Acta Mathematica et Informatica Universitatis Ostraviensis

Ladislav Skula

Fermat and Wilson quotients for p-adic integers

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 167--181

Persistent URL: http://dml.cz/dmlcz/120531

Acta Mathematica et Informatica Universitatis Ostraviensis 6 (1998) 167-181

Fermat and Wilson Quotients for p-Adic Integers

Ladislav Skula

Abstract: Using the p-adic limit, the notions of Fermat and Wilson quotients for composite moduli are transferred to those for p-adic integers. Some theorems on these quotients are presented which in particular are analogous to results of Eisenstein, Lerch, Friedmann and Tamarkine.
Key Words: Fermat quotient, Euler quotient, Wilson quotient, p-adic numbers.
Supported by the Grant Agency of the Czech Republic, No. 201/97/0433

Mathematics Subject Classification: Primary 11A07; Secondary 11S80, 11B68

1. Introduction

Let p be a prime and a an integer not divisible by p. As it is well-known the *Fermat quotient of p with base a* is the integer

$$q\{a,p) = \frac{{}_a\mathbf{p}\text{-}\mathbf{i}\ \_\ \mathbf{j}}{V}.$$

The first generál statements on this quotient are due to Eisenstein ([E], 1850):

(El) *If p is odd, then*

$$2g(2,p) = \wedge_{\mathbf{n=l}}^{P-I} (\sim {}^1) {}^{n\,"\,1} \sim ({}^{m\,o\,d} \wedge$$

$$(= - V - \pmod p)).$$

(E2) *If u,v are integers and p\ uv, then*

$$q\{uv,p) = q(u,p) + q(v,p) \pmod p$$

(the "logarithmic property").

(E3) *// u,v* G Z *and p\u, then*

$$q(u + pv,p) = q(u,p) - \frac{v}{u} \pmod p.$$

As a corollary of (E3) we have for integers $a, b, p \nmid ab$:

$$a \equiv b \pmod{p^2} \implies q(a,p) \equiv q(b,p) \pmod{p}.$$

Thus by (E2) we can consider the function $q(\ ,p)$ as a homomorphism from the multiplicative group $((\mathbf{Z}/p^2\mathbf{Z})^*, \cdot)$ into the additive group $(\mathbf{Z}/p\mathbf{Z}, +)$ of the respective residue class rings.

According to Euler's well-known theorem generalizing Fermat's little theorem we can define for relatively prime integers $m \geq 2$ and a the ***Euler quotient*** (or the (*generalized*) *Fermat quotient for composite moduli*) of m with base a by

$$q(a,m) = \frac{a^{\varphi(m)} - 1}{m}.$$

For this quotient similar laws are satisfied as (E1) - (E3). In [ADS1] the Fermat quotient for composite moduli m is investigated in more detail. Some formulas presented there for the case $m = p^n$ directly invite to use a limit process and to transfer this notion to the p-adic case. This is established in Section 3 in greater detail by means of the projective limit. In Section 4 Lerch's expression of the Fermat quotient is transferred to the p-adic case and in Section 6 the Friedmann-Tamarkine congruence is presented for the Fermat quotient for p-adic integers.

Similarly, the notion of the Wilson quotient is transferred to the p-adic case by means of the p-adic limit in Section 5. Here a theorem (Theorem 5.7) is derived presenting this "p-adic" Wilson quotient by means of the p-adic limit of expressions containing certain Bernoulli numbers.

The reader is referred for the basic facts on p-adic numbers to the book [BS] and for the theory of projective systems to the book [K].

2. Notations and Fundamental Assertions

Throughout this paper we will use the following notations:

- p a prime,
- n a positive integer,
- $\mathbf{Z}$ the ring of (rational) integers,
- $\mathbf{Z}(n)$ the additive group of the ring of residue classes mod p^n, thus $\mathbf{Z}(n) = (\mathbf{Z}/p^n\mathbf{Z}, +)$,
- $\mathbf{Z}(n)^*$ the multiplicative group of the invertible elements of the ring of residue classes mod p^n, thus $\mathbf{Z}(n)^* = ((\mathbf{Z}/p^n\mathbf{Z})^*, \cdot)$,
- φ_n the canonical (ring) homomorphism from the ring $(\mathbf{Z}/p^{n+1}\mathbf{Z}, +, \cdot)$ onto the ring $(\mathbf{Z}/p^n\mathbf{Z}, +, \cdot)$; this homomorphism will be also considered as (group) homomorphism from the group $\mathbf{Z}(n+1)$ onto the group $\mathbf{Z}(n)$ or from the group $\mathbf{Z}(n+1)^*$ onto the group $\mathbf{Z}(n)^*$,
- $(\mathbf{Z}_p, +, \cdot)$ the ring of p-adic integers with p-adic topology,
- $\mathbf{Z}_p$ the additive group of the ring $(\mathbf{Z}_p, +, \cdot)$,
- $\mathbf{Z}_p^*$ the multiplicative group of the invertible elements of the ring $(\mathbf{Z}_p, +, \cdot)$,
- ψ_n the canonical (ring) homomorphism from the ring $(\mathbf{Z}_p, +, \cdot)$ onto the ring $(\mathbf{Z}/p^n\mathbf{Z}, +, \cdot)$, also considered as the group homomorphism from the group

