[7] J.-P. Massias, *Majoration explicite de l'ordre maximum d'un élément du groupe symétrique*, Ann. Fac. Sci. Toulouse Math. 6 (1984), p. 269–280.
[8] — *Ordre maximum d'un élément du groupe symétrique et applications*, Thèse de 3ème cycle soutenue le 30 Mai 1984 à l'Université de Limoges.
[9] J.-L. Nicolas, *Ordre maximal d'un élément du groupe des permutations et highly composite numbers*, Bull. Soc. Math. France 97 (1969), p. 129–191.
[10] — *Sur l'ordre maximum d'un élément dans le groupe S_n des permutations*, Acta Arith. 14 (1968), p. 315–332.
[11] — *Calcul de l'ordre maximum d'un élément du groupe symétrique S_n*, R.I.R.O. 3e année, n° R-2/1969, p. 43–50.
[12] — *Ordre maximum d'un élément du groupe des permutations et nombres très hautement abondants*, C. R. Acad. Sc. Paris, Série A, 266 (1968), p. 513–515.
[13] — *Ordre maximal d'un élément d'un groupe de permutations*, ibid. 270 (1970), p. 1473–1476.
[14] — *Petites valeurs de la fonction d'Euler*, J. Number Theory 17 (1983), p. 375–388.
[15] G. Robin, *Sur la différence* $\mathrm{Li}(\theta(x))-\pi(x)$, Ann. Fac. Sci. Toulouse Math. 6 (1984), p. 257–268.
[16] — *Méthodes d'optimisation pour un problème de théorie des nombres*, R.A.I.R.O. Informatique théorique, 17 (1983), p. 239–247.
[17] A. Schinzel, *Reducibility of lacunary polynomials, III*, Acta Arith. 34 (1978), p. 227–266.
[18] S. M. Shah, *An inequality for the arithmetical function $g(x)$*, J. Indian Math. Soc. 3 (1939), p. 316–318.
[19] H. Siebert, *Montgomery's weighted sieve for dimension two*, Monatsh. Math. 82 (1976), p. 327–336.
[20] M. Szalay, *On the maximal order in S_n and S_n^**, Acta Arith. 37 (1980), p. 321–331.
[21] L. G. Valiant et M. S. Paterson, *Deterministic one counter automata*, J. Comput. System Sci. 10 (1975), p. 340–350.
[22] P. M. B. Vitanyi, *On the size of DOL Languages. L Systems* (Third Open House, Comput. Sci. Dept., Aarhus Univ., Aarhus, 1974), pp. 78–92, 327–338. Lectures Notes in Computer Science, Vol. 15, Springer, Berlin 1974.

U.E.R. DES SCIENCES DE LIMOGES
DÉPARTEMENT DE MATHÉMATIQUES
123 RUE ALBERT THOMAS
87060 Limoges Cédex (France)

Reçu le 11.11.1985 (1553)

ACTA ARITHMETICA
L (1988)

On the degree of an irreducible factor of the Bernoulli polynomials

by

NORIAKI KIMURA (Chiba, Japan)

Introduction. In the present note we intend to consider the degree of an irreducible factor of certain polynomials, in particular, the Bernoulli polynomials, which are defined by

$$\frac{te^{xt}}{e^t-1} = \sum_{m=0}^{\infty} B_m(x)\frac{t^m}{m!}.$$

When m is odd $\geqslant 3$, it is well known that $B_m(x)$ has the three linear factors x, $x-\frac{1}{2}$ and $x-1$. Conversely Inkeri [2] has shown that if $B_m(x)$, $m \geqslant 3$ has rational roots, then m is odd and $B_m(x)$ does not have other linear factors with rational coefficients. Moreover Carlitz [1] has shown that $B_{2m+1}(x)/x(x-1)(x-\frac{1}{2})$, where $2m+1 = k(p-1)+1$, $1 \leqslant k \leqslant p$, p an odd prime has an irreducible factor over the rational field Q of degree $\geqslant 2m+1-p$.

