3 Bernoulli numbers

Definition of the Bernoulli numbers B_m

Motivation

- We know that $\sum_{k=1}^n k = \frac{1}{2}n(n+1)$ and $\sum_{k=1}^n k^2 = \frac{1}{6}n(n+1)(2n+1)$; but what is $\sum_{k=1}^n k^m$ in general?
- We know that $\sum_{n=1}^\infty n^{-2} = \pi^2/6$; but what is $\sum_{n=1}^\infty n^{-m}$ in general?
- Does $x^n + y^n = z^n$ have any solutions with $x, y, z \in \mathbb{N}$ and $n \geq 3$?

In all cases it turns that there is an answer which involves Bernoulli numbers.

Definition. $F(t) = \dfrac{t}{e^t - 1}$ with $F(0) = 1$.

$1/F(t) = t^{-1}(e^t - 1) = 1 + \frac{t}{2!} + \frac{t^2}{3!} + \frac{t^3}{4!} + \dots$, so setting $F(0) = 1$ makes sense. Expand $F(t)$ as a Taylor series:

$$F(t) = \frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!}.$$

Definition. The rational number B_m is called the mth **Bernoulli Number**.

$F(t)$ is called the "exponential generating function" for the B_m.

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
B_m	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$	0	$\frac{7}{6}$	0

m	16	17	18	19	20	21	22	23	24	25	26
B_m	$-\frac{3617}{510}$	0	$\frac{43867}{798}$	0	$-\frac{174611}{330}$	0	$\frac{854513}{138}$	0	$-\frac{236364091}{2730}$	0	$\frac{8553103}{6}$

In the problem sheet, we will show that $F(t) - F(-t) = -t$; hence $B_1 = -\frac{1}{2}$, and $B_m = 0$ for all odd $m > 1$.

Proposition 3.1. $\displaystyle\sum_{k=0}^{m-1} \binom{m}{k} B_k = 0$ *for all* $m \geqslant 2$.

Proof. Compare the coefficients on both sides of the identity $t = (e^t - 1)F(t)$. $\square$

Corollary 3.2. *For all* $m \geqslant 1$, $\displaystyle B_m = \frac{-1}{m+1} \sum_{k=0}^{m-1} \binom{m+1}{k} B_k.$

The sum of m-th powers of consequtive integers

We wish to find a general formula for $1^m + 2^m + 3^m + \dots + (n-1)^m$.

- $1 + 2 + 3 + \dots + (n-1) = \frac{1}{2}n(n-1)$;
- $1^2 + 2^2 + 3^2 + \dots + (n-1)^2 = \frac{1}{6}n(n-1)(2n-1)$;
- $1^3 + 2^3 + 3^3 + \dots + (n-1)^3 = ?$

Notation. For $m \in \mathbb{N}$ let $\mathcal{S}_m(n) = 1^m + 2^m + 3^m + \dots + (n-1)^m$.

Our aim is to compute $\mathcal{S}_m(n)$, using Bernoulli numbers.

Theorem 3.3. *For all* $m \in \mathbb{N}$, $\mathcal{S}_m(n) = \sum_{k=0}^{m} \binom{m}{k} B_{m-k} \frac{n^{k+1}}{k+1}$.

For example, $\mathcal{S}_3(n) = \frac{1}{4}(n^4 - 2n^3 + n^2) = \left(\frac{1}{2}n(n-1)\right)^2$.

Proof. Evaluate $A = \sum_{a=0}^{n-1} e^{at}$ in two ways. Using $e^{at} = \sum_{m=0}^{\infty} a^m \frac{t^m}{m!}$ gives

$$A = \sum_{m=0}^{\infty} \frac{t^m}{m!} \mathcal{S}_m(n).$$

Summing A as a geometric series gives

$$A = \frac{e^{nt} - 1}{e^t - 1} = \frac{e^{nt} - 1}{t} \frac{t}{e^t - 1} = \frac{e^{nt} - 1}{t} F(t),$$

which leads to

$$A = \left(\sum_{k=0}^{\infty} n^{k+1} \frac{t^k}{(k+1)!} \right) \left(\sum_{j=0}^{\infty} B_j \frac{t^j}{j!} \right).$$

Comparing coefficients gives the result. □

Lemma 3.4. *If* $p-1$ *divides* m, *then* $\mathcal{S}_m(p) \equiv -1 \pmod{p}$, *otherwise* $\mathcal{S}_m(p) \equiv 0 \pmod{p}$.

