A REMARK ON THE PAPER OF A. SIMALARIDES: "CONGRUENCES MOD p^n FOR THE BERNOULLI NUMBERS"

I. Slavutskii
4 Hamarva Str., P.O.B. 23393, Akko, Israel
(*Submitted October 11998-Final Revision June 1999*)

In the paper under discussion, the author presented interesting p^n-divisibility criteria for Bernoulli numbers (B.n.) of the form $B_{(2k-1)p^n+1}$, with an odd prime p, $k=1,2,\ldots,(p-3)/2$, and $n\in\mathbf{N}$. However, the central part of the work (Theorem 2) can be proved directly in a short and elementary way by relying on the classical methods of G. F. Voronoi. In [2] the author first proves a p-adic analog of Voronoi's congruence (Theorem 1) using Fourier analysis, then derives Theorem 2 from this proof as a corollary by reducing mod p^n the Teichmüller character involved in Theorem 1.

Theorem ([2]): Let p be a prime >3. If a is an integer with $(a,p)=1$, then

$$\{a-a^{p^{n-1}(p-2k)}\}B_{(2k-1)p^n+1}\equiv\sum_{i=1}^{p-1}i^{p^{n-1}(2k-1)}[ai/p]\pmod{p^n}$$

for every $k\geq 1$ such that $p-1$ does not divide $2k$. Here $[x]$ is the greatest integer $\leq x$.

Remark: By von Staudt-Clausen's theorem and Kummer's congruence for B.n., we will rewrite the above congruence in the equivalent form

$$\{a-a^{p^{n-1}(p-2k)}\}B_z/z\equiv\sum_{i=1}^{p-1}i^{z-1}[ai/p]\pmod{p^n}\tag{1}$$

with $z=(2k-1)p^{n-1}+1$, $p>3$.

Indeed, $(2k-1)p^n+1=(2k-1)p^{n-1}(p-1)+z$, and $p-1$ does not divide $(2k-1)p^m+1=2kp^m-(p^m-1)$ for an integer $m\geq 0$. Hence, $B_{(2k-1)p^n+1}\equiv((2k-1)p^n+1)B_z/z\equiv B_z/z\pmod{p^n}$. Thus, we can give the proof of the theorem in the form (1).

Proof: Let $S:=\sum_{i=1}^{p-1}i^z$ with $z=(2k-1)p^{n-1}+1$, $n\in\mathbf{N}$. Then, by Voronoi's idea (see, e.g., [8] or [3]), we have

$$\begin{aligned}S&=\sum_{i=1}^{p-1}(ai-[ai/p]p)^z\\&=a^z\sum_{i=1}^{p-1}i^z-pz\sum_{i=1}^{p-1}(ai)^{z-1}[ai/p]+\sum_{j=2}^{z}(-1)^j\binom{z}{j}p^j\sum_{i=1}^{p-1}(ai)^{z-j}([ai/p])^j\end{aligned}$$

or

$$S(a^z-1)/z=p\sum_{i=1}^{p-1}(ai)^{z-1}[ai/p]+\sum_{j=2}^{z}(-1)^{j-1}\binom{z-1}{j-1}(p^j/j)\sum_{i=1}^{p-1}(ai)^{z-j}([ai/p])^j.$$

Consequently,

$$S(a^z-1)/z\equiv p\sum_{i=1}^{p-1}(ai)^{z-1}[ai/p]\pmod{p^{n+1}},\tag{2}$$

because

$$\operatorname{ord}_p\left\{\binom{z-1}{j-1}p^j/j\right\} = \operatorname{ord}_p\left\{\binom{z-2}{j-2}(z-1)p^j/(j(j-1))\right\}$$
$$\geq \operatorname{ord}_p\{p^{n+1}p^{j-2}/(j(j-1))\} \geq n+1 \text{ for } j \geq 2 \text{ and } p \geq 3.$$

On the other hand, $S = (B_{z+1}(p) - B_{z+1})/(z+1)$ or

$$S(a^z-1)/z = (a^z-1)B_z p/z + pB_{z-1}(a^z-1)/2$$
$$+\sum_{j=3}^{z+1}(a^z-1)(z-1)\binom{z-2}{j-3}p^j B_{z+1-j}/(j(j-1)(j-2)),$$

if we assume that $\binom{0}{0}=1$ and that an empty sum is equal to zero.