$\mathbf{Z}_p$ onto the group $\mathbf{Z}(n)$ or from the group $\mathbf{Z}_p^*$ onto the group $\mathbf{Z}(n)^*$, thus for $\alpha = \sum_{i=0}^{\infty} a_i p^i \in \mathbf{Z}_p$ ($a_i \in \mathbf{Z}$, $0 \le a_i < p$) we have $\psi_n(\alpha) = \sum_{i=0}^{n-1} a_i p^i + p^n\mathbf{Z}$,

$v(\alpha)$ the p-adic exponent of a p-adic integer α,

$\lim_{k\to\infty} \alpha_k$ the p-adic limit for p-adic integers α_k, similarly all topological notions (continuity, convergence, infinite series, etc.) concern the p-adic topology,

$q(a, p^n)$ the Fermat quotient of (composite moduli) p^n (the Euler quotient of p^n) with base a ($a \in \mathbf{Z}, p \nmid a$) (see, e.g. [ADS1]), thus $q(a,p^n) = \frac{a^{p^{n-1}(p-1)}-1}{p^n}$.

Since for each p-adic integer α not divisible by p we have

$$\alpha^{p^{n-1}(p-1)} \equiv 1 \pmod{p^n},$$

the p-adic number $q(\alpha,p^n) = \frac{\alpha^{p^{n-1}(p-1)}-1}{p^n}$ is p-adic integer. In this way the former function $q(\ ,p^n)$ is extended to all p-adic integers not divisible by p.

Proposition 2.1. *(a) The function $q(\ ,p^n)$ is a uniformly continuous mapping from $\mathbf{Z}_p^*$ into $\mathbf{Z}_p$.*

If we assume that $\alpha, \beta \in \mathbf{Z}_p^*$, then we have:

(b)
$$q(\alpha,p^n) \equiv q(\beta,p^n) \pmod{p^n}$$

provided that $\alpha \equiv \beta \pmod{p^{n+1}}$,

(c)
$$q(\alpha\beta,p^n) \equiv q(\alpha,p^n) + q(\beta,p^n) \pmod{p^n}.$$

Proof. For $\alpha, \beta \in \mathbf{Z}_p^*$ there exists $\gamma \in \mathbf{Z}_p$ such that $\alpha^{p^{n-1}(p-1)} - \beta^{p^{n-1}(p-1)} = (\alpha - \beta)\gamma$, hence

$$v(q(\alpha,p^n) - q(\beta,p^n)) \ge v(\alpha - \beta) - n.$$

This proves part (a). Part (b) is obvious and part (c) follows from (b) and the logarithmic property for the Fermat quotient of p^n. □

Notation. Let $A = a + p^{n+1}\mathbf{Z} \in \mathbf{Z}(n+1)^*$, $a \in \mathbf{Z}$, $p \nmid a$. Put $q_n(A) = q(a,p^n) + p^n\mathbf{Z} \in \mathbf{Z}(n)$. Using Proposition 2.1 (b), (c) we get that q_n *is a group homomorphism from the group* $\mathbf{Z}(n+1)^*$ *into the group* $\mathbf{Z}(n)$.

Proposition 2.2. *(a) Let p be an odd prime or $p = 2$ and $n = 1$. Then q_n is surjective and for $A \in \mathbf{Z}(n+1)^*$ we have $q_n(A) = 0$ if and only if $A^{p-1} = 1$.*

(b) Let $p = 2$ and $n \ge 2$. Then $q_n(\mathbf{Z}(n+1)^*) = 2\mathbf{Z}(n)$ and for $A \in \mathbf{Z}(n+1)^*$ we have $q_n(A) = 0$ if and only if $A = \pm 1$.

(The symbols 0 and 1 denote the zero element and the unity in the rings of residue classes mod p^n and mod p^{n+1}, respectively.)

