MINIMUM PERIODS MODULO n FOR BERNOULLI POLYNOMIALS

WILFRIED HERGET
Technische Universität, Clausthal, Fed. Rep. Germany
(Submitted September 1980)

1. It is known that the sequence of the Bernoulli numbers b_m, defined by

$$b_0 = 1,$$

$$b_m = -\frac{1}{m+1}\sum_{i=0}^{m-1}\binom{m+1}{i}b_i \qquad (m > 0),$$

is periodic after being reduced modulo n (where n is any positive integer), cf. [3]. [In this note, we use the symbols b_m for the Bernoulli numbers and $B_m(x)$ for the Bernoulli polynomials.] In [3] we proved

Theorem 1: Let $p \in \mathbb{P}$, $\mathbb{P}$ being the set of primes, $p \geq 3$, and $e,k,m \in \mathbb{N}$. For $k,m \geq e+1$, we have:

$$b_k \ n\text{-integral and } k \equiv m \bmod p^e(p-1) \Rightarrow b_m \ n\text{-integral and } b_k \equiv b_m \bmod p^e.$$

In this note, we shall give some analogous results about the sequence of the Bernoulli polynomials $B_m(x)$ reduced modulo n (Theorem 6) and the polynomial functions over $\mathbb{Z}_n$ generated by the Bernoulli polynomials (Theorem 4). Here, $\mathbb{Z}_n$ is the ring of integers modulo n, where $n \in \mathbb{N}$, $n \geq 2$, and the Bernoulli polynomials in $\mathbb{Q}[x]$ are defined by

$$B_m(x) = \sum_{i=0}^{m}\binom{m}{i}b_i x^{m-i},\ m \in \{0, 1, 2, \ldots\}.$$

Similar questions about Euler numbers and polynomials were asked by Professor L. Carlitz and Jack Levine in [2].

2. In [4] we discussed in which cases it is possible to define (in a natural way) analogs of Bernoulli polynomials in $\mathbb{Z}_n$. In this section, we shall prove the periodicity of the sequence of the polynomial functions B_m over $\mathbb{Z}_n$ generated by the Bernoulli polynomials. Each polynomial $F(x) \in \mathbb{Q}[x]$ generates a polynomial function $F : \mathbb{Z} \to \mathbb{Q}$ by

$$x \mapsto F(x). \tag{1}$$

Now, considering (1) in $\mathbb{Z}_n$, we get a function $F : \mathbb{Z}_n \to \mathbb{Z}_n$ if and only if

(a) all values of F are interpretable mod n, and
(b) the relation (1) preserves congruence properties.

For this, it is useful to introduce the following notations ([4], p. 28).

Definition 1: A function $F : \mathbb{Z} \to \mathbb{Q}$ is said to be acceptable mod n, iff

(a) $\forall\, x$, $F(x)$ is n-integral,
(b) $x \equiv y \bmod n \Rightarrow F(x) \equiv F(y) \bmod n$.

A polynomial $F(x) \varepsilon \mathbb{Q}[x]$ is said to be acceptable mod n if this is true for its polynomial function.

Definition 2: Two functions $F,G : \mathbb{Z} \to \mathbb{Q}$ are said to be equivalent mod n iff

(a) F,G are acceptable mod n,
(b) $\forall\, x,\ F(x) \equiv G(x) \bmod n$.

Two polynomials $F(x), G(x) \varepsilon \mathbb{Q}[x]$ are said te be equivalent mod n if this is true for their polynomial functions. We write

$$F \sim G \bmod n \quad \text{and} \quad F(x) \sim G(x) \bmod n,$$

respectively.

From [4], p. 29, we have the following

Theorem 2: $B_m(x)$ is acceptable mod n

$$\Leftrightarrow b_m \text{ is } n\text{-integral and } mS_{m-1}(n) \equiv 0 \bmod n,$$

where

$$S_m(x) = \begin{cases} \displaystyle\sum_{k=0}^{x-1} k^m & \text{for } m \varepsilon \{0, 1, 2, \ldots\},\ x \varepsilon \mathbb{N} \\ 0 & \text{for } m = -1 \text{ or } x = 0. \end{cases}$$

A more explicit characterization of $B_m(x)$ acceptable mod n gives (cf. [4], p. 31)

Theorem 3:

(a) For $m > 1$ and $2 \nmid n$ we have: $B_m(x)$ acceptable mod n

$$\Leftrightarrow \forall\, p \varepsilon \mathbb{P} : (p \mid n \Rightarrow p - 1 \nmid m \text{ and } (p - 1 \nmid m - 1 \text{ or } p \mid m)).$$

(b) For $k \varepsilon \mathbb{N}$ we have: $B_m(x)$ acceptable mod $2k \Leftrightarrow m = 0$.

Now, we may state our first new assertion. (By Theorem 3, it suffices to discuss the case $n = p^e$, p a prime, $p \geq 3$.)

