ACTA ARITHMETICA
Online First version

The denominators of the Bernoulli numbers

by

CARL POMERANCE (Hanover, NH) and
SAMUEL S. WAGSTAFF, JR. (West Lafayette, IN)

In memory of Andrzej Schinzel (1937–2021)

1. Introduction. Long before the proof of Andrew Wiles, it was thought that the path to Fermat's Last Theorem (FLT) led through the Bernoulli numbers. Defined by the series

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty}B_n\frac{t^n}{n!},$$

the *Bernoulli numbers* B_n are rationals, in lowest terms N_n/D_n, and both the sequence of numerators N_n and denominators D_n have a connection to FLT. It is known since Ernst Kummer that FLT holds for any odd prime that does not divide the class number of the cyclotomic field $\mathbb{Q}[e^{2\pi i/p}]$ (such primes are called "regular"), and that a condition for this to occur is that $p \nmid N_n$ for all even $n \le p-3$. The so-called first case of FLT for a prime exponent p is when p divides none of the powers. Sophie Germain proved this case when $2p+1$ is also a prime; we now call such primes p *Germain primes*. If p is a Germain prime, then $2p+1 \mid D_{2p}$, giving the connection to Bernoulli denominators.

This paper considers the density of n with a fixed value of D_n, the distribution of distinct values of D_n, and some other related problems. Note that $B_0=1$, $B_1=-1/2$, and $B_{2k+1}=0$ for all integers $k>0$. So, we only consider the remaining cases D_{2k}, $k>0$. We have a precise formula for D_{2k} in these cases given by the theorem of Karl von Staudt and Thomas Clausen: *D_{2k} is the product of the primes p for which $p-1 \mid 2k$.*

2020 *Mathematics Subject Classification*: Primary 11B05; Secondary 11B68, 11N25, 11N37, 11Y60.
Key words and phrases: shifted prime, Bernoulli number, asymptotic density.
Received 1 June 2021; revised 1 November 2021.
Published online *.

DOI: 10.4064/aa210601-16-11

From the von Staudt–Clausen theorem we immediately see that D_{2k} is squarefree and a multiple of 6. We set some notation. For a positive integer m let $T_m = \{p \text{ prime} : p-1 \mid m\}$. Thus, $T_m = \{2\}$ when m is odd. For even m, we have, for example, $T_2 = \{2,3\}$, $T_4 = \{2,3,5\}$, $T_6 = \{2,3,7\}$, $T_8 = T_4$, $T_{10} = \{2,3,11\}$, etc. As we have seen, D_{2k} is the product of the primes in T_{2k}.

For $n > 0$ even, let

$$\mathcal{S}_n = \{m > 0 \text{ even} : T_m = T_n\} = \{m > 0 \text{ even} : D_m = D_n\}.$$

Then $\mathcal{S}_2 = \{2, 14, 26, 34, 38, \ldots\}$, $\mathcal{S}_4 = \{4, 8, 68 \ldots\}$, etc. So $\mathcal{S}_n$ is the set of all even m for which B_m has the same denominator as B_n, namely, the product of the primes in T_n. In 1980, Erdős and the second author [3] proved that $\mathcal{S}_n$ has a positive asymptotic density for every even n. Sunseri [11] proved that the density of $\mathcal{S}_2$ is at least as large as the density of $\mathcal{S}_n$ for every even $n > 0$. We will give a simple proof below of a slightly stronger version of Sunseri's result.

Let

$$\mathcal{D} := \{D_n : n > 0 \text{ even}\} = \{6, 30, 42, 66, \ldots\}.$$

Further, for $d \in \mathcal{D}$, let $F_d = \min\{n : D_n = d\}$. For example, $F_6 = 2$, $F_{30} = 4$, $F_{42} = 6$, and $F_{66} = 10$. Let

$$\mathcal{F} := \{F_d : d \in \mathcal{D}\} = \{2, 4, 6, 10, \ldots\}.$$

Let λ denote the Carmichael λ-function. In particular, for n squarefree, $\lambda(n) = \operatorname{lcm}\{p-1 : p \mid n\}$, where p denotes a prime variable. We characterize $\mathcal{F}$ as the set of values of $\lambda(n)$ for $n > 2$ squarefree, and use this characterization plus some results on the distribution of the image of λ to get good approximations to the counting functions of $\mathcal{D}$ and $\mathcal{F}$.

In this paper, p always denotes a prime. For $p > 2$, we have $D_{p-1} = dp$ for some even integer d. We show that but for a set of primes of relative density 0 in the set of primes, this number d itself is in $\mathcal{D}$. Further, we show that for each fixed $d \in \mathcal{D}$, the relative density of the primes p with $D_{p-1} = dp$ is positive, and the sum of these densities is 1.

2. Characterization of $\mathcal{F}$. Here we give a connection between the set $\mathcal{F}$ and the image of the Carmichael λ-function.

Proposition 1. *For each $d \in \mathcal{D}$ we have $F_d = \lambda(d)$. Further,*

$$\mathcal{F} = \{\lambda(m) : m > 2 \textit{ squarefree}\}.$$

Proof. Let $d \in \mathcal{D}$ and suppose n has $D_n = d$. If p is a prime factor of d, then we have $p-1 \mid n$, by von Staudt–Clausen. Thus, $\lambda(d) \mid n$. Clearly if $a \mid b$, with a, b even, then $D_a \mid D_b$. Thus, $D_{\lambda(d)} \mid D_n = d$. Also, $p \mid d$ implies that $p-1 \mid \lambda(d)$, which implies that $p \mid D_{\lambda(d)}$. Since d is squarefree, we thus have

