Bernoulli Numbers

Junior Number Theory Seminar – University of Texas at Austin

September 6th, 2005

Matilde N. Lalín

I will mostly follow [2].

Definition and some identities

Definition 1 *Bernoulli numbers are defined as* $B_0 = 1$ *and recursively as*

$$(m+1)B_m = -\sum_{k=0}^{m-1} \binom{m+1}{k} B_k,$$

so we find $B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, B_6 = \frac{1}{42}, \dots, B_{12} = -\frac{691}{2730}, \dots$

Lemma 2

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

PROOF. Write $\frac{t}{\mathrm{e}^t-1} = \sum_{m=0}^{\infty} a_m \frac{t^m}{m!}$ and multiply by $\mathrm{e}^t - 1$,

$$t = \sum_{n=1}^{\infty} \frac{t^n}{n!} \sum_{m=0}^{\infty} a_m \frac{t^m}{m!},$$

equate coefficients for t^{m+1} gives $a_0 = 1$ and

$$\sum_{k=0}^{m} \binom{m+1}{k} a_k = 0.$$

$\square$

Theorem 3 *(J. Bernoulli) Let* m *be a positive integer and define*

$$S_m(n) = 1^m + \dots + (n-1)^m,$$

then

$$(m+1)S_m(n) = \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}.$$

PROOF. In $e^{kt} = \sum_{m=0}^{\infty} k^m \frac{t^m}{m!}$ substitute $k = 0, 1, \dots, n-1$ and add,

$$\sum_{m=0}^{\infty} S_m(n) \frac{t^m}{m!} = 1 + \mathrm{e}^t + \dots + \mathrm{e}^{(n-1)t} = \frac{\mathrm{e}^{nt} - 1}{t} \frac{t}{\mathrm{e}^t - 1}$$

$$= \sum_{k=1}^{\infty} n^k \frac{t^{k-1}}{k!} \sum_{j=0}^{\infty} B_j \frac{t^j}{j!}$$

now equate the coefficients of t^m and multiply by $(m+1)!$. $\square$

Definition 4

$$B_m(x) = \sum_{k=0}^{m} \binom{m}{k} B_k x^{m-k}$$

are called Bernoulli polynomials.

So $B_0(x) = 1$, $B_1(x) = x - \frac{1}{2}$, etc.

Then Theorem 3 may be stated as

$$S_m(n) = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}).$$

Lemma 5

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

PROOF. First note that

$$B'_m(x) = \sum_{k=0}^{m-1} \binom{m}{k} (m-k) B_k x^{m-1-k} = mB_{m-1}(x).$$

Also

$$\int_0^1 B_m(x)\mathrm{d}x = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k = 0, \qquad m \geq 1.$$

Now let $F(x,t) = \sum_{m=0}^{\infty} B_m(x) \frac{t^m}{m!}$, differentiating,

$$\frac{\partial}{\partial x} F(x,t) = \sum_{m=1}^{\infty} B_{m-1}(x) \frac{t^m}{(m-1)!} = tF(x,t).$$

Now we solve using separation of variables, $F(x,t) = T(t)\mathrm{e}^{xt}$, then

$$\int_0^1 F(x,t)\mathrm{d}x = \int_0^1 T(t)\mathrm{e}^{xt}\mathrm{d}x = T(t)\frac{\mathrm{e}^t - 1}{t}$$

but

$$\int_0^1 F(x,t)\mathrm{d}x = \sum_{m=0}^{\infty} \frac{t^m}{m!} \int_0^1 B_m(x)\mathrm{d}x = 1$$

and this proves the statement (Castellanos, [1]). □

Proposition 6 *1.* $B_m(x+1) - B_m(x) = \sum_{k=0}^{m} \binom{m}{k} B_{m-k}(x) = mx^{m-1}$ *(Roman [5]).*

2. $B_m(1-x) = (-1)^m B_m(x)$.

3. $B_m = \sum_{k=0}^{m} \frac{1}{k+1} \sum_{r=0}^{k} (-1)^r \binom{k}{r} r^m$ *(Rademacher [4]).*

4. $\sum_{k=0}^{m} (-1)^{k+m} \binom{m}{k} B_m(k) = m!$ *(Ruiz [6]).*

5. $B_m(kx) = k^{q-1} \sum_{j=0}^{k-1} B_m\left(x + \frac{j}{k}\right)$.

Euler MacLaurin sum formula (Rademacher, [4]).

