for some nonzero integer U. Finally, $u_0 = u_\rho$, and $u_n | u_0$ for $n = 0, 1, \ldots$.

Proof: By Lemma 7 and the fact that $\{u_n\}$ is a kth order recurrent sequence, the sequence $\{u_n\}$ is periodic with period M. Letting ρ be the fundamental period, we now show that the denominator of the generating function $H(t)/K(t)$ must be of the form $1 - t^\rho$:

$$\begin{aligned}\frac{H(t)}{K(t)} &= u_0 + u_1 t + \cdots + u_{\rho-1}t^{\rho-1} + u_0 t^\rho + u_1 t^{\rho+1} + \cdots \\ &= u_0(1 + t^\rho + t^{2\rho} + \cdots) + u_1 t(1 + t^\rho + t^{2\rho} + \cdots) + \cdots \\ &= (u_0 + u_1 t + \cdots + u_{\rho-1}t^{\rho-1})(1 + t^\rho + t^{2\rho} + \cdots) \\ &= (u_0 + u_1 t + \cdots + u_{\rho-1}t^{\rho-1})\frac{1}{1 - t^\rho}.\end{aligned}$$

If $H(t)$ has no linear factors $1 - rt$ with $r^\rho = 1$, then $H(t)$ has no linear factors in common with $K(t)$. This means that no recurrence order for $\{u_n\}$ can be less than ρ.

We see that $\rho_i^{e_i} | \rho$ and $(\rho_i^{e_i}, \rho_j^{e_j}) = 1$ for $1 \le i < j \le t$, so that

$$u_\rho = U u_{\rho_1^{e_1}} u_{\rho_2^{e_2}} \cdots u_{\rho_t^{e_t}}$$

for some integer U. For $n \ge 1$, we have $u_{n\rho} = u_\rho$ and $u_n | u_{n\rho}$, so that $u_n | u_\rho$. That $u_0 = u_\rho$, so that $u_n | u_0$ for all n, follows from

$$\begin{aligned}a_k u_0 &= u_k - a_2 u_{k-1} - \cdots - a_k u_1 \\ &= u_{\rho+k} - a_2 u_{\rho+k-1} - \cdots - a_k u_{\rho+1} \\ &= a_k u_\rho.\end{aligned}$$

REFERENCES

1. Marshall Hall, "Divisibility Sequences of Third Order," *Amer. J. Math.*, Vol. 58 (1936), pp. 577-584.
2. John Riordan, *Combinatorial Identities* (New York: John Wiley & Sons, 1968).

*****

MINIMUM PERIODS MODULO *n* FOR BERNOULLI NUMBERS

W. HERGET
Technische Universitat, Braunschweig, Fed. Rep. Germany

The Bernoulli numbers B_m may be defined by

$$(1)\quad \begin{aligned}B_0 &= 1 \\ B_m &= \frac{1}{m+1}\sum_{i=0}^{m-1}\binom{m+1}{i}B_i \quad (m > 0).\end{aligned}$$

By the Kummer congruence, we have [2, p. 78 (3.3)],

$$(2)\quad \sum_{i=0}^{r} (-1)^i \binom{r}{i}\frac{B_{m+iw}}{m+iw} \equiv 0 \bmod p^{re},$$

with $w := p^{e-1}(p - 1)$, where $r \ge 1$, $e \ge 1$, $m > re$, p prime such that $p - 1 \nmid m$. With $r = 1$ we get, in particular

$$\frac{B_{m+p^{e-1}(p-1)}}{m+p^{e-1}(p-1)} \equiv \frac{B_m}{m} \mod p^e, \tag{3}$$

where $m > e$, $p - 1 \nmid m$.

Therefore, the sequence of the Bernoulli numbers is periodic after being reduced modulo n (where n is any integer) in the following sense. A rational a/b with $a, b \in Z$, $\gcd(a, b) = 1$, may be interpreted as an element of Z_n, the ring of integers modulo n, if and only if the congruence relation $yb \equiv a \mod n$ has a unique solution $y \in \{0, 1, 2, \ldots, n-1\}$, i.e., if and only if $\gcd(b, n) = 1$. In this case, a/b is said to be *n-integral*.

