ACTA ARITHMETICA
LXII.4 (1992)

On the degrees of irreducible factors of higher order Bernoulli polynomials

by

Arnold Adelberg (Grinnell, Ia.)

1. Introduction. In this paper, we generalize the current results on the p-Eisenstein behavior of first and higher order Bernoulli polynomials [4], [6–9], using the machinery of [1]. In so doing, we provide a broader framework for the known results, all of which are either immediate consequences or special cases of our more general results. Because of an explicit formula for the coefficients in terms of falling factorials established in [1], the polynomials $A_n(x,-k)$ which we consider here are actually translates of the standard higher order Bernoulli polynomials $B_n^{(\omega)}(x)$, but *all* of our significant results apply equally well to the standard polynomials and their ordinary coefficients, with $\omega = n-k+1$. The main results are summarized using standard notations in the research announcement [2].

Our approach differs from the usual one in that we make no use of congruence properties of the Bernoulli numbers, and in particular do not use the von Staudt–Clausen Theorem, which is an essential ingredient of the usual approach. Instead we characterize the behavior of the p-adic poles of the coefficients in terms of the base p expansion of n. The p-Eisenstein situation occurs when the highest order pole is simple.

The *Bernoulli polynomials* $B_n(x)$ are defined by (cf. [11, 12])

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

The *arbitrary order Bernoulli polynomials* $B_n^{(\omega)}(x)$ are defined by

$$\left(\frac{t}{e^t-1}\right)^{\omega} e^{xt} = \sum_{n=0}^{\infty} B_n^{(\omega)}(x)\frac{t^n}{n!}\,,$$

which are called *higher order*, or more precisely *first* or *higher order*, if $\omega \in \{1,2,\ldots,n\}$. They are monic degree n rational polynomials.

In [4], Carlitz showed that if $n = k(p-1)p^r$ where $0<k<p$, then $B_n(x)$

is irreducible (always with respect to $\mathbb{Q}$ unless otherwise indicated), namely that $pB_n(x)$ is p-Eisenstein. He also showed that if $2m+1 = k(p-1)+1$ where p is an odd prime and $1 \le k \le p$, then $B_{2m+1}/x(x-\frac{1}{2})(x-1)$ has an irreducible factor of degree $\ge 2m+1-p$.

Let $S(n) = S(n,p)$ be the p-adic digit sum of n, i.e., if $n = \sum n_i p^i$ is the base p expansion, where all digits satisfy $0 \le n_i \le p-1$, then $S(n) = \sum n_i$.

McCarthy showed in [7] that $pB_{2m}(x)$ is p-Eisenstein iff $S(2m) = p-1$.

In [6], Kimura defined a function $N(n,p)$, determined by the base p expansion of n, which he used to strengthen the results of Carlitz and McCarthy; namely, he showed that if $S(n,p) \ge p-1$, then $B_n(x)$ has an irreducible factor of degree $\ge N(n,p)$.

We will generalize Kimura's and McCarthy's results and determine all instances of even partial p-Eisenstein behavior of the first and higher order Bernoulli polynomials. Our main tool is an analysis of the nature of the p-adic poles of the coefficients, which turns out to be remarkably regular and uniform.

In the notation of [1], the polynomials we actually consider are

$$A_n(x,s) = n!A_n(x,0,s)\,,$$

with exponential generating function

$$(1+t)^x\left(\frac{\ln(1+t)}{t}\right)^s = \sum_{n=0}^{\infty} A_n(x,s)\frac{t^n}{n!}\,.$$

These are the Narumi polynomials [12, p. 127].

It has been shown that $A_n(x,s) = B_n^{(n+s+1)}(x+1)$, so in particular, $A_n(x,-n) = B_n(x+1)$ for first order, with $s \in \{-1,\ldots,-n\}$ for $\omega \in \{1,\ldots,n\}$. To establish the boundaries of our study, it should be noted that $A_n(x,0) = (x)_n$ and $A_n(x,-(n+1)) = (1+x)^n$. We will show that the Kimura bound [6, Theorems 1, 2], although sharp for $s=-n$, is far from best for the full range $s \in \{-1,\ldots,-n\}$.

Finally, it has been shown that if n is odd then $2x-(n+s-1) \mid A_n(x,s)$ and it was proved in [1] that $A_n(x,s)$ is absolutely irreducible for n even > 0, and that the above linear factor is the only non-trivial factor for n odd. The results in this paper enable us to determine the instances of p-Eisenstein behavior leading to *rational* irreducibility of this type.

2. Preliminaries. Throughout this paper, p will be a fixed but arbitrary prime, and all numbers are assumed to be positive integers, unless otherwise indicated.

