \not| \binom{p^{l+a-1}+m}{p^l+m}$, where $0 \le m \le i \le p^{l+1} - p^l - 1$. Consider the case $m = i + 1$. We are interested in the case when $i+1 < p^{l+1} - p^l$. Then $\binom{p^{l+a-1}+i+1}{p^l+i+1} = \frac{p^{l+a-1}+i+1}{p^l+i+1}\binom{p^{l+a-1}+i}{p^l+i}$. We know $\frac{p^{l+a-1}+i+1}{p^l+i+1}$ is not divisible by p. By the induction hypothesis we have $p^a \not| \binom{p^{l+a-1}+i+1}{p^l+i+1}$. This completes the proof. $\square$

By applying the Chinese Remainder Theorem we can generalize the above lemma as follows.

Lemma 2 *Let m_1 and m_2 be any two relatively prime positive integers. If $\binom{j}{k}$ mod m_1 and $\binom{j}{k}$ mod m_2 has the cycle length l_1 and l_2, respectively, then $\binom{j}{k}$ mod $m_1 m_2$ has the cycle length $l_1 l_2$.*

Theorem 3 *Let $m = p_1^{a_1} \cdots p_r^{a_r}$ be an arbitrary positive integer, where the p_i's are distinct prime numbers and the a_i's are positive integers. Let $e_i = \lfloor \log_{p_i} k \rfloor$ for $1 \le i \le r$, then $\binom{j}{k}$ mod m has the cycle length $\prod_{i=1}^r p_i^{a_i+e_i}$.*

Proof. By Lemmas 1 and 2. $\square$

2 Lower bounds on representing boolean functions

Let $P(x_1, \cdots, x_n) \in Z_m[x_1, \cdots, x_n]$ be a polynomial representing a Boolean function $f(x_1, \cdots, x_n)$. If the degree of P is d, then we can write $P(x_1, \cdots, x_n) = \sum_{A \subseteq [n]; |A| \le d} c_A X_A$. We use $\delta(f, m)$ to denote the lowest degree among such polynomials that represent f. Recall that we define $f(A) = f(a_1, \cdots, a_n)$, where $a_i = 1$ if $i \in A$; 0 otherwise. $P(A)$ is defined similarly. For convenience, for each $A \subseteq [n]$ we use b_A to denote $P(A)$. Since P represents f, it is clear that if $f(A) = 0$ then $b_A = 0$ and if $f(A) = 1$ then b_A can be any non-zero integer in Z_m. If there are M different assignments in $\{0,1\}^n$ satisfying f then by a simple counting argument there are $(m-1)^M$ multilinear polynomials in Z_m representing f. For any $A \subseteq [n]$ it is clear that $X_D(A) = 0$ if $D \not\subseteq A$ and $X_D(A) = 1$ if $D \subseteq A$. Thus $b_A = P(A) = \sum_{D \subseteq A; |D| \leq d} c_D$. There are 2^n possible inputs. With the given boolean function we can choose a set of b_A's such that $b_A = 0$ if $f(A) = 0$ and $b_A \neq 0$ if $f(A) = 1$. Then we can set up a system of linear equations with $\sum_{i=0}^{d} \binom{n}{i}$ variables if the representing polynomial has degree d. By solving the linear equations, we prove some useful relations among b_D's and c_A's over any ring Z_m. Actually, Lemma 4.1 is a special case of the well known Möbius inversion theorem [4].

Lemma 4 *[6]*

1. *If $A \subset [n]$ and $|A| \leq d$ then*

$$c_A = \sum_{D \subseteq A} (-1)^{|A|-|D|} b_D.$$

2. *If $A \subseteq [n]$ and $|A| > d$ then*

$$b_A = \sum_{D \subset A; |D| \leq d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} b_D.$$

¿From the above lemma we know the first $(\sum_{i=0}^{d} \binom{n}{i})$ b_A's will determine the coefficients of the polynomial P and the rest of the b_A's. With the above lemmas we can prove several lower bounds systematically. The key of the proof relies on the periodic property of the binomial coefficients modulo m.