By the famous von Staudt-Clausen theorem we have for integer i and prime p (cf. [1] and [2]),

$$B_{2i}\ p\text{-integral} \Longleftrightarrow p - 1 \nmid 2i.$$

Since $B_0 = 1$, $B_1 = -1/2$ and $B_{2i+1} = 0$ for $i \in N$, we get

$$B_m\ p\text{-integral} \Longleftrightarrow p - 1 \nmid m \vee m = 0 \vee m \in \{3, 5, 7, \ldots\}. \tag{4}$$

Now let $L(n)$ be the smallest integer greater than 1 with the following property:

$$\exists m_0 \forall k,\ m \geq m_0:$$
$$\big(B_k\ n\text{-integral} \wedge k \equiv m \mod L(n) \Rightarrow B_m\ n\text{-integral} \wedge B_k \equiv B_m \mod n\big). \tag{5}$$

$L(n)$ is called the *period-length* of the sequence $\{B_k \mod n\}$.

The smallest possible integer m_0 in (5) is then called the *preperiod* of $\{B_k \mod n\}$ and will be denoted by $V(n)$.

If $n = n_1 n_2$, where n_1, n_2 are coprime, then clearly

$$L(n) = \operatorname{lcm}\big(L(n_1), L(n_2)\big) \quad \text{and} \quad V(n) = \max\big(V(n_1), V(n_2)\big).$$

Hence, it suffices to discuss the case $n = p^e$, p a prime. We will prove

Theorem 1: (a) $L(2^e) = L(3^e) = 2$

(b) $V(2^e) = V(3^e) = 2$

(c) $L(p^e) = p^e(p-1)$, where $p > 3$

(d) $V(p^e) \leq e + 1$.

Proof: If $2|n$ or $3|n$, none of the B_{2i} is n-integral by (4); since $B_2 = 0$, this proves (a) and $V(2^e)$, $V(3^e) \leq 2$. But $V(2^e) = 1$ and $V(3^e) = 1$, respectively, is impossible because $B_1 = -1/2$ is not 2-integral and $B_1 \not\equiv 0 \mod 3^e$. So we get (b) too.

Now let $p > 3$. From (3) we have, for $m > e$, $p - 1 \nmid m$, $t \geq 0$,

$$\frac{B_{m+tp^{e-1}(p-1)}}{m + tp^{e-1}(p-1)} \equiv \frac{B_m}{m} \mod p^e;\text{ hence,}$$

$$k = m + sp^e(p-1) \wedge p - 1 \nmid m \wedge m > e \Rightarrow B_k \equiv B_m \mod p^e. \tag{6}$$

Consequently, $L(p^e) | p^e(p-1)$. On the other hand, we first prove $p - 1 | L(p^e)$: suppose $p - 1 \nmid L(p^e)$; we may choose $m \geq V(p^e) + L(p^e)$ such that $p - 1 | m$ (and therefore $m \neq 0$ and $m \notin \{3, 5, 7, \ldots\}$), hence by (4) B_m is not p-integral. For $k := m - L(p^e)$, we have $k \equiv m \mod p^e$, $k \geq V(p^e)$ and $p - 1 \nmid k$, hence by (4) B_k is p-integral. But this is a contradiction to (5). So $L(p^e) = p^i(p-1)$ where $i \in \{0, \ldots, e\}$. It remains to show $i = e$. For this, we choose $q \in N$ such that $s := \big(qp(p-1) + 2\big)p^e > V(p^e)$. Because $p^e | s$ and $p - 1 \nmid s$, we have

$B_s \equiv 0 \bmod p^e$ [2, p. 78, Theorem 5]. Now suppose $i < e$. Then, $B_k \equiv B_s \equiv 0 \bmod p^e$ if $k \equiv s \bmod p_i(p - 1)$. Take

$$k := s + (p - 1)p^i = \big(2 + (qp^2 + 3)(p - 1)\big)p^i = 2 + t(p - 1),$$

where

$$t := 2\frac{p^i - 1}{p - 1} + (qp^2 + 3)p^i \in N;$$

then by (3) with $e = 1$ and $m = 2$,

$$\frac{B_2}{2} \equiv \frac{B_{2+(p-1)}}{2 + (p - 1)} \equiv \cdots \equiv \frac{B_k}{k} \bmod p,$$

where $B_k \equiv 0 \bmod p^e$. But, $p^e|s$ and $p^e\nmid(p - 1)p^i$ gives $p^e\nmid k$ and, therefore, $B_2/2 \equiv 0 \bmod p$, contradictory to $B_2 = 1/6$. Hence, $i = e$ holds, and thus

$$L(p^e) = p^e(p - 1) \quad \text{and} \quad V(p^e) \le e + 1$$

by (6).

