Dartmouth Number Theory Seminar
May 25, 2021

Denominators of Bernoulli numbers

Carl Pomerance, Dartmouth College

(Joint work with Sam Wagstaff)

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.

n:	0	1	2	3	4	5	6	7	8	9	10	11	12
B_n:	1	$\frac{-1}{2}$	$\frac{1}{6}$	0	$\frac{-1}{30}$	0	$\frac{1}{42}$	0	$\frac{-1}{30}$	0	$\frac{5}{66}$	0	$\frac{-691}{2730}$

The Bernoulli numbers are perhaps most famous for their appearance in the formula:

$$\zeta(2k) \;=\; |B_{2k}|\frac{(2\pi)^{2k}}{2(2k)!}. \quad \text{(E.g., } \zeta(2) = \frac{\pi^2}{6}.\text{)}$$

They were originally found to be of use when adding consecutive powers:

$$\sum_{k<N} k^m \;=\; \frac{1}{m+1}\sum_{j=0}^{m} B_j \binom{m+1}{j} N^{m-j+1}.$$

E.g., $1^4 + 2^4 + \cdots + (N-1)^4 = \frac{1}{5}N^5 - \frac{1}{2}N^4 + \frac{1}{3}N^3 - \frac{1}{30}N$.

Write

$$B_n = \frac{N_n}{D_n}, \ \ \gcd(N_n, D_n) = 1, \ \ D_n > 0.$$

After Kummer, we say an odd prime p is *regular* if p does not divide the class number of the cyclotomic field $\mathbb{Q}[e^{2\pi i/p}]$. He showed (1850) that Fermat's Last Theorem holds for regular primes, the first irregular prime being 37. And he showed that an odd prime p is regular if and only if it does not divide any N_n for n even, $n < p$.

There are also criteria for irregular primes to satisfy FLT, and before Wiles we knew FLT for every exponent up to several million.

It's conjectured that a positive proportion of primes are regular and a positive proportion are irregular, but the only thing known for sure is that there are infinitely many irregular primes. As far as I know the best lower estimate for the number of irregular primes up to x is the following.

Luca, Pizarro-Madariaga, & P, 2015: The number of irregular primes up to x is $\geq (1+o(1))\log\log x/\log\log\log x$.

There is also a slightly tenuous connection of FLT to the Bernoulli denominators D_n. Sophie Germain showed that the Fermat equation for prime exponent p has no solutions coprime to p if $2p+1$ is also prime. It turns out that $2p+1$ prime implies that $2p+1 \mid D_{2p}$.

In some sense, the Bernoulli denominators D_n are much less mysterious than the numerators N_n. Key here is

von Staudt, Clausen, 1840: For $n > 0$ even, D_n is the product of those primes p with $p - 1 \mid n$.

For example, we can immediately see for $n = 100$ that $D_{100} = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 101$, so that $D_{100} = 33{,}330$.

Some consequences are that when n is even, D_n is squarefree and divisible by 6.

One might ask if $D_n = 6$ infinitely often. We have this for $n = 2, 14, 26, 34, 38, 62, 74, 86, 94, 98$ looking up to 100. In fact this holds for about 15% of the even numbers up to 10^9.

The criterion for an even n to have $D_n = 6$ is that no prime $p > 3$ has $p - 1 \mid n$. In particular, n is not divisible by any Germain prime $q > 2$, since if $q \mid n$ we have $2q \mid n$, and so $p = 2q + 1 \mid D_n$. But there are many other conditions for n.

Erdős, Wagstaff, 1980: For each $\epsilon > 0$ there is some bound B such that the asymptotic density of the integers divisible by a shifted prime $p - 1 > B$ is $< \epsilon$.

That is, very few integers are divisible by a large shifted prime. As a consequence, $\{n \text{ even} : D_n = 6\}$ has positive asymptotic density.

How in the world can it be that only a few integers are divisible by a large shifted prime $p-1$? The integers not divisible by any prime $p > B$ are quite sparsely distributed, their counting function is of the shape $(\log x)^{O(1)}$. But by Erdős–Wagstaff, it is the opposite for shifted primes; though almost all n have a large divisor p, very few n have a large divisor $p-1$.

This is due to a century-old result of Hardy and Ramanujan about the "normal" number of prime factors of n: it is $\log\log n$. In fact, the normal number of prime factors $\leq B$ of an integer is $\log\log B$. The same is true for shifted primes $p-1$ from an old result of Erdős. Thus, if $n = (p-1)m$, where $p > B$, then normally one would expect $\log\log B$ primes below B in $p-1$ and the same for m, so that n itself would have $2\log\log B$ primes below B, which is definitely *not* normal.

Erdős and Wagstaff more generally proved that for any d which appears as some D_m for m even, there is a positive proportion of even n with $D_n = d$.

But they gave no clue as to what these proportions actually are. This was addressed by Sunseri in his 1979 PhD thesis who showed that the density for $d = 6$ is at least as big as the other densities.

P & Wagstaff, 2021: The density for $d = 6$ is at least 1/3 larger than the next biggest density.

We conjecture that the next biggest density occurs for $d = 30$, followed by $d = 42$.

Of interest is which numbers can appear as a Bernoulli denominator D_n. Other than being squarefree multiples of 6, what else can we say? Up to 10^9 there are 1,893,060 of them, out of 50,660,598 squarefree multiples of 6.