Proof. In case (a) we have, by property (E3), $q(1+p,p^n) \equiv -1 \pmod{p}$, hence $p \nmid q(1+p,p^n)$. Using the logarithmic property of the Fermat quotient of p^n and the existence of a primitive root mod p^n we get that q_n is surjective and $q_n(A) = 0$ for an element $A \in \mathbf{Z}(n+1)^*$ if and only if $A^{p-1} = 1$.

For $n \ge 2$ we have $q(5, 2^n) = 2k$ for an odd integer k. Let $a \in \mathbf{Z}$, $2 \nmid a$. Then there exists an integer x such that $0 \le x \le 2^{n-1} - 1$ and $a \equiv \pm 5^x \pmod{2^{n+1}}$, which implies $q(a,2^n) \equiv xq(5,2^n) \pmod{2^n} = 2kx$, and we are done. □

Proposition 2.3. *With exception of the case $p = 2$ and $n = 1$ we have*

$$q(\alpha, p^{n+1}) \equiv q(\alpha, p^n) \ (mod\ p^n)$$

for each $\alpha \in \mathbf{Z}_p^*$.

Proof. Since $2 | q(\alpha, 2^n)$ for each odd α and $n \geq 2$, we get the proposition from Proposition 4.1 of ([ADS1]) for $\alpha \in \mathbf{Z}$ $(p \nmid \alpha)$. Using Proposition 2.1 (b) we obtain the general case. □

Immediately from this proposition we get:

Proposition 2.4. *If p is odd or $p = 2$ and $n \geq 2$, then the following diagram is commutative:*

$$\begin{tikzcd}
\mathbf{Z}(n+1)^* \arrow[r, "q_n"] & \mathbf{Z}(n) \\
\mathbf{Z}(n+2)^* \arrow[r, "q_{n+1}"] \arrow[u, "\varphi_{n+1}"] & \mathbf{Z}(n+1) \arrow[u, "\varphi_n"']
\end{tikzcd}$$

3. Fermat Quotient for p-Adic Integers

Let $\mathcal{I}$ be the set of all positive integers in the case where p is odd and the set of all integers ≥ 2 in the case $p = 2$. For $m, n \in \mathcal{I}$, $m \geq n$ denote by φ_n^m the (group) homomorphism $\varphi_n^m = \varphi_n \circ \varphi_{n+1} \circ \cdots \circ \varphi_m$. Then $\{\mathcal{I}, \mathbf{Z}(n), \varphi_n^m\}$ is a projective system whose projective limit is given by the family of (group) homomorphisms $\{\psi_n : \mathbf{Z}_p \to \mathbf{Z}(n) | n \in \mathcal{I}\}$. According to Proposition 2.4 the following diagram is commutative for each $n \in \mathcal{I}$:

$$\begin{tikzcd}
 & \mathbf{Z}(n) \\
\mathbf{Z}_p^* \arrow[ur, "q_n \circ \psi_{n+1}"] \arrow[dr, "q_{n+1} \circ \psi_{n+2}"'] & \\
 & \mathbf{Z}(n+1) \arrow[uu, "\varphi_n"']
\end{tikzcd}$$

Using the properties of the projective limit we can state:

Theorem 3.1. *There exists a unique continuous homomorphism q from the group $\mathbf{Z}_p^*$ into the group $\mathbf{Z}_p$ such that the following diagram is commutative for each $n \in \mathcal{I}$:*

$$\begin{tikzcd}
\mathbf{Z}(n+1)^* \arrow[r, "q_n"] & \mathbf{Z}(n) \\
\mathbf{Z}_p^* \arrow[r, dashed, "q"] \arrow[u, "\psi_{n+1}"] & \mathbf{Z}_p \arrow[u, "\psi_n"']
\end{tikzcd}$$

Definition 3.1 The mapping q in Theorem 3.1 will be called the *Fermat quotient for the p-adic integers*, or simply *p-adic Fermat quotient.*

Using the definition of q and Proposition 2.2 we can derive the following theorem:

Theorem 3.2. *(a) For $p \neq 2$ the mapping q is surjective and for $\alpha \in \mathbf{Z}_p^*$ we have $q(\alpha) = 0$ if and only if $\alpha^{p-1} = 1$.*

(b) If $p = 2$, then $q(\mathbf{Z}_2^*) = 2\mathbf{Z}_2$ and for $\alpha \in \mathbf{Z}_2^*$ we have $q(\alpha) = 0$ if and only if $\alpha = \pm 1$.