$\nu_p = p$-adic valuation of $\mathbb{Q}$, i.e. $\nu_p(m) =$ highest power of $p \mid m$ if $m \in \mathbb{Z}$ and $\nu_p(m/n) = \nu_p(m) - \nu_p(n)$, with $\nu_p(0) = \infty$. If $b > 0$, we say r has a *pole of order* b if $\nu_p(r) = -b$.

We say that $f(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{Q}[x]$ is *p-Eisenstein down to degree d* if

$$(*)\qquad \begin{gathered} \nu_p(a_0) = 1, \quad \nu_p(a_i) > 0 \quad \text{if } 0 < i < n-d\,, \\ \nu_p(a_{n-d}) = 0, \quad \text{and} \quad \nu_p(a_i) \ge 0 \quad \text{for } i > n-d\,. \end{gathered}$$

We refer to this as (partial) *p-Eisenstein behavior*; $f(x)$ is said to be *p-Eisenstein* if it is p-Eisenstein to degree 0.

The following are standard and/or easy to demonstrate (cf. [10, Ch. 4]).

(1) If $f(x)$ is p-Eisenstein down to degree d and $c \in \mathbb{Z}$, then so is $f(x+c)$.

(2) If $f(x)$ is p-Eisenstein down to degree d, then $f(x)$ has an irreducible factor of degree $\ge n-d$. (In particular, p-Eisenstein implies irreducible.)

(3) If $f(x) = \sum_{i=0}^{n} b_i (x)_{n-i}$ in terms of the falling factorials, the coefficients (a_i) of $f(x)$ satisfy $(*)$ iff the coefficients (b_i) satisfy $(*)$.

We also need some standard results about ν_p of factorials and binomial coefficients, where $[x]$ = integer part of x and $\lceil x \rceil$ = least integer $\ge x$.

$$\text{(a)}\qquad \nu_p(n!) = \sum_{e=1}^{\infty} \left[\frac{n}{p^e}\right] = \frac{n - S(n)}{p-1}\,, \quad \text{whence} \quad \nu_p(n!) \le \left\lceil \frac{n}{p-1} \right\rceil - 1 \quad \text{if } n > 0\,.$$

$$\text{(b)}\qquad \nu_p\binom{n+m}{n} = \frac{S(n) + S(m) - S(n+m)}{p-1}\,.$$

(In particular, $S(n+m) \le S(n) + S(m)$.)

$$\text{(c)}\qquad \nu_p\binom{n+m}{n} = \#\text{ of carries in base } p \text{ addition of } n \text{ and } m\,.$$

$$\text{(d)}\qquad p \nmid \binom{n}{m} \quad \text{iff } n_i \ge m_i \text{ for all digits of the } p\text{-adic expansions}$$

(Lucas's Theorem).

It is convenient to introduce some non-standard notations, namely

$$m \prec n \quad \text{if } p \nmid \binom{n}{m} \qquad \text{and} \qquad m \perp \delta \quad \text{if } m \prec m+\delta, \text{ i.e. } p \nmid \binom{m+\delta}{m}\,.$$

By (d), $\prec$ is a partial order, and clearly $m \prec n$ implies $m \le n$. Obviously if m and m' have non-zero digits in different places, then $(m+m') \prec n$ iff $m \prec n$ and $m' \prec n$. (Observe that $n > m$ iff $n_i > m_i$ for the largest i such that $n_i \ne m_i$.) Also by (c), $m \perp \delta$ iff $S(m+\delta) = S(m) + S(\delta)$. Finally, since

$$\binom{-k}{m} = (-1)^m \binom{k+m-1}{m}\,,$$

we have

$$p \nmid \binom{-k}{m} \quad \text{iff } k-1 \perp m\,.$$

The following lemma can be proved without too much difficulty.

LEMMA 2.1. *Let* $n > 0$ *and suppose that* $p-1 \mid n$. *Let* $q = n/(p-1) = \sum_{i=r}^{s} q_i p^i$, *with* $q_r \neq 0$. *The following are equivalent*:

(i) $p \nmid \binom{-n}{q}$.

(ii) $q_r > q_{r+1} \geq q_{r+2} \geq \ldots \geq q_s$.

(iii) $S(n) = p-1$.

Proof.

$$n - 1 + q = pq - 1 = \sum_{i=r+1}^{s} q_i p^{i+1} + (q_r - 1)p^{r+1} + (p-1)\sum_{i=0}^{r} p^i\,.$$

The equivalence of (i) and (ii) follows immediately by Lucas's Theorem.

$$n = (p-1)q = \sum_{i=r+2}^{s+1} (q_{i-1} - q_i)p^i + (q_r - q_{r+1} - 1)p^{r+1} + (p - q_r)p^r\,.$$

It follows that if (ii) holds, then $S(n) = p-1$, by telescoping the digit sum. Suppose on the other hand that (ii) fails. If $q_r \leq q_{r+1}$, then $S(n) \geq p + q_r - q_{r+1} - 1 + p - q_r = p - q_{r+1} + p - 1 > p-1$, while if $q_r > q_{r+1}$ and f is the lowest place where $q_{f-1} < q_f$, the same argument shows $S(n) \geq p - q_f + p - 1 > p - 1$.

