Kangweon–Kyungki Math. Jour. **3** (1995), No. 2, pp. 143–152

MIRIMANOFF'S POLYNOMIAL, BERNOULLI NUMBERS AND FERMAT QUOTIENTS

Jae Moon Kim

§1. Introduction

Let p be an odd prime and $\mathbb{F}_p$ be the finite field with p elements. Let $f(t) = \frac{(1-t)^p - (1-t^p)}{p}$ be a polynomial in $\mathbb{F}_p[t]$. The polynomial $f(t)$ was first introduced by D. Mirimanoff in 1905 to show the following criterion on Fermat's last theorem(F.L.T.) (see [**1**]) : if p does not divide B_{p-7} or B_{p-9}, then the first case of F.L.T. holds, where B_n is the nth Bernoulli number. He also used the same polynomial $f(t)$ to prove the following striking theorem: if $2^{p-1} \not\equiv 1 \mod p^2$, then the first case of the F.L.T. holds. The only two exceptions for $p < 3 \times 10^9$ are 1093 and 3511. This theorem was first proved by A. Wieferich and thus named as Wieferich criterion. But Mirimanoff's proof is substantially simpler and more instructive. Actually he derived many more properties of $f(t)$ and proved that if $3^{p-1} \not\equiv 1 \mod p^2$, then the first case of the F.L.T. holds. A computation shows that for $p = 1093$ and 3511, $3^{p-1} \not\equiv 1 \mod p^2$. This guarantees that there are no integer solutions of $x^p + y^p + z^p = 0$ and $p \nmid xyz$ for all $p < 3 \times 10^9$.

For an integer a with $(a,p) = 1$, Fermat little theorem says that $a^{p-1} \equiv 1 \mod p$, hence $a^{p-1} - 1/p$ is an integer. We denote this integer by $q_p(a)$ and call it the Fermat quotient of a with base p. Thus we can rephrase Mirimanoff's result as follows: if either $q_p(2)$ or $q_p(3)$ is not congruent to 0 modulo p, then the first case of the F.L.T. is true. After Mirimanoff's work on F.L.T. with his polynomial $f(t)$, many other distinguished mathematicians such as Frobenius, Vandiver and Morishima extended Mirimanoff's result by studying vanishing of Fermat quotients $q_p(a) \mod p$ for various prime p's and a's.

In this paper, we introduce a new polynomial $g(t)$ in $\mathbb{F}_p[t]$ given by $g(t) = (1-t)^{p-2} + \frac{1}{2}(1-t)^{p-3} + \cdots + \frac{1}{p-1}$. We will also view $g(t)$

Received May 19, 1994.

This paper was supported by research fund of Inha University, 1993

as a polynomial in $\mathbb{Z}_p[t]$ whenever necessary, where $\mathbb{Z}_p$ is the ring of p-adic integers. Here $\frac{1}{k}$, for $1 \leq k \leq p-1$, means the multiplicative inverse of k in $\mathbb{F}_p$ (or $\mathbb{Z}_p$). This polynomial $g(t)$ is very closely related with the Mirimanoff's polynomial $f(t)$. Indeed we will show in section 2 that $f(t) \equiv tg(1-t) \mod p$. Thus values of $g(t)$ are related with Fermat quotients. For instance, by letting $t=-1$, we have $-g(2) \equiv f(-1) \equiv \frac{2^p-2}{p} \equiv 2q_p(2) \mod p$. Therefore the Fermat quotient $q_p(2) \equiv 0 \mod p$ iff $g(2) \equiv 0 \mod p$.

The aim of this paper is to examine properties of the polynomial $g(t)$ and to study special values of $g(t)$. They will turn out to be related with Bernoulli numbers and Fermat quotients. This paper is organized as follows. In the next section, we prove various properties of $g(t)$. The relations between $g(t)$ and $f(t)$ will be also discussed in the same section. In section 3, we study two applications of $g(t)$. One of them is to express certain generalized Bernoulli number in terms of a value of $g(t)$. The other is to examine the vanishing of the Fermat quotient $q_p(l)$ in terms of values of $g(t)$, where l is a prime such that $p \equiv 1 \pmod{l}$. To be precise, we will show that $q_p(l) \equiv \sum_{\substack{s\in R\\ s\neq 1\\ s^l=1}} g(s) \pmod{p}$, where $R = \{w \in \mathbb{Z}_p \mid w^{p-1}=1\}$ is the group of all $p-1$th roots of 1 in $\mathbb{Z}_p$. This can be thought of as a generalization of the following congruence discovered by Eisenstein (see[**2**]):

$$q_p(2) \equiv \frac{1}{2}\left(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{p-1}\right) \pmod{p}.$$