$d \mid D_{\lambda(d)}$. Hence, $d = D_{\lambda(d)}$ and $\lambda(d) = F_d$. This proves the first assertion and that $\mathcal{F} \subset \{\lambda(m) : m > 2,\ \text{squarefree}\}$. Say $m > 2$ is squarefree and $n = \lambda(m)$. Let $d = D_n$. By the von Staudt–Clausen theorem, $m \mid d$, so that $n = \lambda(m) \mid \lambda(d)$. As we saw above, whenever $d = D_n$, we have $\lambda(d) \mid n$. Thus, $n = \lambda(d) = \lambda(m)$ and the proposition follows. ∎

3. $\mathcal{S}_2$ has the greatest density. We introduce more notation. Let $\mathcal{A}$ denote a set of positive integers and write $\mathcal{B}(\mathcal{A})$ for the set of all positive integer multiples of the elements of $\mathcal{A}$. Let $A(x)$ denote the counting function of $\mathcal{A}$. Write $\mathrm{d}(\mathcal{A}) = \lim_{x\to\infty} A(x)/x$ for the asymptotic density of $\mathcal{A}$, if it exists. For a real number t, write $\mathcal{A}^{(t)}$ for $\{a \in \mathcal{A} : a > t\}$.

We record the following result from [10, Lemmas 1, 2].

Proposition 2. *Suppose that $\mathcal{A}$ is a set of positive integers not containing 1 with the property that*

$$\lim_{t\to\infty} \limsup_{x\to\infty} \mathcal{B}(\mathcal{A}^{(t)})(x)/x = 0. \tag{1}$$

Then $\mathrm{d}(\mathcal{B}(\mathcal{A}))$ exists and is < 1.

Note that condition (1) essentially asserts that most numbers are not divisible by a large member of $\mathcal{A}$.

If n is even, let

$$\mathcal{U}_n = \{mn : D_{mn} = D_n\}.$$

Note that if $n \in \mathcal{F}$, then $\mathcal{U}_n = \mathcal{S}_n$. For r prime, let

$$\mathcal{U}_{n,r} = \{mn \in \mathcal{U}_n : r \nmid m\}.$$

Lemma 1. *With the above notation, the sets $\mathcal{U}_n$ and $\mathcal{U}_{n,r}$ have positive asymptotic densities.*

Remark 1. When $n \in \mathcal{F}$, the result that $\mathcal{U}_n$ has positive asymptotic density follows from [3, Theorem 3].

Proof of Lemma 1. Let

$$\mathcal{A}_n = \{(p-1)/\gcd(p-1,n) : p-1 \nmid n\}.$$

It follows from [3, Theorem 2] that condition (1) holds for $\mathcal{A} = \mathcal{A}_n$. Indeed, $\mathcal{A}_n$ is the disjoint union over the divisors d of n of the sets $\mathcal{A}_{n,d} := \{(p-1)/d : d = \gcd(p-1,n),\ p-1 \nmid n\}$, and since (1) holds for each separate $\mathcal{A}_{n,d}$ by [3, Theorem 2], and since n is fixed, it holds too for $\mathcal{A}_n$. Thus, from Proposition 2 we see that $\mathcal{B}(\mathcal{A}_n)$ has an asymptotic density < 1. Let $\mathcal{C}_n = \mathbb{N} \setminus \mathcal{B}(\mathcal{A}_n)$. Then $\mathcal{C}_n$ has a positive asymptotic density. Our first assertion now follows upon noting that $\mathcal{U}_n = n\mathcal{C}_n = \{nm : m \in \mathcal{C}_n\}$. Indeed, if $p-1 \mid n$ then $p-1 \mid nm$ for all m, and if $p-1 \mid nm$ for some p with $p-1 \nmid n$, then $(p-1)/\gcd(p-1,n) \mid m$, so that $m \notin \mathcal{C}_n$.

The second assertion follows from the same argument applied to $\mathcal{A} = \mathcal{A}_n \cup \{r\}$. ■

LEMMA 2. *If r is prime and n is even, then*

$$\mathrm{d}(\mathcal{U}_{nr,r}) \le \frac{1}{r}\mathrm{d}(\mathcal{U}_{n,r}) \quad \textit{and} \quad \mathrm{d}(\mathcal{U}_n) \le \frac{r}{r-1}\mathrm{d}(\mathcal{U}_{n,r}).$$

Equality in the second assertion occurs only if $D_{nr^i} = D_n$ for all $i \ge 0$.

REMARK 2. It is not clear if there are any pairs n, r with $D_{nr^i} = D_n$ for all $i \ge 0$. However, if there are only finitely many Fermat primes, with $p = 2^{2^k} + 1$ being the largest one, then $D_{(p-1)2^i} = D_{p-1}$ for all $i \ge 0$.

Proof of Lemma 2. Consider the map $m \mapsto m/r$ on $\mathcal{U}_{nr,r}$. Let $m \in \mathcal{U}_{nr,r}$. We would like to show that $m/r \in \mathcal{U}_{n,r}$. Suppose $r^J \,\|\, n$. Clearly $r^J \,\|\, m/r$ and $n \mid m/r$, so it remains to show that $D_{m/r} = D_n$. If $p-1 \mid n$ then $p-1 \mid m/r$, since $n \mid m/r$. Further, if $p-1 \mid m/r$, then $p-1 \mid m$, so that $p-1 \mid nr$, since $D_m = D_{nr}$. But $r^{J+1} \nmid m/r$, so that $r^{J+1} \nmid p-1$. That is, $p-1 = ur^i$, where $u \mid n/r^J$ and $i \le J$. Hence $p-1 \mid n$ and $m/r \in \mathcal{U}_{n,r}$. The first assertion of the lemma follows.

