ARCHIVUM MATHEMATICUM (BRNO)
Tomus 35 (1999), 299 – 303

LEUDESDORF'S THEOREM AND BERNOULLI NUMBERS

I. Sh. Slavutskii

Abstract. For $m \in \mathbb{N}$, $(m,6)=1$, it is proved the relations between the sums

$$W(m,s)=\sum_{i=1,(i,m)=1}^{m-1} i^{-s}, \qquad s \in \mathbb{N},$$

and Bernoulli numbers. The result supplements the known theorems of C. Leudesdorf, N. Rama Rao and others. As the application it is obtained some connections between the sums $W(m,s)$ and Agoh's functions, Wilson quotients, the indices irregularity of Bernoulli numbers.

1. Denote $W(m,s)=\sum_{i=1,(i,m)=1}^{m-1} i^{-s}$ with $m,\ s \in \mathbb{N}$. As a generalization of the known Wolstenholme's theorem [11] C. Leudesdorf has proved

Theorem 1 [6].
$$W(m,1) \equiv 0 (\operatorname{mod} m^2),\ \ (m,6)=1\,.$$

Some extensions of the result is contained in the known monograph of G. H. Hardy and E. M. Wright ([4], Ch. VIII). See also [7].

Here we study the connection between the sums $W(m,s)$ and Bernoulli numbers (or Agoh's functions containing Bernoulli numbers). These relations may be considered as the further generalization of Leudesdorf's theorem.

2. First of all we will remind some notations. Below Bernoulli polynomials $B_n(x)$, $n \geq 0$, can be defined by

$$B_n(x)=\sum_{r=0}^{n}(n!/(r!(n-r)!))B_r x^{n-r}\,,$$

where Bernoulli numbers B_n are defined by the generating function

$$t/(e^t-1)=\sum_{n=0}^{\infty} B_n t^n/n!\,, \qquad |t|<2\pi\,.$$

1991 *Mathematics Subject Classification*: Primary 11A07; Secondary 11B68.
Key words and phrases: Wolstenholme-Leudesdorf theorem, p-integer number, Bernoulli number, Wilson quotient, irregular prime number.
Received November 18, 1997.

As known, $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_{2n+1} = 0$ for $n \in \mathbb{N}$ (see, e.g., [10], Ch. V or [3]). We will also use Agoh's functions

$$H_n(m) = \prod_{p|m} (1 - p^{n-1}) B_n\,, \qquad n \geq 0\,,$$

with the product taken over all primes divisors p of m. With the help of the functions it follows (see, e.g., [1],§2)

$$\sum_{i=1,(i,m)=1}^{m-1} i^n = \sum_{i=1}^{n+1} (n!/((i-1)!(n+1-i)!)) H_{n+1-i}(m) m^i / i\,. \tag{1}$$

Further, by Fermat-Euler theorem $1 \equiv i^{\varphi(m^2)} (\operatorname{mod} m^2), (m,i) = 1$, we have $i^{-s} \equiv i^t (\operatorname{mod} m^2)$ with $t = (\varphi(m^2) - 1)s$, so that

$$W(m,s) \equiv \sum_{i=1,(i,m)=1}^{m-1} i^t (\operatorname{mod} m^2)$$

or

$$W(m,s) \equiv \sum_{i=1}^{t+1} (t!/((i-1)!(t+1-i)!)) H_{t+1-i}(m) m^i / i (\operatorname{mod} m^2)\,. \tag{2}$$

Now, if $(m,6) = 1$ then for a prime number p with $p|m$ it follows that $p \geq 5$. Hence, by Staudt-Clausen theorem (for denominators of Bernoulli numbers) we obtain

$$\operatorname{ord}_p (B_{t+1-i} m^{i-2} / i) \geq 0$$

for $i \geq 3$ and for all prime numbers $p \geq 5$ with $p|m$. Thus, using the values of Agoh's functions $H_i(m)$ we conclude from the congruence (2) that

$$W(m,s) \equiv m \prod_{p|m} (1 - p^{t-1}) B_t + (tm^2/2) \prod_{p|m} (1 - p^{t-2}) B_{t-1} (\operatorname{mod} m^2)\,. \tag{3}$$

Now we are in position to prove

Theorem 2. *In the above notations it follows*

$$W(m,s) \equiv \left\{ \begin{array}{ll} m \prod_{p|m} (1 - p^{t-1}) B_t & \textit{for } 2|s \\ (t/2) m^2 \prod_{p|m} (1 - p^{t-2}) B_{t-1} & \textit{otherwise} \end{array} \right\} (\operatorname{mod} m^2)\,.$$

Proof. First suppose that $2|s$. Then $t-1$ is the odd number, $B_{t-1} = 0$ and the congruence (3) implies

$$W(m,s) \equiv m \prod_{p|m} (1 - p^{t-1}) B_t (\operatorname{mod} m^2)\,. \tag{4}$$

In the second case the number t is the odd number and we have

$$W(m,s) \equiv (t/s) m^2 \prod_{p|m} (1 - p^{t-2}) B_{t-1} (\operatorname{mod} m^2)\,. \tag{5}$$

□

The congruence (4) and (5) are contained all known generalizations of Leudesdorf's theorem.