Indeed, if $l=2$, the sum $\sum_{\substack{s\in R\\ s^l=1\\ s\neq 1}} g(s)$ involves only one term $g(-1)$. But $g(-1) \equiv -\frac{1}{2}g(2) \equiv q_p(2) \mod p$ (proposition 1), which is clearly congruent to $\frac{1}{2}(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{p-1})$ modulo p.

§2. Mirimanoff's polynomial $f(t)$ and $g(t)$

In this section, we will describe some properties of $g(t)$. We will see, in proposition 1, that $g(t)$ comes from the Mirimanoff's polynomial which has been exhaustively studied since 1910's. The Mirimanoff's polynomial $f(t)$ is defined by $f(t) = \frac{(1-t)^p-(1-t^p)}{p}$ as a polynomial in

$\mathbb{F}_p[t]$. In the following lemma, some properties of $f(t)$ are given. For many other features of $f(t)$, we refer [**1**].

LEMMA 1.

(1) $t^p f(\frac{1}{t}) = -f(t)$.

(2) $f(1-t) = f(t)$.

(3) $f(t) \equiv -\sum_{i=1}^{p-1} \frac{1}{i} t^i \pmod{p}$.

(Proof) (1) and (2) can be easily checked from the definition of $f(t)$. We will prove (3).

$$\begin{aligned} f(t) &= \frac{(1-t)^p - (1-t^p)}{p} \\ &= \frac{\sum_{i=0}^{p} \binom{p}{i}(-t)^i - (1-t^p)}{p} \\ &= \frac{\sum_{i=1}^{p-1} \binom{p}{i}(-1)^i t^i}{p}. \end{aligned}$$

But

$$\begin{aligned} \frac{\binom{p}{i}}{p} &= \frac{p(p-1)\cdots(p-i+1)}{p \cdot i!} \\ &= \frac{p-1}{1} \cdot \frac{p-2}{2} \cdots \frac{p-i+1}{i-1} \cdot \frac{1}{i} \\ &\equiv (-1)^{i-1} \frac{1}{i} \pmod{p}, \end{aligned}$$

since $\frac{p-k}{k} \equiv -1 \pmod{p}$ when $(p,k) = 1$. Thus,

$$\begin{aligned} f(t) &\equiv \sum_{i=1}^{p-1} (-1)^{i-1} \frac{1}{i} (-1)^i t^i \pmod{p} \\ &= -\sum_{i=1}^{p-1} \frac{1}{i} t^i. \end{aligned}$$

By using these properties, we obtain the following congruences for $g(t)$.

PROPOSITION 1.

(1) $tg(1-t) \equiv f(t) \pmod p$.
(2) $tg(1-t) \equiv (1-t)g(t) \pmod p$.
(3) $g(t) \equiv t^{p-1}g(\frac{1}{t}) \pmod p$.

(Proof) (1) By (1) and (3) of the above lemma, we have

$$\begin{aligned} tg(1-t) &= t(t^{p-2} + \frac{1}{2}t^{p-3} + \cdots + \frac{1}{p-1}) \\ &= t^p(\frac{1}{t} + \frac{1}{2}\frac{1}{t^2} + \cdots + \frac{1}{p-1}\frac{1}{t^{p-1}}) \\ &\equiv -t^p f(\frac{1}{t}) \pmod p \\ &= f(t). \end{aligned}$$

(2) By lemma 1,(2) and proposition 1,(1) above, we obtain

$$tg(1-t) \equiv f(t) = f(1-t) \equiv (1-t)g(t) \pmod p.$$

(3) By applying above consequences appropriately, we get

$$(1-t)g(t) \equiv f(t) = -t^p f(\frac{1}{t}) \equiv -t^p(1-\frac{1}{t})g(\frac{1}{t}) = (1-t)t^{p-1}g(\frac{1}{t}).$$

Hence $g(t) \equiv t^{p-1}g(\frac{1}{t}) \pmod p$.

