INVOLVE 2:4(2009)

A complete classification of $\mathbb{Z}_p$-sequences corresponding to a polynomial

Leonard Huang

(Communicated by Andrew Granville)

Let p be a prime number and set $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. A $\mathbb{Z}_p$-sequence is a function $S : \mathbb{Z} \to \mathbb{Z}_p$. Let $\mathcal{R}$ be the set $\{P \in \mathbb{R}[X] \mid P(\mathbb{Z}) \subseteq \mathbb{Z}\}$. We prove that the set of sequences of the form $(P(n) \pmod p)_{n\in\mathbb{Z}}$, where $P \in \mathcal{R}$, is precisely the set of periodic $\mathbb{Z}_p$-sequences with period equal to a p-power. Given a $\mathbb{Z}_p$-sequence, we will also determine all $P \in \mathcal{R}$ that correspond to the sequence according to the manner above.

1. Preliminaries

Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ and $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$.

Definition 1. Define the sequence $(P_i)_{i\in\mathbb{N}_0}$ of polynomials in $\mathbb{R}[X]$ as follows:

$$P_0 = 1 \quad \text{and} \quad \text{for all } i \in \mathbb{N} : P_i = \binom{X}{i} = \frac{\prod_{j=0}^{i-1}(X-j)}{i!}.$$

Lemma 2 [Niven et al. 1991, pp. 42–43, Problems 11, 14, 15]. *We have*

$$\mathcal{R} = \Big\{\sum_{i=0}^{m} c_i P_i \mid m \in \mathbb{N}_0, c_0, \ldots, c_m \in \mathbb{Z}\Big\}.$$

Proof. Clearly, $\mathcal{R} \supseteq \big\{\sum_{i=0}^{m} c_i P_i \mid m \in \mathbb{N}_0, c_0, \ldots, c_m \in \mathbb{Z}\big\}$, so we only need to prove the reverse inclusion.

Let $P \in \mathcal{R}$ have degree m. If the system of equations

$$P(j) = \sum_{i=0}^{m} c_i P_i(j), \quad j = 0, \ldots, m, \tag{1}$$

MSC2000: 11B83.

Keywords: $\mathbb{Z}_p$-sequences, polynomials, free abelian group.

in the unknowns $c_0, \ldots, c_m$ has a solution $(c_0, \ldots, c_m) \in \mathbb{Z}^{m+1}$, then $P = \sum_{i=0}^{m} c_i P_i$ because P and $\sum_{i=0}^{m} c_i P_i$ are polynomials of degree at most m that agree at the $m+1$ points $0, \ldots, m$. However, (1) is equivalent to the system

$$c_j = P(j) - \sum_{i=0}^{j-1} \binom{j}{i} c_i, \quad j = 0, \ldots, m,$$

which clearly has a unique solution $(c_0, \ldots, c_m) \in \mathbb{Z}^{m+1}$. □

Lemma 3. *Let p be a prime number. For every $k \in \mathbb{N}$,*

$$\binom{p^k}{0} \equiv 1 \pmod{p} \quad \textit{and} \quad \textit{for all } i \in \{1, \ldots, p^k - 1\} : \binom{p^k}{i} \equiv 0 \pmod{p}.$$

Proof. The first identity is clearly true. When $i \in \{1, \ldots, p^k - 1\}$, we have

$$\frac{p^k}{i} = \frac{\binom{p^k}{i}}{\binom{p^k - 1}{i-1}}.$$

Write i as $p^l m$, where $l \in \mathbb{N}_0$ and m is a positive integer not divisible by p. From the equation

$$\frac{p^{k-l}}{m} = \frac{p^k}{i} = \frac{\binom{p^k}{i}}{\binom{p^k - 1}{i-1}},$$

we immediately obtain

$$p^{k-l} \binom{p^k - 1}{i-1} = m \binom{p^k}{i}.$$

Since $i < p^k$, we have $k - l \geq 1$. Thus p divides $m\binom{p^k}{i}$, and since it does not divide m, it must divide $\binom{p^k}{i}$. This proves that

$$\binom{p^k}{i} \equiv 0 \pmod{p}.$$

As $i \in \{1, \ldots, p^k - 1\}$ was arbitrary, Lemma 3 is true. □

Lemma 4. *Let p be a prime number. Then, for every $n \in \mathbb{Z}$, $k \in \mathbb{N}_0$ and $i \in \{0, \ldots, p^k - 1\}$,*

$$\binom{n + p^k}{i} \equiv \binom{n}{i} \pmod{p}. \tag{2}$$

Proof. Let $k \in \mathbb{N}_0$. Define a well-ordering $\prec$ on $\{0, \ldots, p^k - 1\} \times \mathbb{N}_0$ by setting $(i, n) \prec (i', n')$ if either (i) $i < i'$, or (ii) $i = i'$ and $n < n'$. By the principle of induction, it suffices to prove the following statements:

(A) For every $i \in \{0, \ldots, p^k - 1\}$,

$$\binom{0+p^k}{i} \equiv \binom{0}{i} \pmod{p}.$$

(B) Given $(i^*, n^*) \in \{0, \ldots, p^k - 1\} \times \mathbb{N}_0$, if

$$\text{for every } (i,n) \preceq (i^*, n^*): \quad \binom{n+p^k}{i} \equiv \binom{n}{i} \pmod{p}, \tag{3}$$

and

$$\text{for every } (i,n) \preceq (i^*, n^*): \quad \binom{-n+p^k}{i} \equiv \binom{-n}{i} \pmod{p}, \tag{4}$$

then, respectively,

$$\binom{n^*+1+p^k}{i^*} \equiv \binom{n^*+1}{i^*} \pmod{p} \tag{5}$$

and

$$\binom{-(n^*+1)+p^k}{i^*} \equiv \binom{-(n^*+1)}{i^*} \pmod{p}. \tag{6}$$

Statement (A) holds by Lemma 3. For Statement (B), we consider two cases: (i) $i^* = 0$ and (ii) $i^* > 0$. In Case (i), (B) is vacuously true. In Case (ii), we deduce (5) from (3) by applying Pascal's Rule:

$$\begin{aligned} \binom{n^*+1+p^k}{i^*} &= \binom{n^*+p^k}{i^*-1} + \binom{n^*+p^k}{i^*} && \text{(by Pascal's Rule)} \\ &\equiv \binom{n^*}{i^*-1} + \binom{n^*}{i^*} && \text{(from (3))} \\ &\equiv \binom{n^*+1}{i^*} \pmod{p} && \text{(by Pascal's Rule again).} \end{aligned}$$

In a similar fashion, we deduce (6) from (4):

$$\begin{aligned} \binom{-(n^*+1)+p^k}{i^*} &= \binom{-n^*+p^k}{i^*} - \binom{-(n^*+1)+p^k}{i^*-1} \\ &\equiv \binom{-n^*}{i^*} - \binom{-(n^*+1)}{i^*-1} \equiv \binom{-(n^*+1)}{i^*} \pmod{p}. \end{aligned}$$

Therefore (B) is true in Case (ii). Since $k \in \mathbb{N}_0$ was arbitrary, Lemma 4 is true. □

Corollary 5. *For every $i \in \mathbb{N}_0$, the sequence $\left(\binom{n}{i} \pmod{p}\right)_{n\in\mathbb{Z}}$ is periodic with period equal to a p-power.*

Proof. Choose $k \in \mathbb{N}_0$ such that $i < p^k$. By Lemma 4, $\binom{n+p^k}{i} \equiv \binom{n}{i} \pmod{p}$ for every $n \in \mathbb{Z}$. This clearly implies the claim. □

Corollary 6. *For every $P \in \mathcal{R}$, the sequence $(P(n) \pmod{p})_{n\in\mathbb{Z}}$ is periodic with period equal to a p-power.*

Proof. Let $P \in \mathcal{R}$. By Lemma 2, there exist $m \in \mathbb{N}_0$ and $c_0, \dots, c_m \in \mathbb{Z}$ such that $P = \sum_{i=0}^{m} c_i P_i$. Then,

$$(P(n) \pmod{p})_{n \in \mathbb{Z}} = \left(\sum_{i=0}^{m} c_i P_i(n) \pmod{p} \right)_{n \in \mathbb{Z}}.$$

By Corollary 5, each $(P_i(n) \pmod{p})_{n \in \mathbb{Z}}$ is periodic with period equal to a p-power. We conclude that $(P(n) \pmod{p})_{n \in \mathbb{Z}}$ is also periodic with period equal to a p-power. □

2. Main results

Theorem 7. *Let $p\mathcal{R}$ be the subset of $\mathcal{R}$ obtained by multiplying every $P \in \mathcal{R}$ by p. A polynomial $P \in \mathcal{R}$ lies in $p\mathcal{R}$ if and only if p divides $P(n)$ for all $n \in \mathbb{Z}$; in symbols,*

$$p\mathcal{R} = \left\{ P \in \mathcal{R} \mid (P(n) \pmod{p})_{n \in \mathbb{Z}} = (0)_{n \in \mathbb{Z}} \right\}.$$

Proof. It is clear that every polynomial in $p\mathcal{R}$ corresponds to $(0)_{n \in \mathbb{Z}}$, so let us suppose that $P \in \mathcal{R}$ satisfies

$$(P(n) \pmod{p})_{n \in \mathbb{Z}} = (0)_{n \in \mathbb{Z}}.$$

Then, by Lemma 2, there exist $m \in \mathbb{N}_0$ and $c_0, \dots, c_m \in \mathbb{Z}$ such that $P = \sum_{i=0}^{m} c_i P_i$. We claim that $c_0, \dots, c_m \equiv 0 \pmod{p}$.

