Czechoslovak Mathematical Journal

Štefan Porubský

Voronoi's congruence via Bernoulli distributions

Czechoslovak Mathematical Journal, Vol. 34 (1984), No. 1, 1–5

Persistent URL: http://dml.cz/dmlcz/101920

CZECHOSLOVAK MATHEMATICAL JOURNAL
Mathematical Institute of the Czechoslovak Academy of Sciences
V. *34* (*109*), PRAHA 26. 3. 1984, No 1

VORONOI'S CONGRUENCE VIA BERNOULLI DISTRIBUTIONS

ŠTEFAN PORUBSKÝ, Bratislava

(Received December 29, 1979, in revised form January 29, 1981)

In 1889 Voronoi [8] (or see [4]) proved the following remarkable congruence for the Bernoulli numbers B_k (in the even index notation):

If $B_{2k} = P_{2k}/Q_{2k}$ *with relatively prime* P_{2k} *and* Q_{2k} *is the* $2k^{\text{th}}$ *Bernoulli number then*

$$(1) \qquad (a^{2k} - 1) P_{2k} \equiv 2ka^{2k-1} Q_{2k} \sum_{s=1}^{N-1} s^{2k-1} \left[\frac{sa}{N}\right] \bmod N \text{ [1]}$$

for an arbitrary modulus N *and a relatively prime to* N.

This congruence was later re-discovered (or re-proved) by many authors in various forms, e.g. [1], [2], [6] or [7], however, in the case of a prime modulus. In 1966 Slavutskij [5] proved the following generalization of (1):

$$(2) \qquad 2(a^m - 1)\frac{B_m}{m} \equiv 2a^{m-1} \sum_{s=1}^{N-1} s^{m-1} \left[\frac{as}{N}\right] + (1 - a) B_{m-1} N \bmod N,$$

where $N > 1$, $a \neq 0$, m > 1 are integers with a relatively prime to N.

In this note we will deduce an extension of (2) from the distribution property of Bernoulli polynomials and discuss some connections with the known results.

Theorem. *Given a positive integer* N *and a rational number* c *prime to* N (i.e., the denominator and the numerator of c are relatively prime to N) *then*

$$(3) \qquad (c^{2k} - 1)\frac{B_{2k}}{k} \equiv 2c^{2k-1} \sum_{s=1}^{N-1} s^{2k-1} \left[\frac{sc}{N}\right] \bmod N$$

and

$$(4) \qquad \frac{c - 1}{2} B_{2k} N \equiv \sum_{s=1}^{N-1} s^{2k} \left[\frac{sc}{N}\right] \bmod N$$

for all $k = 1, 2, 3, \ldots$.

[1]) $[x]$ denotes the greatest integer in x.

We preface the proof of the theorem by the following two familiar lemmas.

Lemma 1. *For positive integers N and k we have*

$$2\sum_{x=0}^{N-1} x^{2k-1} \equiv 0 \bmod N .$$

Proof. The result is trivial for $k = 1$. Let therefore $k > 1$. Then

$$\sum_{x=0}^{N-1} x^{2k-1} = \frac{1}{2k}\sum_{j=1}^{2k}\binom{2k}{j} B_{2k-j}N^j = N^2\sum_{j=2}^{2k}\binom{2k-1}{j-1} B_{2k-j}\frac{N^{j-2}}{j} .$$

We now show that the rational number N^{j-2}/j is N-integral for $j > 2$. If $j = 3$ this can be easily seen. If $j > 3$ then for every prime p dividing N and j we have

$$(j-2).\operatorname{ord}_p(N) \geqq j - 2 \geqq \frac{\log j}{\log 2} \geqq \operatorname{ord}_p(j),$$

as desired.

Finally, the Clausen-von Staudt theorem implies that the least common denominator of non-zero numbers from among the Bernoulli numbers $B_{2k-2}, B_{2k-3}, \ldots, B_1, B_0$ is a product of primes to the first degree, and Lemma 1 follows immediately.

Lemma 2. *For positive integers N and k we have*

$$\sum_{x=0}^{N-1} x^{2k} \equiv NB_{2k} \bmod N .$$

Consequently, if N possesses the property that for every prime p dividing N we have $p - 1 \nmid 2k$ then

$$\sum_{x=0}^{N-1} x^{2k} \equiv 0 \bmod N .$$

The proof of Lemma 2 follows by obvious modifications of the preceding one.

In what follows the terminology and notation is borrowed from [3].