Proof. Let g be a primitive element modulo p. Then

$$(g^m - 1) \cdot \mathcal{S}_m(p) \equiv (g^m - 1) \cdot \sum_{k=0}^{p-2} (g^k)^m = g^{m \cdot (p-1)} - 1 \equiv 0 \pmod{p}.$$

If $(p-1) \nmid m$, then $g^m \not\equiv 1$ and so $\mathcal{S}_m(p) \equiv 0 \pmod{p}$. Otherwise $\mathcal{S}_m(p) \equiv p - 1 \equiv -1 \pmod{p}$. □

Riemann's zeta-function

Definition. The Riemann zeta-function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots$$

Remark. It diverges when $s = 1$, but we will see later that $\zeta(s)$ converges for $s > 1$. Here we are only interested in $\zeta(s)$ for **integer** values of s: we will give a formula valid for all **positive even** integers.

Theorem 3.5 (Euler). *For all* $m \in \mathbb{N}$,

$$\zeta(2m) = (-1)^{m+1} \frac{(2\pi)^{2m}}{2\,(2m)!} B_{2m}.$$

Proof. See separate non-examinable handout. □

Examples: Taking $m = 1$ and using $B_2 = \frac{1}{6}$ gives $\zeta(2) = \pi^2/6$. Taking $m = 2$ and using $B_4 = -\frac{1}{30}$ gives $\zeta(4) = \pi^4/90$.

Corollary 3.6. *(i). For all $m \in \mathbb{N}$, the sign of B_{2m} is $(-1)^{m+1}$.*

(ii). The sequence $|B_{2m}|$ grows like $\frac{2(2m)!}{(2\pi)^{2m}} \sim 4\sqrt{\pi m} \cdot \left(\frac{m}{e\pi}\right)^{2m}$.

(iii). For all even $m \geqslant 18$ we have $|B_m| > m$.

Proof. $\zeta(2m) > 0$ since it is the sum of a series of positive terms, so $(-1)^{m+1} B_{2m} = \frac{2\,(2m)!}{(2\pi)^{2m}}\zeta(2m) > 0$. Since $\zeta(2m) > 1$, we have $|B_{2m}| > \frac{2(2m)!}{(2\pi)^{2m}}$. The second expression follows from Stirling's formula. Now for $m = 9$, we get $B_{18}/18 > 3$ and the function $B_{2m}/2m$ increases quickly in m. $\square$

Congruences for Bernoulli Numbers

The Theorems stated in this lecture give information about the numerators and denominators of the (rational) Bernoulli numbers B_m. The first one tells us exactly what the denominator is.

Notation. For $m \in \mathbb{N}$ set $\Delta_m = \{\text{primes } p \text{ such that } (p-1) \mid m\}$.

Theorem 3.7 (Clausen & von Staudt). *For all* **even** *$m \in \mathbb{N}$,*

$$C_m = B_m + \sum_{q \in \Delta_m} \frac{1}{q} \in \mathbb{Z}.$$

In particular, the denominator of B_m is precisely $\prod_{q\in\Delta_m} q$.

Example: For $m = 50$ we have $\Delta_{50} = \{2, 3, 11\}$, so $B_{50} + \frac{1}{2} + \frac{1}{3} + \frac{1}{11} = B_{50} + \frac{61}{66} \in \mathbb{Z}$. In fact, $B_{50} + \frac{61}{66} = 7500866746076964366855721$.