Theorem 4: Let $p \varepsilon \mathbb{P}$, $p \geq 3$, and $e,k,m \varepsilon \mathbb{N}$.

(a) For $k,m \geq e + 1$, we have:

$$B_k \text{ acceptable mod } p \text{ and } k \equiv m \bmod p^e(p - 1)$$
$$\Rightarrow B_m \text{ acceptable mod } p \text{ and } B_k \sim B_m \bmod p^e.$$

(b) $p^e(p - 1)$ is the smallest period length of the sequence of the Bernoulli polynomials in the sense of (a).

For the proof of this theorem, we need the following

Lemma: Let $p \varepsilon \mathbb{P}$, $p \geq 3$, $e \varepsilon \mathbb{N}$. Then

$$x^{\lambda(p^e) + V(p^e)} \equiv x^{V(p^e)} \bmod p^e \text{ for all } x,$$

where both $V(p^e) = e$ and $\lambda(p^e) = p^{e-1}(p - 1)$ are minimal for this property.

For the proof of this lemma, see [5], Theorem 1.

Proof of Theorem 4(a): Let $k,m > e$, $k \equiv m \bmod p^e(p-1)$ and B_k be acceptable mod p, so that b_k is p-integral and $kS_{k-1}(p) \equiv 0 \bmod p$. By Theorem 1, b_m is p-integral with $b_k \equiv b_m \bmod p^e$. Furthermore, from $k \equiv m \bmod p^e(p-1)$, and $k,m > e$, we have $k \cdot i^{k-1} \equiv m \cdot i^{m-1} \bmod p^e$ for all i, by the lemma above. Then

$$kS_{k-1}(x) = k\sum_{i=0}^{x-1} i^{k-1} \equiv m\sum_{i=0}^{x-1} i^{m-1} = mS_{m-1}(x) \bmod p^e$$

for all x. Now we use (5) from [4]:

$$B_m(x) = mS_{m-1}(x) + b_m.$$

Thus B_m is p-integral, too, and $B_k(x) \equiv B_m(x) \bmod p^e$ for all x; i.e.,

$$B_k \sim B_m \bmod p^e.$$

Proof of Theorem 4(b): Let B_k and B_m be acceptable mod p, let $k,m \geq e+1$, and let $B_k \sim B_m \bmod p^e$. Then $B_k(x) \equiv B_m(x) \bmod p^e$ for all x. We shall show that $k \equiv m \bmod p^e(p-1)$ if $p^e \nmid m$. Obviously this would prove the assertion. First, we get $b_k = B_k(0) \equiv B_m(0) = b_m \bmod p^e$, hence $kS_{k-1}(x) \equiv mS_{m-1}(x) \bmod p^e$ for all x; and moreover,

$$kx^{k-1} \equiv mx^{m-1} \bmod p^e \text{ for all } x, \tag{2}$$

since

$$kx^{k-1} = kS_{k-1}(x+1) - kS_{k-1}(x).$$

Putting $x = 1$ in (2) shows $k \equiv m \bmod p^e$. Let $d = \text{g.c.d.}(k, p^e)$. We know that $\text{g.c.d.}(m, p^e) = d$, and $d = p^i$ with $0 \leq i < e$, since $p^e \nmid k$. Thus (2) implies

$$x^{k-1} \equiv x^{m-1} \bmod p^{e-i} \text{ for all } x.$$

But this is possible only if $k - 1 \equiv m - 1 \bmod (p-1)$; i.e., $k \equiv m \bmod (p-1)$. Together with $k \equiv m \bmod p^e$, we have $k \equiv m \bmod p^e(p-1)$, and the theorem is proved.

Remark 1: The minimum period length of the Bernoulli polynomial functions mod n is the same as that of the Bernoulli numbers mod n.

Remark 2: By a very similar argument one may prove that when B_m is acceptable mod p, $m \equiv 0 \bmod p^e \Leftrightarrow B_m \sim 0 \bmod p^e$. For this, notice that $m \equiv 0 \bmod p^e$ implies $b_m \equiv 0 \bmod p^e$ ([1], p. 78, Theorem 5).

Remark 3: Let $v(p^e)$ denote the preperiod length of $B_m \bmod p^e$. Then Theorem 4 implies $v(p^e) \leq e + 1$. Using Remark 2 one may slightly improve this inequality for special cases with $e \geq p$. For instance, $v(3^3) = 3$.

3. In this section we shall discuss the periodicity of Bernoulli polynomials reduced modulo n.

Definition 3: A polynomial $F(x) = a_0 + a_1x + \cdots + a_rx^r \in \mathbb{Q}[x]$ is said to be n-integral if and only if the coefficients $a_0, a_1, \ldots, a_r$ are all n-integral.