Let $R = \{w \in \mathbb{Z}_p \mid w^{p-1} = 1\}$ be the group of $p-1$th roots of 1 in the ring of p-adic integers $\mathbb{Z}_p$.

COROLLARY. *For $s \in R$, $g(s) \equiv g(\frac{1}{s}) \pmod p$.*

(Proof) Put $t = s$ in the congruence (3) of the above lemma. Since $s^{p-1} = 1$, we have $g(s) \equiv g(\frac{1}{s}) \mod p$.

PROPOSITION 2. *Let $s \neq \pm 1$ be any $p-1$th root of 1 in $\mathbb{Z}_p$. Then*

$$g(s) + g(-s) \equiv g(s^2) \pmod p$$

(Proof) Since $(1-t)g(t) \equiv f(t) \pmod{p}$, we have

$$\begin{aligned} g(s)+g(-s) &\equiv \frac{f(s)}{1-s}+\frac{f(-s)}{1+s} \pmod{p} \\ &= \frac{(1-s)^p-(1-s^p)}{p(1-s)}+\frac{(1+s)^p-(1+s^p)}{p(1+s)} \\ &= \frac{(1-s)^{p-1}-1}{p}+\frac{(1+s)^{p-1}-1}{p} \\ &= \frac{(1-s)^{p-1}+(1+s)^{p-1}-2}{p} \end{aligned}$$

Since $(1 \pm s)^{p-1} \equiv 1 \pmod{p}$ by Fermat little theorem, we have

$$((1-s)^{p-1}-1)((1+s)^{p-1}-1) \equiv 0 \pmod{p^2}.$$

From this, we obtain

$$(1-s)^{p-1}+(1+s)^{p-1}-2 \equiv (1-s^2)^{p-1}-1 \pmod{p^2}.$$

Hence

$$g(s)+g(-s) \equiv \frac{(1-s^2)^{p-1}-1}{p} \pmod{p}.$$

On the other hand, since $s^{2p}=s^2$,

$$\begin{aligned} g(s^2) &\equiv \frac{(1-s^2)^p-(1-s^{2p})}{p(1-s^2)} \pmod{p} \\ &= \frac{(1-s^2)^{p-1}-1}{p}. \end{aligned}$$

Therefore, $g(s)+g(-s) \equiv g(s^2) \pmod{p}$.

§3. Generalized Bernoulli numbers and Fermat quotients

In this section, we study two applications of the Mirimanoff's polynomial $g(t)$. First, we relate certain generalized Bernoulli number with a special value of $g(t)$. Let p be an odd prime such that $p \equiv 1 \pmod{5}$ and let χ be the nontrivial even character of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, where ζ_5 is a primitive 5th root of 1, i.e., $\chi = \left(\frac{\cdot}{5}\right)$ is the quadratic character.

PROPOSITION 3. *Let ω be the Teichmüller character of $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Then,*

$$B_{1,\chi\omega^{-1}} \equiv 2 \sum_{k=0}^{(p-6)/5} \frac{1}{5k+2} \mod p.$$

(Proof) For any Dirichlet character ρ, we know $B_{1,\rho} = \frac{1}{f}\sum_{a=1}^{f} a\rho(a)$ where f is the conductor of the character ρ (see [**3**]). Since the conductor of the character $\chi\omega^{-1}$ is $5p$, we have

$$\begin{aligned} B_{1,\chi\omega^{-1}} &= \frac{1}{5p} \sum_{0\le a<5p} a\chi\omega^{-1}(a) \\ &= \frac{1}{5p} \sum_{\substack{0\le x\le 4 \\ 0\le y\le p-1}} (xp+y)\chi(xp+y)\omega^{-1}(xp+y). \end{aligned}$$

Since $xp+y \equiv x+y \mod 5$, and since $xp+y \equiv y \mod p$, we obtain

$$\begin{aligned} B_{1,\chi\omega^{-1}} &= \frac{1}{5p} \sum_{\substack{0\le x\le 4 \\ 0\le y\le p-1}} (xp+y)\chi(x+y)\omega^{-1}(y) \\ &= \frac{1}{5} \sum_{\substack{0\le x\le 4 \\ 0\le y\le p-1}} x\chi(x+y)\omega^{-1}(y) + \frac{1}{5p} \sum_{\substack{0\le x\le 4 \\ 0\le y\le p-1}} y\chi(x+y)\omega^{-1}(y). \end{aligned}$$