Theorem 3.3. *(a) We have for each $\alpha \in \mathbf{Z}_p^*$ and each $n \in \mathcal{I}$*

$$q(\alpha) \equiv q(\alpha, p^n) \ (mod\ p^n).$$

(b) The sequence of mappings $\{q(\ ,p^n)\}_{n-1}^{\infty}$ converges uniformly to the mapping q.

(c) The mapping q is uniformly continuous.

Proof. According to Proposition 2.3 there exists $\lim_{\nu \to \infty} q(\alpha, p^\nu)$ for each $\alpha \in \mathbf{Z}_p^*$, which will be denoted by $f(\alpha)$. By Proposition 2.1 (c) f is a homomorphism from the group $\mathbf{Z}_p^*$ into the group $\mathbf{Z}_p$.

Assume that $n \in \mathcal{I}$ and $\alpha \in \mathbf{Z}_p^*$. Then there exists an integer $m \geq n$ such that $v(f(\alpha) - q(\alpha, p^m)) \geq n$. Using Proposition 2.3 we get

$$v(f(\alpha) - q(\alpha, p^n)) \geq \min\{v(f(\alpha) - q(\alpha, p^m)), v(q(\alpha, p^m) - q(\alpha, p^n)\} \geq n,$$

from which we obtain that the sequence $\{q(\ ,p^n)\}_{n=1}^{\infty}$ converges uniformly to f and $f(\alpha) \equiv q(\alpha, p^n) \pmod{p^n}$.

Since the p-adic valuation v is non-Archimedean ([BS], Chapt. 1, Sec. 4, Ex. 4) and $q(\ ,p^n)$ are uniformly continuous (Proposition 2.1 (a)), the mapping f is uniformly continuous.

It is easy to see (Proposition 2.1 (b)) that for each $n \in \mathcal{I}$ the following diagram is commutative:

$$\begin{tikzcd}
\mathbf{Z}(n+1)^* \arrow[r, "q_n"] & \mathbf{Z}(n) \\
\mathbf{Z}_p^* \arrow[u, "\psi_{n+1}"] \arrow[r, "f"] & \mathbf{Z}_p \arrow[u, "\psi_n"']
\end{tikzcd}$$

The result follows from the uniqueness of q. □

In the following theorem we use the symbol log for the p-adic logarithm and we apply *Leopoldt's* formula ([Lp],(0))

$$\log H = \lim_{n \to \infty} \frac{H^{p^n} - 1}{p^n}$$

to the p-adic integer $H = \alpha^{p-1}$, where $\alpha \in \mathbf{Z}_p^*$:

Theorem 3.4. *If $\alpha \in \mathbf{Z}_p^*$, then*

$$q(\alpha) = \frac{\log \alpha^{p-1}}{p}.$$

4. Lerch's Expression for the Fermat Quotient

In his paper [Lr1] in 1905, Lerch presented the following expression for the Fermat quotient of an odd prime with base a $(a \in \mathbf{Z}, p \nmid a)$:

$$aq(a,p) \equiv \sum_{x=1}^{p-1} \frac{1}{x}\left[\frac{ax}{p}\right] \pmod p. \tag{L1}$$

This form was generalized by Lerch in [Lr2] (1906) for Fermat quotients of composite moduli m $(m \in \mathbf{Z}, m \geq 2)$ for base a $(a \in \mathbf{Z}, (m,a) = 1))$:

$$aq(a,m) = a\frac{a^{\varphi(m)}-1}{m} \equiv \sum_{x=1}^{m} \frac{1}{x}\left[\frac{ax}{m}\right] \pmod m \tag{L2}$$

(see [ADS1], Theorem 2.3 and Historical remarks, p.34).

To state an analogous formula for the Fermat quotient q we will define for a p-adic number $\xi = \sum_{i=-m}^{\infty} x_i p^i$ $(x_i \in \mathbf{Z}, 0 \leq x_i \leq p-1, m \in \mathbf{Z},\ m \geq 0)$ the integral part $[\xi]_p$ of ξ with respect to p by

$$[\xi]_p = \sum_{i=0}^{\infty} x_i p^i \in \mathbf{Z}_p.$$

Clearly, if $\omega \in \mathbf{Z}$, then $\left[\frac{\omega}{p^n}\right]_p = \left[\frac{\omega}{p^n}\right]$.

