POWER-SUM DENOMINATORS

BERND C. KELLNER AND JONATHAN SONDOW

Abstract. The *power sum* $1^n + 2^n + \cdots + x^n$ has been of interest to mathematicians since classical times. Johann Faulhaber, Jacob Bernoulli, and others who followed expressed power sums as polynomials in x of degree $n+1$ with rational coefficients. Here we consider the denominators of these polynomials, and prove some of their properties. A remarkable one is that such a denominator equals $n+1$ times the squarefree product of certain primes p obeying the condition that the sum of the base-p digits of $n+1$ is at least p. As an application, we derive a squarefree product formula for the denominators of the Bernoulli polynomials.

Figure 1. Johann Faulhaber (1580–1635). †

1. Introduction

Johann Faulhaber was "known in his day as The Great Arithmetician of Ulm" (see [7, p. 106], [31, p. 152]). In his 1631 book *Academia Algebrae* [11], Faulhaber worked out formulas for *power sums* $1^n + 2^n + \cdots + x^n$ as polynomials in x of degree $n+1$ with rational coefficients. He found that

$$\begin{aligned}
1^0 + 2^0 + \cdots + x^0 &= x,\\
1^1 + 2^1 + \cdots + x^1 &= \frac{1}{2}(x^2 + x),\\
1^2 + 2^2 + \cdots + x^2 &= \frac{1}{6}(2x^3 + 3x^2 + x),
\end{aligned}$$

2010 *Mathematics Subject Classification.* 11B68 (Primary), 11B83 (Secondary).
Key words and phrases. Denominator, power sum, Bernoulli numbers and polynomials, sum of base-p digits.

$$\begin{aligned}
1^3 + 2^3 + \cdots + x^3 &= \frac{1}{4}(x^4 + 2x^3 + x^2), \\
1^4 + 2^4 + \cdots + x^4 &= \frac{1}{30}(6x^5 + 15x^4 + 10x^3 - x), \\
1^5 + 2^5 + \cdots + x^5 &= \frac{1}{12}(2x^6 + 6x^5 + 5x^4 - x^2),
\end{aligned}$$

and so on up to $n = 17$ (see [8, 19, 25, 32]; a comprehensive survey of Faulhaber's life and mathematical work is given in [27]). The fractions in these formulas naturally lead one to consider the denominators.

Definition 1. For $n \geq 0$, the nth *power-sum denominator* is the smallest positive integer d_n such that $d_n \cdot (1^n + 2^n + \cdots + x^n)$ is a polynomial in x with *integer* coefficients.

The first few values of d_n (see [29, Sequence A064538]) are

$$d_n = 1, 2, 6, 4, 30, 12, 42, 24, 90, 20, 66, 24, 2730, 420, 90, 48, 510, \ldots .$$

In this article, we study the power-sum denominators and related numbers and prove some of their properties. We first collect some fairly straightforward ones. Throughout the paper, p always denotes a prime.

Theorem 1. *The sequence of power-sum denominators d_n for $n \geq 0$ has the following properties:*

(i) $p \mid d_n \implies p \leq n + 1$.
(ii) *d_n is divisible by $n + 1$, and we have a squarefree quotient*
$$q_n \stackrel{\text{def}}{=} \frac{d_n}{n+1}.$$
(iii) *d_n is even for all $n \geq 1$, while q_n is odd if and only if $n = 2^r - 1$ for some $r \geq 0$.*
(iv) $$p \mid q_n \implies p \leq M_n \stackrel{\text{def}}{=} \begin{cases} \dfrac{n+2}{2}, & \text{if } n \text{ is even,} \\ \dfrac{n+2}{3}, & \text{if } n \text{ is odd.} \end{cases}$$

The first few quotients (see [29, Sequence A195441]) are

$$q_n = 1, 1, 2, 1, 6, 2, 6, 3, 10, 2, 6, 2, 210, 30, 6, 3, 30, 10, 210, 42, 330, \ldots .$$

Their values can be computed from the following surprising and remarkable formula. As usual, an empty product is defined to be 1.

Theorem 2. *For all $n \geq 0$, we have the prime factorization*

$$q_n = \prod_{\substack{p \leq M_n \\ s_p(n+1) \geq p}} p, \tag{1}$$

where q_n and M_n are as in Theorem 1, and $s_p(n)$ denotes the sum of the base-p digits of n, as defined in Section 6. Moreover, the bound M_n is sharp for infinitely many even (respectively, odd) values of n. In particular, the sequence $(q_n)_{n \geq 0}$ is unbounded.

Example 1. To illustrate Theorems 1 and 2, we compute the table

n	M_n	q_n	d_n
19	7	$2\cdot 3\cdot 7 = 42$	$20\cdot q_{19} = 840$
20	11	$2\cdot 3\cdot 5\cdot 11 = 330$	$21\cdot q_{20} = 6930$

which depends on the values of $s_p(n+1)$ given by

p	2	3	5	7
$s_p(20)$	2	4	4	8

and

p	2	3	5	7	11
$s_p(21)$	3	3	5	3	11

.

The rest of the paper is organized as follows. The next section is devoted to preliminaries, including Bernoulli's formula for power sums and the von Staudt–Clausen theorem on Bernoulli numbers. In Section 3 we consider some properties of the binomial coefficients and we prove five lemmas. Section 4 contains the proof of Theorem 1. In Section 5 we use a congruence on binomial coefficients due to Hermite and Bachmann to give another formula for the quotients q_n. In Section 6 we prove Theorem 2 using p-adic methods, including results of Legendre and Lucas. In the final section the theorems are applied to the denominators of the Bernoulli polynomials.