For the second, note that $\mathcal{U}_n$ is contained in the disjoint union of those sets $\mathcal{U}_{nr^i,r}$ for $i = 0, 1, \ldots$ with $D_{nr^i} = D_n$. By the first part of the lemma applied i times, $\mathrm{d}(\mathcal{U}_{nr^i,r}) \le r^{-i}\mathrm{d}(\mathcal{U}_n)$. It remains to note that $\sum_{i\ge 0} r^{-i} = r/(r-1)$. Note also that in the possible case that each D_{nr^i} equals D_n, we are expressing $\mathcal{U}_n$ as an infinite disjoint union of sets with positive asymptotic density. Asymptotic density is not necessarily countably additive, but in this case there is no issue since $\bigcup_{i\ge k} \mathcal{U}_{nr^i,r}$ is contained in the multiples of r^k and so has upper density which tends to 0 as $k \to \infty$. ■

THEOREM 1. *If $a, b \in \mathcal{F}$ with $a \mid b$, then*

$$\mathrm{d}(\mathcal{S}_b) \le \frac{1}{\varphi(b/a)}\mathrm{d}(\mathcal{S}_a). \tag{2}$$

In addition, $\mathrm{d}(\mathcal{S}_4) \le \frac{3}{4}\mathrm{d}(\mathcal{S}_2)$.

REMARK 3. Since every member of $\mathcal{F}$ is even, Theorem 1 in the case $a = 2$ shows that $\mathrm{d}(\mathcal{S}_2)$ is at least one-third larger than every other $\mathrm{d}(\mathcal{S}_n)$.

Proof of Theorem 1. Let r be a prime factor of b/a with $r^K \,\|\, b/a$. By the second part of Lemma 2,

$$\mathrm{d}(\mathcal{S}_b) = \mathrm{d}(\mathcal{U}_b) \le \frac{r}{r-1}\mathrm{d}(\mathcal{U}_{b,r}).$$

Repeatedly applying the first part of Lemma 2, we have

$$\mathrm{d}(\mathcal{U}_{b,r}) \le \frac{1}{r}\mathrm{d}(\mathcal{U}_{b/r,r}) \le \cdots \le \frac{1}{r^K}\mathrm{d}(\mathcal{U}_{b/r^K,r}),$$

so that

$$\mathrm{d}(\mathcal{U}_b) \le \frac{1}{\varphi(r^K)}\mathrm{d}(\mathcal{U}_{b/r^K,r}).$$

Thus, (2) follows by induction on the number of distinct prime divisors of b/a.

Now suppose that $a = 2$, $b = 4$, and follow the above proof. Note that D_{16} is divisible by 17, but D_4 is not. Thus, $\mathcal{S}_4 = \mathcal{U}_{4,2} \cup \mathcal{U}_{8,2}$, and

$$\mathrm{d}(\mathcal{S}_4) = \mathrm{d}(\mathcal{U}_{4,2} \cup \mathcal{U}_{8,2}) \le \frac{3}{2}\mathrm{d}(\mathcal{U}_{4,2}).$$

Also

$$\mathrm{d}(\mathcal{U}_{4,2}) \le \frac{1}{2}\mathrm{d}(\mathcal{U}_{2,2}) = \frac{1}{2}\mathrm{d}(\mathcal{U}_2) = \frac{1}{2}\mathrm{d}(\mathcal{S}_2).$$

Hence $\mathrm{d}(\mathcal{S}_4) \le \frac{3}{4}\mathrm{d}(\mathcal{S}_2)$. ■

Remark 4. The proof shows that $\mathrm{d}(\mathcal{S}_6) \le \frac{1}{2}\mathrm{d}(\mathcal{S}_2)$ and $\mathrm{d}(\mathcal{S}_{10}) \le \frac{1}{4}\mathrm{d}(\mathcal{S}_2)$, for example, but provides no way to compare $\mathrm{d}(\mathcal{S}_4)$ with $\mathrm{d}(\mathcal{S}_6)$, or $\mathrm{d}(\mathcal{S}_6)$ with $\mathrm{d}(\mathcal{S}_{10})$.

Corollary 1. *Measured by the asymptotic density of their sets of subscripts, more Bernoulli numbers have denominator* 6 *than any other integer.*

Remark 5. Every even number n is in some $\mathcal{S}_f$ for $f \in \mathcal{F}$, namely for $f = \lambda(D_n)$. Moreover, the sets $\mathcal{S}_f$ for $f \in \mathcal{F}$ are pairwise disjoint. It follows that $\sum_{f\in\mathcal{F}} \mathrm{d}(\mathcal{S}_f) \le \frac{1}{2}$. In fact, we have

$$\sum_{f\in\mathcal{F}} \mathrm{d}(\mathcal{S}_f) = \frac{1}{2}, \tag{3}$$

as asserted in [3, Corollary, p. 111]. The proof follows immediately from [3, Theorem 2], which asserts ([1]) that for each $\epsilon > 0$ there is some number B such that the upper density of those integers divisible by some $p-1 > B$ is $< \epsilon$. (That is, (1) holds.) So, to prove (3), note that there are only finitely many $d \in \mathcal{D}$ not divisible by any prime $p > B + 1$, since members of $\mathcal{D}$ are squarefree, so there are only finitely many $f \in \mathcal{F}$ not divisible by any $p-1 > B$. The numbers n in all other sets $\mathcal{S}_f$ are divisible by some $p-1 > B$ so they comprise a set of upper density $< \epsilon$. Thus, the sum in (3) is $> \frac{1}{2} - \epsilon$.

