ON PERIODICITIES OF CERTAIN SEQUENCES OF RESIDUES

BY

WILLIAM F. TRENCH

Reprinted from the AMERICAN MATHEMATICAL MONTHLY
Vol. 67, No. 7, August-September, 1960

ON PERIODICITIES OF CERTAIN SEQUENCES OF RESIDUES

WILLIAM F. TRENCH, R.C.A. Missile and Surface Radar Division

Let H be the class of polynomials $F(x)$ such that $F(m)$ is an integer whenever m is an integer. It is not difficult to show that H is identical with the class of polynomials of the form

$$F(x) = \sum_{j=0}^{K} a_j \binom{x}{j},$$

where a_j is an integer for $0 \leqq j \leqq K$. Let M be an arbitrary positive integer:

$$M = \prod_{i=1}^{n} P_i^{k_i},$$

where $P_1, \cdots, P_n$ are distinct primes and $k_i \geqq 1$ $(1 \leqq i \leqq n)$. Let K be a positive integer, and $r_1, \cdots, r_n$ be integers chosen so that

$$P_i^{r_i-1} \leqq K < P_i^{r_i} \qquad (1 \leqq i \leqq n). \tag{1}$$

Finally, define

$$N = \prod_{i=1}^{n} P_i^{k_i+r_i-1}.$$

The symbols M, N, and K will retain these meanings throughout the paper.

Since $\Delta^{K+1}F(m)=0$ for every integer m,* it is clear that the sequence $\{F(m) \pmod{M}\}$ must have a period which does not exceed M^K. It is our purpose to determine the exact periods of such sequences.

LEMMA 1. *The sequence* $\{\binom{m}{K} \pmod{M}\}$ $(m=\cdots, -1, 0, 1, \cdots)$ *is periodic with fundamental period* N.

Proof. Expand $\binom{m+N}{K}$ about $N=0$ to obtain

$$\binom{m+N}{K} = \binom{m}{K} + \sum_{j=1}^{K}\binom{N}{j}\binom{m}{K-j}. \tag{2}$$

We first show that $\binom{N}{j}$ is divisible by M for $j=1, \cdots, K$. Write

$$\binom{N}{j} = \frac{N}{i}\cdot\frac{N-1}{1}\cdot\frac{N-2}{2}\cdots\frac{N-(j-1)}{j-1}\cdot \tag{3}$$

If $1\leqq R\leqq j-1$, the highest power of P_i which divides R is $P_i^{r_i-1}$, since $j\leqq K < P_i^{r_i}$. Hence, since $P_i^{r_i-1}$ is a factor of N, $N-R$ is divisible by $P_i^{q_i}$ $(q_i\leqq r_i-1)$ if and only if R is. On the other hand, since j is not divisible by $P_i^{r_i}$, the factor $P_i^{k_i}$ in the numerator of N/j is not cancelled. As this argument holds for $i=1, \cdots, n$, we can conclude that

$$\binom{N}{j} \equiv 0 \pmod{M} \qquad (j = 1, \cdots, K),$$

and the periodicity follows from (2).

If N' is a second period, then the greatest common divisor of N and N' is also a period. Let $(N, N') = \prod_{i=1}^{n} P_i^{q_i}$. If N is not the fundamental period, then there is a subscript i such that $q_i < r_i+k_i-1$. Without loss of generality, assume that $i=1$. Then

$$N_1 = P_1^{r_1+k_1-2}\prod_{i=2}^{n} P_i^{r_i+k_i-1}$$

is also a period. We will show that this is impossible for any $K \geqq P_1^{r_1-1}$. First we assert that

* Δ is the forward difference operator. That is, $\Delta F(m) = F(m+1) - F(m)$.

$$\binom{N_1}{P_1^{r_1-1}} \not\equiv 0 \pmod{M}. \tag{4}$$

This is obvious if $r_1=1$. If $r_1>1$, expand as in (3). For $R=1, 2, \cdots, P_1^{r_1-1}$, it can again be seen that the powers of P_1 in factors of the form $(N_1-R)/R$ are cancelled. Now $N_1/P_1^{r_1-1}$ is not divisible by $P_1^{k_1}$, and (4) follows.

Next let $K=P_1^{r_1-1}+j$ with $j>0$. If $\{\binom{m}{K} \pmod{M}\}$ has period N_1, it follows that

$$\binom{N_1+\nu}{P_1^{r_1-1}+j} \equiv 0 \pmod{M} \qquad (\nu = 0, 1, \cdots, j).$$

However, this leads to a contraction of (4), because we could then write

$$\binom{N_1}{P_1^{r_1-1}} = \sum_{\nu=0}^{j} (-1)^{j-\nu} \binom{N_1+\nu}{P_1^{r_1-1}+j} \binom{j}{\nu} \equiv 0 \pmod{M}.$$

This completes the proof of Lemma 1.