2. Preliminaries

In his *Ars Conjectandi* [4, pp. 96–98] of 1713, Jacob Bernoulli generalized Faulhaber's formulas, but without giving a rigorous proof. Later a proof followed as a special case of the more general *Euler–Maclaurin summation formula*, which was independently found (cf. [15, p. 402]) by Euler [9, pp. 17–18] and Maclaurin [22, pp. 676–677] around 1735. In modern terms, *Bernoulli's formula* for power sums (see [7, pp. 106–109]) states that for $n \geq 1$,

$$S_n(x) \stackrel{\text{def}}{=} 1^n + 2^n + \cdots + (x-1)^n = \frac{B_{n+1}(x) - B_{n+1}}{n+1}, \tag{2}$$

where the nth *Bernoulli polynomial* $B_n(x)$ is defined symbolically as

$$B_n(x) \stackrel{\text{def}}{=} (B+x)^n \stackrel{\text{def}}{=} \sum_{k=0}^{n} \binom{n}{k} B_k\, x^{n-k} \tag{3}$$

and the *Bernoulli numbers* $B_0, B_1, B_2, \ldots$ are rational numbers defined by the generating function

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!} \quad (|t| < 2\pi).$$

It turns out that $B_n = 0$ for odd $n > 1$ (see, e.g., [17, Section 7.9]). The sequence of nonzero Bernoulli numbers starts with

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \tag{4}$$

and continues with

$$B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30},\ B_{10} = \frac{5}{66},\ B_{12} = -\frac{691}{2730},\ \ldots.$$

Definition 2. Every rational number $\rho \in \mathbb{Q}$ can be written uniquely in lowest terms as a fraction $\rho = \nu/\delta$ with $\nu \in \mathbb{Z}$ and $\delta \in \mathbb{N}$. We define $\operatorname{denom}(\rho) \stackrel{\text{def}}{=} \delta$. (In particular, if $m \in \mathbb{Z}$, then $\operatorname{denom}(m) = 1$.) This definition extends uniquely to polynomials $p(x) \in \mathbb{Q}[x]$ by defining $\operatorname{denom}\bigl(p(x)\bigr)$ to be the smallest positive integer d such that $d \cdot p(x) \in \mathbb{Z}[x]$.

A fundamental property of the nonzero Bernoulli numbers B_n is the simple shape of their denominators. By the famous *von Staudt–Clausen theorem* (cf. [7, p. 109], [17, Section 7.9]), independently found by von Staudt [30] and Clausen [5] in 1840,

$$\operatorname{denom}(B_n) = \prod_{(p-1)\,|\,n} p \quad (n \in 2\mathbb{N}), \tag{5}$$

where n is even and the product runs over all primes p such that $p-1$ divides n (thus always including the primes 2 and 3). Together with B_0 and B_1, all nonzero Bernoulli numbers have a squarefree denominator.

The *integer-valued* polynomial $S_n(x) \in \mathbb{Q}[x]$ satisfies the functional equation

$$S_n(x+1) = S_n(x) + x^n = 1^n + 2^n + \cdots + x^n \quad (x \in \mathbb{N}). \tag{6}$$

Definitions 1 and 2 yield that $d_n = \operatorname{denom}(S_n(x+1))$. As we now show, it is also true that

$$d_n = \operatorname{denom}\bigl(S_n(x)\bigr). \tag{7}$$

This enables a link to Bernoulli's formula (2) and the Bernoulli polynomials.

The case $n = 0$ of (7) is easily seen directly. For $n \geq 1$, we obtain from formulas (2), (3), and (4) that

$$S_n(x) = \frac{x^{n+1}}{n+1} - \frac{x^n}{2} + \cdots . \tag{8}$$

Comparison with (6) shows that $S_n(x)$ differs from $S_n(x+1)$ by the summand x^n, which only results in a sign change from $-\frac{1}{2}$ to $+\frac{1}{2}$ in the coefficient of x^n in (8). This sign change has no effect on the denominators of the polynomials in question, so (7) holds. (All of this will be shown in more detail in the proof of Theorem 1.)

Revisiting the formulas of Faulhaber on the first page, one might notice the simple pattern $\frac{1}{d_n} \times$ polynomial. The next lemma clarifies this observation that the numerator is always 1, as a supplement to our study of power-sum denominators. (We omit the trivial case $n = 0$ here, since $S_n(x)$ is defined for $n \geq 1$.)

Lemma 1. *For $n \geq 1$, we have*

$$S_n(x) = \frac{1}{d_n} \cdot p_n(x),$$

where the coefficients of the polynomial $p_n(x) \in \mathbb{Z}[x]$ are coprime.

Proof. From (7) we deduce the decomposition

$$S_n(x) = \frac{a_n}{d_n} \cdot p_n(x),$$

where a_n and d_n are coprime positive integers, and $p_n(x) \in \mathbb{Z}[x]$ has coprime coefficients. Since $S_n(x)$ is integer-valued, we infer that $S_n(x) \equiv 0 \pmod{a_n}$ for $x = 1, 2, \ldots$. In particular, $1 = S_n(2) \equiv 0 \pmod{a_n}$, which implies $a_n = 1$. □

The lemma confirms the observation that, in Faulhaber's formulas on the first page, the integer coefficients of the nth polynomial are coprime. Moreover, their sum must equal the denominator d_n, as one sees by setting $x = 1$.

3. Lemmas

Before we give proofs of our theorems, we need several more lemmas.

Lemma 2. *For $n \geq 1$, define*

$$T_n(x) \stackrel{\text{def}}{=} (n+1)\frac{S_n(x)}{x}.$$

Then $T_n(x)$ is a monic polynomial in $\mathbb{Q}[x]$, and is given by

$$T_n(x) = \sum_{k=0}^{n} \binom{n+1}{k} B_k\, x^{n-k}.$$

Proof. From (2) and (3), it follows that

$$T_n(x) = \frac{B_{n+1}(x) - B_{n+1}}{x} = \sum_{k=0}^{n} \binom{n+1}{k} B_k\, x^{n-k} \in \mathbb{Q}[x].$$

Since the coefficient of x^n is $\binom{n+1}{0} B_0 = 1$ by (4), the polynomial $T_n(x)$ is monic. $\square$

Lemma 3. *For any integers $m \geq k \geq 0$, we compute the denominators*

$$D_{m,k} \stackrel{\text{def}}{=} \operatorname{denom}\left(\binom{m}{k} B_k\right) = \prod_{p\, \in\, \mathcal{P}_{m,k}} p,$$

where the sets $\mathcal{P}_{m,k}$ of primes are defined by the following cases:

(i) $\mathcal{P}_{m,k} \stackrel{\text{def}}{=} \emptyset$, *if $k = 0$ or $k \geq 3$ is odd.*

(ii) $\mathcal{P}_{m,k} \stackrel{\text{def}}{=} \begin{cases} \emptyset, & \text{if } k = 1 \text{ and } m \text{ is even}, \\ \{2\}, & \text{if } k = 1 \text{ and } m \text{ is odd}. \end{cases}$

(iii) $\mathcal{P}_{m,k} \stackrel{\text{def}}{=} \left\{p : (p-1) \mid k \text{ and } p \nmid \binom{m}{k}\right\}$, *if $k \geq 2$ is even.*

Proof. Recall that $B_0 = 1$ and $B_1 = -\frac{1}{2}$ by (4), and that $B_k = 0$ for odd $k > 1$.