From [4], p. 32, we have, for the Bernoulli polynomials,

Theorem 5: Let $p \in \mathbb{P}$, $e \in \mathbb{N}$, and $m \in \mathbb{N} \cup \{0\}$ with p-adic representation

$$m = \sum_{k=0}^{s} m_k p^k.$$

Then

$$B_m(x) \in \mathbb{Q}[x] \text{ is } p^e\text{-integral if and only if } \sum_{k=0}^{s} m_k < p - 1.$$

Remark 4: Each n-integral polynomial is acceptable mod n, but there are polynomials acceptable mod n that are not n-integral (cf. [4], pp. 32-33). If we reduce the coefficients of any n-integral $B_m(x)$, we still get a polynomial of degree m, since the coefficient of x^m is 1. Consequently, no periodicity appears. But by the lemma above we have

$$x^{p^{e-1}(p-1)+e} \equiv x^e \bmod p^e \text{ for all } x.$$

Hence, any p-integral polynomial $F(x)$ is equivalent to a reduced polynomial with degree $< p^{e-1}(p - 1) + e$ having coefficients in $\{0, 1, \ldots, p^e - 1\}$. We shall denote such a polynomial $F(x)$, reduced mod n, by $\tilde{F}(x)$.

Remark 5: If $\tilde{F}_1(x)$ and $\tilde{F}_2(x)$ are reduced polynomials of $F(x)$ mod n, then

$$\tilde{F}_1(x) \sim \tilde{F}_2(x) \sim F(x) \bmod n.$$

We conjecture that the sequence of the Bernoulli polynomials, reduced mod n, is periodic in a strong sense too, with a proof here only for $n = p$, $p \in \mathbb{P}$.

Theorem 6: Let $p \in \mathbb{P}$, $k,m \geq 2$, and suppose $B_k(x)$, $B_m(x)$ are p-integral. If $k \equiv m \bmod p(p - 1)$, then

$$\tilde{B}_k(x) = \tilde{B}_m(x) \text{ in } \mathbb{Z}_p[x].$$

Proof: $B_k(x)$, $B_m(x)$ p-integral implies $B_k(x)$, $B_m(x)$ acceptable mod p (Remark 4). By Theorem 4 we get

$$B_k(x) \sim B_m(x) \bmod p, \text{ hence}$$
$$\tilde{B}_k(x) \sim \tilde{B}_m(x) \bmod p, \text{ i.e.,}$$
$$\tilde{B}_k(x) - \tilde{B}_m(x) \equiv 0 \bmod p \text{ for all } x.$$

The degree of this difference polynomial is $<\lambda(p) + V(p) = p - 1 + 1 = p$, but it has p zeros in $\mathbb{Z}_p$, hence it must be the zero polynomial, and we have

$$\tilde{B}_k(x) = \tilde{B}_m(x) \text{ in } \mathbb{Z}_p[x].$$

Remark 6: The question, whether Theorem 6 holds for arbitrary modulus n, remains open. The proof above fails in $\mathbb{Z}_n$ when $n \notin \mathbb{P}$, since $\tilde{B}_k(x) \sim \tilde{B}_m(x) \bmod n$ does not imply $\tilde{B}_k(x) = \tilde{B}_m(x)$ in $\mathbb{Z}_n[x]$. For example, let $e > 1$ and

$$F(x) = p^{e-1}\prod_{i=0}^{p-1}(x - i),$$

$$G(x) = \prod_{i=0}^{p^e-1}(x - i).$$

Then $F(x) \sim G(x)$ (~ 0) mod p^e, but $F(x) \neq G(x)$ in $\mathbb{Z}_{p^e}[x]$. Or, if $n = p_1p_2$, where $p_1, p_2 \in \mathbb{P}$ and $p_1 \neq p_2$, then one may consider the polynomials

$$p_2\prod_{i=0}^{p_1-1}(x - i) \quad \text{and} \quad p_1\prod_{i=0}^{p_2-1}(x - i)$$

for a counterexample.

Remark 7: The assumption in Theorem 6 that both $B_k(x)$ and $B_m(x)$ are p-integral cannot be weakened, since $B_k(x)$ p-integral and $k \equiv m \bmod p(p-1)$ does not imply B_m p-integral. For example

$$B_2(x) = x^2 - x + \frac{1}{6}$$

is 5-integral, while $B_{22}(x)$ is not so by Theorem 2, even though $22 \equiv 2 \bmod 5 \cdot 4$.

References

1. L. Carlitz. "Bernoulli Numbers." *The Fibonacci Quarterly* 6, no. 3 (1968): 71-85.
2. L. Carlitz & J. Levine. "Some Problems Concerning Kummer's Congruences for the Euler Numbers and Polynomials." *Trans. Amer. Math. Soc.* 96 (1960):23-37.
3. W. Herget. "Minimum Periods Modulo n for Bernoulli Numbers." *The Fibonacci Quarterly* 16, no. 6 (1978):544-548.
4. W. Herget. "Bernoulli-Polynome in den Restklassenringen $\mathbb{Z}_n$." *Glasnik Matematički* 14, no 34 (1979):27-33.
5. D. Singmaster. "A Maximal Generalization of Fermat's Theorem." *Mathematics Magazine* 39 (1966):103-107.

*****