Let $\mathcal{D}$ be the set of Bernoulli denominators D_n. Given $d \in \mathcal{D}$ we can consider the least f with $D_f = d$, denote this f by F_d. Let $\mathcal{F}$ be the set of all F_d for $d \in \mathcal{D}$. That is, $\mathcal{F}$ is the set of first occurrences.

Lemma. For $d \in \mathcal{D}$, we have $F_d = \lambda(d)$. Every even m with $D_m = d$ has $\lambda(d) \mid m$. In addition, $\mathcal{F} = \{\lambda(n) : n > 2, n \text{ squarefree}\}$.

Here $\lambda(n)$ gives the exponent of $(\mathbb{Z}/n\mathbb{Z})^*$, it is the lcm of the $p-1$ for the primes $p \mid n$, when n is squarefree.

Lemma. For $d \in \mathcal{D}$, we have $F_d = \lambda(d)$. Every even m with $D_m = d$ has $\lambda(d) \mid m$. In addition, $\mathcal{F} = \{\lambda(n) : n > 2, n \text{ squarefree}\}$.

Proof. If $D_m = d$, then d is squarefree and for each $p \mid d$, $p - 1 \mid m$, so that $\lambda(d) \mid m$. This implies that $D_{\lambda(d)} \mid D_m = d$. Also, $p \mid d$ implies $p - 1 \mid \lambda(d)$, so that $p \mid D_{\lambda(d)}$, which implies $d \mid D_{\lambda(d)}$. Thus, $D_{\lambda(d)} = d$ and $F_d = \lambda(d)$.

To complete the proof we should show that for $n > 2$ and squarefree we have $\lambda(n) \in \mathcal{F}$. Since $n > 2$, $\lambda(n)$ is even; let $d = D_{\lambda(n)}$. Since n is squarefree, we have $n \mid d$, so that $\lambda(n) \mid \lambda(d)$. But by the first part, $\lambda(d) \mid \lambda(n)$, so they are equal. □

Let $F(x) = \#(\mathcal{F} \cap [1, x])$. By the lemma,

$$F(x) = \#\{\lambda(n) \le x : n > 2, \text{ squarefree}\}.$$

Ford, Luca, & P, 2014: We have $\#\{\lambda(n) \le x\} = x/(\log x)^{\beta + o(1)}$ as $x \to \infty$, where $\beta = 1 - (1 + \log\log 2)/\log 2 = 0.08607\ldots$.

The proof shows the same holds if n is restricted to squarefree numbers.

Corollary. We have $F(x) = x/(\log x)^{\beta + o(1)}$ as $x \to \infty$.

Note that $F(10^9) = 212{,}656{,}697$.

Let $D(x) = \#(\mathcal{D} \cap [1, x])$. Note that if $d \in \mathcal{D}$, then $F_d = \lambda(d) \in \mathcal{F}$ and $\lambda(d) < d$. Further, $\lambda(d)$ determines d, since the lemma implies that $d = D_{\lambda(d)}$. Thus,

$$D(x) \le \#\{\lambda(n) : n \le x\}.$$

Luca & P, 2014: We have $\#\{\lambda(n) : n \le x\} = x/(\log x)^{1+o(1)}$ as $x \to \infty$.

Corollary. As $x \to \infty$, $D(x) \le x/(\log x)^{1+o(1)}$.

For a lower bound, we show that for a positive proportion δ of primes p we have $6p \in \mathcal{D}$, so that $D(x) \ge (\frac{\delta}{6} + o(1))x/\log x$. Hence, $D(x) = x/(\log x)^{1+o(1)}$ as $x \to \infty$.

In fact, we show that for each $d \in \mathcal{D}$ the relative density in the set of primes of those p with $D_{p-1} = dp$ exists and is positive. Probably the largest of these densities is for $d = 6$ but we were not able to show this.

We do know that the sum of the densities is 1. A consequence (but actually part of the proof) is that for "almost all" primes p, D_{p-1}/p is in $\mathcal{D}$. The proof of this uses a result in the paper of Luca, Pizarro-Madariaga, & P mentioned above.

Probably there are infinitely many p with $D_{p-1}/p \notin \mathcal{D}$. We can prove this on assumption of Dickson's prime k-tuples conjecture. This conjecture implies there are infinitely many twin primes, and similarly for many other linear prime configurations. For example, there should be infinitely many Germain primes. The case of interest here: there should be infinitely many primes $p \equiv 3 \pmod 4$ such that $q = 2p - 1$ is prime. If $p > 3$ is such a prime, consider $d = D_{q-1}/q$. If $d = D_n$ for some n, we have $p \mid d$, so that $p - 1 \mid n$. Also $5 \mid d$, so $4 \mid n$. But $\operatorname{lcm}\{4, p-1\} = q - 1$, so $q \mid d$, contradicting D_{q-1} squarefree.

The problem of getting a lower bound for the distribution of irregular primes is strangely difficult. Let C_n denote the numerator of B_n/n in lowest terms. Then for n even, every prime divisor of C_n is irregular, as follows from some a result of Kummer.

Recall the formula for even n,

$$\zeta(n) \;=\; |B_n| \frac{(2\pi)^n}{2n!}.$$

View this, keeping in mind the sizes of the various quantities. We have $\zeta(n) \approx 1$. The expression $(2\pi)^n$ of course grows exponentially, but it can't touch $n!$. The Bernoulli denominator D_n can occasionally be fairly big, with $\log(D_n)$ of magnitude $n/\log\log n$, but not bigger than this (Erdős, P, & Schmutz, 1991). Putting this together, we have $C_n = n^{n+O(n/\log n)}$. And each prime factor of this huge number is irregular.

Thank you