(i). It follows that $D_{m,0} = 1$, and $D_{m,k} = 1$ if $k \geq 3$ is odd. This shows case (i).

(ii). We have $D_{m,1} = \operatorname{denom}\left(-\frac{m}{2}\right)$, so $D_{m,1} = 1$ if m is even, while $D_{m,1} = 2$ if m is odd. Case (ii) follows.

(iii). By the von Staudt–Clausen theorem in (5), $\operatorname{denom}(B_k)$ is squarefree. Thus $D_{m,k}$ is the product of the primes given by (5) (with k in place of n), but excluding prime factors of $\binom{m}{k}$. This proves case (iii). $\square$

Hereafter, we will use the convention that $\max(\emptyset) \stackrel{\text{def}}{=} 0$.

Lemma 4. *For odd $m \geq 3$ and $k = 2, 4, \ldots, m-1$, the set $\mathcal{P}_{m,k}$ defined in Lemma 3 satisfies the bound*

$$\max(\mathcal{P}_{m,k}) \leq \min\left(k+1, \frac{m+1}{2}\right).$$

Proof. If $P_{m,k} = \emptyset$, the bound holds vacuously, and we are done. Otherwise, fix $p \in P_{m,k}$. Then $(p-1) \mid k$, so the trivial bound $p \leq k+1$ holds. It remains to show that $p \leq m_o \stackrel{\text{def}}{=} \frac{1}{2}(m+1)$ when $k \leq m-1$.

Case 1. If $k < m_o$, then $p \leq k+1 \leq m_o$ and we are done.

Case 2. If $m_o \leq k \leq m-1$, assume first that $p - 1 < k$. Then the integer $\frac{k}{p-1} \geq 2$, so $p - 1 \leq \frac{1}{2}k \leq \frac{1}{2}(m-1) < m_o$. Thus $p \leq m_o$.

Case 3. There remains the possibility that $m_o \le k \le m-1$ and $p-1=k$. But then $m-p+2 \le p \le m$, so the binomial coefficient

$$\binom{m}{k} = \binom{m}{p-1} = \frac{m(m-1)\cdots p \cdots (m-p+2)}{(p-1)!} \tag{9}$$

is divisible by the prime p, contradicting $p \in \mathcal{P}_{m,k}$. This completes the proof. $\square$

Lemma 5. *For even $m \ge 4$ and $k = 2,4,\ldots,m-2$, the set $\mathcal{P}_{m,k}$ defined in Lemma 3 satisfies the bound*

$$\max(\mathcal{P}_{m,k}) \le \min\left(k+1, \frac{m+1}{3}\right).$$

Proof. As in the proof of Lemma 4 through Case 1, it suffices to show that $p \in \mathcal{P}_{m,k}$ implies $p \le m_e \overset{\text{def}}{=} \frac{1}{3}(m+1)$ when $m_e \le k \le m-2$.

If $p = 2$, then $m = 4$ would imply that $\binom{m}{k} = \binom{4}{2} = 6$ is divisible by p, contradicting $p \in \mathcal{P}_{m,k}$. Thus if $p = 2$, then $m \ge 6$, which implies $p \le m_e$. So from now on we assume that p is odd. Set $k' \overset{\text{def}}{=} \frac{k}{p-1} \in \mathbb{N}$.

Case 1. If $k' \ge 3$, then $p - 1 \le \frac{1}{3}k \le \frac{1}{3}(m-2) = m_e - 1$, so $p \le m_e$.

Case 2. If $k' = 2$, then $2p = k+2 \le m$. If in addition $m - 2p + 3 \le p$, then

$$\binom{m}{k} = \binom{m}{2p-2} = \frac{m(m-1)\cdots 2p \cdots p \cdots (m-2p+3)}{1 \cdot 2 \cdots p \cdots (2p-2)}$$

is divisible by p, contradicting $p \in \mathcal{P}_{m,k}$. Hence $p < m - 2p + 3$, so $3p \le m+2$. Now, p odd and m even imply $3p \le m+1$, so $p \le m_e$.

Case 3. If $k' = 1$, then $p = k+1 < m$. If in addition $m - p + 2 \le p$, then (9) implies that $p \mid \binom{m}{k}$, a contradiction. Thus $2p < m+2$. As $2p$ and m are even, we therefore get $2p \le m$. Now, if $m_e < p$, then $m - p + 1 < 2p$, so

$$\binom{m}{k} = \binom{m}{p-1} = \frac{m(m-1)\cdots 2p \cdots (m-p+2)}{(p-1)!}$$

is divisible by p, contradicting $p \in \mathcal{P}_{m,k}$. Thus $p \le m_e$, and we are done. $\square$

For the next lemma we need some properties of binomial coefficients modulo 2. Drawing *Pascal's triangle* (mod 2), with a dot for the digit 1 and a blank for 0, one obtains down to row $2^r - 1$ for $r \ge 2$ a dotted, framed triangle Δ_r with a self-similar pattern (see Figures 2 and 3 as well as [33, Fig. 2, p. 567] and [16]). Letting $r \to \infty$ while scaling to an equilateral triangle of fixed size, this leads to a fractal, which is subdivided recursively and is called the *Sierpiński gasket*, introduced in [28].

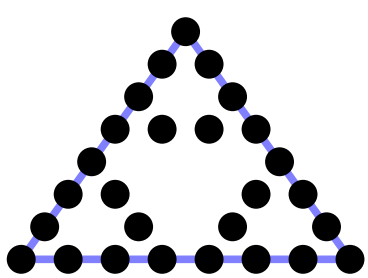

FIGURE 2. Pascal's triangle (mod 2): Δ_3.