¿From Lemma 3 we prove lower bounds for OR and other functions.

Theorem 5 *Let m be any non-prime-power composite number. If the* OR *function of n variables is represented by a symmetric polynomial modulo m, then the degree is $\Omega(n^{1/r})$, where r is the number of distinct primes dividing m.*

Proof. Let P be a symmetric polynomial of degree d that represents the OR function over Z_m. Say $m = \prod_{i=1}^{r} p_i^{a_i}$. Suppose $p_i^{e_i} \leq d < p_i^{e_i+1}$ for $1 \leq i \leq r$. It is clear that $P(\emptyset) = b_\emptyset = 0$ and $P(A) = b_A \neq 0$ if $A \subseteq [n]$ and $A \neq \emptyset$. Since P is symmetric for any $A, B \subseteq [n]$, if $|A| = |B|$ then $b_A = b_B$ and so $c_A = c_B$. Thus we can use $c_{|A|}$ to indicate c_A and the others of the same cardinality. Consider the case $|A| > d$. It is easy to see $b_A = \sum_{i=1}^{d} \binom{|A|}{i} c_i$. By Theorem 3, we know $\binom{|A|}{d}$ mod m has the cycle length $\prod_{j=1}^{r} p_j^{e_j+a_j}$, when $|A|$ ranges over the non-negative integers. We denote the cycle length as L. If $i > j$ then the cycle length of $\binom{|A|}{i}$ mod m is a multiple of the cycle length of $\binom{|A|}{j}$ mod m. Thus $\binom{0+L}{i} \equiv 0 \pmod{m}$, for $1 \leq i \leq d$, since $\binom{0}{i} \equiv 0 \pmod{m}$. We must have $n < L$ otherwise $b_A = 0$ for $|A| = L$, which contradicts the definition of the OR function. Hence, $n < L = \prod_{j=1}^{r} p_j^{e_j+a_j} \leq md^r$, and therefore $d = \Omega(n^{1/r})$. $\Box$

It is still open to find an upper bound for the non-symmetric case. To resolve the problem, we can either try to improve the lower bound or find a small upper bound for the non-symmetric representation of the OR function.

Theorem 6 *Let m be a positive composite integer which is not a prime power then* $\delta(\neg\mathrm{MOD}_m, m) = \Omega(n)$.

Proof. Let P be a representing polynomial of the $\neg\mathrm{MOD}_m$ function of degree d. Choose p^l such that $p^l | m$ and $p^l \not| \, c_\emptyset$, where p is a prime factor of m. Such p and l exist, since $c_\emptyset \not\equiv 0 \pmod{m}$. It is clear $b_\emptyset = c_\emptyset$. WLOG, let $n = p^{k+l} + p^k - 1$, where k is an arbitrary integer. From Lemma 4.2, we have $b_A = \sum_{D \subset A; |D| \leq d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} b_D$, for $|A| > d$. We are interested in the sets $A \subset [n]$ with $|A| = p^{k+l}$ and the sum of the corresponding b_A's.

$$\begin{aligned}
\sum_{A \subset [n]} b_A &= \sum_{A \subset [n]} \sum_{D \subset A; |D| \leq d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} b_D \\
&= \sum_{D \subset [n]; |D| \leq d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} \binom{n-|D|}{|A|-|D|} b_D \\
&= \sum_{D \subset [n]; |D| \leq d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} \binom{n-|D|}{n-|A|} b_D.
\end{aligned}$$

It's clear $n - |A| = p^k - 1$ and $b_A \equiv 0 \pmod{m}$, since $m \not| \, |A|$ and by the definition of the $\neg\mathrm{MOD}_m$ function. If $0 < |D| < p^k$ then $n - |D| = p^{k+l} + (p^k - |D| - 1)$. And so $\binom{n-|D|}{n-|A|} = \binom{n-|D|}{p^k-1} \equiv \binom{p^k-|D|-1}{p^k-1} \equiv 0 \pmod{p^l}$, since by Lemma 1, $\binom{j}{p^k-1} \mod p^l$ has the cycle length p^{k+l-1}. Therefore, we have

$$\begin{aligned}
0 &\equiv (-1)^d \binom{|A|-1}{d} \binom{n}{n-|A|} b_\emptyset \pmod{p^l} \\
&\equiv (-1)^d \binom{|A|-1}{d} b_\emptyset \pmod{p^l}.
\end{aligned}$$