To prove the claim, we use mathematical induction. By our hypothesis,

$$P(0) = \sum_{i=0}^{m} c_i P_i(0) = c_0 \equiv 0 \pmod{p}.$$

Hence, the claim is true for c_0. Next, suppose that $k \in \mathbb{N}_0$ and that the claim is true for c_j for every $j \leq k$. If $j = m$, we are done. If $j < m$, then

$$P(j+1) = \sum_{i=0}^{m} c_i P_i(j+1) \equiv c_{j+1} \equiv 0 \pmod{p}.$$

Hence, the claim is true for c_{j+1} as well. By induction, the claim is true for all $c_0, \dots, c_m$. This shows that $P \in p\mathcal{R}$. □

Theorem 8. *The set of sequences of the form $(P(n) \pmod{p})_{n \in \mathbb{Z}}$, where $P \in \mathcal{R}$, is precisely the set of periodic $\mathbb{Z}_p$-sequences with period equal to a p-power.*

Proof. By virtue of Corollary 6, we only have to prove that every periodic $\mathbb{Z}_p$-sequence with period equal to a p-power corresponds to some $P \in \mathcal{R}$.

Let $k \in \mathbb{N}_0$. Define A to be the set

$$\left\{ \sum_{i=0}^{p^k-1} c_i P_i \;\Big|\; c_1, \dots, c_{p^k-1} \in \{0, \dots, p-1\} \right\},$$

and B to be set of all periodic $\mathbb{Z}_p$-sequences with period equal to p^l, where $0 \le l \le k$. By Lemma 4 and Theorem 7, every polynomial in A corresponds to a unique sequence in B. Since $|A| = |B| = p^{p^k}$, the correspondence is actually one-to-one. Therefore, every periodic $\mathbb{Z}_p$-sequence with period p^k corresponds to a unique polynomial of the form

$$\sum_{i=0}^{p^k-1} c_i P_i,$$

where $c_1, \dots, c_{p^k-1} \in \{0, \dots, p-1\}$. Since k was arbitrary, Theorem 8 is proven.

The theorem, however, would not be of much use unless the coefficients c_i can be determined. Hence, let S be a periodic $\mathbb{Z}_p$-sequence with period p^k, where $k \in \mathbb{N}_0$. By the first part, there exist $c_1, \dots, c_{p^k-1} \in \{0, \dots, p-1\}$ such that

$$S = \left(\sum_{i=0}^{p^k-1} c_i P_i(n) \pmod p \right)_{n \in \mathbb{Z}}.$$

From this identity, we obtain the equations

$$S(j) = \sum_{i=0}^{p^k-1} c_i \binom{j}{i}, \qquad j = 0, \dots, p^k - 1.$$

Some algebraic manipulation shows that the c_i's satisfy

$$c_i \equiv \sum_{j=0}^{i} (-1)^j \binom{i}{j} S(i-j) \pmod p, \qquad i = 0, \dots, p^k - 1. \qquad \square$$

Corollary 9. *Let S be a periodic $\mathbb{Z}_p$-sequence with period p^k, where $k \in \mathbb{N}_0$. Then, the set of all $P \in \mathfrak{R}$ which correspond to S is*

$$\left(\sum_{i=0}^{p^k-1} c_i P_i \right) + p\mathfrak{R},$$

where c_i is the least positive residue of $\sum_{j=0}^{i} (-1)^j \binom{i}{j} S(i-j) \pmod p$ for every $i = 0, \dots, p^k - 1$.

Proof. Let c_i satisfy the hypothesis given in the corollary. By Theorem 8,

$$S - \left(\sum_{i=0}^{p^k-1} c_i P_i(n) \pmod p \right)_{n\in\mathbb{Z}} = (0)_{n\in\mathbb{Z}}.$$

The corollary now follows directly from Theorem 7. □

With both theorems and Corollary 9, we have a complete classification of $\mathbb{Z}_p$-sequences corresponding to a polynomial. Let us now look at some examples.

3. Examples

Example 10. To determine whether or not a $\mathbb{Z}_p$-sequence corresponds to a polynomial, simply investigate its periodicity. For example, the $\mathbb{Z}_7$-sequence

$$\dots, \widehat{4}, 0, 6, 4, 0, 6, \dots$$

(the $\frown$ marks the zeroth element of the sequence) does not correspond to any polynomial because, although periodic, it has period 3, which is not a power of 7.