Remark 1. The preceding lemma shows that if $S(n) = p-1$ then $n/(p-1)$ has non-zero digits in all places below the top digit of n, down to the bottom non-zero digit of n. (It has a non-zero digit in the place of the top digit iff $n = (p-1)p^r$.)

We now turn to Kimura's function $N(n,p) = N(n)$ which we will use only when $S(n) \geq p-1$. In this case, $N(n) =$ the smallest t such that $t \prec n$ and $S(t) \geq p-1$. This is equivalent to $N(n) =$ smallest $t > 0$ such that $t \prec n$ and $p-1 \mid t$, which is essentially Kimura's definition [6, Lemma 4]. Thus if $n = \sum_{i=0}^{m} n_i p^i$ is the base p expansion and r is such that $\sum_{i=0}^{r} n_i \leq p-1$ while $\sum_{i=0}^{r+1} n_i > p-1$, then

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

so that $S(N(n)) = p-1$.

The next lemma follows easily from (c).

LEMMA 2.2. *Suppose that* $p-1 \mid \delta$ *and* $\delta \perp \delta/(p-1)$. *Then* $\delta = 0$.

Proof. Observe that $\delta + \delta/(p-1) = \delta p/(p-1)$. Hence if $\delta \neq 0$ and f is the lowest place where the digit $q_f \neq 0$, then there is a carry in place f for the base p sum.

We can deduce the following lemma, characterizing $N(n)$.

LEMMA 2.3. *Suppose $N(n) \prec t \prec n$ and $p-1 \mid t$. Then $p \nmid \binom{-n}{\frac{t}{p-1}}$ iff $t = N(n)$.*

Proof. If $\delta = t - N(n)$, then

$$n - 1 + \frac{t}{p-1} = \left(N(n) - 1 + \frac{N(n)}{p-1}\right) + \left(\delta + \frac{\delta}{p-1}\right).$$

Since there is no carry in the sum of the top digit of $N(n)$ and the bottom digit of δ, and otherwise the two summands have non-zero digits in different places, this lemma follows from the previous two.

3. p-adic analysis of the higher order Bernoulli polynomials. Recall that from [1, 3.1ii and 3.2ii],

$$A_n(x,s) = \sum_{i=0}^{n} b_i(s)(x)_{n-i},$$

where

$$|b_i(s)| = \sum_{w(u)=i} (n)_i \binom{s}{d(u)} \binom{d(u)}{u_1 u_2 \ldots} \frac{1}{2^{u_1} 3^{u_2} \ldots},$$

where the sum is over all sequences $(u) = (u_1, u_2, \ldots) = (r_1 - r_2, r_2 - r_3, \ldots)$ of non-negative integers, eventually zero, with weight $w(u) = \sum j u_j = i$ and arbitrary degree $d(u) = \sum u_j$.

It is convenient to abbreviate the term

$$\tau_u = (n)_{w(u)} \binom{s}{d(u)} \binom{d(u)}{u_1 u_2 \ldots} \frac{1}{2^{u_1} 3^{u_2} \ldots} = (n)_{w(u)} \frac{(s)_{d(u)}}{u! \wedge^u},$$

and to take $w(u)$ as the weight of τ_u.

We say that (u) or τ_u is *concentrated in place* $p-1$ if $u_j = 0$ for all $j \neq p-1$. Fix $k \in \{1, \ldots, n\}$ and let $s = -k$.

Clearly if $w(u) < p-1$, then $\nu_p(\tau_u) \geq 0$ since p first occurs in the denominator when $j = p-1$, whereas if $w(u) = i$ and (u) is concentrated in place $p-1$, then $p-1 \mid i$ and

$$\begin{aligned}\nu_p(\tau_u) &= \nu_p\left((n)_i \binom{-k}{\frac{i}{p-1}}\right) - \frac{i}{p-1} = \nu_p\left(\frac{n!}{(n-i)!}\right) - \frac{i}{p-1} + \nu_p\binom{-k}{\frac{i}{p-1}} \\ &= \frac{S(n-i) - S(n)}{p-1} + \nu_p\binom{-k}{\frac{i}{p-1}}.\end{aligned}$$

The following lemma shows that the terms concentrated in place $p-1$ determine the pole structure.