Let $f(x)$ smooth. Since $B_1'(x) = 1$,

$$\int_0^1 f(x)\mathrm{d}x = B_1(x)f(x)|_0^1 - \int_0^1 B_1(x)f'(x)\mathrm{d}x$$

$$= \ldots = \sum_{m=1}^{q} (-1)^{m-1} \left. \frac{B_m(x)}{m!} f^{(m-1)}(x) \right|_0^1 + (-1)^q \int_0^1 \frac{B_q(x)}{q!} f^{(q)}(x)\mathrm{d}x$$

Evaluating in $x = 1$,

$$f(1) = \int_0^1 f(x)\mathrm{d}x + \sum_{m=1}^{q} (-1)^m \frac{B_m}{m!}(f^{(m-1)}(1) - f^{(m-1)}(0)) + (-1)^{q-1} \int_0^1 \frac{B_q(x)}{q!} f^{(q)}(x)\mathrm{d}x.$$

Changing $f(x)$ by $f(n-1+x)$ and adding, we obtain the formula

$$\sum_{n=a+1}^{b} f(n) = \int_a^b f(x)\mathrm{d}x + \sum_{m=1}^{q} (-1)^m \frac{B_m}{m!}(f^{(m-1)}(b) - f^{(m-1)}(a)) + R_q$$

where

$$R_q = \frac{(-1)^{q-1}}{q!} \int_a^b B_q(x - [x]) f^{(q)}(x)\mathrm{d}x$$

An integral and some identities

Proposition 7 *We have:*

$$\int_0^\infty \frac{x \log^k x \mathrm{d}x}{(x^2+a^2)(x^2+b^2)} = \left(\frac{\pi}{2}\right)^{k+1} \frac{P_k\left(\frac{2\log a}{\pi}\right) - P_k\left(\frac{2\log b}{\pi}\right)}{a^2 - b^2}.$$

where

$$P_k(x) = \frac{2\mathrm{i}^{k+1}}{k+1}\left(B_{k+1}\left(\frac{x}{\mathrm{i}}\right) - 2^k B_{k+1}\left(\frac{x}{2\mathrm{i}}\right)\right) + \frac{(2^{k+1}-2)\mathrm{i}^{k+1}}{k+1} B_{k+1}$$

PROOF. (Idea) We first prove that

$$\int_0^\infty \frac{x^\alpha \mathrm{d}x}{(x^2+a^2)(x^2+b^2)} = \frac{\pi(a^{\alpha-1} - b^{\alpha-1})}{2\cos\frac{\pi\alpha}{2}(b^2 - a^2)} \qquad \text{for} \quad 0 < \alpha < 1, \quad a, b \neq 0$$

by first computing

$$\int_0^\infty \frac{x^\alpha \mathrm{d}x}{x^2 + a^2} = \frac{\pi a^{\alpha-1}}{2\cos\frac{\pi\alpha}{2}}.$$

We note that the polynomials P_k may be defined recursively as

$$P_k(x) = \frac{x^{k+1}}{k+1} + \frac{1}{k+1} \sum_{j>1\,(\mathrm{odd})}^{k+1} (-1)^{\frac{j+1}{2}} \binom{k+1}{j} P_{k+1-j}(x).$$

The idea, suggested by Rodriguez-Villegas, is to obtain the value of the integral in the statement by differentiating k times the integral of with α and then evaluating at $\alpha = 1$. Let

$$f(\alpha) = \frac{\pi(a^{\alpha-1} - b^{\alpha-1})}{2\cos\frac{\pi\alpha}{2}(b^2 - a^2)}$$

which is the value of the integral with α. In other words, we have

$$f^{(k)}(1) = \int_0^\infty \frac{x\log^k x\mathrm{d}x}{(x^2+a^2)(x^2+b^2)}.$$

By developing in power series around $\alpha = 1$, we obtain

$$f(\alpha)\cos\frac{\pi\alpha}{2} = \frac{\pi}{2(b^2-a^2)}\sum_{n=0}^{\infty}\frac{\log^n a - \log^n b}{n!}(\alpha-1)^n.$$

By differentiating k times,

$$\sum_{j=0}^{k}\binom{k}{j}f^{(k-j)}(\alpha)\left(\cos\frac{\pi\alpha}{2}\right)^{(j)} = \frac{\pi}{2(b^2-a^2)}\sum_{n=0}^{\infty}\frac{\log^{n+k} a - \log^{n+k} b}{n!}(\alpha-1)^n.$$