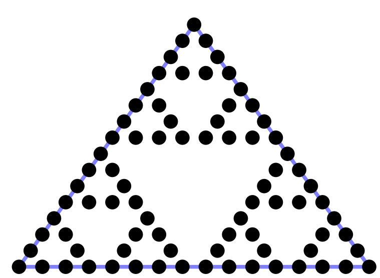

FIGURE 3. Pascal's triangle (mod 2): Δ_4.

In the mth row of Pascal's triangle, the entries $\binom{m}{k} \not\equiv 0 \pmod{p}$ with $0 \le k \le m$ can be counted as follows. Writing m as a string $\alpha_\ell \alpha_{\ell-1} \cdots \alpha_0$ of base-p digits α_j $(0 \le j \le \ell)$, the number of such entries equals

$$\#_p(m) \stackrel{\text{def}}{=} (\alpha_0 + 1)(\alpha_1 + 1) \cdots (\alpha_\ell + 1).$$

The case $p = 2$, which we use below, was proved by Glaisher [14], and the general case by Fine [12]. Since $\binom{m}{0} = \binom{m}{m} = 1$, we deduce that

$$\begin{aligned} \binom{m}{k} \text{ is even} \quad (0 < k < m) \quad &\iff \quad \#_2(m) = 2 \\ &\iff \quad m = 2^r \quad (r \ge 1). \end{aligned} \tag{10}$$

As a complement, it follows easily that $\binom{m}{0}, \binom{m}{1}, \ldots, \binom{m}{m}$ are all odd if and only if $m = 2^r - 1$ $(r \ge 0)$. This explains, together with $\binom{m}{0} = \binom{m}{m} = 1$ in each row, why the above mentioned triangle Δ_r is always framed.

We now consider a special case, which we use later.

Lemma 6. *Let $m \ge 4$ be even. The binomial coefficients $\binom{m}{2}, \binom{m}{4}, \ldots, \binom{m}{m-2}$ are all even if and only if m is a power of 2.*

Proof. In view of (10), it suffices to show that if m is even and k is odd, then $\binom{m}{k}$ is also even. Indeed, since k is odd and so $m - (k-1)$ is even, we have

$$\binom{m}{k} = \frac{m - (k-1)}{k} \binom{m}{k-1} \equiv 0 \pmod{2}. \qquad \square$$

4. Proof of Theorem 1

We can now prove our first main result.

Proof of Theorem 1. The case $n = 0$ is trivial, with $d_0 = q_0 = M_0 = 1$ satisfying all required properties. For the rest of the proof, we assume that $n \ge 1$.

(i), (ii). By (7) we have $d_n = \operatorname{denom}(S_n(x))$. Combining Lemmas 2 and 3 shows that

$$T_n(x) = (n+1) \frac{S_n(x)}{x} = \sum_{k=0}^{n} \frac{N_{n+1,k}}{D_{n+1,k}} \, x^{n-k},$$

where the denominators $D_{n+1,k}$ are determined by Lemma 3, while the numerators $N_{n+1,k}$ are certain integers that play no role in the proof. Since the $D_{n+1,k}$ are squarefree, the least common multiple

$$l_n \stackrel{\text{def}}{=} \operatorname{lcm}(D_{n+1,1}, \ldots, D_{n+1,n}) \tag{11}$$

is also squarefree. Since $T_n(x) \in \mathbb{Q}[x]$ is a monic polynomial, l_n is the smallest positive integer with the property that

$$l_n \cdot T_n(x) \in \mathbb{Z}[x].$$

Comparing this to the numbers d_n and q_n, we observe that

$$d_n = (n+1) \, l_n \quad \text{and} \quad q_n = l_n.$$

Using Lemma 3 and definition (11), we further obtain that

$$q_n = \prod_{p \,\in\, \mathcal{P}_{n+1}} p, \quad \text{where} \quad \mathcal{P}_n \stackrel{\text{def}}{=} \bigcup_{k=1}^{n-1} \mathcal{P}_{n,k}. \tag{12}$$

From the construction of the sets $\mathcal{P}_{n+1,k}$ (see Lemma 3), we infer that

$$\max(\mathcal{P}_{n+1}) \leq n+1. \tag{13}$$

This proves (i) and (ii).

(iii). Let $m = n+1$. We have to show that q_n is odd if and only if $m = 2^r$ with $r \geq 1$. By (12), we know that

$$2 \nmid q_n \quad \iff \quad 2 \notin \mathcal{P}_{m,k} \quad (1 \leq k < m).$$

Recall Lemma 3. Since $\mathcal{P}_{m,1} = \{2\}$ if m is odd, and $\mathcal{P}_{m,1} = \emptyset$ otherwise, there remains the case where m is even. If $m = 2$, then $\mathcal{P}_m = \emptyset$ and therefore $q_n = 1$ is odd and we are done. Now let $m \geq 4$ be even. Remember that $\mathcal{P}_{m,k} = \emptyset$ for odd $k \geq 3$, and that if k is even, then $2 \notin \mathcal{P}_{m,k}$ implies $2 \mid \binom{m}{k}$. With the help of Lemma 6, we finally deduce that $2 \notin \mathcal{P}_{m,k}$, for $k = 2, 4, \ldots, m-2$, if and only if m is a power of 2. As a consequence, the product $m\, q_n = (n+1)\, q_n = d_n$ is always even for $n \geq 1$. This shows (iii).

(iv). We first compute the cases $q_1 = 1 = M_1$, $q_2 = 2 = M_2$, $q_3 = 1 = \lfloor M_3 \rfloor$. Now take $n \geq 4$ and set $m = n+1$ again. We will refine (13) to show that

$$\max(\mathcal{P}_m) \leq M_n. \tag{14}$$

Note that $M_n \geq 2$ for $n \geq 4$. Following the arguments of part (iii) and noting that $\max(\mathcal{P}_{m,1}) \leq 2$, the inequality (14) evidently turns into

$$\max(\mathcal{P}_{m,k}) \leq M_n \quad (k = 2, 4, \ldots, m - \delta_m), \tag{15}$$

where

$$\delta_m \stackrel{\text{def}}{=} \begin{cases} 1, & \text{if } m \text{ is odd}, \\ 2, & \text{if } m \text{ is even}. \end{cases} \tag{16}$$

Case m odd. We apply Lemma 4 to get $\frac{m+1}{2} = \frac{n+2}{2} = M_n$.