In the case of an even index McCarthy [5] has shown that $pB_{2m}(x)$ is an Eisenstein polynomial (and therefore irreducible over Q) if and only if there exists a prime p such that $\sum m_i = p-1$, where $2m = \sum m_i p^i$, $0 \leqslant m_i \leqslant p-1$ for all i, is the p-adic expansion of $2m$.

In Section 1 we first deal with properties concerning the divisibility of the binomial coefficients and in Section 2 those results are applied to the polynomials, whose coefficients contain the binomial coefficients, and we shall obtain some generalizations of the results mentioned above in the rest of this note.

1. Let p be a prime number and n an arbitrary positive integer. Let

$$n = \sum_{i=0}^{h} n_i p^i \qquad (0 \leqslant n_i \leqslant p-1 \text{ for all } i \text{ and } n_h \neq 0)$$

be the p-adic notation of n. We define $A(n, p)$ by

$$A(n, p) = \sum_{i=0}^{h} n_i.$$

The following two lemmas are well known.

LEMMA 1. *$p-1|n$ if and only if $p-1|A(n, p)$.*

LEMMA 2. *The binomial coefficient $\binom{n}{a}$ is not divisible by p if and only if $n_i \geqslant a_i$ for all i, where $a=\sum a_i p^i$, $0 \leqslant a_i \leqslant p-1$ for all i.*

Schäffer [7] has shown the following

LEMMA 3. *$p|\binom{n}{t}$ for all integers t such that $p-1|t$ and $0<t<n$ if and only if $A(n, p) \leqslant p-1$.*

We can supplement Schäffer's lemma as follows.

LEMMA 4. *There exists an integer $N(n, p)$ with $0<N(n, p) \leqslant n$ and $p \nmid \binom{n}{N(n, p)}$ such that if $p-1|t$, $0<t<N(n, p)$, then $p|\binom{n}{t}$.*

Proof. If $A(n, p) \leqslant p-1$, then we can put

$$N(n, p)=n \tag{1}$$

by Schäffer's Lemma 3.

If $A(n, p)>p-1$, then there exists an integer r $(0<r \leqslant h-1)$ such that

$$\sum_{i=0}^{r} n_i \leqslant p-1 \quad \text{and} \quad \sum_{i=0}^{r+1} n_i > p-1.$$

Set

$$N(n, p)=\sum_{i=0}^{r} n_i p^i+(p-1-\sum_{i=0}^{r} n_i) p^{r+1}. \tag{2}$$

Then $p \nmid \binom{n}{N(n, p)}$ by Lemma 2. Let $t=\sum_{i=0}^{r+1} t_i p^i$, $0 \leqslant t_i \leqslant p-1$ be an integer such that $p-1|t$ and $0<t<N(n, p)$. If $p \nmid \binom{n}{t}$, then it follows by Lemma 2 that

$$t_i \leqslant n_i \quad \text{for} \quad i=0, \ldots, r,$$

and by assumption $t<N(n, p)$ that

$$t_{r+1} \leqslant p-1-\sum_{i=0}^{r} n_i.$$

Since equality can not hold for all $i=0, \ldots, r, r+1$, we have

$$\sum_{i=0}^{r+1} t_i < \sum_{i=0}^{r} n_i+p-1-\sum_{i=0}^{r} n_i=p-1.$$

On the other hand by Lemma 1 and by assumption $0<t$ we have

$$p-1 \leqslant \sum_{i=0}^{r+1} t_i.$$

Hence we obtain

$$p-1 \leqslant \sum_{i=0}^{r+1} t_i < p-1,$$

which is a contradiction and this completes the proof.

We can easily verify the following lemma about the relations between $A(n, p)$ and $N(n, p)$, which is defined by (1) and (2).

LEMMA 5. (a) $N(n, p)<n \Leftrightarrow A(n, p)>p-1$.
(b) $N(n, p)=n \Leftrightarrow A(n, p) \leqslant p-1$.
(c) $N(n, p)=n$, $p-1|n \Leftrightarrow A(n, p)=p-1$.
(d) $N(n, p)=n$, $p-1 \nmid n \Leftrightarrow A(n, p)<p-1 \Leftrightarrow A(N(n, p), p)<p-1$.
(e) $p-1|N(n, p) \Leftrightarrow A(n, p) \geqslant p-1 \Leftrightarrow A(N(n, p), p)=p-1$.