One of the essential features of the Bernoulli polynomials $B_k(X)$ is the fact that the family of functions

$$E_k^{(M)}(x) = M^{k-1}\frac{1}{k}B_k\left(\left\langle\frac{x}{M}\right\rangle\right), \quad M \text{ an integer}$$

(with $\langle t\rangle$ denoting the fractional part of t) defines a *distribution* on the projective system $\{\mathbf{Z}/M\mathbf{Z}\}$ ordered by divisibility. This means that the following relation is satisfied for $y \in \mathbf{Q}/\mathbf{Z}$:

$$M^{k-1}\sum_{x \bmod M} B_k\left(\left\langle y + \frac{x}{M}\right\rangle\right) = B_k(\langle My\rangle). \tag{5}$$

This relation is, however, nothing else as a rewritten form of the well-known result due to J. L. Raabe,

$$B_k(X) = M^{k-1} \sum_{a=0}^{M-1} B_k\left(\frac{X+a}{M}\right).$$

Given a rational number c, $c \neq 1$, prime to the integer N, we regularize this distribution defining

$$E_{k,c}^{(M)}(x) = E_k^{(M)}(x) - c^k E_k^{(M)}(c^{-1}x), \quad x \in \mathbf{Z}/M\mathbf{Z}.$$

If $D(k)$ is the least common denominator of the coefficients of the polynomial $B_k(X)$ then a routine computation ([3], p. 38) gives

$$E_{k,c}^{(M)}(x) \equiv x^{k-1} E_{1,c}^{(M)}(x) \mod \frac{M}{k \cdot D(k)} \mathbf{Z}\left[c, \frac{1}{c}\right]. \tag{6}$$

Proof of the theorem. Since the theorem is true for $c = 1$, we can suppose $c \neq 1$. Let

$$d = \prod_{p|N} p^{\operatorname{ord}_p(kD(k))}.$$

Then

$$k \cdot D(k) = d \cdot D$$

with an integer D prime to N. It is plain that the rational number c is also prime to Nd.

On the other hand, the distribution property (5) yields

$$\sum_{x \in \mathbf{Z}/Nd\mathbf{Z}} E_{k,c}^{(Nd)}(x) = \sum_x \{E_k^{(Nd)}(x) - c^k E_k^{(Nd)}(c^{-1}x)\} =$$

$$= \sum_x E_k^{(Nd)}(x) - c^k \sum_x E_k^{(Nd)}(x) = (1 - c^k)\frac{B_k}{k}.$$

Using (6) we get

$$(1 - c^k)\frac{B_k}{k} \equiv \sum_{x=0}^{Nd-1} x^{k-1} E_{1,c}^{(Nd)}(x) \mod \frac{N}{D} \mathbf{Z}\left[c, \frac{1}{c}\right].$$

Since D and c are prime to N, we can write

$$(1 - c^k)\frac{B_k}{k} \equiv \sum_{x=0}^{Nd-1} x^{k-1} E_{1,c}^{(Nd)}(x) \mod N.$$

Note that $E_{1,c}^{(Nd)}(x)$ is N-integral ([3], Theorem 2.1(i), p. 39). Therefore

$$\sum_{x=0}^{Nd-1} x^{k-1} E_{1,c}^{(Nd)}(x) = \sum_{w=0}^{N-1} \sum_{t=0}^{d-1} (w + tN)^{k-1} E_{1,c}^{(Nd)}(w + tN) \equiv$$

$$\equiv \sum_{w=0}^{N-1} w^{k-1} \sum_{t=0}^{d-1} E_{1,c}^{(Nd)}(w + tN) \mod N =$$

$$= \sum_{w=0}^{N-1} w^{k-1} E_{1,c}^{(N)}(w),$$

the last equality being again a consequence of (5). If $x = 0, 1, \ldots, N-1$ then

$$E_{1,c}^{(N)}(x) = -B_0 \left\{ c \left\langle \frac{c^{-1}x}{N} \right\rangle - \frac{x}{N} \right\} + (1-c) B_1 = c \left[\frac{c^{-1}x}{N} \right] + \frac{c-1}{2} .$$

Combining the above results we obtain

$$(7) \qquad (1-c^k) \frac{B_k}{k} \equiv \sum_{w=0}^{N-1} w^{k-1} c \left[\frac{c^{-1}w}{N} \right] + \frac{c-1}{2} \sum_{w=0}^{N-1} w^{k-1} \mod N .$$

After the substitution $c \mapsto c^{-1}$, which is a bijection on the set of rationals prime to N, our lemmas give the desired results, as stated in theorem.