Case m even. Lemma 5 yields $\frac{m+1}{3} = \frac{n+2}{3} = M_n$.

Both cases establish (15) and, consequently, (14). By (12), this shows the bounds in (iv). This completes the proof of Theorem 1. □

5. Further properties

Here we give an intermediate result that shows another formula for the values of q_n, which we need later on.

Theorem 3. *Let q_n and M_n be defined as in Theorem 1. For any fixed $n \geq 0$ we have*

$$q_n = \prod_{p \,\leq\, M_n} p^{\varepsilon_p}, \tag{17}$$

where ε_p, which depends on n, is defined for $p = 2$ by

$$\varepsilon_2 \stackrel{\text{def}}{=} \begin{cases} 0, & \text{if } n = 2^r - 1 \text{ for some } r \geq 0, \\ 1, & \text{otherwise}, \end{cases}$$

and for an odd prime $p \leq M_n$ by

$$\varepsilon_p \stackrel{\text{def}}{=} \begin{cases} 0, & \text{if } p \nmid (n+2) \text{ and } p \mid \binom{n+1}{j(p-1)} \text{ for all } j = 2, 3, \ldots, \left\lfloor \frac{n}{p-1} \right\rfloor - 1, \\ 1, & \text{otherwise}. \end{cases}$$

For a refinement step in the proof of Theorem 3, we need the following congruence. See Hermite [18] for the case m odd, and Bachmann [2, Eq. (116), p. 46] for the general case. For a recent elementary proof, see [23].

Lemma 7 (Hermite, Bachmann)**.** *If p is a prime and $m \geq 1$, then*

$$\sum_{1 \leq j \leq \frac{m-1}{p-1}} \binom{m}{j(p-1)} \equiv 0 \pmod{p}. \tag{18}$$

Proof of Theorem 3. By Theorem 1 we know that q_n is the product of certain primes $p \leq M_n$. Thus, to show (17), we have to determine the exponents ε_p.

If $p = 2$, then the value of ε_2 is given by Theorem 1 part (iii) for $n \geq 1$. Since $M_0 = 1$, the case $n = 0$ does not occur here. So we are done in case $p = 2$.

We now consider the case of an odd prime $p \leq M_n$. Since $M_n \leq 2$ if $n \leq 3$, we may fix $n \geq 4$. Set $m = n + 1$ and recall the definition of δ_m in (16). As in the proof of Theorem 1 and in relation (12), we have that

$$p \nmid q_n \quad \iff \quad p \notin \mathcal{P}_m$$

and by Lemma 3 we obtain that

$$p \nmid q_n \quad \iff \quad p \notin \mathcal{P}_{m,k} \quad (k = 2, 4, \ldots, m - \delta_m).$$

Note that $p \nmid q_n$ is equivalent to $\varepsilon_p = 0$. Recall from Lemma 3 that $p \in \mathcal{P}_{m,k}$ if and only if $(p-1) \mid k$ and $p \nmid \binom{m}{k}$. As $m - \delta_m$ and $p - 1$ are even, we have

$$L \stackrel{\text{def}}{=} \left\lfloor \frac{m-1}{p-1} \right\rfloor = \left\lfloor \frac{m-\delta_m}{p-1} \right\rfloor .$$

Substituting $k \mapsto j(p-1)$ for those k with $(p-1) \mid k$, we finally conclude that

$$\varepsilon_p = 0 \quad \iff \quad p \mid \binom{m}{j(p-1)} \quad (j = 1, 2, \ldots, L)\,. \tag{19}$$

We then infer by using (18) that

$$\sum_{1 \leq j < L} \binom{m}{j(p-1)} \equiv 0 \pmod{p} \quad \implies \quad \binom{m}{L(p-1)} \equiv 0 \pmod{p}.$$

Thus, we may replace the last index L with $L - 1$ in (19). It remains to show in case $j = 1$ that $p \mid \binom{m}{p-1}$ is equivalent to $p \nmid (m+1)$. To see this, note first that

$$p \mid \binom{m}{p-1} \quad \iff \quad p \mid m(m-1)\cdots(m-(p-2)).$$

Now, since $m, m-1, \ldots, m-(p-2)$, and $m+1$ represent the p different residue classes modulo p, we deduce the desired equivalence. This completes the proof of Theorem 3. $\square$

6. Proof of Theorem 2

Before giving the proof, we first introduce some notation and two preliminary results.

For a prime p, the *p-adic valuation* of an integer $x > 0$, denoted by $v_p(x)$, gives the exponent of the highest power of p that divides x. Any integer $x \geq 0$ can be written as a finite *p-adic expansion*

$$x = \alpha_0 + \alpha_1\, p + \cdots + \alpha_r\, p^r$$

with some $r \geq 0$ and unique *base-p digits* α_j satisfying $0 \leq \alpha_j \leq p-1$ for $j = 0, 1, \ldots, r$. (In case $x > 0$, we assume that $\alpha_r > 0$, unless r is prescribed, when trailing zeros may occur.) The sum of the digits of this expansion defines the function

$$s_p(x) \stackrel{\text{def}}{=} \alpha_0 + \alpha_1 + \cdots + \alpha_r.$$

Note that $s_p(x) = 0$ if and only if $x = 0$. Comparing the two equations above, one simply observes that

$$s_p(x) \equiv x \pmod{(p-1)}. \tag{20}$$

A further property, proved by Legendre [20, pp. 8–10] (see also [24, p. 77]), is that

$$v_p(x!) = \frac{x - s_p(x)}{p-1},$$

also implying (20) at once. An easy application to binomial coefficients provides that

$$v_p\left(\binom{m}{k}\right) = \frac{s_p(k) + s_p(m-k) - s_p(m)}{p-1}. \tag{21}$$

We are ready now to prove our second main result.