But $\sum_{0\le x\le 4} \chi(x+y) = 0$, and $\omega^{-1}(y) \equiv y^{-1} \mod p$ if $(y,p) = 1$. Thus,

$$\begin{aligned} &B_{1,\chi\omega^{-1}} \\ &\equiv \frac{1}{5} \sum_{\substack{0\le x\le 4 \\ 1\le y\le p-1}} x\chi(x+y)\frac{1}{y} + \frac{1}{5p} \sum_{0\le y\le p-1} y\omega^{-1}(y) \sum_{0\le x\le 4} \chi(x+y) \pmod p \\ &= \frac{1}{5} \sum_{1\le y\le p-1} \frac{1}{y} \sum_{0\le x\le 4} x\chi(x+y). \end{aligned}$$

Since χ is the quadratic character $\left(\frac{\cdot}{5}\right)$, we have $\chi(1) = \chi(4) = 1$, and $\chi(2) = \chi(3) = -1$. Hence

$$\sum_{0 \le x \le 4} x\chi(x+y) = \begin{cases} 0 & \text{if } y \equiv 1 \text{ or } 3 \pmod 5 \\ 5 & \text{if } y \equiv 2 \pmod 5 \\ -5 & \text{if } y \equiv 4 \pmod 5). \end{cases}$$

Therefore,

$$\begin{aligned} B_{1,\chi\omega^{-1}} &\equiv \frac{1}{5}\left(\sum_{\substack{1 \le y \le p-1 \\ y \equiv 2 \mod 5}} \frac{1}{y} \cdot 5 + \sum_{\substack{1 \le y \le p-1 \\ y \equiv 4 \mod 5}} \frac{1}{y} \cdot (-5) \right) \pmod p \\ &= \left(\frac{1}{2} + \frac{1}{7} + \cdots + \frac{1}{p-4}\right) + \left(-\frac{1}{4} - \frac{1}{9} - \cdots - \frac{1}{p-2}\right) \\ &\equiv \left(\frac{1}{2} + \frac{1}{7} + \cdots + \frac{1}{p-4}\right) + \left(\frac{1}{p-4} + \frac{1}{p-9} + \cdots + \frac{1}{2}\right) \pmod p \\ &= 2\sum_{k=0}^{(p-6)/5} \frac{1}{5k+2}. \end{aligned}$$

This completes the proof.

Let s be a primitive 5th root in $\mathbb{Z}_p$. In the following theorem, we interpret $B_{1,\chi\omega^{-1}}$ by the special value $g(-s)$.

THEOREM 1. $g(-s)^2 \equiv \frac{5}{4} {B_{1,\chi\omega^{-1}}}^2 \pmod p$.

(Proof) First, we calculate $sg(1-s)$. Since $s^5 = 1$ in $\mathbb{Z}_p$, $s^{5k+i} = s^i$ for any integers k and i. Thus, we get

$$\begin{aligned} sg(1-s) &= s^{p-1} + \frac{1}{2}s^{p-2} + \cdots + \frac{1}{p-1}s \\ &= \left(1 + \frac{1}{6} + \cdots + \frac{1}{p-5}\right) + \left(\frac{1}{2} + \frac{1}{7} + \cdots + \frac{1}{p-4}\right)s^4 \\ &\quad + \left(\frac{1}{3} + \frac{1}{8} + \cdots + \frac{1}{p-1}\right)s^3 + \left(\frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{p-2}\right)s^2 \\ &\quad + \left(\frac{1}{5} + \frac{1}{10} + \cdots + \frac{1}{p-1}\right)s. \end{aligned}$$

Let $A_i = \frac{1}{i} + \frac{1}{i+5} + \cdots + \frac{1}{p-6+i}$ for $i = 1, 2, 3, 4, 5$. Then we have the following congruences

$$\begin{aligned}
A_3 &= \frac{1}{3} + \frac{1}{8} + \cdots + \frac{1}{p-3} \\
&\equiv -\left(\frac{1}{p-3} + \frac{1}{p-8} + \cdots + \frac{1}{3}\right) = -A_3 \pmod{p}, \\
A_4 &= \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{p-2} \\
&\equiv -\left(\frac{1}{p-4} + \frac{1}{p-9} + \cdots + \frac{1}{2}\right) = -A_2 \pmod{p}, \\
A_5 &= \frac{1}{5} + \frac{1}{10} + \cdots + \frac{1}{p-1} \\
&\equiv -\left(\frac{1}{p-5} + \frac{1}{p-10} + \cdots + 1\right) = -A_1 \pmod{p}.
\end{aligned}$$