Now we may improve this last inequality as follows:

Theorem 2:

1. $V(p) = 2$ for p prime.
2. Let p be a prime, $p > 3$ and $e \in \{2, 4, 6, \ldots\}$. Then,
   (a) $B_e \not\equiv 0 \bmod p \wedge p - 1\nmid e \Rightarrow V(p^e) = e + 1$.
   (b) k maximal such that
   $$\forall 0 \le i \le k: (B_{e-2i} \equiv 0 \bmod p^{2i+1} \vee p - 1|e - 2i)$$
   $$\Rightarrow V(p^e) = e - 1 - 2k.$$
3. Let p be a prime, $p > 3$ and $e \in \{3, 5, 7, \ldots\}$. Then,
   (a) $B_{e-1} \not\equiv 0 \bmod p^2 \wedge p - 1\nmid e - 1 \Rightarrow V(p^e) = e$.
   (b) k maximal such that
   $$\forall 0 \le i \le k: (B_{e-1-2i} \equiv 0 \bmod p^{2i+2} \vee p - 1|e - 1 - 2i)$$
   $$\Rightarrow V(p^e) = e - 2 - 2k.$$

Proof: By Theorem 1(d), we have $V(p) \le 2$. But $V(p) < 2$ is impossible since $B_1 = -1/2 \not\equiv 0 \bmod p$ and $B_{1+L(p)} = 0$, thus $V(p) = 2$.

For the proof of the other assertions we note that [4, p. 321, Cor.]:

$$\sum_{i=0}^{r} (-1)^i \binom{r}{i} B_{m+i\nu}(1 - p^{m-1+i\nu}) \equiv 0 \bmod p^{r(\omega+1)-1},$$

where p prime, $p \ne 2$, $p - 1|\nu$, and p^ω is the highest power of p contained in ν.

Setting $r := 1$ and $\nu := k - m$, we get

$$B_m(1 - p^{m-1}) - B_k(1 - p^{k-1}) \equiv 0 \bmod p^e,$$

where $p^e(p - 1)|k - m$ and $k \ge m \ge 1$. Because

$$k - 1 \ge m + p^e(p - 1) - 1 \ge p^e(p - 1) \ge 3^e \cdot 2 \ge e,$$

we have, for $k > m \ge 1$, $p - 1\nmid m$:

$$k \equiv m \bmod p^e(p - 1) \Rightarrow B_k - B_m \equiv p^{m-1}B_m \bmod p^e. \tag{7}$$

Now it is easy to verify the assertions.

It is not very difficult to derive the following corollary, which gives the value of $V(p^e)$ "explicitly" for regular p (a prime p is said to be *regular* if and only if $B_k \not\equiv 0 \bmod p$ for each $k \in \{2, 4, \ldots, p - 3\}$.

Corollary 1: Let p be regular, $p > 3$ and $e > 0$.

(a) If $2|e$ then

$$V(p^e) = e + 1 \Longleftrightarrow p\nmid e \wedge p - 1\nmid e$$

$$V(p^e) \leq e - 1 \Longleftrightarrow p|e \vee p - 1|e$$

$$V(p^e) \leq e - 3 \Longleftrightarrow (p|e \wedge p - 1|e - 2) \vee (p - 1|e \wedge p^3|e - 2)$$

$$\Longleftrightarrow e \equiv 2p \bmod p(p - 1) \vee e \equiv 2 - 2p^3 \bmod p^3(p - 1)$$

$$V(p^e) = e - 5 \Longleftrightarrow p = 5 \wedge e \equiv 252 \bmod 500$$

$$V(p^e) \geq e - 5.$$

(b) If $2\nmid e$ then

$$V(p^e) = e \Longleftrightarrow p^2\nmid e - 1 \wedge p - 1\nmid e - 1$$

$$V(p^e) \leq e - 2 \Longleftrightarrow p^2|e - 1 \vee p - 1|e - 1$$

$$V(p^e) \leq e - 4 \Longleftrightarrow (p^2|e - 1 \wedge p - 1|e - 3) \vee (p - 1|e - 1 \wedge p^4|e - 3)$$