4. Statistics for the $\mathcal{S}_n$. If one defines $\mathcal{S}_1$ as $\{n : T_n = T_1 = \{2\}\}$, then we merely have the set of odd numbers, having density $\frac{1}{2}$. What about the densities of the various $\mathcal{S}_n$ with n even? We have proved that $\mathcal{S}_2$ has density at least $\frac{1}{3}$ more than the next largest density. Numerical calculation suggests that $\mathcal{S}_2$ has density about 0.07, followed by $\mathcal{S}_4$ (0.03) and $\mathcal{S}_6$ (0.01) in that order. We know from the proof of Theorem 1 that $\mathrm{d}(\mathcal{S}_4)$ is the largest of the $\mathrm{d}(\mathcal{S}_n)$ for $4 \mid n$ and that $\mathrm{d}(\mathcal{S}_6)$ is the largest of the $\mathrm{d}(\mathcal{S}_n)$ for $6 \mid n$. As

([1]) This result has been sharpened in the recent papers [5], [9].

mentioned, the proof does not allow us to compare $\mathrm{d}(\mathcal{S}_4)$ and $\mathrm{d}(\mathcal{S}_6)$. It follows from the methods in [3], [11] that the densities are effectively computable in principle, and so in principle it is possible to resolve this issue, though such calculations appear currently to be infeasible.

Tables 1 and 2 give the number of elements in $\mathcal{S}_n$ for $n = 2k \le 112$ up to 10^m for $m = 5$, 7 and 9. In these tables, $2k$ and $2k'$ are the smallest two elements of $\mathcal{S}_{2k}$, so that $2k \in \mathcal{F}$. The partial densities may be computed easily from the counts. Note that, in the range from 10^5 to 10^9, the partial densities tend to decrease when T_{2k} contains few primes and increase when T_{2k} contains many primes.

The tables suggest that

$$\mathrm{d}(\mathcal{S}_2) > \mathrm{d}(\mathcal{S}_4) > \mathrm{d}(\mathcal{S}_6) > \mathrm{d}(\mathcal{S}_{10}) > \mathrm{d}(\mathcal{S}_{16})$$

are the five largest densities of the $\mathcal{S}_{2k}$. In other words, the five most popular denominators of Bernoulli numbers seem to be 6, 30, 42, 66, 510, in that order.

To form $\mathcal{S}_2$, begin with the set $\mathcal{T}$ of even positive integers. This is the set of positive integers divisible by both $2-1$ and $3-1$. Now delete from $\mathcal{T}$ all multiples of $q-1$ for all primes $q > 4$. Some primes $q > 4$ may be skipped

Table 1. Number of elements of $\mathcal{S}_{2k}$ below various limits

First $2k$	Second $2k'$	T_{2k}	Count $\le 10^5$	Count $\le 10^7$	Count $\le 10^9$
2	14	$\{2,3\}$	7992	758582	73129588
4	8	$\{2,3,5\}$	3423	320500	30579077
6	114	$\{2,3,7\}$	1371	125712	11923816
10	50	$\{2,3,11\}$	1080	99675	9457553
12	24	$\{2,3,5,7,13\}$	495	49498	4751091
16	32	$\{2,3,5,17\}$	713	67742	6379485
18	54	$\{2,3,7,19\}$	397	38502	3671790
20	340	$\{2,3,5,11\}$	289	27745	2609924
22	154	$\{2,3,23\}$	566	52508	4959735
28	56	$\{2,3,5,29\}$	309	29692	2793858
30	1770	$\{2,3,7,11,31\}$	138	13615	1309849
36	3924	$\{2,3,5,7,13,19,37\}$	72	7846	799642
40	6680	$\{2,3,5,11,41\}$	92	10044	950144
42	294	$\{2,3,7,43\}$	124	12645	1199553
44	484	$\{2,3,5,23\}$	160	15325	1433972
46	322	$\{2,3,47\}$	261	24295	2290634
48	10128	$\{2,3,5,7,13,17\}$	26	4572	497209
52	104	$\{2,3,5,53\}$	164	16638	1558130
58	406	$\{2,3,59\}$	235	20607	1935087

Table 2. Number of elements of $\mathcal{S}_{2k}$ below various limits

First $2k$	Second $2k'$	T_{2k}	Count $\le 10^5$	Count $\le 10^7$	Count $\le 10^9$
60	13620	$\{2,3,5,7,11,13,31,61\}$	21	2917	340111
66	3894	$\{2,3,7,23,67\}$	77	7202	680301
70	350	$\{2,3,11,71\}$	83	8815	818849
72	12024	$\{2,3,5,7,13,19,37,73\}$	12	2137	259257
78	1014	$\{2,3,7,79\}$	71	6771	636574
80	160	$\{2,3,5,11,17,41\}$	39	5960	610485
82	574	$\{2,3,83\}$	150	13715	1293383
84	168	$\{2,3,5,7,13,29,43\}$	16	2924	339634
88	968	$\{2,3,5,23,89\}$	53	5593	528007
90	14670	$\{2,3,7,11,19,31\}$	17	2629	284131
92	184	$\{2,3,5,47\}$	116	10822	1017455
96	20256	$\{2,3,5,7,13,17,97\}$	7	1645	196489
100	1700	$\{2,3,5,11,101\}$	34	4115	393270
102	1734	$\{2,3,7,103\}$	50	5041	473949
106	1378	$\{2,3,107\}$	120	10794	1007709
108	11772	$\{2,3,5,7,13,19,37,109\}$	14	1593	190046
110	550	$\{2,3,11,23\}$	72	6481	609261
112	224	$\{2,3,5,17,29,113\}$	41	4135	422188

because the multiples of $q-1$ were deleted when multiples of $r-1$ were removed for some prime $r<q$. For example, multiples of $13-1$ were deleted when multiples of $7-1$ were removed. However, we must always delete the multiples of $q-1$ whenever $p=(q-1)/2$ is prime. Recall that the prime p is called a *Germain prime* if $2p+1$ is also prime. Thus, it is necessary to remove all multiples of the Germain primes from $\mathcal{T}$ to form $\mathcal{S}_2$. But it is not sufficient to delete multiples of Germain primes because, for example, $q=239$ is prime but $p=(q-1)/2=119$ is not prime and not divisible by a Germain prime.