Further, since by the Staudt-Clausen theorem, pB_{z+1-j} is p-integral, we obtain

$$\operatorname{ord}_p\{(z-1)p^j B_{z+1-j}/(j(j-1)(j-2))\} \geq \operatorname{ord}_p\{p^{j-3}/(j(j-1)(j-2))\} + n+1 \geq n+1$$

for $j \geq 3$ and $p > 3$. Hence, it follows that

$$S(a^z-1)/z \equiv (a^z-1)B_z p/z \pmod{p^{n+1}}. \tag{3}$$

With the help of $a^{p^{n-1}(p-1)} \equiv 1 \pmod{p^n}$, $(a, p) = 1$, we conclude that

$$(a^z-1)/a^{z-1} \equiv a - a^{p^{n-1}(p-1)-(2k-1)p^{n-1}} \equiv a - a^{p^{n-1}(p-2k)} \pmod{p^n}. \tag{4}$$

Note that the above transformation is useful for applications considered by the author (in the case $1 \leq k \leq (p-3)/2$, $p > 3$).

Congruences (2), (3), and (4) yield the interesting form (1) of Voronoi's congruence (with a short interval of summation in the right-hand side part).

Remark 1: It should be noted that Voronoi has proved his famous congruence (a) for an arbitrary modulus > 1 (not only prime power!) and (b) without the restriction that $p-1$ does not divide $2k$ (see [8] and [3]).

Remark 2: There is an interesting equivalent variant of Voronoi's congruence due to Vandiver (see [7] and [5]).

Remark 3: It is clear from what has been said here that a congruence similar to (1) can be obtained for generalized Bernoulli numbers $B_{n,\chi}$ belonging to a Dirichlet character (with the corresponding conductor). For relevant facts, see [4], and [9, chs. 4 and 5].

Remark 4: Finally, for more information on the history of the Voronoi congruence, see [6] or [1].

ACKNOWLEDGMENT

The author is very grateful to the anonymous referee for useful comments on the first variant of this note.

REFERENCES

1. Š. Porubský. "Voronoï Type Congruences for Bernoulli Numbers." (In Voronoï Impact on Modern Science.) *Proc. Inst. of Math., Nat. Acad. Sci. Ukraine, Kiev,* **21** (1998):71-98.
2. A. Simalarides. "Congruences Mod p^n for the Bernoulli Numbers." *The Fibonacci Quarterly* **36.3** (1998):276-81.
3. I. Slavutskii. "Generalized Voronoi Congruence and the Number of Classes of Ideals of an Imaginary Quadratic Field, II." (In Russian). *Izv. Vyssh. Uchebn. Zaved. Matematika*, No. 4 (1966):118-26. MR 35#4192.
4. I. Slavutskii. "Local Properties of Bernoulli Numbers and a Generalization of the Kummer-Vandiver Theorem." (In Russian). *Izv. Vyssh. Uchebn. Zaved. Matematika*, No. 3 (1972): 61-69. MR 46#151.
5. I. Slavutskii. "p-Adic Continuous Uehara Functions and Voronoi Congruence." (In Russian). *Izv. Vyssh. Uchebn. Zaved. Matematika*, No. 4 (1987):59-64. Eng. Trans. in *Soviet Math.* (*IZV, Matematika*), **31.4** (1987):79-85. MR 88*k*:11019.
6. I. Slavutskii. "Outline of the History of Research on the Arithmetic Properties of Bernoulli Numbers: Staudt, Kummer, Voronoi." (In Russian.) *Istor.-mat. Issled* **32/33** (1990):158-81. MR 92*m*:11001.
7. H. S. Vandiver. "On Developments in an Arithmetic Theory of the Bernoulli and Allied Numbers." *Scripta math.* **25.4** (1961):273-303.
8. G. F. Voronoi. "On Bernoulli Numbers." (In Russian.) *Proc. Khar'kovsk. Math. Soc.* (2), **2** (1889):129-48. Also in *Collected Works*, Vol. I, pp. 7-23, Kiev, 1952. MR 16-2*d*.
9. L. C. Washington. *Introduction to Cyclotomic Fields*. New York: Springer-Verlag, 1982.

AMS Classification Number: 11B68

❖❖❖