2. Since the following Lemma 6 is well known, we omit its proof here.

LEMMA 6 (An extension of the Eisenstein criterion). *Let*

$$f(x)=\sum_{j=0}^{m} a_{m-j} x^j$$

be a polynomial of degree m with (p-)integral coefficients. If there exist a prime p and an integer r $(0 \leqslant r \leqslant m)$ such that

$$p|a_{m-j} \quad \text{for} \quad j=r+1, \ldots, m, \quad p \nmid a_{m-r} \quad \text{and} \quad p^2 \nmid a_0,$$

then $f(x)$ has an irreducible factor of degree $\geqslant m-r$.

LEMMA 7. *Let $m \leqslant n$ and let p be a prime number. Let b_{js} be p-integral rational numbers and*

$$f(x)=\sum_{j=0}^{m} a_{m-j} x^j \quad \text{where} \quad a_{m-j}=\sum_{s=0}^{m-j} b_{js}\binom{n}{s},$$

be a polynomial.

Suppose that

$$\begin{aligned} &p|b_{js} \quad \text{if} \quad p-1 \nmid s \text{ or } s=0, \\ &p \nmid b_{js} \quad \text{if} \quad s=m-j,\ p-1|s \text{ and } s \neq 0, \\ &p^2 \nmid b_{m0}. \end{aligned} \tag{3}$$

Suppose

$$N(n, p) \leqslant m \tag{4}$$

and

$$A(n, p) \geqslant p-1, \tag{5}$$

then $f(x)$ has an irreducible factor of degree $\geqslant N(n, p)$.

Proof. Since

$$a_0 = b_{m0},$$

$$a_{m-j} = b_{j0} + \sum_{\substack{0<s<m-j \\ p-1 \nmid s}} b_{js}\binom{n}{s} + \sum_{\substack{0<s<m-j \\ p-1 \mid s}} b_{js}\binom{n}{s} + b_{j,m-j}\binom{n}{m-j} \quad \text{for} \quad j = 0, \ldots, m-1,$$

the assumption (3), Lemma 3 and Lemma 4 imply that if $0 \leqslant m-j < N(n, p)$, that is, $m - N(n, p) < j \leqslant m$, then $p \mid a_{m-j}$ and $p^2 \nmid a_0$.

On the other hand the condition (5) implies $p-1 \mid N(n, p)$ by Lemma 5. Therefore (6) with the assumption (3) and Lemma 4 imply $p \nmid a_{N(n,p)}$. It follows from Lemma 6 that $f(x)$ has an irreducible factor of degree $\geqslant N(n, p)$, which completes the proof.

COROLLARY. *If either $m < N(n, p)$ or $A(n, p) < p-1$, then every coefficient of $f(x)$ is divisible by p.*

LEMMA 8. *The notation being as in Lemma 7, let $m = n$ and b_{js} satisfy the assumption (3). Then $f(x)$ is an Eisenstein polynomial with respect to p if and only if $A(m, p) = p-1$.*

Proof. By Lemma 5 it is enough to show that $f(x)$ is an Eisenstein polynomial with respect to p if and only if $N(m, p) = m$ and $p-1 \mid m$. Assume that $f(x)$ is an Eisenstein polynomial for p, namely the coefficient a_{m-j} satisfies

$$p \mid a_{m-j} \quad \text{for} \quad j = 1, \ldots, m, \quad p \nmid a_m \quad \text{and} \quad p^2 \nmid a_0. \tag{7}$$

If $N(m, p) < m$, then it follows from the proof of Lemma 7 that the coefficient $a_{N(m,p)}$ of $x^{m-N(m,p)}$ is not divisible by p, which is contrary to the assumption (7). If $p-1 \nmid m = N(m, p)$, then (6) with the assumption (3) shows that $p \mid a_m$, which is a contradiction. Conversely if $N(m, p) = m$ and $p-1 \mid m$, then the proof of Lemma 7 shows that (7) holds, that is, $f(x)$ is an Eisenstein polynomial. This completes the proof.