If we let $d < p^k$, then $\binom{j}{d} \pmod{p^l}$ has the cycle length at most p^{k+l-1}. Thus,

$$\begin{aligned}
0 &\equiv (-1)^d \binom{|A|-1}{d} b_\emptyset \pmod{p^l} \\
&\equiv (-1)^d \binom{p^{l+\lfloor \log_p d \rfloor} - 1}{d} b_\emptyset \pmod{p^l} \\
&\equiv b_\emptyset \sum_{i=0}^{d} (-1)^i \binom{p^{l+\lfloor \log_p d \rfloor}}{i} \pmod{p^l} \qquad (1) \\
&\equiv b_\emptyset \pmod{p^l}.
\end{aligned}$$

The modular equality in (1) follows from the identity $\sum_{i=0}^{n}(-1)^i\binom{m}{i} = (-1)^n\binom{m-1}{n}$. It leads to a contradiction. Therefore , $d \geq p^k = \frac{n+1}{p^l+1}$. The theorem is clear now for the case of $n = p^{k+l} + p^k - 1$. For the case $p^{k+l} + p^k - 1 < n < p^{k+1+l} + p^{k+1} - 1$, the MOD_m-degree must be at least p^k, which is at least $\frac{n+1}{p^{l+1}+p}$. And the proof is completed. $\square$

By following the above proof we have an immediate corollary.

Corollary 7 *Let p be a prime number which is not a factor of m, then $\delta(\neg\mathrm{MOD}_p, m) = \Omega(n)$.*

3 Iterating m-ary Gray code

Let ℓ and m be positive integers greater than one. An m-ary Gray code of dimension ℓ is a sequence of α^ℓ distinct m-ary strings of length ℓ, such that any two adjacent strings differ in exactly one position. So a Gray code corresponds to a bijection, mapping integers between 0 and $m^\ell - 1$ to m-ary strings of length ℓ. When viewing such integers in base m with ℓ digits, the mapping can be seen as a permutation among m-ary strings of length ℓ. Sharma and Khanna [5] defined one such mapping, denoted by $\mathcal{K}$, in the following way.

Definition. [5] $\mathcal{K}(x_1x_2\cdots x_\ell) = g_1g_2\cdots g_\ell$, where

$$g_i = \begin{cases} x_1 & \text{if } i = 1, \\ x_i - x_{i-1} \pmod{m} & 1 < i \leq \ell. \end{cases}$$

Equivalently, $\mathcal{K}^{-1}(g_1g_2\cdots g_\ell) = x_1x_2\cdots x_\ell$, where

$$x_i = \begin{cases} g_1 & \text{if } i = 1, \\ g_i + x_{i-1} \pmod{m} & 1 < i \leq \ell. \end{cases}$$

Culberson [1] and Lichtner [3] studied the number of distinct sets of codes that can be generated by repeated applications of the mapping $\mathcal{K}$. This is the same question as determining the order of the mapping $\mathcal{K}$, defined in the following.

Definition. Let $\mathcal{K}^0 = \mathcal{I}$, the identity mapping, i.e. $\mathcal{I}(x) = x$ for all x. For $i \geq 0$, let $\mathcal{K}^{i+1} = \mathcal{K} \circ \mathcal{K}^i$, i.e. $\mathcal{K}^{i+1}(x) = \mathcal{K}(\mathcal{K}^i(x))$. The order of $\mathcal{K}$ is the smallest positive integer m such that $\mathcal{K}^m = \mathcal{I}$. Similarly, we can define $\mathcal{K}^{-(i+1)} = \mathcal{K}^{-1} \circ \mathcal{K}^{-i}$ for $i \geq 0$.