Proof of Theorem 2. Fix $n \geq 0$ and set $m = n+1$. With the help of Theorem 3 and its proof, we will show that (17) is equivalent to (1). To do so, we have to show for all primes $p \leq M_n$ that

$$\varepsilon_p = 1 \quad \Longleftrightarrow \quad s_p(m) \geq p. \tag{22}$$

If $n < 2$, then $M_n = 1$, and we are done. Now assume that $n \geq 2$, so that $m \geq 3$. As in the proof of Theorem 3, we set

$$L \stackrel{\text{def}}{=} \left\lfloor \frac{m-1}{p-1} \right\rfloor.$$

Case ε_2. Since $m \geq 3$, Theorem 3 implies that $\varepsilon_2 = 0$ if and only if m is a power of 2. The latter is equivalent to $s_2(m) = 1$, as well as to m having only one digit equal to 1 in its binary expansion. Thus if $\varepsilon_2 = 1$, then we must have $s_2(m) \geq 2$, and conversely. This shows (22) for $p = 2$.

Case ε_p for odd $p \leq M_n$. "$\Rightarrow$": If $\varepsilon_p = 1$, then we deduce from (19) that there exists a positive index $j \leq L$ such that

$$p \nmid \binom{m}{j(p-1)}, \quad \text{that is,} \quad v_p\left(\binom{m}{j(p-1)}\right) = 0.$$

Using (21) we then obtain that

$$s_p(m) = s_p(j(p-1)) + s_p(m - j(p-1)). \tag{23}$$

As $j \geq 1$, we conclude by (20) that $s_p(j(p-1)) \geq p-1$. Since $m > j(p-1)$ by $j \leq L$, we have $s_p(m - j(p-1)) \geq 1$. Applying these estimates to (23), we finally infer that $s_p(m) \geq p$.

"$\Leftarrow$": We now suppose that $s_p(m) \geq p$. The bound $p \leq M_n$ implies that $m > p$. Therefore, in the p-adic expansion

$$m = \alpha_0 + \alpha_1\, p + \cdots + \alpha_r\, p^r, \tag{24}$$

we have $r \geq 1$ and $\alpha_r > 0$. Since $m > j(p-1)$ when $1 \leq j \leq L$, the p-adic expansion

$$j(p-1) = \beta_{j,0} + \beta_{j,1}\, p + \cdots + \beta_{j,r}\, p^r \tag{25}$$

has $\alpha_r \geq \beta_{j,r} \geq 0$ and the digits $\beta_{j,0}, \ldots, \beta_{j,r}$ cannot all be equal to the digits $\alpha_0, \ldots, \alpha_r$. By Lucas's theorem [21, pp. 417–420] (for a modern proof, see [12] or [24, p. 70]), we obtain

$$\omega_j \stackrel{\text{def}}{=} \binom{m}{j(p-1)} \equiv \binom{\alpha_0}{\beta_{j,0}} \binom{\alpha_1}{\beta_{j,1}} \cdots \binom{\alpha_r}{\beta_{j,r}} \pmod{p}, \tag{26}$$

using the convention that $\binom{\alpha}{\beta} = 0$ if $\alpha < \beta$. We will deduce that $\omega_j \not\equiv 0 \pmod{p}$ for some index j. To do so, we construct unique digits $\beta'_0, \ldots, \beta'_r$, as follows. (Remember that $r \geq 1$ and $\alpha_r \geq 1$.)

- Set $\beta'_r \stackrel{\text{def}}{=} \alpha_r - 1$.
- Set $\beta'_k \stackrel{\text{def}}{=} \min \left(\alpha_k,\, (p-1) - \sum_{\ell=k+1}^{r} \beta'_\ell \right)$ iteratively for $k = r-1, r-2, \ldots, 0$.

Roughly speaking, the digits β'_k are "filled up" by the digits α_k, until the partial sum $\beta'_{k+1} + \cdots + \beta'_r$ reaches $p-1$; the remaining β'_k are then set equal to zero.

To explain this procedure in a more striking manner, imagine the following picture. We take $p-1$ marbles, which we use to fill $r+1$ cups arranged in a row and numbered $k = 0, 1, \ldots, r$. These cups, whose contents represent the digits β'_k, are initially empty. (The actual procedure above omits this step and iteratively sets each digit β'_k to its final value.) We put $\alpha_r - 1$ marbles into the cup with index $k = r$, while we fill the other cups (successively having index $k = r-1, r-2, \ldots, 0$) with up to α_k marbles, if possible. We stop this process when we have used all the marbles. (The actual procedure does not stop and sets all remaining β'_k equal to zero.) In total, we have placed at most $\alpha_r - 1 + \alpha_{r-1} + \cdots + \alpha_0 = s_p(m) - 1$, but not exceeding $p-1$, marbles in the cups. Therefore, all β'_k satisfy $0 \leq \beta'_k \leq p-1$. It follows that if $s_p(m) \geq p$, then all $p-1$ marbles necessarily have been distributed over the cups.

Since $s_p(m) \geq p$, that is, $\alpha_0 + \cdots + \alpha_r \geq p$, we obtain the following properties:

(i) $s_p(b) = p-1$, where $b \stackrel{\text{def}}{=} \beta'_0 + \beta'_1\, p + \cdots + \beta'_r\, p^r$.
(ii) $\alpha_k \geq \beta'_k$ for $k = 0, 1, \ldots, r-1$.
(iii) $\alpha_r > \beta'_r$.

By using (20), property (i) implies that $(p-1) \mid b$. From property (iii) and the expansion (24) we conclude that $b < m$. Therefore, taking the index $j = b/(p-1)$, which satisfies $1 \leq j \leq L$, the digits $\beta'_0, \ldots, \beta'_r$ equal the digits $\beta_{j,0}, \ldots, \beta_{j,r}$, since $j(p-1) = b$, as used in (25) and (26). Furthermore, by properties (ii) and (iii), all binomial coefficients

$$\binom{\alpha_k}{\beta_{j,k}} = \binom{\alpha_k}{\beta'_k} \not\equiv 0 \pmod{p} \quad (k = 0, 1, \ldots, r).$$

Applying Lucas's theorem in (26), we finally achieve $\omega_j \not\equiv 0 \pmod{p}$. By (19) this shows that $\varepsilon_p = 1$.

All cases for ε_2 and ε_p show that (22) holds, proving the formula for q_n in (1).

To complete the proof of Theorem 2, it suffices to show that the bound M_n on the prime factors p of q_n, given by Theorem 1, is sharp for infinitely many even (respectively, odd) values of n. To see this, let p be any odd prime and set $n_0 = 2p-2$. Then n_0 is even and $M_{n_0} = p$. Since the p-adic expansion of n_0 is $n_0 = (p-2) + p$, we have $s_p(n_0 + 1) = (p-1) + 1 = p$, ensuring that $p \mid q_{n_0}$.