Table 3 lists the number of elements of $\mathcal{S}_{2k}$ below 10^6 in each residue class modulo 8 and the first few odd primes. (The residue classes >7 modulo 11 and 13 are omitted to make the table fit on a page. The missing values are similar to the last ones shown in that row of the table.) The value "total" is the number of elements of $\mathcal{S}_{2k}$ less than 10^6.

The elements of $\mathcal{S}_2$ are all $\equiv 2 \pmod 4$ and seem to be equally distributed between $2 \pmod 8$ and $6 \pmod 8$. For each Germain prime p, the residue class $0 \pmod p$ is empty because these classes were removed from $\mathcal{T}$ when $\mathcal{S}_2$ was formed. The elements of $\mathcal{S}_2$ appear to be equally distributed among other residue classes modulo Germain primes.

Table 3. Number of elements $\leq 10^6$ of $\mathcal{S}_{2k}$ in residue classes

Modulus	0	1	2	3	4	5	6	7
				$2k = 2$, total $= 77696$				
8	0	0	38849	0	0	0	38847	0
3	0	31612	46084					
5	0	18636	18565	19097	21398			
7	9179	11168	11175	11080	11309	11125	12660	
11	0	7661	7671	7682	7730	7726	7649	7627
13	5116	5959	5980	5975	5970	5972	6079	6035
				$2k = 4$, total $= 33001$				
8	9490	0	0	0	23511	0	0	0
3	0	15877	17124					
5	0	7868	7244	9186	8703			
7	0	5186	5176	5328	5274	6089	5948	
11	0	3160	3198	3206	3179	3191	3200	3338
13	0	2693	2633	2679	2637	2695	2682	2669
				$2k = 6$, total $= 12996$				
8	0	0	6508	0	0	0	6488	0
3	12996	0	0					
5	0	2859	3346	2867	3924			
7	0	2012	1990	1940	2351	2004	2699	
11	0	1264	1243	1252	1257	1239	1227	1224
13	0	1042	1044	1023	1025	1018	1028	1068
				$2k = 10$, total $= 10339$				
8	0	0	5175	0	0	0	5164	0
3	0	4954	5385					
5	10339	0	0	0	0			
7	0	1545	1948	1632	1643	1571	2000	
11	0	987	973	1009	989	991	1203	999
13	0	846	856	850	836	816	841	830

The elements of $\mathcal{S}_4$ are all divisible by 4 because $5 \in T_4$. At first it was puzzling why there are so many more of them that are 4 (mod 8) than 0 (mod 8). However, those members of $\mathcal{S}_4$ that are 4 (mod 8) comprise $\mathcal{U}_{4,2}$ and those that are 0 (mod 8) comprise $\mathcal{U}_{8,2}$, using the notation introduced in the previous section. In the proof of Theorem 1 we saw that $\mathrm{d}(\mathcal{U}_{8,2}) \leq \frac{1}{2}\mathrm{d}(\mathcal{U}_{4,2})$, since dividing a member of $\mathcal{U}_{8,2}$ by 2 gives a member of $\mathcal{U}_{4,2}$. This explains part of the favoring of 4 (mod 8) over 0 (mod 8), but not all. In fact, multiplying a member of $\mathcal{U}_{4,2}$ by 2 does not always give a member of $\mathcal{U}_{8,2}$. Another force at work here is that if $m > 3$ is odd, then $4m \in \mathcal{S}_4$ if and only if for each $d \mid m$ with $d > 3$, both $2d+1$ and $4d+1$ are composite. But for $8m \in \mathcal{S}_4$, there is the additional requirement that $8d+1$ is composite.

As we mentioned earlier, every element of $\mathcal{S}_{2k}$ is divisible by its least element $2k$. There are no multiples of 7 in $\mathcal{S}_4$, $\mathcal{S}_6$ or $\mathcal{S}_{10}$ because 29, 43 and 71, respectively, are prime. Similarly, there are no multiples of 13 in $\mathcal{S}_4$, $\mathcal{S}_6$ or $\mathcal{S}_{10}$ because 53, 79 and 131 are prime.

5. The distribution of distinct Bernoulli denominators. Let $D(x), F(x)$ be the counting functions of $\mathcal{D}$ and $\mathcal{F}$, respectively, and let

$$\beta = 1 - (1 + \log\log 2)/\log 2 = 0.08607\ldots,$$

the Erdős–Tenenbaum–Ford constant.

THEOREM 2. *We have, as* $x \to \infty$,

$$D(x) = x/(\log x)^{1+o(1)}, \qquad F(x) = x/(\log x)^{\beta+o(1)}.$$

In particular, $\mathrm{d}(\mathcal{D}) = \mathrm{d}(\mathcal{F}) = 0$.