LEMMA 3.1. *If (u) is not concentrated in place $p-1$, then τ_u dominates a term of lower weight, i.e. there exists (u') with $w(u') < w(u)$ and $\nu_p(\tau_u) \geq \nu_p(\tau_{u'})$, whence τ_u dominates a term of lower weight concentrated in place $p-1$.*

Proof. Case 1. Suppose there exists $i < p-1$ with $u_i > 0$. Construct (u') by replacing u_i by 0 and increasing u_{p-1} by $\left\lceil \frac{u_i}{p-1} \right\rceil - 1$. This clearly decreases degree and weight, and since $\nu_p(u_i!) \leq \left\lceil \frac{u_i}{p-1} \right\rceil - 1$, we get the desired domination.

Case 2. Suppose there exists $i > p-1$ with $u_i > 0$. Construct (u') by replacing u_i by 0 and increasing u_{p-1} by u_i. This clearly preserves degree and decreases weight. Since

$$\nu_p((u_{p-1}+u_i)!) \geq \nu_p(u_{p-1}!) + \nu_p(u_i!)\,,$$

the domination is obvious unless $i = kp^\alpha - 1$, $\alpha > 1$, where $(k,p) = 1$. In this case,

$$w(u) - w(u') = u_i(kp^\alpha - p) \geq u_i(\alpha - 1)p\,.$$

Hence

$$\nu_p(\wedge^u) = \nu_p(\wedge^{u'}) + u_i(\alpha - 1)$$

and

$$\nu_p((n)_{w(u)}) \geq \nu_p((n)_{w(u')}) + u_i(\alpha - 1)\,,$$

since for any m, $\nu_p((m)_{rp}) \geq r$. This again establishes the domination.

Now, if (u') is not concentrated in place $p-1$, repeat the argument with (u) replaced by (u'). Since the weights are decreasing, eventually we get a term concentrated in place $p-1$ dominated by τ_u.

Let $a \in \{0, -1, -2, \ldots\}$. We then deduce immediately from the preceding lemma and remarks, using standard properties of valuations of sums,

COROLLARY 3.2. *If t is the smallest i such that $\nu_p(b_i) < a$, then*

(i) *$p-1 \mid t$, and if τ_u is concentrated in place $p-1$ and has weight t, then $\nu_p(\tau_u) < a$,*

(ii) *$\nu_p(\tau_u) \geq a$ for all (u) with $w(u) \leq t$ except for the term τ_u in* (i),

(iii) $\dfrac{S(n-t) - S(n)}{p-1} + \nu_p\binom{-k}{\frac{t}{p-1}} < a$ *and* $\dfrac{S(n-i) - S(n)}{p-1} + \nu_p\binom{-k}{\frac{i}{p-1}} \geq a$ *if $i < t$ and $p-1 \mid i$,*

(iv) *if* $i < t$, $p-1 \mid i$, $p \nmid \binom{n}{i}$ *and* $\frac{S(i)}{p-1} > -a$, *then* $p \mid \binom{-k}{\frac{i}{p-1}}$.

The last condition follows from the second part of the previous one.

It is not hard to further describe and indeed characterize t by a theorem which implies that the first pole is simple, the second higher pole has order 2, etc., and which enables us to determine where they occur from the base p expansion of n. All subsequent results of this paper follow fairly easily from this theorem. Let $a \in \{0, -1, -2, \ldots\}$ as above.

We say that l is a *segment of* n, starting in place r, if $n = \sum_{i=0}^{m} n_i p^i$ and $l = \sum_{i=r}^{s} n_i p^i$. (This includes $l = 0$ if $s < r$.) If $r = 0$, we call l a *bottom segment.*

THEOREM 3.3. *If* t *is the smallest* i *such that* $\nu_p(b_i) < a$, *then*

(i) $p \nmid \binom{-k}{\frac{t}{p-1}}$,

(ii) $p \nmid \binom{n}{t}$,

(iii) $\frac{S(n) - S(n-t)}{p-1} = \frac{S(t)}{p-1} = 1 - a$,

(iv) $\nu_p(b_t) = a - 1$,

(v) *the only digits of* n *that* t *and* $n - t$ *can share are top digits of segments of* t *divisible by* $p - 1$,

(vi) t *is the smallest* i *such that*

$$p - 1 \mid i, \quad p \nmid \binom{n}{i}, \quad \frac{S(i)}{p-1} > -a \quad \text{and} \quad p \nmid \binom{-k}{\frac{i}{p-1}}.$$

Proof. Assume that $S(\Delta) = p - 1$ and that $\Delta/(p-1) \prec t/(p-1)$, e.g. $\Delta = N(t)$. Let $t_1 = t - \Delta$, so $0 \le t_1 < t$, $p-1 \mid t_1$, and $t_1/(p-1) \prec t/(p-1)$, whence by (iii) of the preceding corollary,

$$\begin{aligned}
a &\le \frac{S(n-t_1) - S(n)}{p-1} + \nu_p\binom{-k}{\frac{t_1}{p-1}} \\
&= \frac{S(n-t_1) - S(n-t)}{p-1} + \frac{S(n-t) - S(n)}{p-1} + \nu_p\binom{-k}{\frac{t_1}{p-1}} \\
&\le \frac{S(\Delta)}{p-1} + \frac{S(n-t) - S(n)}{p-1} + \nu_p\binom{-k}{\frac{t_1}{p-1}} \\
&\le 1 + \frac{S(n-t) - S(n)}{p-1} + \nu_p\binom{-k}{\frac{t}{p-1}} \le a\,.
\end{aligned}$$