In the same manner as the above we have

LEMMA 9. *The notation and the conditions being as in Lemma 7, and $m < n$. $f(x)$ is an Eisenstein polynomial with respect to p if and only if $N(n, p) = m$.*

3. In the following we shall apply the results obtained in Section 2.

1. $B_m(x)$, m; even. The Bernoulli polynomials are given explicitly as

$$B_m(x) = \sum_{j=0}^{m} \binom{m}{j} B_j x^{m-j},$$

where B_j is the jth Bernoulli number in Nörlund's notation [6]. As well known by the von Staudt–Clausen theorem we have

$$\begin{aligned} pB_j &\equiv 0 \pmod p \quad \text{for} \quad p-1 \nmid j, \\ pB_j &\equiv -1 \pmod p \quad \text{for} \quad p-1 \mid j,\ j \neq 0, \\ B_0 &= 1. \end{aligned} \tag{8}$$

Therefore we can apply Lemma 7 and Lemma 8 to

$$pB_{2m}(x) = \sum_{j=0}^{2m} x^j \left(pB_{2m-j}\binom{2m}{2m-j} \right),$$

setting $b_{js} = pB_{2m-j}$ $(s = 2m-j)$; $= 0$ $(s \neq 2m-j)$, and we obtain the following

THEOREM 1. *If $A(2m, p) \geqslant p-1$, then $B_{2m}(x)$ has an irreducible factor of degree $\geqslant N(2m, p)$.*

COROLLARY (McCarthy). *$pB_{2m}(x)$ is an Eisenstein polynomial with respect to a prime p and therefore irreducible over Q if and only if $A(2m, p) = p-1$.*

2. $B_m(x)$, m; odd. We start with the following formula ([1], p. 477):

$$2^{2m+1} B_{2m+1}(\tfrac{1}{2}x + \tfrac{1}{2}) = x(x^2-1)\beta_{2m+1}(x),$$

where

$$\beta_{2m+1}(x) = \sum_{j=0}^{m-1} x^{2j} \left(\sum_{s=0}^{m-1-j} D_{2s}\binom{2m+1}{2s} \right), \quad m \geqslant 1,$$

and

$$D_{2s} = 2(1-2^{2s-1})B_{2s}, \quad D_{2s+1} = 0. \tag{9}$$

We note that for an odd prime p (8) and (9) imply

$$\begin{aligned} pD_{2s} \equiv pB_{2s} &\equiv -1 \pmod p \quad (p-1 \mid 2s,\ 2s > 0), \\ pD_{2s} &\equiv 0 \pmod p \quad (p-1 \nmid 2s), \\ D_0 &= 1. \end{aligned}$$

Setting $b_{js} = 0$ (j; odd); $= pD_s$ (j; even) and replacing m and n in Lemma 7 by $2m-2$ and $2m+1$ respectively and applying Lemma 7 to $p\beta_{2m+1}(x)$, we have

THEOREM 2. *Let $2m+1 \geqslant 5$. If $A(2m+1, p) > p-1$, then $\beta_{2m+1}(x)$ has an irreducible factor of degree $\geqslant N(2m+1, p)$.*

Proof. If $A(2m+1, p) > p-1$ for $p = 2$, then $N(2m+1, p) = 1$ and the theorem is trivial. For $p \geqslant 3$, it remains to show $N(2m+1, p) \leqslant 2m-2$.

Let $2m+1 = \sum_{i=0}^{h} m_i p^i$, $0 \leqslant m_i \leqslant p-1$, $m_h \neq 0$. Since $A(2m+1, p) > p-1$, we have for some r, $0 \leqslant r < h$,

$$\sum_{i=0}^{r} m_i \leqslant p-1, \quad \sum_{i=0}^{r+1} m_i > p-1 \quad \text{and}$$

$$N(2m+1, p) = \sum_{i=0}^{r} m_i p^i + (p-1-\sum_{i=0}^{r} m_i) p^{r+1}.$$

If $N(2m+1, p) > 2m-2$, then it follows

$$3 > (\sum_{i=0}^{r+1} m_i - p + 1) p^{r+1} + \sum_{i=r+2}^{h} m_i p^i.$$

Consequently we have $h = r+1$, $r = 0$, $p = 2$, $m_0 = m_1 = 1$ and $2m+1 = 3$. This completes the proof.