Proof. Note that Proposition 1 implies that the function sending $d \in \mathcal{D}$ to $\lambda(d) \in \mathcal{F}$ is a bijection. Thus,

$$D(x) = \#\{\lambda(d) : d \in \mathcal{D},\, d \le x\} \le \#\{\lambda(n) : n \le x\}.$$

Further, the second part of Proposition 1 implies that

$$\begin{aligned} F(x) &= \#\{\lambda(n) : n > 2 \text{ squarefree}, \lambda(n) \le x\} \\ &\le \#\{\lambda(n) : n \text{ such that } \lambda(n) \le x\}. \end{aligned}$$

In [8, Theorem 1.3] it is shown that

$$\#\{\lambda(n) : n \le x\} = x/(\log x)^{1+o(1)} \quad \text{as } x \to \infty,$$

and [8, Theorem 1.1] implies that

$$\#\{\lambda(n) : \lambda(n) \le x\} \le x/(\log x)^{\beta+o(1)} \quad \text{as } x \to \infty. \tag{4}$$

So the upper bounds implicit in the theorem follow. In [6] it is shown that equality holds in (4). In fact, the method of proof gives the same bound for $\#\{\lambda(n) \le x : n \text{ squarefree}\}$, so by this result, the proof for $\mathcal{F}$ is complete. We show in Theorem 3 below that $\mathcal{D}$ contains the numbers $6p$ for a positive proportion of the primes p, so the lower bound for $\mathcal{D}$ will follow from the prime number theorem. ■

REMARK 6. Looking at small values of $\mathcal{F}$ it seems that many are of the form $p-1$ with p prime. Every $p-1$ is in $\mathcal{F}$ for $p > 2$ prime, as is easily seen, but Theorem 2 shows that most members of $\mathcal{F}$ are not in this form.

Table 4 shows the growth rate of $\mathcal{F}$, the set of first elements $2k$ of the $\mathcal{S}_{2k}$. These numbers were found by computing the fractional parts of all B_{2k} for $2k \le 10^m$ via a sieve, as in [3], sorting them and counting the unique values.

Table 4. Number of elements $\leq 10^m$ of $\mathcal{F}$

m	5	6	7	8	9
$F(10^m)$	24662	235072	2261011	21876975	212656697
$R(10^m)$	.476	.478	.479	.480	.481

Table 5. Number of elements $\leq 10^m$ of $\mathcal{D}$

m	5	6	7	8	9
$D(10^m)$	513	3649	27936	226111	1893060
$D(10^m)/\pi(10^m)$	.053	.046	.042	.039	.037

High enough precision was used to distinguish close but not equal fractional parts.

There are a number of problems where the expression $x/(\log x)^\beta$ arises, and in some of these a secondary factor of $(\log\log x)^c$ arises in the denominator, sometimes with $c = 3/2$ (see [4]) and sometimes with $c = 1/2$ (see [1] and [5]). We have no compelling reason to suggest such a factor here, but we have noticed that $F(x)$ has a ratio with $f(x) := x/((\log x)^\beta(\log\log x)^{1/2})$ that stays fairly constant. In Table 4 we have also recorded the ratios $R(x) = F(x)/f(x)$.

Table 5 shows the growth rate of $\mathcal{D}$, the set of Bernoulli denominators. These counts were computed with Mathematica using the criterion that an even $d > 2$ is in $\mathcal{D}$ if and only if $d = D_{\lambda(d)}$. The counts were then checked via the sieve procedure that we used for Table 4. Note that Theorem 2 does *not* assert that $D(x)/\pi(x)$ tends to a limit or is bounded, but we do know that these ratios have a positive $\liminf$.

5.1. A partition of the set of primes. Given an odd prime p, the least n with $p \mid D_n$ is evidently $p-1$. Let $d_p = D_{p-1}/p$. For example,

$$d_3 = 2, \quad d_5 = 6, \quad d_7 = 6, \quad d_{11} = 6, \quad d_{13} = 210, \quad d_{17} = 30, \quad d_{19} = 42.$$

For d even, let

$$\mathcal{P}_d = \{p \text{ prime} : d_p = d\},$$

so that the sets $\mathcal{P}_d$ give a partition of the odd primes.

Lemma 3. *For each odd prime p we have $\lambda(d_p) \mid p-1$. Further, $\lambda(d_p) < p-1$ if and only if $d_p \in \mathcal{D}$.*

Proof. Note that d_p is the product of those primes $q < p$ where $q-1 \mid p-1$. Thus, $\lambda(d_p)$ is a least common multiple of some of the divisors of $p-1$, so we must have $\lambda(d_p) \mid p-1$ and $D_{\lambda(d_p)} \mid D_{p-1}$. Also, $d_p \mid D_{\lambda(d_p)}$ since this holds for all squarefree numbers larger than 2. If $\lambda(d_p) = p-1$, then $p \mid D_{\lambda(d_p)}$. But $p \nmid d_p$, so $d_p \neq D_{\lambda(d_p)}$ and $d_p \notin \mathcal{D}$. If $\lambda(d_p) < p-1$, then $D_{\lambda(d_p)} \mid d_p$ since

$q \mid D_{\lambda(d_p)}$ implies $q-1 \mid \lambda(d_p)$, which implies $q-1 \mid p-1$ and $q < p$, so that $q \mid d_p$. Hence $d_p = D_{\lambda(d_p)}$ and $d_p \in \mathcal{D}$. ∎

A consequence of Lemma 3 is that if $d \notin \mathcal{D}$, then $\#\mathcal{P}_d \le 1$. Indeed, if $p \in \mathcal{P}_d$ with $d \notin \mathcal{D}$, the lemma implies that $\lambda(d) = p-1$, so p is uniquely determined from d. On the other hand, in the next theorem, we see that if $d \in \mathcal{D}$, then $\mathcal{P}_d$ is a quite thick set of primes.