It is evident that our theorem implies the congruence (2). Moreover, if N is a prime then our approach is different from that used by Johnson [1] and leading to no restrictions on the modulus N. Johnson's result is contained in the following one which is a consequence of (7) rather than of the theorem itself.

Corollary 1. *Under the hypotheses of Theorem we have*

$$(c^{2k}-1) \frac{B_{2k}}{2k} \equiv c^{2k-1} \sum_{s=1}^{N-1} s^{2k-1} \left[\frac{sc}{N} \right] \mod N$$

provided N is odd, or N is even with $N(c-1) \equiv 0 \mod 8$.

If $N(c-1) \not\equiv 0 \mod 8$ and N is even, the congruence of Corollary 1 need not be longer true, take for instance

$$k = 2 , \quad N = 6 , \quad c = 7 .$$

Thus, in a certain sense, our theorem gives a best possible generalization of Voronoi's original congruence. "The best one" is the following:

Corollary 2. *Under the hypotheses of Theorem we have*

$$(c^{2k}-1) \frac{B_{2k}}{2k} + \frac{c^{2k}-c^{2k-1}}{2} \cdot \frac{2k-1}{2} B_{2k-2} N^2 \equiv c^{2k-1} \sum_{x=1}^{N-1} x^{2k-1} \left[\frac{cx}{N} \right] \mod N$$

for $k = 2, 3, \ldots$.

It is clear from the last congruence that the case "*N is even and $N(c-1) \not\equiv 0 \mod 8$*" is the only one in which $N(c-1)$ cannot absorb, if necessary, the whole denominator of the second term, that is, the only case in which the second term on the left hand side does not vanish mod N, and thus it leads to multiplication by 2.

The proof of Corollary 2 follows from (6) by using the following refinement of Lemma 1:

$$\sum_{x=0}^{N-1} x^{2k-1} \equiv \frac{2k-1}{2} B_{2k-2} N^2 \mod N \quad \text{for} \quad k = 2, 3, \ldots ,$$

whose proof is left to the reader.

The following generalization of a congruence of Vandiver ([5] or [6]) can be proved using Johnson's ideas of [1]:

Corollary 3. *Given a positive integer N and an integer c prime to N, then*

$$(1 - c^{2k}) \frac{B_{2k}}{k} \equiv 2c^{2k-1} \sum_{v=1}^{c-1} \sum_{s=1}^{[vN/c]} s^{2k-1} \mod N .$$

It is plain that for integral c, (3) is equivalent to the congruence of Corollary 3. As to (4), it does not seem to be generally known. For instance, it gives the following "odd index" analogon of the previous congruence:

Corollary 4. *If N possesses the property that for every prime p dividing N we have $p - 1 \nmid 2k$, then*

$$\sum_{v=1}^{c-1} \sum_{s=1}^{[vN/c]} s^{2k} \equiv 0 \mod N$$

for every integer c prime to N.

References

[1] *W. Johnson:* p-adic proofs of congruences for the Bernoulli numbers, J. Number Th. *7* (1975), 251–265.

[2] *O. Grün:* Eine Kongruenz für Bernoullische Zahlen, Jahresber. d. Deutschen Math. Verein. *50* (1940), 111–112.

[3] *S. Lang:* Cyclotomic Fields, Springer-Verlag, New York 1978.

[4] *J. Uspenski* and *M. Heaslet:* Elementary Number Theory, McGraw-Hill, New York 1939.

[5] *J. Slavutskij:* Generalized Voronoi's congurence and the number of classes of ideals of an imaginary quadratic field II (Russian), Izv. Vyšš. Učebn. Zavedenij, Math. *4* (*53*) (1966), 118–126.

[6] *H. S. Vandiver:* Symmetric functions formed by systems of elements of a finite algebra and their connection with Fermat's quotient and Bernoulli numbers, Ann. Math. *18* (1917), 105–114.

[7] *H. S. Vandiver:* On Bernoulli numbers and Fermat's last theorem, Duke Math. J. *3* (1937), 569–584.

[8] *G. F. Voronoi:* On Bernoulli numbers (Russian), Commen. Charkov Math. Soc. *2* (1890), 129–148; or in Collected Papers, Vol. I, Publ. House Of the Ukrainian Acad. Sci., Kiev 1952.

Author's address: 814 73 Bratislava, ul. Obrancov mieru 49, ČSSR (Matematický ústav SAV).