A similar argument applied to odd $n_1 = 3p - 2$ shows that $M_{n_1} = p$ and $p \mid q_{n_1}$. Theorem 2 follows. $\square$

7. Applications

The formulas for q_n are intimately connected with the Bernoulli polynomials $B_n(x)$ by (2). Therefore, we can reformulate Theorem 2 in a way that describes the denominators of these polynomials.

Theorem 4. *For $n \geq 1$ let*

$$\mathfrak{D}_n \stackrel{\text{def}}{=} \operatorname{denom}\bigl(B_n(x)\bigr).$$

The values $\mathfrak{D}_n$ have the following properties:

(i) *If $n = 1$, then $\mathfrak{D}_n = 2$.*

(ii) *If $n \geq 3$ is odd, then*

$$\mathfrak{D}_n = \prod_{\substack{p \leq \frac{n+1}{2} \\ s_p(n) \geq p}} p.$$

(iii) *If $n \geq 2$ is even, then*

$$\mathfrak{D}_n = \prod_{(p-1) \mid n} p \quad \times \prod_{\substack{(p-1) \nmid n \\ p \leq \frac{n+1}{3} \\ s_p(n) \geq p}} p.$$

In particular, $\mathfrak{D}_n$ is even and squarefree for all $n \geq 1$, and the sequence $(\mathfrak{D}_n)_{n \geq 1}$ is unbounded. Moreover,

$$\operatorname{denom}\bigl(B_n\bigr) \mid \operatorname{denom}\bigl(B_n(x)\bigr) \quad (n \geq 1). \tag{27}$$

The first few values of $\mathfrak{D}_n$ (see [29, Sequence A144845]) are

$$\mathfrak{D}_n = 2, 6, 2, 30, 6, 42, 6, 30, 10, 66, 6, 2730, 210, 30, 6, 510, 30, 3990, 210, \ldots .$$

Proof of Theorem 4. As a result of Theorem 1, we obtain by (2) and (7) that

$$q_{n-1} = \operatorname{denom}\bigl(B_n(x) - B_n\bigr) \quad (n \geq 1). \tag{28}$$

(i). Since $B_1(x) = x - \frac{1}{2}$ by (3) and (4), we get $\mathfrak{D}_1 = 2$, which is even and squarefree. Then from $B_1 = -\frac{1}{2}$ by (4), relation (27) holds for $n = 1$. This shows (i).

(ii). Let $n \geq 3$ be odd. Then $B_n = 0$, so by (28) we obtain

$$\mathfrak{D}_n = \operatorname{denom}\bigl(B_n(x)\bigr) = q_{n-1}.$$

The squarefree product formula for $\mathfrak{D}_n$ follows by applying Theorem 2 to q_{n-1}. Since $n \geq 3$ is odd, q_{n-1} must be even by Theorem 1 part (iii). As $\operatorname{denom}(B_n) = 1$ in this case, (27) trivially holds. This shows (ii).

(iii). Let $n \geq 2$ be even. Recall the von Staudt–Clausen theorem in (5), namely,

$$D_n \stackrel{\text{def}}{=} \operatorname{denom}(B_n) = \prod_{(p-1) \mid n} p. \tag{29}$$

Since $B_n(x) - B_n$ has no constant term (see the proof of Lemma 2), we deduce that

$$\begin{aligned}\mathfrak{D}_n &= \operatorname{denom}\big((B_n(x) - B_n) + B_n\big)\\ &= \operatorname{lcm}\big(\operatorname{denom}(B_n(x) - B_n), \operatorname{denom}(B_n)\big)\\ &= \operatorname{lcm}(q_{n-1}, D_n).\end{aligned}$$

Thus, $D_n \mid \mathfrak{D}_n$, which shows (27). As $2 \mid D_n$ by (29), we then infer that $\mathfrak{D}_n$ is even. Since D_n and q_{n-1} are squarefree, so is $\mathfrak{D}_n$. Finally, we get

$$\mathfrak{D}_n = D_n \times \frac{q_{n-1}}{\gcd(q_{n-1}, D_n)},$$

where the second factor does not include primes that divide D_n. By Theorem 2, the result follows. This proves (iii).

It remains to show that the sequence $(\mathfrak{D}_n)_{n \geq 1}$ is unbounded. Since parts (ii) and (iii) imply that $q_{n-1} \mid \mathfrak{D}_n$ for $n \geq 2$, Theorem 2 gives the result again. □

To put Theorem 4 in the context of known results, we note a special property of the values of the Bernoulli polynomials at rational arguments, namely,

$$k^n \left(B_n \left(\frac{h}{k} \right) - B_n \right) \in \mathbb{Z} \quad (k \in \mathbb{N},\, h \in \mathbb{Z}). \tag{30}$$

This result is due to Almkvist and Meurman [1]; for a different proof, see [6, pp. 70–71]. As a complement, from (28) we have

$$q_{n-1}\big(B_n(x) - B_n\big) \in \mathbb{Z}[x]. \tag{31}$$

We argue that relations (30) and (31) are independent. On the one hand, (31) at once implies (30) but with an extra factor q_{n-1}. To see this, set $x = h/k$ in (31), multiply by k^n, and recall that $B_n(x)$ is a polynomial of degree n. On the other hand, (30) holds when k is any prime, whether or not it divides the denominator q_{n-1} in (31).

It is an astonishing fact that the denominators of $S_n(x)$ and $B_n(x) - B_n$ can be easily computed, without knowledge of the Bernoulli numbers, from the formulas in Theorems 1 and 2, giving a link to p-adic theory via the function $s_p(n)$. By contrast, the formula for the denominator of $B_n(x)$ in Theorem 4 part (iii) is more complicated, being separated into two products and requiring the von Staudt–Clausen theorem.

It is quite remarkable that surprising new properties of the power sum $S_n(x)$ are still being revealed four centuries after 1614. Already in that year, in his book *Newer Arithmetischer Wegweyser* [10], Faulhaber published formulas he had initially found up to $n = 7$ (see [3, 26]), extending the classical formulas for $n = 1, 2, 3, 4$.