We evaluate in $\alpha = 1$,

$$\sum_{j=0\,(\text{odd})}^{k}(-1)^{\frac{j+1}{2}}\binom{k}{j}f^{(k-j)}(1)\left(\frac{\pi}{2}\right)^j = \frac{\pi(\log^k a - \log^k b)}{2(b^2-a^2)}.$$

As a consequence, we obtain

$$f^{(k)}(1) = \frac{1}{k+1}\sum_{j>1\,(\text{odd})}^{k+1}(-1)^{\frac{j+1}{2}}\binom{k+1}{j}f^{(k+1-j)}(1)\left(\frac{\pi}{2}\right)^{j-1} + \frac{\log^{k+1} a - \log^{k+1} b}{(k+1)(a^2-b^2)}.$$

When $k = 0$,

$$f^{(0)}(1) = f(1) = \frac{\log a - \log b}{a^2-b^2} = \frac{\pi}{2}\frac{P_0\left(\frac{2\log a}{\pi}\right) - P_0\left(\frac{2\log b}{\pi}\right)}{a^2-b^2}.$$

The general result follows by induction on k and the definition of P_k. □

Theorem 8 *We have the following identities:*

- *For* $1 \le l \le n$*:*

$$\begin{aligned} &s_{n-l}(1^2,\ldots,(2n-1)^2) \\ &= n\sum_{s=0}^{n-l}s_{n-l-s}(2^2,\ldots,(2n-2)^2)\frac{1}{l+s}B_{2s}\binom{2(l+s)}{2s}(2^{2s}-2)(-1)^{s+1}. \end{aligned}$$

- *For* $1 \le n$*:*

$$\left(\frac{(2n)!}{2^n n!}\right)^2 = 2n\sum_{s=1}^{n}s_{n-s}(2^2,\ldots,(2n-2)^2)\frac{1}{s}B_{2s}(2^{2s}-1)(-1)^{s+1}.$$

- *For* $0 \leq l \leq n$:

$$\begin{aligned}&(2l+1)s_{n-l}(2^2,\ldots,(2n)^2)\\ &= (2n+1)\sum_{s=0}^{n-l} s_{n-l-s}(1^2,\ldots,(2n-1)^2)B_{2s}\binom{2(l+s)}{2s}(2^{2s}-2)(-1)^{s+1}.\end{aligned}$$

- *For* $1 \leq n$:

$$\sum_{s=1}^{n} s_{n-s}(2^2,\ldots,(2n-2)^2)(-1)^{s+1}\frac{2^{2s}(2^{2s}-1)}{s}B_{2s} = 2(2n-1)!$$

where

$$s_l(a_1,\ldots,a_k) = \begin{cases} 1 & \text{if} \quad l=0 \\ \sum_{i_1<\ldots<i_l} a_{i_1}\ldots a_{i_l} & \text{if} \quad 0<l\leq k \\ 0 & \text{if} \quad k<l \end{cases}$$

are the elementary symmetric polynomials, i.e.,

$$\prod_{i=1}^{k}(x+a_i) = \sum_{l=0}^{k} s_l(a_1,\ldots,a_k)x^{k-l}$$

Some big classic results

Theorem 9 *(Euler)*

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

PROOF. We will need

$$\cot x = \frac{1}{x} - 2\sum_{n=1}^{\infty}\frac{x}{n^2\pi^2-x^2}.$$

This identity may be deduced by applying the logarithmic derivative to

$$\sin x = x\prod_{n=1}^{\infty}\left(1-\frac{x^2}{n^2\pi^2}\right).$$

Then

$$x\cot x = 1 - 2\sum_{n=1}^{\infty}\frac{x^2}{n^2\pi^2}\sum_{k=0}^{\infty}\left(\frac{x}{n\pi}\right)^{2k} = 1 - 2\sum_{m=1}^{\infty}\zeta(2m)\frac{x^{2m}}{\pi^{2m}}$$

On the other hand,

$$x\cot x = x\frac{\cos x}{\sin x} = x\frac{\mathrm{i}(\mathrm{e}^{\mathrm{i}x}+\mathrm{e}^{-\mathrm{i}x})}{\mathrm{e}^{\mathrm{i}x}-\mathrm{e}^{-\mathrm{i}x}} = \mathrm{i}x + \frac{2ix}{\mathrm{e}^{2\mathrm{i}x}-1} = 1 + \sum_{n=2}^{\infty}B_n\frac{(2\mathrm{i}x)^n}{n!}$$

and compare coefficients of x^{2m}.