If $N(2m+1, p) = 2m-2$, then $p = 3$ and $2m+1 = 5$ or 7. It follows therefore from Lemma 9 that only $3\beta_5(x)$ and $3\beta_7(x)$ are Eisenstein polynomials.

Let p be an odd prime and $2m+1 = k(p-1)+1$, $2 \leqslant k \leqslant p$. Since $2m+1 = (k-1)p + p - k + 1$, $1 \leqslant k-1 \leqslant p-1$, $1 \leqslant p-k+1 \leqslant p-1$, we have

$$A(2m+1, p) = p > p-1$$

and

$$N(2m+1, p) = p-k+1+(k-2)p = (k-1)(p-1) = 2m+1-p.$$

Therefore by Theorem 2 we have the following

COROLLARY (Carlitz). *If $2m+1 = k(p-1)+1$, $2 \leqslant k \leqslant p$ for an odd prime p, then $\beta_{2m+1}(x)$ has an irreducible factor of degree $\geqslant 2m+1-p$.*

3. The polynomial $P_k(x)$ $(k \geqslant 1)$, which is defined by

$$P_k(n) = \sum_{\nu=1}^{n} \nu^k \quad \text{for all integers } n.$$

Using the Bernoulli number and the Bernoulli polynomial, we can write explicitly

$$P_k(x) = \frac{1}{k+1}\{B_{k+1}(x+1) - B_{k+1}\}.$$

If k is even, then

$$B_{k+1} = 0 \quad \text{and} \quad P_k(x) = \frac{1}{k+1} B_{k+1}(x+1),$$

so we shall confine ourselves to the case k odd. Since $P_k(x-1)$ is divisible by $x^2(x-1)^2$ (see [3]), we have

$$(k+1)P_k(x-1) = \sum_{s=0}^{k} \binom{k+1}{s} B_s x^{k+1-s} = x^2(x-1)^2 Q_k(x),$$

where

$$Q_k(x) = \sum_{j=0}^{k-3} x^j \left(\sum_{s=0}^{k-3-j} (k-2-j-s) B_s \binom{k+1}{s} \right).$$

Set

$$m = k-3, \quad n = k+1, \quad b_{js} = (k-2-j-s)pB_s,$$

then by Lemma 7 we can obtain similarly to Theorem 2 the following

THEOREM 3. *If $A(k+1, p) > p-1$, then $Q_k(x)$ has an irreducible factor of degree $\geqslant N(k+1, p)$.*

We note that if $N(k+1, p) = k-3$, then we have $p = 2$ and $k+1 = 6$. Thus only $2Q_5(x)$ is an Eisenstein polynomial.

References

[1] L. Carlitz, *Note on irreducibility of the Bernoulli polynomials*, Duke Math. J. 19 (1952), pp. 475–481.

[2] K. Inkeri, *The real roots of Bernoulli polynomials*, Ann. Uni. Turku. Ser. A, 37 (1959), pp. 9–10.

[3] N. Kimura and H. Siebert, *Über die rationalen Nullstellen der von Potenzsummen der natürlichen Zahlen definierten Polynome*, Proc. Japan Acad. Ser. A, 56 (1980), pp. 354–356.

[4] N. Kimura, *Über die Nullstellen der von Potenzsummen der natürlichen Zahlen definierten Polynome*, ibid. 58 (1982), pp. 326–328.

[5] P. J. McCarthy, *Irreducibility of certain Bernoulli polynomials*, Amer. Math. Monthly 68 (1961), pp. 352–353.

[6] N. E. Nörlund, *Differenzenrechnung*, Springer-Verlag, 1924.

[7] J. J. Schäffer, *The equation $1^p+2^p+3^p+\ldots+n^p = m^p$*, Acta Math. 95 (1956), pp. 155–189.

COLLEGE OF INDUSTRIAL TECHNOLOGY
NIHON UNIVERSITY

Received on 22.11.1985
and in revised form on 4.8.1986 (1561)