Acknowledgment

The authors thank Kieren MacMillan for suggestions on an early version of the paper. We are grateful to the Archive of the City of Ulm for its kind support in providing a digital copy of Sebastian Furck's portrait of Johann Faulhaber [13] in Figure 1, with permission to reprint it. We also appreciate the valuable suggestions of the referees which improved the paper.

References

[1] G. Almkvist and A. Meurman, Values of Bernoulli polynomials and Hurwitz's zeta function at rational points, *C. R. Math. Acad. Sci. Soc. R. Can.* **13** no. 2–3 (1991) 104–108.

[2] P. Bachmann, *Niedere Zahlentheorie*, Part 2, Teubner, Leipzig, 1910; Parts 1 and 2 reprinted in one volume, Chelsea, New York, 1968, http://gdz.sub.uni-goettingen.de/dms/load/toc/?PPN=PPN379887479.

[3] J. Beery, Sums of Powers of Positive Integers – Johann Faulhaber (1580–1635), Germany, *Convergence* (July 2010), http://www.maa.org/press/periodicals/convergence/sums-of-powers-of-positive-integers-johann-faulhaber-1580-1635-germany.

[4] J. Bernoulli, *Ars Conjectandi*, Basel, 1713, DOI: 10.3931/e-rara-9001.

[5] T. Clausen, Lehrsatz aus einer Abhandlung über die Bernoullischen Zahlen, *Astr. Nachr.* **17** (1840) 351–352.

[6] H. Cohen, *Number Theory, Volume II: Analytic and Modern Tools*, Graduate Texts in Mathematics, Vol. 240, Springer–Verlag, New York, 2007.

[7] J. H. Conway and R. K. Guy, *The Book of Numbers*, Springer–Verlag, New York, 1996.

[8] A. W. F. Edwards, A quick route to sums of powers, *Amer. Math. Monthly* **9** (1986) 451–455.

[9] L. Euler, Inventio summae cuiusque seriei ex dato termino generali, E47, *Comment. Acad. Sc. Petrop.* **8** (1741) 9–22, http://eulerarchive.maa.org/pages/E047.html.

[10] J. Faulhaber, *Newer Arithmetischer Wegweyser*, Johann Meder, Ulm, 1614.

[11] ———, *Academia Algebrae*, Johann Remmelin, Augsburg, 1631, DOI: 10.3931/e-rara-16627.

[12] N. J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54** (1947) 589–592.

[13] S. Furck, *Portrait of Johann Faulhaber*, copperplate engraving, about 1630, Stadtarchiv Ulm, F 4 Bildnis 100, http://www.stadtarchiv-ulm.findbuch.net/php/main.php?ar_id=3766#4620342042696c646e69737365x252.

[14] J. Glaisher, On the residue of a binomial-theorem coefficient with respect to a prime modulus, *Quart. J. Pure Appl. Math.* **30** (1899) 150–156.

[15] J. V. Grabiner, Was Newton's calculus a dead end? The continental influence of Maclaurin's *Treatise of Fluxions*, *Amer. Math. Monthly* **104** (1997) 393–410.

[16] A. Granville, Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle, *Amer. Math. Monthly* **99** (1992) 318–331. Correction, *Amer. Math. Monthly* **104** (1997) 848–851.

[17] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Fifth edition. Oxford Univ. Press, Oxford, 1989.

[18] C. Hermite, Extrait d'une lettre à M. Borchardt, *J. Reine Angew. Math.* **81** (1876) 93–95, http://www.digizeitschriften.de/dms/img/?PID=PPN243919689_0081|log8.

[19] D. E. Knuth, Johann Faulhaber and sums of powers, *Math. Comp.* **61** (1993) 277–294, DOI: 10.1090/S0025-5718-1993-1197512-7.

[20] A.-M. Legendre, *Essai sur la Théorie des Nombres*. Second edition. Courcier, Paris, 1808, http://gallica.bnf.fr/ark:/12148/bpt6k62826k/f37.

[21] É. Lucas, *Théorie des Nombres*, Gauthier–Villars, Paris, 1891.

[22] C. Maclaurin, *A Treatise of Fluxions in Two Books*, Ruddimans, Edinburgh, 1742.

[23] K. MacMillan and J. Sondow, Proofs of power sum and binomial coefficient congruences via Pascal's identity, *Amer. Math. Monthly* **118** (2011) 549–551.

[24] V. H. Moll, *Numbers and Functions: From a Classical-Experimental Mathematician's Point of View*. Student Mathematical Library, Vol. 65, American Mathematical Society, Providence, RI, 2012.

[25] J. J. O'Connor and E. F. Robertson, Johann Faulhaber, MacTutor History of Mathematics, http://www-history.mcs.st-and.ac.uk/Biographies/Faulhaber.html.

[26] I. Schneider, Potenzsummenformeln im 17. Jahrhundert, *Hist. Math.* **10** (1983) 286–296, DOI: 10.1016/0315-0860(83)90079-4.

[27] ———, *Johannes Faulhaber 1580–1635, Rechenmeister in einer Welt des Umbruchs*, Vita Mathematica **7**, Birkhäuser–Verlag, Basel, 1993.

[28] W. Sierpiński, Sur une courbe dont tout point est un point de ramification, *C. R. Acad. Sci. Paris* **160** (1915) 302–305.

[29] N. J. A. Sloane, ed., The On-Line Encyclopedia of Integer Sequences, http://oeis.org.

[30] K. G. C. von Staudt, Beweis eines Lehrsatzes die Bernoullischen Zahlen betreffend, *J. Reine Angew. Math.* **21** (1840) 372–374, http://www.digizeitschriften.de/dms/img/?PID=GDZPPN002142562.
[31] J. Stopple, *A Primer of Analytic Number Theory: From Pythagoras to Riemann*, Cambridge Univ. Press, Cambridge, 2003.
[32] F. J. Swetz and V. J. Katz, Mathematical Treasures – Johann Faulhaber's *Academia Algebrae*, *Convergence* (January 2011), http://www.maa.org/press/periodicals/convergence/mathematical-treasures-johann-faulhabers-academia-algebrae.
[33] S. Wolfram, Geometry of binomial coefficients, *Amer. Math. Monthly* **91** (1984) 566–571.

Göttingen, Germany
E-mail address: bk@bernoulli.org

New York, USA
E-mail address: jsondow@alumni.princeton.edu