We can immediately generalize to

THEOREM 1. *Let*

$$F(x) = \sum_{j=0}^{K} a_j \binom{x}{j} \tag{5}$$

be in H. If $(a_K, M)=1$, *the sequence* $\{F(m) \pmod{M}\}$ *is periodic, with fundamental period N.*

Proof. If K is the least integer which satisfies (1), we can infer from Lemma 1 that $\{a_K\binom{m}{K} \pmod{M}\}$ has fundamental period N, while all lower degree terms have periods which are proper divisors of N. Thus the conclusion follows for this case. Assume that $K-r-1$, $(r \geqq 0)$, is the least integer which satisfies (1), and that the theorem is true when $K-r$ is the smallest such integer. Consider

$$\Delta F(x) = F(x+1) - F(x) = \sum_{j=0}^{K-1} a_{j+1} \binom{x}{j}.$$

In this equation, $K-1$ plays the role of K in (5). From the induction assumption, the sequence $\{\Delta F(m) \pmod{M}\}$ has the fundamental period N. From this it follows that the fundamental period of $\{F(m) \pmod{M}\}$ is not less than N, while from Lemma 1 it follows that it is not greater than N.

COROLLARY. *If $F(x)$ is any polynomial in H, of degree K, then the sequence* $\{F(m) \pmod{M}\}$ *has a fundamental period of the form*

$$N_1 = \prod_{i=1}^{n} P_i^{j_i}, \quad \textit{where} \quad 0 \leqq j_i \leqq r_i + k_i - 1 \ (i = 1, \cdots, n).$$

As a partial converse to Theorem 1, we have

THEOREM 2. *Let* $\{f_m\}$ $(-\infty < m < \infty)$ *be a sequence of integers, and let*

$$\Delta^{K+1} f_m \equiv 0 \pmod{M} \qquad (m = 0, \pm 1, \pm 2, \cdots).$$

Then there is in H *a polynomial* $F(x)$ *of degree not exceeding* K, *such that*

$$F(m) \equiv f_m \pmod{M} \qquad (m = 0, \pm 1, \pm 2, \cdots). \tag{6}$$

Consequently, the sequence $\{f_m(\bmod M)\}$ *has a fundamental period which divides* N.

Proof. Define

$$F(x) = \sum_{r=0}^{K} \Delta^r f_0 \binom{x}{r}.$$

Then

$$F(m) = f_m \qquad (m = 0, 1, \cdots, K). \tag{7}$$

Since $F(x)$ is of degree not greater than K, we have

$$0 = \Delta^{K+1} F(m) \equiv \Delta^{K+1} f_m \pmod{M} \qquad (-\infty < m < \infty),$$

and (6) follows from (7) by a trivial induction.

It can also be stated that, if in addition to the hypothesis of Theorem 2, there is an integer m such that $(\Delta^K f_m, M) = 1$, then the fundamental period of $\{f_m \pmod{M}\}$ is precisely N.

In the case where M is a prime, we can obtain a stronger result.

THEOREM 3. *Let* P *be a prime, and* $F(x)$ *a polynomial in* H, *of degree* K, *such that the coefficient of* $\binom{x}{K}$ *is not divisible by* P. *Then, if* $P^{r-1} \leqq K < P^r$, *the sequence* $\{F(m) \pmod{P}\}$ *is periodic with fundamental period* P^r. *Conversely, if a sequence of integers* $\{f_m\}$, $(-\infty < m < \infty)$, *is such that* $\{f_m \pmod{P}\}$ *has fundamental period* P^r, *then there is a polynomial* $F(x)$ *in* H, *with* $P^{r-1} \leqq \deg F(x) < P^r$, *and*

$$F(m) \equiv f_m \pmod{P} \qquad (-\infty < m < \infty). \tag{8}$$

Proof. The first statement is a special case of Theorem 1. For the converse, let $\{f_m \pmod{P}\}$ have the assumed periodicity, and consider the linear system in the P^r unknowns $\{a_i\}$:

$$\sum_{n=0}^{m} a_n \binom{m}{n} \equiv f_m \pmod{P} \quad (m = 0, 1, \cdots, P^r - 1).$$

Since this is a diagonal system, with coefficients on the diagonal equal to unity, there is a unique solution $\{a_n\}$ in the field of integers modulo P. Define

$$F(x) = \sum_{n=0}^{P^r-1} a_n \binom{x}{n}.$$

Then $F(x)$ satisfies (8) for $m=0, 1, \cdots, P^r-1$. By the corollary to Theorem 1, $\{F(m) \pmod P\}$ also has period P^r, and therefore $F(x)$ satisfies (8) for all m. Deg $F(x) \geqq P^{r-1}$, since if not $\{F(m) \pmod P\}$ would have period P^{r-1}, and so would $\{f_m \pmod P\}$, contrary to assumption.

For an alternate proof of the converse, one can observe that $\Delta^{P^r} f_m \equiv 0 \pmod P$ for all m, and the conclusion essentially follows from Theorem 2.

Acknowledgement. The work reported here was stimulated by an attempt to prove [1], which follows from Theorem 3 for $P=2$.

The referee has pointed out that Lemma 1 has appeared previously in [2]. The result is obtained there for $m=0, 1, \cdots$, by a lengthy argument involving a chain of six lemmas and two theorems which are weaker than Lemma 1.

References

1. M. Hausner, Problem E 1365, this Monthly, vol. 16, 1959, p. 312.

2. S. Zabek, Sur la periodicite modulo m des suites de nombres $\binom{n}{k}$, Ann. Univ. Mariae Curie-Sklodowska, Sect. 10, 1956, pp. 37–47.