THEOREM 3. *For each $d \in \mathcal{D}$ there is a positive constant c_d such that the relative density of $\mathcal{P}_d$ in the set of prime numbers is c_d.*

Sketch of proof. First note that if $p \in \mathcal{P}_d$ then $p \equiv 1 \pmod{\lambda(d)}$. From [7, Theorem 3] it follows that there is an absolute constant $c > 0$ such that for any $3 \le z \le x$, the number of primes $p \le x$ such that $p-1$ has a divisor of the form $q-1$ with q prime and $z < q < p$ is $O(\pi(x)/(\log z)^c)$. This result is completely analogous to [3, Theorem 2]. We apply this to primes $p \equiv 1 \pmod{\lambda(d)}$, which comprise a positive proportion of all primes by the prime number theorem for residue classes. So, it follows from the method in [3, Theorem 3] that the set

$$\{p \equiv 1 \pmod{\lambda(d)} : q-1 \mid p-1 \text{ implies } q-1 \mid \lambda(d) \text{ or } q = p\},$$

where p, q are understood as primes, has a positive relative density c_d in the set of all primes. Since $\prod_{q-1 \mid \lambda(d)} q = d$ by Proposition 1, for such primes p we have $D_{p-1} = dp$. ∎

We conjecture that c_6 is the largest of the densities c_d. Table 6 has some counts for $d = 6, 30, 42, 66$ plus fractions of all primes to the same bounds.

We noticed in tabulating $\mathcal{D}$ that there are quite a few more values of $d \in \mathcal{D}$ with $d/6 \equiv 2 \pmod 3$ than with $d/6 \equiv 1 \pmod 3$. This phenomenon may be due to the robust size of $\mathcal{P}_6$ as seen in Table 6: every member of $\mathcal{P}_6$ when divided by 6 is $\equiv 2 \pmod 3$. To be sure, the other cases in Table 6 count against this trend, but when counting members of $\mathcal{D}$ up to x, the $\mathcal{P}_6$ members involve primes to $x/6$, while the other cases involve primes

Table 6. Number of primes $p \le 10^k$ with $D_{p-1} = dp$ and fraction of all primes to 10^k

d	$k=5$	6	7	8	9
6	1135	8772	71421	601804	5189442
	.1183	.1117	.1075	.1045	.1021
30	600	4312	34065	278709	2358192
	.0626	.0549	.0513	.0484	.0464
42	480	3543	27722	226087	1896172
	.0500	.0451	.0417	.0392	.0373
66	275	1933	14859	120565	1010251
	.0287	.0246	.0224	.0209	.01999

to $x/30$ and smaller. There may well be other forces at play here, but this observation may partially demystify the phenomenon. We do not know if this imbalance continues asymptotically since we do not know if $D(x)$ is of order of magnitude $\pi(x)$. (Note that the "$o(1)$" in Theorem 2 may have some significance.)

We have seen in the proof of Theorem 3 that for many primes p we have $D_{p-1} = dp$ with $d \in \mathcal{D}$. However, this is not true for all odd primes. For example, note that $D_{12} = 210 \cdot 13$ and $210 \notin \mathcal{D}$. We show that this is uncommon.

THEOREM 4. *There is a positive constant c such that the number of primes $p \le x$ with $D_{p-1}/p \notin \mathcal{D}$ is $O(\pi(x)/(\log x)^c)$.*

Proof. Let $p \le x$ be a prime and let q be the largest prime factor of $p-1$. Let $B = x^{1/\log\log x}$. If $q \le B$, that is, $p-1$ is a B-smooth number, we can bound the number of such p by the number of B-smooth numbers at most x. By a standard result of de Bruijn, this count is $O_k(x/(\log x)^k)$ for any fixed k. In particular it holds for $k = 2$, so we may ignore such primes and assume that $q > B$. Next, we again apply [7, Theorem 3] mentioned in the proof of Theorem 3. We apply this with $z = B$, so the number of primes $p \le x$ divisible by some shifted prime $r-1$ with $B < r < p$ is negligible. Thus, we may assume that $p-1$ has no such divisor. Let n be the largest B-smooth divisor of $p-1$, so that $n \le (p-1)/q < p-1$. Then $D_{p-1} = D_n p$, so that $D_{p-1}/p \in \mathcal{D}$. ∎

REMARK 7. Similarly to Remark 5, we have

$$\sum_{d\in\mathcal{D}} c_d = 1.$$

This follows from Theorem 4 and from the fact that for large B, the primes p divisible by some shifted prime $q-1 > B$ with $q < p$ are sparse, which follows from [7, Theorem 3].

One might wonder how strong Theorem 4 is, or even if there are infinitely many primes as described in the theorem. We can prove this conditionally on the prime k-tuples conjecture. Further, from the Hardy–Littlewood quantitative form of k-tuples, we can show there are quite a few of these primes.

THEOREM 5. *Assuming the prime k-tuples conjecture, there are infinitely many primes p with $D_{p-1}/p \notin \mathcal{D}$. Assuming the quantitative form of this conjecture due to Hardy and Littlewood, the number of such primes $p \le x$ is $\gg \pi(x)/\log x$.*

Proof. Let q be a prime with $q \equiv 3 \pmod 4$, $q > 3$, and $p = 2q-1$ prime. Let d be such that $D_{p-1} = dp$. Suppose that $d = D_n$ for some n. Since $4 \mid p-1$ and $p > 5$, we have $5 \mid d$, so that $4 \mid n$. Also $q \mid d$, so $q-1 \mid n$.

Hence $\mathrm{lcm}(4, q-1) = 2(q-1) = p-1 \mid n$. This implies that $p \mid D_n = d$ contradicting $D_{p-1} = dp$ squarefree. Thus, $D_{p-1}/p \notin \mathcal{D}$. The prime k-tuples conjecture implies there are infinitely many such p, and the quantitative form implies that there are $\gg \pi(x)/\log x$ of them at most x. ∎

Table 7 illustrates Theorems 4 and 5 by showing the number of primes p for which $D_{p-1}/p \notin \mathcal{D}$.

Table 7. Number of $p \le 10^m$ with $D_{p-1}/p \notin \mathcal{D}$

m	5	6	7	8	9
Count	4183	34647	293117	2525121	22119959
Count$/\pi(10^m)$	.436	.441	.441	.438	.435

A puzzle here: These counts are holding steady at about 44% of the primes, yet Theorem 4 says the fraction should decay to 0, though maybe the decay is slow. This is similar to the decay of $F(10^m)/10^m$ seen in Table 4, though it definitely seems more glacial in Table 7.