Corollary 1.

(a) *If* $2|s$ *and* $(p,m)=1$ *for all prime numbers* p *such that* $(p-1)|s$, *then*

$$W(m,s) \equiv 0 \ (\operatorname{mod} m)\,. \tag{4'}$$

(b) *Let* s *be an odd number. If* 1) $p-1$ *don't divide* $s+1$ *for every prime number* p *with* $p|m$; *or* 2) $p|s$ *for all prime numbers* p *that* $(p-1)|(s+1)$ *and* $p|m$, *then it follows*

$$W(m,s) \equiv 0 \ (\operatorname{mod} m^2)\,. \tag{5'}$$

Indeed, in the case $2|s$ *the congruence (4') is the consequence of Staudt-Clausen theorem. On the other hand, if* s *is an odd number then:* 1) *for every prime number* p *with* $p|m$ *we have* $t-1 \equiv -(s+1)(\operatorname{mod}(p-1))$ *and (again by Staudt-Clausen theorem)* $\operatorname{ord}_p B_{t-1} \geq 0$ *provided that* $p-1$ *don't divide* $s+1$; 2) *for a prime number* p *with* $(p-1)|(s+1)$ *and* $p|m$ *we obtain that* $\operatorname{ord}_p(tB_{t-1}) = \operatorname{ord}_p(sB_{t-1}) \geq 0$. *In the both cases the congruence (5') follows.*

It is evident that the congruence (5') with $s=1$ contains Leudesdorf's theorem because $p>3$.

3. Consider now the special case. Namely, let be $m=p^l$, $l \in \mathbb{N}$ where $p \geq 5$ is a prime number. Then the congruence (4) implies

$$W(p^l,s) \equiv p^l B_t (\operatorname{mod} p^{2l})\,, \tag{6}$$

where $t=(\varphi(p^{2l})-1)s, 2|s$. If $(p-1)|s$ then $\operatorname{ord}_p B_t = -1$. So that denoting for a brevity $\alpha = \operatorname{ord}_p W(p^l,s)$, in this case we have $\alpha = l-1$. Otherwise, $\alpha \geq l$.

Turning now to the congruence (5) with an odd number s we obtain

$$W(p^l,s) \equiv (t/2)p^{2l}B_{t-1}(\operatorname{mod} p^{2l}),\ t=(\varphi(p^{2l})-1)s\,. \tag{7}$$

Further, if $s \equiv a(\operatorname{mod}(p-1))$ and $1 \leq a < p-2$ then

$$t-1 \equiv -(a+1)(\operatorname{mod}(p-1)), \qquad 2 \leq a+1 < p-1\,,$$

so that $\operatorname{ord}_p B_{t-1} \geq 0$ and from the congruence (7) we conclude that $\alpha \geq 2l$.

If $a=p-2$, e.g., $t-1 \equiv 0(\operatorname{mod}(p-1))$, then $\alpha \geq 2l$ for $p|s$ and $\alpha \geq 2l-1$ otherwise. Thus, we obtain

Corollary 2. *Let* s *be a natural number and* $s \equiv a(\operatorname{mod}(p-1))$, $1 \leq a \leq p-1$. *In the above notations we have*

- (i) $\alpha \geq 2l$ *for an odd natural* s *with* $1 \leq a < p-3$ *or for* $s \equiv p-2(\operatorname{mod}(p-1))$ *with* $p|s$;
- (ii) $\alpha \geq 2l-1$ *for* $s \equiv p-2(\operatorname{mod}(p-1))$ *and* $(p,s)=1$;
- (iii) $\alpha \geq l$ *for an even natural* s *with* $1 \leq a \leq p-3$;
- (iv) $\alpha = l-1$ *for* $s \equiv 0(\operatorname{mod}(p-1))$.

Remark. In theorem 4 of the paper [2] we can find the try of a proof of Corollary 2, but the cited paper, unfortunately, contains some mistakes (both in the formulations and in the proofs of the theorems).

4. Here we will indicate two examples of connections between the results and some "popular" objects of the theory of numbers.