Note that the order of $\mathcal{K}$ is the same as the order of $\mathcal{K}^{-1}$, and we will work on $\mathcal{K}^{-1}$ instead. Lichtner [3] derived an explicit formula for the order of $\mathcal{K}^{-1}$. In this note, we give a much simpler proof for Lichtner's result. The key idea is an observation on a simple connection between the order of $\mathcal{K}^{-1}$ and the period of binomial coefficients modulo m. Then the result follows immediately from a known periodic property of binomial coefficients modulo m [2, 6, 8].

Let $x = x_1x_2\cdots x_\ell$. Define $x^i = \mathcal{K}^{-i}(x)$ for $i \geq 0$, with $x^0 = \mathcal{K}^0(x) = x$. Let x^i_j denote the j-th digit of x^i. Here are some simple facts.

Lemma 8 *[3]*

1. $x^i_j \equiv x^i_{j-1} + x^{i-1}_j \pmod{m}$, *where* $i \geq 1$ *and* $1 < j \leq \ell$.

2. $x^i_j \equiv \sum_{k=1}^{j} \binom{i+j-k-1}{j-k} x_k \pmod{m}$, *where* $i \geq 1$ *and* $1 \leq j \leq \ell$.

3. *If* $\binom{i+j-2}{j-1} \equiv 0 \pmod{m}$, *for* $2 \leq j \leq \ell$, *then* $x^i = x$.

4. *Let* $x = x_1 x_2 \cdots x_\ell$ *be an* m*-ary string such that* $x_1 \not\equiv 0 \pmod{m}$ *and* $GCD(x_1, m) = 1$. *If there is an* j, $2 \leq j \leq \ell$, *such that* $\binom{i+j-2}{j-1} \not\equiv 0 \pmod{m}$, *then* $x^i \neq x$.

Lemma 8.1-2 follows from the definition of $\mathcal{K}$ and by induction. Lemma 8.3-4 follows from Lemma 8.1-2.

¿From now on, we assume that m has the form of

$$m = p_1^{n_1} \cdots p_q^{n_q},$$

where p_i's are distinct primes and n_i's are positive integers. Litchner generalized Culberson's result [1] and proved the following theorem.

Theorem 9 *[3] Let* $\ell > 1$ *and let* $e_i = \lfloor \log_{p_i}(\ell - 1) \rfloor$ *for* $1 \leq i \leq q$. *Then the order of* $\mathcal{K}^{-1}$ *is exactly* $L = \prod_{i=1}^{q} p_i^{n_i + e_i}$.

We will give a simpler proof of Litchner's theorem above, given the following known result on the period of the function $f_{m,k}$, defined as

$$f_{m,k}(x) = \binom{x}{k} \pmod{m}.$$

We restate lemma 3 as following.

Lemma 10 *[2, 6, 8] Let* k *be a positive integer and let* $d_i = \lfloor \log_{p_i} k \rfloor$ *for* $1 \leq i \leq q$. *Then the period of the function* $f_{m,k}$ *is exactly* $\prod_{i=1}^{q} p_i^{n_i + d_i}$.

Corollary 11 *For any positive integers* k_1, k_2 *with* $k_1 \leq k_2$, *the period of* f_{m,k_1} *divides the period of* f_{m,k_2}.

Our main technical contribution is the following simple connection.

Lemma 12 *The order of* $\mathcal{K}^{-1}$ *is the same as the period of the function* $f_{m,\ell-1}$.

Lemma 10 and Lemma 12 together imply Theorem 9 immediately. It remains to prove Lemma 12.