5.2. Further problems. The first few Bernoulli denominators all have the form $p-1$ for some primes p: 7, 31, 43, 67, 139, 283, 331. One might wonder whether there are infinitely many $d \in \mathcal{D}$ with $d+1$ composite and infinitely many with $d+1$ prime. Table 8 shows the fractions of prime and composite $d+1$ with $d \in \mathcal{D}$ below various powers of 10. It looks like the composite cases predominate. A possible proof: It likely follows from the proof of [8, Theorem 1.3] that

$$\#\{\lambda(p-1) : p \le x\} \le \pi(x)/(\log x)^{1+o(1)} \tag{5}$$

as $x \to \infty$. We have

$$\begin{aligned}\#\{p \le x : p-1 \in \mathcal{D}\} &= \#\{p \le x : p-1 = D_{\lambda(p-1)}\}\\ &\le \#\{\lambda(p-1) : p \le x\},\end{aligned}$$

so that (5) would imply that $\#\{p \le x : p-1 \in \mathcal{D}\}$ is bounded above by $\pi(x)/(\log x)^{1+o(1)}$. Thus, from Theorem 2, it would be unusual for $d \in \mathcal{D}$ to have $d+1$ prime.

A lower bound of similar quality follows from the strong form of the Hardy–Littlewood conjecture as in Theorem 5. For this, take primes r with

Table 8. Number and fraction of composite and prime $d+1 \le 10^m$ for $d \in \mathcal{D}$

m	3	4	5	6	7	8	9
Composite	4	56	361	2812	22759	189894	1628333
Fraction	.286	.667	.704	.771	.815	.840	.860
Prime	10	28	152	837	5177	36217	264727
Fraction	.714	.333	.296	.229	.185	.160	.140

$q = 2r + 1$ prime and $p = 6q + 1$ prime. Then $\lambda(p - 1) = q - 1 = 2r$, and $D_{2r} = 6q = p - 1$, so $p - 1 \in \mathcal{D}$. By Hardy–Littlewood, the number of such $p \le x$ is $\gg \pi(x)/(\log x)^2$.

Let $\psi(n) \to \infty$ arbitrarily slowly. Then the set

$$\{n \text{ even} : D_n > \psi(n)\}$$

has asymptotic density 0. This follows from Remark 5. On the other hand, there are a fair number of n with D_n large: we have

$$\#\{n \text{ even} : n \le x,\ D_n > n\} \gg x/\log x.$$

This follows from Theorem 3 and the prime number theorem. In addition, it follows from [2, Theorem 1] that there are positive constants c, c' such that $D_n > \exp(n^{c/\log\log n})$ for infinitely many even n and $D_n < \exp(n^{c'/\log\log n})$ always.

In Tables 1 and 2 we recorded the second smallest member of $\mathcal{S}_{2k}$ for $2k \in \mathcal{F}$ with $2k \le 112$. It would be interesting to study the distribution of these numbers.

Acknowledgements. We thank Paul Pollack for reminding us of [7]. And we thank the referee for a careful reading.

S.S.W.'s work was supported by the CERIAS Center at Purdue University.

References

[1] M. Balazard, J.-L. Nicolas, C. Pomerance et G. Tenenbaum, *Grandes déviations pour certaines fonctions arithmétiques*, J. Number Theory 40 (1992), 146–164.

[2] P. Erdős, C. Pomerance and E. Schmutz, *Carmichael's lambda function*, Acta Arith. 58 (1991), 363–385.

[3] P. Erdős and S. S. Wagstaff, Jr., *The fractional parts of the Bernoulli numbers*, Illinois J. Math. 24 (1980), 104–112.

[4] K. Ford, *The distribution of integers with a divisor in a given interval*, Ann. of Math. 168 (2008), 367–433.

[5] K. Ford, *Integers divisible by a large shifted prime*, Acta Arith. 178 (2017), 163–180.

[6] K. Ford, F. Luca and C. Pomerance, *The image of Carmichael's λ-function*, Algebra Number Theory 8 (2014), 2009–2025.

[7] F. Luca, A. Pizarro-Madariaga and C. Pomerance, *On the counting function of irregular primes*, Indag. Math. 26 (2015), 147–161.

[8] F. Luca and C. Pomerance, *On the range of Carmichael's universal-exponent function*, Acta Arith. 162 (2014), 289–308.

[9] N. McNew, P. Pollack and C. Pomerance, *Numbers divisible by a large shifted prime and large torsion subgroups of CM elliptic curves*, Int. Math. Res. Notices 2017, no. 18, 5525–5553.

[10] C. Pomerance and A. Sárközy, *On homogeneous multiplicative hybrid problems in number theory*, Acta Arith. 49 (1988), 291–302.

[11] R. F. Sunseri, *Zeros of p-adic L-functions and densities relating to Bernoulli numbers*, Ph.D. thesis, Univ. of Illinois, Urbana, IL, 1980; http://homes.cerias.purdue.edu/~ssw/sunseri.pdf.

Carl Pomerance
Mathematics Department
Dartmouth College
Hanover, NH 03784, USA
E-mail: carl.pomerance@dartmouth.edu

Samuel S. Wagstaff, Jr.
Center for Education and Research
in Information Assurance and Security
and Department of Computer Sciences
Purdue University
West Lafayette, IN 47907-1398, USA
E-mail: ssw@cerias.purdue.edu

Abstract (will appear on the journal's web site only)

We study the asymptotic density of the set of subscripts of the Bernoulli numbers having a given denominator. We also study the distribution of distinct Bernoulli denominators and some related problems.