Thus all the inequalities are actually equalities, so

$$\nu_p(b_t) = \frac{S(n-t)-S(n)}{p-1} + \nu_p\binom{-k}{\frac{t}{p-1}} = a-1\,,$$

$$\nu_p\binom{-k}{\frac{t_1}{p-1}} = \nu_p\binom{-k}{\frac{t}{p-1}}\,,$$

and

$$S(n-t_1) = S(\Delta) + S(n-t), \quad \text{i.e. } n-t \perp \Delta\,.$$

It follows that $\nu_p\binom{-k}{\frac{t}{p-1}} = 0$, since if not, and r is the lowest place where there is a carry base p for $k-1+t/(p-1)$, i.e. $(k-1)_r + \left(\frac{t}{p-1}\right)_r \ge p$, and if $\Delta = \left(\frac{t}{p-1}\right)_r p^r(p-1)$, then $t_1/(p-1)$ and $t/(p-1)$ agree in all places except place r and $\left(\frac{t_1}{p-1}\right)_r = 0$, so

$$\nu_p\binom{-k}{\frac{t_1}{p-1}} < \nu_p\binom{-k}{\frac{t}{p-1}}\,,$$

contradicting the above equation.

Next assume $\left(\frac{t}{p-1}\right)_r \ne 0$, and let $\Delta = (p-1)p^r$. Then $n-t \perp \Delta$, whence $(n-t)_r = 0$.

Therefore $n-t$ has non-zero digits only in the places where $t/(p-1)$ is zero.

Now, let $\Delta_0 = N(t)$. Then $n-t \perp \Delta_0$ and $n-t$ has zero digits in all the places of Δ_0 except possibly the top place. Next consider $\Delta_1 = N(t-\Delta_0)$. The same argument shows $n-t \perp \Delta_1$, and if Δ_1 and Δ_0 share a digit of n in place r, then $(n-t)_r = 0$. Continue the process. Since $p-1 \mid t$, t is the sum of these Δ_i, so $n-t \perp t$, and the theorem follows.

We can deduce easily from the preceding theorem and Lemmas 2.2 and 2.3

Corollary 3.4. *Let l be a bottom segment of n with $S(n-l) \ge p-1$. Let $k = n-l$. Then $t = N(n-l)$ is the smallest i such that $\nu_p(b_i) < 0$, $\nu_p(b_t) = -1$, and $\nu_p(b_i) \ge -1$ for all i.*

Proof. Observe that $t = \Delta = N(n-l)$, following the notation of the previous proof.

If $l' < l$ is any smaller segment of n, then $k-1$ has all digits $p-1$ in the places of l, so $p \mid \binom{-k}{\frac{N(n-l')}{p-1}}$. Since $p \nmid \binom{-k}{\frac{N(n-l)}{p-1}}$ and $p \mid \binom{-k}{\frac{N(n-l-l_1-N(n-l))}{p-1}}$

if l_1 is a bottom segment of $n-l-N(n-l)$ by the lemmas, the result follows immediately.

Remark 2. Let t_j be the smallest i such that $\nu_p(b_i) < -j$ for $j = 0, 1, \ldots, -a$. Then $\nu_p(b_i) = -j-1$ if $i = t_j$ by (iv), so there are no gaps in the orders of the poles. We can use (v) to construct t as follows: there is a (unique) sequence $l_0, l_1, \ldots, l_{-a}$ of segments of $n-t$ such that l_{j+1} is a bottom segment of $n - t_j - \sum_{\lambda=0}^{j} l_\lambda$ and

$$t_{j+1} - t_j = N\Big(n - t_j - \sum_{\lambda=0}^{j+1} l_\lambda\Big) = N_{j+1}\,.$$

Thus the higher order poles come in the natural order. In particular, $t_0 = N(n - l_0) = N_0$ gives the first pole (simple), where l_0 is a bottom segment of n, and $t_1 = t_0 + N(n - t_0 - l_0 - l_1)$ gives the first higher pole (double), where l_1 is a bottom segment of $n - t_0 - l_0$. Hence $t_j = \sum_{\lambda=0}^{j} N_\lambda$, where $S(N_\lambda) = p-1$, and the N_λ give the degree differences for the successively higher order poles. The sequences (t_j) and (l_j) can be determined recursively together from n and k as follows: l_{j+1} is the smallest segment l of $n - t_j$ starting in the place of the highest digit of t_j such that

$$p \nmid \binom{-k}{\frac{N(n - t_j - \sum_{\lambda=0}^{j} l_\lambda - l)}{p-1}}\,,$$

and $t_{j+1} - t_j = N(n - t_j - \sum_{\lambda=0}^{j+1} l_\lambda)$, with initial condition $t_{-1} = 0$.