Example 11. The $\mathbb{Z}_3$-sequence

$$\dots, \widehat{1}, 0, 1, 2, 0, 1, 1, 0, 2, \dots$$

is periodic with period $9 = 3^2$, so it corresponds to a polynomial. The proof of Theorem 8 says that the sequence corresponds to

$$\binom{X}{0} + 2\binom{X}{1} + 2\binom{X}{2} + \binom{X}{3} + 2\binom{X}{4} + \binom{X}{5} + \binom{X}{6} + 2\binom{X}{7} + 2\binom{X}{8}.$$

4. Conclusion

We can add some algebraic flavor to the classification problem as follows. Let $\mathcal{S}$ denote the set of periodic $\mathbb{Z}_p$-sequences with period equal to a p-power. It is not difficult to see that $\mathcal{S}$ forms an abelian group under component-wise addition. Notice also that $\mathcal{R}$ is a free abelian group generated by the set $\{P_i \mid i \in \mathbb{N}_0\}$ and that the mapping

$$\phi : \mathcal{R} \to \mathcal{S},$$
$$\phi : P \mapsto (P(n) \pmod p)_{n\in\mathbb{Z}}$$

is a surjective group homomorphism. By the first isomorphism theorem for groups, $\mathcal{R}/\ker(\phi) \cong \mathcal{S}$. However, Theorem 7 says that $\ker(\phi) = p\mathcal{R}$, so we obtain $\mathcal{R}/p\mathcal{R} \cong \mathcal{S}$. This elegant algebraic identity summarizes much of the effort invested in this paper.

Theorem 8 may be generalized so as to obtain a complete classification of all $\mathbb{Z}_m$-sequences corresponding to a polynomial for an arbitrary integer $m \geq 2$. The first step to doing this is to consider the case when m is a prime-power. It would be too good to be true for Lemma 4 to hold if we replace p in (2) by p^a for arbitrary $a \in \mathbb{N}$, and indeed it is.[1] We have the following counterexample:

$$\binom{4+3^2}{3} \equiv 7 \pmod 9 \quad \text{but} \quad \binom{4}{3} \equiv 4 \pmod 9.$$

However, an analogous equation for prime-powers may be obtained from the following proposition (see Theorem 1 of [Granville 1997]):

Proposition 12. *Let p be a prime number. For any positive integer a, define $(a!)_p$ to be the product of those positive integers $\le a$ which are not divisible by p. Let q, m, n and r be positive integers such that $n = m + r$. Write n in base p as $\sum_{i=0}^{d} n_i p^i$ and let N_j be the least positive residue of $[n/p^j] \pmod{p^q}$ for each $j \ge 0$ (so that $N_j = \sum_{i=0}^{q-1} n_{j+i} p^i$). Also, make the corresponding definitions for m_j, M_j, r_j and R_j. Let e_j denote the number of 'carries', when adding m and r in base p, on and beyond the j-th digit. Then,*

$$\frac{(\pm 1)^{e_{q-1}}}{p^{e_0}} \binom{n}{m} \equiv \left(\prod_{j=0}^{d} \frac{(N_j!)_p}{(M_j!)_p (R_j!)_p} \right) \pmod{p^q},$$

where $(\pm 1) = -1$ except if $p = 2$ and $q \ge 3$.

We will not attempt to generalize Theorem 8 in this paper because it would take us too far afield.

Acknowledgments

I thank Dr. Fedor Duzhin from the School of Physical and Mathematical Sciences (SPMS), Nanyang Technological University, for first sparking my interest in this problem. Many thanks also go to Dr. Sinai Robins (SPMS) for the initial advice he gave on preparing this paper, and to Magdalene Lee for her unwavering support of my mathematical endeavors. I express my warmest gratitude, however, to the anonymous referee who painstakingly reviewed this paper and, at the same time, corrected many of the flaws in my practice of mathematical exposition.

References

[Granville 1997] A. Granville, "Arithmetic properties of binomial coefficients, I: Binomial coefficients modulo prime powers", pp. 253–276 in *Organic mathematics* (Burnaby, BC, 1995), edited by J. Borwein et al., CMS Conf. Proc. **20**, Amer. Math. Soc., Providence, RI, 1997. MR 99h:11016 Zbl 0903.11005

[1] Note that Theorem 7 still holds if we replace p by p^a, or even by any integer ≥ 2. It is only for Theorem 8 that this method fails, which, in turn, happens because it fails for Lemmas 3 and 4.

[Niven et al. 1991] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., Wiley, New York, 1991. MR 91i:11001 Zbl 0742.11001

Received: 2008-10-25 Revised: 2009-09-15 Accepted: 2009-09-15

huan0074@ntu.edu.sg

School of Physical and Mathematical Sciences,
Nanyang Technological University, SPMS-04-01,
21 Nanyang Link, 637371, Singapore