Proof. Let p be any prime, the aim is to show that the denominator of C_m is coprime to p. The theorem can be proven by induction on even m. First, $m = 2$ is easy. Let $m > 2$ be even. Then $B_{m-1} = 0$. The formula for $\mathcal{S}_m(p)$ can be written as

$$\mathcal{S}_m(p) = B_m \cdot p + \sum_{k=2}^{m} \binom{m}{k} p\, B_{m-k} \frac{p^k}{k+1} \tag{1}$$

By induction, pB_{m-k} has no p in the denominator. In the problem sheet, we prove that, if $k \geqslant 2$, then the numerator of $p^k/(k+1)$ is divisible by p. Hence the sum is a rational number whose numerator is divisible by p. If $p \notin \Delta_m$, then $\mathcal{S}_m(p) \equiv 0 \pmod p$ by lemma 3.4. So B_m, and hence C_m, have no p in the denominator. If $p \in \Delta_m$, then $\mathcal{S}_m(p) + 1$ is divisible by p. So $B_m + \frac{1}{p}$, and hence C_m, have no p in the denominator. $\square$

Finally, a congruence which tells us something about the numerator of B_m.

Theorem 3.8 (The Kummer Congruences). *Let $m \in \mathbb{N}$ be even and $p \notin \Delta_m$. Then*

$$m \equiv n \pmod{p-1} \implies \frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

by which we mean that the numerator of $\frac{B_m}{m} - \frac{B_n}{n}$ is divisible by p.

More generally, $m \equiv n \pmod{(p-1)p^k}$ implies

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} \pmod{p^k}.$$

Examples: $B_6/6 - B_2/2 = \frac{-5}{63}$ is divisible by $p = 5$ as $6 \equiv 2 \pmod{p-1}$. So is $B_{10}/10 - B_2/2 = \frac{-5}{66}$ or $B_{18}/18 - B_2/2 = \frac{21335}{7182}$.

Regular and irregular primes and Fermat's Last Theorem

Definition. The odd prime number p is called **regular** if p does not divide the numerator of B_m for all even $m \leqslant p-3$. Otherwise p is **irregular**.

Examples: $p = 3, 5, 7, \ldots, 31$ are all regular, but 37 is irregular: $B_{32} = -\frac{7709321041217}{510}$ and $7709321041217 = 37 \cdot 683 \cdot 305065927$.
The significance of regularity comes from the following application.

Theorem 3.9 (Kummer, 1850). *Let p be an odd regular prime. Then the equation*

$$x^p + y^p = z^p$$

has no solution in positive integers.

Proof. Omitted (uses Algebraic Number Theory). $\square$

Question: How many regular primes are there?
Answer: No-one knows, but computer calculations suggest that 61% of primes are regular and 39% are irregular. What we can prove is this:

Theorem 3.10. *There are infinitely many irregular primes.*

Proof. Take the complete list of all irregular primes $p_1, p_2, \ldots, p_r$. Consider $N = 2\prod_i(p_i - 1)$. By Corollary 3.6 we have $|B_N| > N$ because $N \geqslant 18$. So there exists a prime p which divides the numerator of B_N/N. We will show that p is irregular and not in the set $\{p_1, p_2, \ldots, p_r\}$.
By Theorem 3.7, $p \notin \Delta_N$ since p divides the numerator but not the denominator of B_N. So $(p-1) \nmid N$. Hence $p \neq 2$ and $p \neq p_i$ for $1 \leqslant i \leqslant r$.
Take n with $0 \leqslant n < p-1$ and $n \equiv N \pmod{p-1}$; then n is even and $n > 0$ since $(p-1) \nmid N$, so $2 \leqslant n \leqslant p-3$. By Theorem 3.8 we have

$$\frac{B_n}{n} \equiv \frac{B_N}{N} \equiv 0 \pmod{p},$$

so p divides the numerator of B_n; hence p is irregular. $\square$

Theorem 3.11 (Wiles-Taylor-...). *If $n \geqslant 3$, then $x^n + y^n = z^n$ has no solution in $\mathbb{N}$.*