I. It was recently proved the generalized Carlitz theorem ([9]). In particular, for Bernoulli numbers B_n with $(p-1)|n$ it was proved the congruence

$$pB_{b(p-1)p^{l-1}} \equiv p - 1 + bp^l w_p (\operatorname{mod} p^{l+1}) , \tag{8}$$

where p is an odd prime, b, $l \in \mathbb{N}$ and $w_p = ((p-1)! + 1)/p$ is Wilson quotient. Putting $s \equiv 0(\operatorname{mod}(p-1)p^{l-1})$ in the congruence (6) we obtain (with the help of the congruence (8)) that

$$W(p^l, s) \equiv p^l B_t \equiv p^{l-1}(p - 1 + ptw_p/(p-1))(\operatorname{mod} p^{2l})$$

or

$$W(p^l, s) \equiv p^{l-1}(p-1) - p^l sw_p/(p-1)(\operatorname{mod} p^{2l})$$

or

$$W(p^l, s) \equiv \varphi(p^l) + p^l sw_p (\operatorname{mod} p^{2l})$$

or

$$W(p^l, s)/p^l \equiv 1 - 1/p + sw_p (\operatorname{mod} p^l) \tag{9}$$

As above, here $t = (\varphi(p^{2l}) - 1)s$ and for rational numbers a, b the congruence $a \equiv b(\operatorname{mod} p^l)$ means that $\operatorname{ord}_p(a-b) \geq l$ for the p-integer number $a - b$, as usual.

These congruences supplement some known results of E. Lehmer [5] and others. Let now $s \equiv 0(\operatorname{mod}(p-1)p^{l-1})$ and $\operatorname{ord}_p s = l - 1$. As known, if $w_p \equiv 0(\operatorname{mod} p)$ then p is called Wilson prime number. Therefore, we can note that

$$W(p^l, s)/p^l \equiv 1 - 1/p(\operatorname{mod} p^l), \quad l \in \mathbb{N} , \quad \Longleftrightarrow p \text{ is Wilson prime number.}$$

II. Turn now to the congruence (6) with $l = 1$ and $s = a$, $2|a$, $2 \leq a \leq p-3$ (as above $p > 3$ is a prime number). Since by the known Staudt-Kummer congruence (see Slavutskii [8] for historical details and terminology)

$$B_t/t \equiv B_{p-1-a}/(p-1-a)(\operatorname{mod} p)$$

with $t = (p(p-1) - 1)a = (pa-1)(p-1) + (p-1-a)$ we obtain

$$pB_t \equiv apB_{p-1-a}/(a+1)(\operatorname{mod} p^2) ,$$

so from the congruence (6) it follows

$$W(p, a) \equiv apB_{p-1-a}/(a+1)(\operatorname{mod} p^2), \quad 2|a\,, \ 2 \leq a \leq p-3\,. \tag{10}$$

Further, as known, the pair (p, i) is called irregular if $\operatorname{ord}_p B_i \geq 1$ with $2 \leq i \leq p-3, 2|i$. Then the congruence (10) reduces to

Corollary 3. *For an even integer a with $a < p - 2$ and a prime number $p > 3$ it holds*

$$(p, p-1-a) \text{ is an irregular pair} \quad \Longleftrightarrow W(p, a) \equiv 0(\operatorname{mod} p^2)$$

(e.g., if the last congruence is valid for r such numbers a then the index of irregularity of p equals r).

References

[1] Agoh, T., Dilcher, K., Skula, L., *Wilson quotients for composite moduli*, Comp. Math. **67** (1998). No. 222, 843–861.

[2] Bayat, M., *A generalization of Wolstenholme's theorem*, Amer. Math. Monthly **109** (1997), 557–560.

[3] Dilcher, K., Skula, L., Slavutskii, I. Sh., *Bernoulli numbers. Bibliography (1713–1990)*, Queen's papers in Pure and Applied Mathematics, 1991, No. 87, 175 pp.; Appendix, Preprint (1994), 30 pp.

[4] Hardy, G. H., Wright, E. M., *An introduction to theory of numbers*, 5th ed., Oxford Sci. Publ., 1979.

[5] Lehmer, E., *On congruences involving Bernoulli numbers and quotients of Fermat and Wilson*, Ann. Math. **39** (2) (1938), 350–360.

[6] Leudesdorf, C., *Some results in the elementary theory of numbers*, Proc. London Math. Soc. **20** (1889), 199–212.

[7] Rama Rao, M., *An extention of Leudesdorf theorem*, J. London Math. Soc. **12** (1937), 247–250.

[8] Slavutskii, I., *Staudt and arithmetic properties on Bernoulli numbers*, Hist. Scient. **5** (1995), 70–74.

[9] Slavutskii, I., *About von Staudt congruences for Bernoulli numbers*, to appear.

[10] Washington, L. C., *Introduction to cyclotomic fields*, 2nd ed., Springer-Verlag, New York, 1997.

[11] Wolstenholme, J., *On certain properties of prime numbers*, Quart. J. Math. **5** (1862), 35–39.

St. Hamarva, 4, P.O.Box 23393
Akko, ISRAEL
E-mail: `nick1@luckynet.co.il`