For instance, $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, etc.

Corollary 10 *1.* $(-1)^{m+1}B_{2m} > 0$.

2. $\left|\frac{B_{2m}}{2m}\right| \to \infty$ *or* $B_{2m} \sim (-1)^{m+1}\frac{2(2m)!}{(2\pi)^{2m}}$ *as* $m \to \infty$.

PROOF. The first assertion is consequence of the fact that $\zeta(2m)$ is positive. The second is consequence of the fact that $\zeta(2m) > 1$ implies

$$|B_{2m}| > \frac{2(2m)!}{(2\pi)^{2m}}.$$

$\square$

Theorem 11 *(Claussen, von Staudt) For* $m \geq 1$

$$B_{2m} \equiv -\sum_{(p-1)|2m,\ p\,\mathrm{prime}} \frac{1}{p} \pmod 1$$

We will need the following

Definition 12 *For every rational number* r *and* p *prime write* $r = p^k\frac{a}{b}$ *where* a, b *are integers such that* $p \not| ab$. *Then* $\mathrm{ord}_p(r) = k$. *We say that* r *is* p*-integral if* $\mathrm{ord}_p(r) \geq 0$.

Lemma 13 *Let* p *be a prime number and* k *a positive integer, then*

1. $\frac{p^k}{k+1}$ *is* p*-integral.*

2. $\frac{p^k}{k+1} \equiv 0 \pmod p$ *if* $k \geq 2$.

3. $\frac{p^{k-2}}{k+1}$ *is* p*-integral if* $k \geq 3$ *and* $p \geq 5$.

PROOF. By induction, $k+1 \leq p^k$. Let $k+1 = p^a q$. Then $\frac{p^k}{k+1} = \frac{p^{k-a}}{q} \geq 1$ implies $k \geq a$. For the second case use that $k+1 < p^k$ for $k \geq 2$. The third case is consequence of $k+1 < p^{k-2}$ for $k \geq 3$ and $p \geq 5$. $\square$

Proposition 14 *Let* p *be a prime and* m *a positive integer. Then* pB_m *is* p*-integral. Also, if* m *is even* $pB_m \equiv S_m(p) \pmod p$

PROOF. For the first statement we will use induction. It is clear for $m = 1$. Now note that for $m \geq k$ we have

$$\binom{m+1}{k} = \frac{m+1}{m-k+1}\binom{m}{k}$$

Then Theorem 3 becomes

$$S_m(n) = \sum_{k=0}^{m}\binom{m}{k}B_k\frac{n^{m+1-k}}{m+1-k} = \sum_{k=0}^{m}\binom{m}{k}B_{m-k}\frac{n^{k+1}}{k+1} \tag{1}$$

Now set $n = p$ and since $S_m(p)$ is integer, it suffices to prove that

$$\binom{m}{k}pB_{m-k}\frac{p^k}{k+1}$$

is p-integral for $k = 1, \ldots, m$, but that is true by induction and Lemma 13.

For the congruence it suffices to see that

$$\mathrm{ord}_p\left(\binom{m}{k}\left(pB_{m-k}\frac{p^k}{k+1}\right)\right) \geq 1$$

for $k \geq 1$. By Lemma 13 this is true for $k \geq 2$. The case with $k = 1$ corresponds to $\frac{m}{2}(pB_{m-1})p$ and it is true because m is even and the only nontrivial case is with $m = 2$.

Lemma 15 *Let p be a prime. If $p-1 \not| m$, then $S_m(p) \equiv 0 \pmod{p}$. If $p-1|m$ then $S_m(p) \equiv -1 \pmod{p}$*

PROOF. First suppose that $p-1 \not| m$. Let g be a primitive root modulo p. Then

$$S_m(p) = 1^m + \ldots + (p-1)^m \equiv 1^m + g^m + \ldots + g^{(p-2)m} \pmod{p}$$

and

$$(g^m - 1)S_m(p) \equiv g^{m(p-1)} - 1 \equiv 0 \pmod{p}$$

the result follows. Now suppose that $p-1|m$, then

$$S_m(p) \equiv 1 + 1 + \ldots + 1 \equiv p - 1 \pmod{p}$$

□

PROOF. (Theorem 11) Assume m is even. By Proposition 14, pB_m is p-integral and $\equiv S_m(p) \pmod{p}$. By Lemma 15, B_m is a p-integer if $p-1 \not| m$ and $pB_m \equiv -1 \pmod{p}$ if $p-1|m$. Then