It follows that $k = 1$ gives the biggest possible pole, which has order $\left[\dfrac{S(n)}{p-1}\right]$, with all $l_j = 0$. In particular, there are no poles if $S(n) < p-1$.

It is not hard to show that we can turn around the preceding construction, namely if t is constructed as in the preceding paragraph, then there exists k such that $t_j = \sum_{\lambda=0}^{j} N_\lambda$ is the first i such that $\nu_p(b_i) < -j$ for $j = 0, 1, \ldots, -a$, and $\nu_p(b_i) \ge a-1$ for all i. Thus t exhibits the complete singularity pattern for such k. It can be seen that one way to choose k is to start with $n - l_0$, subtract all the N_λ for $\lambda > 0$ and also the highest place contribution of N_0 if N_0 and N_1 share a digit of n.

The case $p = 2$ is simplest to describe since $S(N) = p-1$ iff N is a 2-power, and there is no sharing of digits. In this case, $N_0, N_1, \ldots, N_{-a}$ are just successively higher powers of 2 that occur in the base 2 expansion of n, and $k = n - l_0 - \sum_{\lambda=1}^{-a} N_\lambda = n - l_0 - (t_{-a} - t_0)$.

Now we turn to the p-Eisenstein behavior of these polynomials. When we say that $A_n(x, -k)$ is p-Eisenstein down to degree d, we *actually refer to* $pA_n(x, -k)$. The condition that we need is a simple highest order pole, which by the above analysis is equivalent to having a (simple) pole, but no pole of order two, i.e.

$$\nu_p(b_0)=0,\ \nu_p(b_i)\ge 0 \text{ for } i<n-d,\ \nu_p(b_{n-d})=-1,\ \nu_p(b_i)\ge -1 \text{ all } i\,.$$

If $S(n) < p-1$, then $(S(n-i)-S(n))/(p-1) > -1$ for all i, so as previously noted there is no p-Eisenstein behavior. The next theorem, which establishes all instances of p-Eisenstein behavior follows immediately from the preceding discussion.

THEOREM 3.5. *If $A_n(x,-k)$ is p-Eisenstein down to degree d, then $d = n-N(n-l)$ for some bottom segment l of the p-adic expansion of n with $S(n-l)\ge p-1$. Conversely, if $d=n-N(n-l)$, then $A_n(x,-(n-l))$ is p-Eisenstein down to degree d; furthermore, $A_n(x,-k)$ is p-Eisenstein down to degree d iff the following three conditions hold*:

(i) $p\mid\binom{-k}{\frac{N(n-l')}{p-1}}$ *for all bottom segments l' of n such that $l'<l$,*

(ii) $p\nmid\binom{-k}{\frac{N(n-l)}{p-1}}$, *and*

(iii) $p\mid\binom{-k}{\frac{N(n-l-l_1-N(n-l))}{p-1}}$ *if l_1 is any bottom segment of $n-l-N(n-l)$.*

(*This condition assumes $S(n-l)-S(l_1)-(p-1)\ge p-1$, so it is vacuous if $S(n-l)<2(p-1)$.*)

The case $p=2$ of this theorem is particularly easy to state: If $A_n(x,-k)$ is 2-Eisenstein down to degree d, then $d=n-2^f$ for some power 2^f in the base 2 expansion of n. Furthermore, $A_n(x,-k)$ is 2-Eisenstein down to degree $n-2^f$ iff $2\nmid\binom{-k}{2^f}$ and $2\mid\binom{-k}{2^g}$ for all other powers 2^g in the base 2 expansion of n iff the base 2 expansion of $k-1$ contains all the 2^g but does not contain 2^f iff $n-2^f\prec k-1$ iff $k-1=n-2^f+m$, where m is any sum of lower powers of 2 not in the base 2 expansion of n. (Observe that $k=n-l$ if m is all these lower powers, where l is the bottom segment of n below 2^f.)

The following corollaries are special cases. Take $l=0$ to get the first three corollaries, and $l=n_0$ to get the last three.

COROLLARY 3.6 (Kimura). *$A_n(x,-n)$ is p-Eisenstein down to degree $n-N(n)$.*

Remark 3. It follows immediately that if $p-1\le S(n)<2(p-1)$, then $A_n(x,-k)$ is p-Eisenstein down to degree $n-N(n)$ iff $p\nmid\binom{-k}{\frac{N(n)}{p-1}}$.

