A SHORT PROOF OF KUMMER'S CONGRUENCE FOR THE BERNOULLI NUMBERS

A PREPRINT

Sumit Kumar Jha

International Institute of Information Technology
Hyderabad, India

kumarjha.sumit@research.iiit.ac.in; sumitkumarjha.iiit@gmail.com

December 18, 2019

ABSTRACT

We give a short proof of Kummer's congruence for the Bernoulli numbers using an explicit formula for them in terms of the Stirling numbers of the second kind.

Keywords Kummer congruence; Bernoulli numbers · Stirling numbers of the second kind · Polylogarithm function

AMS Classification: 11B68

Definition 1. The Bernoulli numbers B_n can be defined by the following generating function

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

where $|t| < 2\pi$.

Theorem 1 (Kummer's congruence). Let $N \geq 1$ be a natural number, and n, m be even natural numbers such that $n, m \geq N + 2$. Suppose that m and n are not divisible by $p - 1$, and that $n \equiv m \pmod{\phi(p^{N+1})}$. Then we have

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p^{N+1}}. \quad (1)$$

Lemma 1. We have

$$(1 - 2^n) \frac{B_n}{n} = \sum_{k=1}^{n-1} \frac{(-1)^k k! S(n-1, k)}{2^{k+1}}, \quad (2)$$

where $S(\cdot, \cdot)$ denotes Stirling number of the second kind.

Proof. The polylogarithm function $\mathbf{Li}_s(z)$ is defined by the following power series in z

$$\mathbf{Li}_s(z) = \sum_{k=1}^{\infty} \frac{z^k}{k^s}, \quad (3)$$

where $|z| < 1$. We know, from [1], that

$$\mathbf{Li}_s(-1) = -\eta(s)$$

where $\eta(s)$ is the Dirichlet's eta function.

Letting $s = -r$, a negative integer, in the preceding equation we have

$$-\eta(-r) = (1 - 2^{r+1}) \frac{B_{r+1}}{r+1} = \mathbf{Li}_{-r}(-1).$$

Now, using the following representation, from [2],

$$\mathbf{Li}_{-r}(-x) = \sum_{k=1}^r k! S(r, k) \left(\frac{1}{1+x} \right)^{k+1} (-x)^k$$

we can derive equation (2). □

Proof of Theorem 1. Let $n = m + a \cdot \phi(p^{N+1})$ for some integer a . Then, we have

$$\begin{aligned}
 (-1)^k k! S(n-1, k) &= \sum_{j=0}^k (-1)^j \binom{k}{j} j^{n-1} \\
 &= \sum_{j=0}^k (-1)^j \binom{k}{j} j^{m+a \cdot \phi(p^{N+1})-1} \\
 &\equiv \sum_{j=0}^k (-1)^j \binom{k}{j} j^{m-1} \pmod{p^{N+1}} \\
 &\equiv (-1)^k k! S(m-1, k) \pmod{p^{N+1}}.
 \end{aligned}$$

where we have used Euler's generalization of the Fermat's little theorem, and the fact that $m, n \geq N+2$.

Thus, we have the following after considering equation (2)

$$(1-2^n) \frac{B_n}{n} \equiv (1-2^m) \frac{B_m}{m} \pmod{p^{N+1}}.$$

Now, since 2 is a primitive root modulo p , and both m and n are not divisible by $p-1$, we have $1-2^n, 1-2^m \in (\mathbb{Z}/p^{N+1}\mathbb{Z})^\times$ with $1-2^n \equiv 1-2^m \pmod{p^{N+1}}$. This gives $\frac{B_n}{n}, \frac{B_m}{m} \in \mathbb{Z}_{(p)}$ ($\mathbb{Z}_{(p)}$ denotes the ring of rational numbers whose denominator is prime to p) and the congruence (1). $\square$

References

1. Prudnikov, A. P.; Marichev, O. I.; and Brychkov, Yu. A. *The Generalized Zeta Function $\zeta(s, x)$, Bernoulli Polynomials $B_n(x)$, Euler Polynomials $E_n(x)$, and Polylogarithms $Li_\nu(x)$* . §1.2 in *Integrals and Series*, Vol. 3: More Special Functions. Newark, NJ: Gordon and Breach, pp. 23-24, 1990.
2. S. E. Landsburg, *Stirling numbers and polylogarithms*, unpublished note, 2009, <http://www.landsburg.com/query.pdf>.