$$B_m + \sum_{p-1|m} \frac{1}{p}$$

is a p-integer for all primes p, then it must be integral. □

More Congruences

Corollary 16 *If $p-1 \not| 2m$, then B_{2m} is p-integral. If $p-1|2m$ then $pB_{2m}+1$ is p-integral and*

$$\mathrm{ord}_p(pB_{2m}+1) = \mathrm{ord}_p\left(p\left(B_{2m} + \frac{1}{p}\right)\right) \geq 1$$

so $pB_{2m} \equiv -1 \pmod{p}$. Also 6 always divides the denominator of B_{2m}.

From now on write $B_m = \frac{U_m}{V_m}$ as a fraction in lowest terms with $V_m > 0$.

Proposition 17 *For m even and > 1,*

$$V_m S_m(n) \equiv U_m n \pmod{n^2}$$

PROOF. We will use equation (1), for $k \geq 1$ write

$$\binom{m}{k}\left(B_{m-k}\frac{n^{k-1}}{k+1}\right)n^2 = A_k^m n^2.$$

If we show that for $p|n$, $p \neq 2,3$, then $\mathrm{ord}_p(A_k^m) \geq 0$ and if $p|n$, $p = 2$ or 3, $\mathrm{ord}_p(A_k^m) \geq -1$, then (A_k^m, n) must divide 6 and the same is true for the greater common divisor between the sum of A_k^m and n. Then we may write

$$S_m(n) = B_m n + \frac{An^2}{lB}$$

with $(B, n) = 1$ and $l|6$. Multiplying by BV_m and using the fact that $6|V_m$ (by Corollary 16) the result is proved.

Use Corollary 16 to see that $\mathrm{ord}_p(B_{m-k}) \geq -1$. Assume $p|n$ and $p \neq 2,3$. The cases $k = 1, 2$ are simple. If $k \geq 3$,

$$\mathrm{ord}_p\left(B_{m-k}\frac{n^{k-1}}{k+1}\right) \geq -1 + (k-1)\mathrm{ord}_p n - \mathrm{ord}_p(k+1) \geq k - 2 - \mathrm{ord}_p(k+1) \geq 0$$

by Lemma 15.

Now let $p = 2$. If $k = 1$, then $B_{m-1} = 0$ for $m > 2$ and $A_1^2 = 2B_1\frac{1}{2} = -\frac{1}{2}$. For $k > 1$ note that $B_{m-k} = 0$ unless k is even or $k = m - 1$. k even implies $\mathrm{ord}_2(k+1) = 0$ and $k = m - 1$, $A_{m-1}^m = -\frac{1}{2}n^{m-2}$ which has order greater or equal to -1.

When $p = 3$, $\mathrm{ord}_3(A_2^m) \geq -1$ and $\mathrm{ord}_3(A_3^m) \geq 1$. For $k \geq 4$, one shows that $\mathrm{ord}_3\left(\frac{3^{k-2}}{k+1}\right) \geq 0$. □

Corollary 18 *Let m be even and p prime with $p - 1 \nmid m$. Then*

$$S_m(p) \equiv B_m p \pmod{p^2}.$$

PROOF. By Theorem 11, $p \nmid V_m$. Now put $n = p$ in the above Proposition and divide by V_m which is permissible since $p \nmid V_m$. □

Proposition 19 *(Voronoi's congruence) Let m even and > 1. Suppose that a and n are positive coprime integers. Then*

$$(a^m - 1)U_m \equiv ma^{m-1}V_m \sum_{j=1}^{n-1} j^{m-1}\left[\frac{ja}{n}\right] \pmod{n}.$$

PROOF. Write $ja = q_j n + r_j$ with $0 \leq r_j < n$. Then

$$j^m a^m \equiv r_j^m + mq_j n r_j^{m-1} \pmod{n^2}.$$

But $r_j \equiv ja \pmod{n}$, then

$$j^m a^m \equiv r_j^m + ma^{m-1}q_j n j^{m-1} \pmod{n^2}.$$

Summing for $j = 1, \ldots, n-1$,

$$S_m(n)a^m \equiv S_m(n) + ma^{m-1}n\sum_{j=1}^{n-1} j^{m-1}\left[\frac{ja}{n}\right] \pmod{n^2}.$$