Since $N(n)=n$ iff $S(n)=p-1$, for our restricted use of $N(n)$, we get

COROLLARY 3.7 (McCarthy). *$A_n(x,-n)$ is p-Eisenstein iff $S(n)=p-1$.*

We can sharpen this as follows:

COROLLARY 3.8. *The following are equivalent*:

(i) $S(n) = p - 1$.
(ii) *There exists* $k \in \{1, \ldots, n\}$ *such that* $A_n(x, -k)$ *is p-Eisenstein.*
(iii) $A_n(x, -n)$ *is p-Eisenstein.*
(iv) $A_n(x, -1)$ *is p-Eisenstein.*

Furthermore, if these conditions hold, $A_n(x, -k)$ *is p-Eisenstein iff* $p \nmid \binom{-k}{\frac{n}{p-1}}$.

R e m a r k 4. It follows that if $n = (p-1)p^r$ and $k \le n$, then $A_n(x, -k)$ is p-Eisenstein. In particular, if $n = 2^r$ and $k \le n$, then $A_n(x, -k)$ is 2-Eisenstein. In fact, it is easy to deduce that $A_n(x, -k)$ is p-Eisenstein for all $k \in \{1, \ldots, n\}$ iff $n = (p-1)p^r$, $r \ge 0$. (If $n \ne (p-1)p^r$ and n_f is the lowest non-zero digit, then let $k - 1 = (p-1)p^f$, so $k \le n$ and $k - 1 \not\perp \dfrac{n}{p-1}$.) More generally, if $n = m(p-1)p^r$ with $1 \le m < p$, then $0 < k \le (p-m)p^r$ and $n \ge k > (m-1)p^{r+1}$ each imply that $A_n(x, -k)$ is p-Eisenstein, namely $n = (m-1)p^{r+1} + (p-m)p^r$, so $S(n) = p - 1$, and each condition implies that $k - 1 \perp n/(p-1)$. Compare this with [8, Theorems 1, 2, 4] and [9, Theorems 1, 2].

COROLLARY 3.9 (*where* $l = n_0$). *Suppose that* $n = m + l$ *where* $l > 0$ *and* $p \nmid (n)_l$. *Then the following are equivalent*:

(i) $S(m) = p - 1$ *and* $p \mid m$.
(ii) *There exists* $k \in \{1, \ldots, n\}$ *such that* $A_n(x, -k)$ *is p-Eisenstein down to degree* l.
(iii) $A_n(x, -m)$ *is p-Eisenstein down to degree* l.

Furthermore, if these conditions hold, $A_n(x, -k)$ *is p-Eisenstein down to degree* l *iff* $p \nmid \binom{-k}{\frac{m}{p-1}}$ *and* $p \mid \binom{-k}{\frac{N(n)}{p-1}}$.

P r o o f. Observe that the conditions $p \nmid (n)_l$ and $p \mid n - l$ are equivalent to $l = n_0$. The result thus follows immediately from the theorem.

COROLLARY 3.10 (*where* $l = n_0 = 1$). *Suppose that* $p \mid n-1$ *and* $S(n-1) = p - 1$. *Then* $A_n(x, -(n-1))$ *is p-Eisenstein down to degree* 1 (*so there is an irreducible factor of degree* $n - 1$). *Also* $A_n(x, -k)$ *is p-Eisenstein down to degree* 1 *iff* $p \nmid \binom{-k}{\frac{n-1}{p-1}}$ *and* $p \mid \binom{-k}{\frac{n-i}{p-1}}$, *where* i *is the largest p-power* $< n$ (*so* $N(n) = n - i$).

We have not seen anything like the following simple corollary in the literature.

Corollary 3.11 (*where* $l = n_0 = 1$, $p = 2$). *If* $n = 2^r + 1$, *with* $r > 0$, *then* $A_n(x, -k)$ *is* p*-Eisenstein down to degree* 1 *iff* k *is even.* (*This is equivalent to* $2 \nmid \binom{-k}{2^r}$ *and* $2 \mid \binom{-k}{1}$.)

These corollaries give the irreducibility of certain instances of $A_n(x, -k)/(2x - (n - k - 1))$ for n odd. We give some additional illustrative computations beyond the case $n = 2^r + 1$, where the Kimura bound only gives the trivial result that there is an irreducible factor of degree ≥ 1, since $N(n) = 1$.

Examples. (1) Let $n = 13$, $p = 3$, $l = 1$. Then $S(12) = 2 = p - 1$ and $p \mid n - 1$, from which it follows that $A_n(x, -k)$ is p-Eisenstein down to degree 1 for $k = 2, 3, 11, 12$, whence $A_n(x, -k)/(2x - (n - k - 1))$ is irreducible for these values.