3.1 Proof of Lemma 12

Let $x = x_1 x_2 \cdots x_\ell$ be an arbitrary m-ary string and let $x^i = \mathcal{K}^{-i}(x)$. Lemma 8.2 states that

$$\begin{aligned}
x_1^i &\equiv \binom{i-1}{0} x_1 \pmod m \\
x_2^i &\equiv \binom{i}{1} x_1 + \binom{i-1}{0} x_2 \pmod m \\
x_3^i &\equiv \binom{i+1}{2} x_1 + \binom{i}{1} x_2 + \binom{i-1}{0} x_3 \pmod m \\
&\vdots \\
x_\ell^i &\equiv \binom{i+\ell-2}{\ell-1} x_1 + \binom{i+\ell-3}{\ell-2} x_2 + \cdots + \binom{i}{1} x_{\ell-1} + \binom{i-1}{0} x_\ell \pmod m
\end{aligned}$$

Observe that there are ℓ different binomial coefficients above, so $\mathcal{K}^{-i}$ is completely determined by the vector $c^i = c_1^i c_2^i \cdots c_\ell^i$, where

$$c_j^i = \binom{i+j-2}{j-1} \pmod m.$$

We use the convention that $\binom{a}{0} = 1$ for any integer a. Note that $c^0 = 100\cdots 0$. As i increases, the vector c^i changes in a periodic fashion, due to the periodic behavior of its components. Recall that $L = \prod_{i=1}^q p_i^{n_i+e_i}$. We show that the period is L and the cycle occurs exactly when the vector becomes $100\cdots 0$ again.

Clearly $c_1^L = 1$. From Lemma 10 and Corollary 11, we know that for $1 < j \le \ell$, $c_j^L = \binom{L+j-2}{j-1} \pmod m = \binom{0+j-2}{j-1} \pmod m = 0$. So $c^L = 100\cdots 0 = c^0$. Now, as $c_1^i = 1$ and for $j > 1$,

$$c_j^i = c_{j-1}^i + c_j^{i-1} \pmod m,$$

we see that the vector c^i is completely determined by the vector c^{i-1}. So the same pattern repeats again from c^L. The cycle could not be shorter since $c_\ell^i = f_{m,\ell-1}(i+\ell-2)$, considered as a function of i, has a period of exactly L. So L is the smallest positive integer i such that $c^i = c^0$.

Since $c^L = 100\cdots 0$, $\mathcal{K}^{-L}$ is the identity mapping. On the other hand, for any positive $i < L$, $c^i \neq 100\cdots 0$. Lemma 8.4, tells us that $\mathcal{K}^{-i}x \neq x$ for any x with $x_1 = 1$, and thus $\mathcal{K}^{-i} \neq \mathcal{I}$. So the order of $\mathcal{K}^{-1}$ is exactly L.

4 Conclusion and Remarks

By using the periodic property of binomial coefficients, we show two applications in computational complexity: first we prove degree lower bounds for representing some boolean functions using polynomials modulo m; secondly we give a proof on the order of the mapping $\mathcal{K}$. Lichtner's proof could have been more straightforward, if he had known the periodic property of binomial coefficients. With the above examples, we expect that this nice property should have more applications to be discovered.

References

[1] J. Culberson, Mutation-crossover isomorphisms and the construction of discriminating functions, *Evolutionary Comput.,* 2 (1995), pp. 279–311.

[2] Y.H. Kwong, Minimum periods of binomial coefficients modulo M, *Fibonacci Quart.,* 27 (1989), pp. 64–79.

[3] J. Lichtner, Iterating an α-ary Gray code, In *SIAM J. Discrete Math.*, 11 (1998), pp. 381–386.

[4] L. Lovász, *Combinatorial Problems and Exercises*, 2nd ed., North-Holland, Amsterdam, 1993.

[5] B.D. Sharma and R.K. Khanna, On m-ary Gray codes, *Inform. Sci.*, 15 (1978), pp. 31-43.

[6] S-C. Tsai, Lower bounds on representing boolean functions as polynomials in Z_m, In *SIAM J. Discrete Math.*, 9 (1996), pp. 55–62.

[7] A. C-C. Yao, *Separating the polynomial-time hierarchy by oracles*, in Proc. 26th IEEE Symposium on Foundations of Computer Science, 1985, pp. 1–10.

[8] S. Zabek, Sur la périodicité modulo m des suits de nombres $\binom{n}{k}$, Ann. Univ. Mariae Curie-Sklodowska, A10 (1956), pp. 37–47.