Now multiply by V_m and use Proposition 17. □

Proposition 20 *If $p-1 \not| m$, then $\frac{B_m}{m}$ is p-integral.*

PROOF. By Theorem 11, B_m is a p-integer. Let $m = p^t m_0$ with $p \not| m_0$. In Voronoi congruence put $n = p^t$. Then $(a^m - 1)U_m \equiv 0 \pmod{p^t}$. Now let a be a primitive root modulo p. Since $p-1 \not| m$, then $p \not| a^m - 1$. Then $U_m \equiv 0 \pmod{p^t}$. Then $\frac{B_m}{m} = \frac{U_m}{mV_m}$ is p-integer. □

Theorem 21 *(Kummer congruences) Suppose $m \geq 2$ is even, p prime, and $p-1 \not| m$. Let $C_m = \frac{(1-p^{m-1})B_m}{m}$. If $m' \equiv m \pmod{\phi(p^e)}$, then $C_{m'} \equiv C_m \pmod{p^e}$.*

PROOF. We will see the case $e = 1$. Let $t = \mathrm{ord}_p(m)$. By Proposition 20, $p^t | U_m$. In Voronoi's congruence, set $n = p^{e+t}$. Since p^t divides both U_m and m, and $\frac{mV_m}{p^t}$ is prime to p, we obtain,

$$\frac{(a^m - 1)B_m}{m} \equiv a^{m-1} \sum_{j=1}^{p^{e+t-1}} j^{m-1} \left[\frac{ja}{p^{e+t}}\right] \pmod{p^e}.$$

The right-hand side is unchanged if we replace m by $m' \equiv m \pmod{p-1}$. Then

$$\frac{(a^{m'} - 1)B_{m'}}{m'} \equiv \frac{(a^m - 1)B_m}{m} \pmod{p}.$$

Choose a to be a primitive root modulo p. Since $p-1 \not| m$ we have $a^{m'} - 1 \equiv a^m - 1 \not\equiv 0 \pmod{p}$. Then

$$\frac{B_{m'}}{m'} \equiv \frac{B_m}{m} \pmod{p}.$$

□

Definition 22 *An odd prime number p is said to be regular if p does not divide the numerator of any of the numbers $B_2, B_4, \ldots, B_{p-3}$. The prime 3 is regular. Equivalently, p is regular if it does not divide the class number of $\mathbb{Q}(\xi_p)$*

The first irregular primes are 37 and 59.

Theorem 23 *(Kummer) Let p be a regular prime. Then $x^p + y^p = z^p$ has no solution in positive integers.*

Theorem 24 *(Jensen) The set of irregular primes is infinite.*

PROOF. Let $\{p_1, \ldots, p_s\}$ be the set of irregular primes. Let $k \geq 2$ be even and $n = k(p_1 - 1) \ldots (p_s - 1)$. Choose k large such that $\left|\frac{B_n}{n}\right| > 1$ and p prime such that $\mathrm{ord}_p\left(\frac{B_n}{n}\right) > 0$. Then $p-1 \not| n$ and so $p \neq p_i$. We will prove that p is also irregular.

Let $n \equiv m \pmod{p-1}$ where $0 < m < p-1$. Then m is even and $2 \leq m \leq p-3$. By the Kummer congruence,

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

Since $\mathrm{ord}_p\left(\frac{B_n}{n}\right) > 0$ and $\mathrm{ord}_p\left(\frac{B_n}{n} - \frac{B_m}{m}\right) > 0$, then

$$\mathrm{ord}_p\left(\frac{B_m}{m}\right) = \mathrm{ord}_p B_m > 0$$

and p is irregular. □

References

[1] D. Castellanos, The Ubiquitous Pi. Part I.*Math. Mag.* 61, 67–98, 1988.

[2] K. Ireland, M. Rosen, A classical introduction to modern number theory. Second edition. Graduate Texts in Mathematics, 84. *Springer-Verlag, New York,* 1990. xiv+389 pp.

[3] M. N. Lalín, Mahler measure of some n-variable polynomial families, (preprint, September 2004, to appear in *J. Number Theory*)

[4] H. Rademacher, Topics in Analytic Number Theory, Die Grundlehren der Mathematischen, Wissenschaften. New York: Springer-Verlag, 1973.

[5] S. Roman, The Bernoulli Polynomials. 4.2.2 *The Umbral Calculus*. New York: Academic Press, pp. 93–100, 1984.

[6] Eric Weisstein's World of Mathematics, http://mathworld.wolfram.com/BernoulliNumber.html