Since $N(13) = 4$, Kimura's analysis only gives an irreducible factor of degree ≥ 4, and McCarthy's higher order theorem [8, Theorem 3], with $p = 5$, only gives an irreducible factor of degree ≥ 8.

The preceding analysis can also be useful when n is even, e.g.

(2) $n = 14$, $p = 3$, $l = 2$. Then $A_{14}(x, -k)$ is 3-Eisenstein down to degree 2 if $k = 3$ or 12, so there is an irreducible factor of degree ≥ 12. On the other hand, $N(14) = 2$, so Kimura's bound only gives an irreducible factor of degree ≥ 2. It is of course known that $B_{14}(x)$ is irreducible [5].

(3) Finally, we consider the "exceptional case" $n = 11$, where there is an additional irreducible quadratic factor for $k = 11$ (cf. [3]).

With $p = 2$, $N(11) = 1$ and $N(10) = 2$, which do not help much, but $N(8) = 8$, so $A_{11}(x, -8)$ has an irreducible factor of degree ≥ 8.

All of the p-Eisenstein results for higher order Bernoulli polynomials which we have seen in the literature can be readily derived from Theorem 3.5 and its corollaries, usually considerably strengthened. As an example, consider the following theorem of McCarthy, with notations slightly changed to conform with our usage.

Theorem M [8, Theorem 3]. *Let* p *be an odd prime*, *and assume that* $n = r(p - 1) + 1$ *where* $0 \leq r - 1 \leq p - \alpha$. *Then* $B_n^{(\alpha)}(x)$ *has an irreducible factor of degree* $\geq n - p$.

We actually prove a stronger if and only if theorem, which contains the preceding result as one direction of the special case where $\alpha < p$.

THEOREM M′. *Let p be an odd prime and $1 \le \alpha \le n$. Assume that $p-1 \mid n-1$ and $2 \le (n-1)/(p-1) \le p$. Then $B_n^{(\alpha)}(x)$ is p-Eisenstein down to degree p iff*

$$\frac{n-p}{p-1} \le \left\lceil \frac{\alpha}{p} \right\rceil p - \alpha .$$

Proof. Let $r = (n-1)/(p-1)$, so $n = r(p-1)+1$ and $(n-p)/(p-1) = r-1$. (Thus if $\alpha < p$, Theorem M follows from our Theorem 3.5; the case $r = 1$ is trivial since then $n = p$ and Theorem M is vacuous.)

Let $q = \left\lceil \frac{\alpha}{p} \right\rceil$, so $0 \le qp - \alpha < p$. Since $rp \ge n \ge \alpha$, we have $r \ge q$. But $n = (r-1)p + (p-r+1)$ so $S(n) = p$ by our hypotheses, whence $p-1 \le S(n) < 2(p-1)$ since p is odd.

Thus if $k = n+1-\alpha$, then $B_n^{(\alpha)}(x)$ is p-Eisenstein down to degree $n - N(n)$ iff $p \nmid \binom{-k}{\frac{N(n)}{p-1}}$.

Since $N(n) = n-p = (r-1)(p-1)$, we must determine when $p \nmid \binom{-k}{r-1}$, i.e. when $k-1 \perp r-1$. But $k-1+r-1 = rp-\alpha = (r-q)p + (qp-\alpha)$ and $0 \le r-q$, $r-1$, $qp-\alpha \le p-1$, so the result follows immediately from Lucas's Theorem.

References

[1] A. Adelberg, *A finite difference approach to degenerate Bernoulli and Stirling polynomials*, Discrete Math., submitted.

[2] —, *Irreducible factors and p-adic poles of higher order Bernoulli polynomials*, C. R. Math. Rep. Acad. Sci. Canada 14 (1992), 173–178.

[3] J. Brillhart, *On the Euler and Bernoulli polynomials*, J. Reine Angew. Math. 234 (1969), 45–64.

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

[5] —, *The irreducibility of the Bernoulli polynomial $B_{14}(x)$*, Math. Comp. 19 (1965), 667–670.

[6] N. Kimura, *On the degree of an irreducible factor of the Bernoulli polynomials*, Acta Arith. 50 (1988), 243–249.

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

[8] —, *Some irreducibility theorems for Bernoulli polynomials of higher order*, Duke Math. J. 27 (1960), 313–318.

[9] —, *Irreducibility of Bernoulli polynomials of higher order*, Canad. J. Math. 14 (1962), 565–567.

[10] I. Niven, H. Zuckerman and H. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, 1991.

[11] N. E. Nörlund, *Differenzenrechnung*, Springer, 1924.
[12] S. Roman, *The Umbral Calculus*, Academic Press, 1984.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
GRINNELL COLLEGE
GRINNELL, IOWA 50112, U.S.A.

Received on 4.9.1991
and in revised form on 23.6.1992 (2167)