Hence we have $A_3 \equiv 0$, $A_4 \equiv -A_2$ and $A_5 \equiv -A_1 \mod p$. Therefore,

$$\begin{aligned}
sg(1-s) &= A_1 + A_2 s^4 + A_3 s^3 + A_4 s^2 + A_5 s \\
&\equiv A_1 + A_2 s^4 - A_2 s^2 - A_1 s \pmod{p} \\
&= A_1(1-s) - A_2 s^2 (1+s)(1-s) \\
&= (1-s)(A_1 - A_2 s^2 - A_2 s^3).
\end{aligned}$$

Since $(1-s)g(s) \equiv sg(1-s) \mod p$ for $s \in R = \{w \in \mathbb{Z}_p \mid w^{p-1} = 1\}$ and since $1 - s \not\equiv 1 \mod p$ for the primitive 5th root s in $\mathbb{Z}_p$, we conclude that

$$g(s) \equiv A_1 - A_2 s^2 - A_2 s^3 \pmod{p}$$

for the primitive 5th root $s \in \mathbb{Z}_p$.

If s is a primitive 5th root in $\mathbb{Z}_p$, then s^2 is also a primitive 5th root in $\mathbb{Z}_p$. And we know that $g(-s) \equiv g(s^2) - g(s) \pmod{p}$ by proposition 2 of section 2. Thus

$$\begin{aligned}
g(-s) &\equiv g(s^2) - g(s) \pmod{p} \\
&\equiv (A_1 - A_2 s^4 - A_2 s^6) - (A_1 - A_2 s^2 - A_2 s^3) \pmod{p} \\
&= A_2(s^2 + s^3 - s^4 - s).
\end{aligned}$$

Since $(s^2+s^3-s^4-s)^2 = 5$ and since $A_2 \equiv \frac{1}{2}B_{1,\chi\omega^{-1}} \pmod p$ by proposition 3, we have

$$g(-s)^2 \equiv {A_2}^2 \cdot 5 \equiv \frac{5}{4}(B_{1,\chi\omega^{-1}})^2 \pmod p$$

as desired.

Finally we prove a criterion on the vanishing of the Fermat quotient $q_p(l)$, where l is a prime satisfying $p \equiv 1 \pmod l$.

THEOREM 2. $q_p(l) \equiv \sum\limits_{\substack{s\in R\\ s\neq 1\\ s^l=1}} g(s) \mod p.$

(Proof) Let $s \neq 1$ be a $p-1$th root of 1 in $\mathbb{Z}_p$ and put $t = 1-s$ in the equation (1) of proposition 1. Then we get

$$\begin{aligned}(1-s)g(s) &\equiv f(1-s)\\ &\equiv f(s)\\ &\equiv \frac{(1-s)^p-(1-s^p)}{p}\\ &\equiv \frac{(1-s)^p-(1-s)}{p}.\end{aligned}$$

Hence $g(s) \equiv \dfrac{(1-s)^{p-1}-1}{p} \mod p.$

Therefore

$$(1-s)^{p-1} \equiv 1+g(s)p \mod p^2.$$

Now let $s \neq 1$ run over all lth roots of 1 in $\mathbb{Z}_p$ to obtain

$$\prod_{\substack{s\in R\\ s^l=1\\ s\neq 1}}(1-s)^{p-1} \equiv \prod_{\substack{s\in R\\ s^l=1\\ s\neq 1}}(1+g(s)p) \mod p^2.$$

Since the left hand side is l^{p-1}, we have

$$l^{p-1} \equiv 1+\Big(\sum_{\substack{s\in R\\ s^l=1\\ s\neq 1}} g(s)\Big)p \mod p^2.$$

Therefore $q_p(l) = \frac{l^{p-1}-1}{p} \equiv \sum g(s) \mod p.$

References

[1] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.
[2] P. Ribenboim, *The little book of big primes*, Springer-Verlag, 1991.
[3] L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.

Department of Mathematics
Inha University
Incheon, 402–751, Korea