$$\Longleftrightarrow e \equiv 2p^2 + 1 \bmod p^2(p - 1) \vee e$$

$$\equiv -2p^4 + 3 \bmod p^4(p - 1)$$

$$V(p^e) = e - 6 \Longleftrightarrow p = 5 \wedge e \equiv 1253 \bmod 2500$$

$$V(p^e) \geq e - 6.$$

For the proof, note that $2\nmid V(p^e)$ holds for $e > 1$ and that in case of regular p and $p - 1\nmid 2i$, we have

$$B_{2i} \equiv 0 \bmod p^e \Longleftrightarrow p^e|2i.$$

The assertions of Corollary 1 with "$\Leftarrow$" are also valid for any irregular prime p.

By Corollary 1, you may see that only for greater integers p^e, the value $V(p^e)$ differs from e and $e + 1$, respectively. We get

Corollary 2: For prime p, $p > 3$, let $e_1 = p - 1$, $e_2 = p$, $e_3 = 2p$, $e_4 = 2p^2 + 1$, $e_5 = 252$, $e_6 = 1253$. Then we have

(a) $V(p^{e_i}) \leq e_i - i$, $i \in \{1, \ldots, 4\}$.

If p is regular, then $V(p^{e_i}) = e_i - i$, $i \in \{1, \ldots, 4\}$, and there is no smaller power of p such that $V(p^e) = e - i$.

(b) $V(5^{e_i}) = e_i - i$, $i \in \{5, 6\}$, and there is no smaller power of 5 such that $V(5^e) = e - i$.

(c) If p is regular and $p > 5$, then $V(p^e) \geq e - 4$.

For irregular primes, it is naturally somewhat more difficult to derive similar results about the smallest power of p such that $V(p^e) = e - i$, where $i \geq 1$. By Theorem 2, we get

$$B_e \equiv 0 \bmod p \wedge 2|e \Rightarrow V(p^e) \leq e - 1;$$

hence, for each irregular prime p, we have $V(p^e) \leq e - 1$ for at least one e such that $e \leq e_1 = p - 1$.

Considering the table of irregular primes in [1] we may compute that $n = 691^{12}$ is the smallest power of an irregular prime such that $V(p^e) = e - 1$.

There are still some open questions:

1. Are there powers $n = p^e$ of some (necessarily irregular) prime p such

that $e < e_i$ and $V(p^e) \leq e - i$, where $i \in \{2, 3, 4\}$? (By the computational results in [5] we may conclude that this does not happen when $p < 30{,}000$.)

2. Is there a power $n = p^e$ of some irregular prime such that

$$V(p^e) \leq e - 5?$$

Final Remark: Professor L. Carlitz and Jack Levine in [3] asked similar questions about Euler numbers and polynomials. Analogous results about the periodicity of the sequence of the Bernoulli polynomials reduced modulo n and the polynomial functions over Z generated by the Bernoulli polynomials will be derived in a later paper.

REFERENCES

1. Z. I. Borevic & I. R. Safarevic, *Number Theory*, "Nauka" (Moscow, 1964; English trans. in *Pure and Applied Mathematics*, Vol. 20 [New York: Academic Press, 1966]).
2. L. Carlitz, "Bernoulli Numbers," *The Fibonacci Quarterly*, Vol. 6, No. 3 (1968), pp. 71-85.
3. L. Carlitz & J. Levine, "Some Problems Concerning Kummer's Congruences for the Euler Numbers and Polynomials," *Trans. Amer. Math. Soc.*, Vol. 96 (1960), pp. 23-37.
4. J. Fresnel, "Nombres de Bernoulli et fonctions L p-adiques," *Ann. Inst. Fourier, Grenoble*, Vol. 17, No. 2 (1967), pp. 281-333.
5. W. Johnson, "Irregular Prime Divisors of the Bernoulli Numbers," *Mathematics of Computation*, Vol. 28, No. 126 (1974), pp. 652-657.

*****

THE RANK-VECTOR OF A PARTITION

HANSRAJ GUPTA
Panjab University, Chandigarh, India

1. INTRODUCTION

The Ferrars graph of a partition may be regarded as a set of nested right angles of nodes. The depth of a graph is the number of right angles it has. For example, the graph