Theorem 4.1. *If $\alpha \in \mathbf{Z}_p^*$, then*

$$\alpha q(\alpha) = \lim_{\nu\to\infty} \sum_{\substack{x=1\\ p\nmid x}}^{p^\nu} \frac{1}{x}\left[\frac{\alpha x}{p^\nu}\right]_p.$$

Proof. Assume that $\alpha \in \mathbf{Z}_p^*$, $\beta \in \mathbf{Z}$ and $\alpha \equiv \beta \pmod{p^{2n}}$. Using Proposition 2.1 (b) and (L2) we get

$$\alpha q(\alpha, p^n) \equiv \sum_{\substack{x=1\\ p\nmid x}}^{p^n} \frac{1}{x}\left[\frac{\beta x}{p^n}\right] \pmod{p^n}.$$

Since $\alpha x \equiv \beta x \pmod{p^{2n}}$ for each rational integer x, there exists $\gamma = \gamma(x) \in \mathbf{Z}_p$ such that $\frac{\alpha x}{p^n} = \frac{\beta x}{p^n} + p^n\gamma$, therefore $\left[\frac{\alpha x}{p^n}\right]_p \equiv \left[\frac{\beta x}{p^n}\right] \pmod{p^n}$ and

$$\alpha q(\alpha, p^n) \equiv \sum_{\substack{x=1\\ p\nmid x}}^{p^n} \frac{1}{x}\left[\frac{\alpha x}{p^n}\right]_p \pmod{p^n}.$$

The result follows. $\square$

Notation. For integers N, k ($N \geq 1, p \nmid N, 0 \leq k \leq N-1$), put

$$s(k,N,n) = \sum_{\substack{\frac{p^n}{N}k < x < \frac{p^n}{N}(k+1) \\ p \nmid x}} \frac{1}{x}.$$

Then Lerch's formula (L2) for Fermat quotient of p^n for base N can be expressed in the following way:

$$Nq(N,p^n) \equiv \sum_{k=0}^{N-1} ks(k,N,n) \pmod{p^n}.$$

Thus we can state:

Theorem 4.2. *If N is a positive integer ($p \nmid N$), then*

$$Nq(N) = \lim_{\nu\to\infty} \sum_{k=0}^{N-1} ks(k,N,\nu).$$

Corollary 4.3. *Let $N \in \{1,2,3,4,6\}$, $0 \leq k \leq N-1$ ($k \in \mathbf{Z}$). Then there exists $\lim_{\nu\to\infty} s(k,N,\nu) = s(k,N)$ and we have*

(a) $s(0,1) = 0$,
(b) $s(1,2) = -s(0,2) = 2q(2)$,
$s(3,4) = -s(0,4) = 3q(2)$,
$s(1,4) = -s(2,4) = q(2)$, *for* $p \neq 2$,
(c) $s(2,3) = -s(0,3) = \frac{3}{2}q(3)$,
$s(1,3) = 0$, *for* $p \neq 3$,
(d) $s(5,6) = -s(0,6) = 2q(2) + \frac{3}{2}q(3)$,
$s(1,6) = -s(4,6) = 2q(2)$,
$s(3,6) = -s(2,6) = 2q(2) - \frac{3}{2}q(3)$, *for* $p \geq 5$.

Proof. The result follows from the congruence

$$s(k,N,n) \equiv -s(N-1-k,N,n) \pmod{p^n}$$

and from Theorem 4.2. □

Remark. For $N = 5$ or $N \geq 7$ ($N \in \mathbf{Z}$) the question which sequences

$$\{s(k,N,\nu)\}_{\nu=1}^{\infty}$$

are convergent ($0 \leq k \leq N-1$) remains an open problem.

Lemma 4.4. *Let N be a positive integer, $p \nmid N$ and suppose there exists*

$$\lim_{n\to\infty} s(0,N,n) = \sigma.$$

Then

$$\sum_{\nu=0}^{\infty}\left(\sum_{\substack{\frac{p^{\nu}}{N}<x<\frac{p^{\nu+1}}{N}\\ p\nmid x}}\frac{1}{x}\right)=\sigma.$$

Proof. Put

$$\sigma_\nu=\sum_{\substack{\frac{p^{\nu}}{N}<x<\frac{p^{\nu+1}}{N}\\ p\nmid x}}\frac{1}{x}$$

for each non-negative integer ν. Then the nth partial sum of the series $\sum_{\nu=0}^{\infty}\sigma_\nu$ equals

$$\sum_{\nu=0}^{n-1}\sigma_\nu=\sum_{\substack{1\le x<\frac{p^{n}}{N}\\ p\nmid x}}\frac{1}{x}=s(0,N,n)$$

and the result follows. □

Corollary 4.5.
(a) If $p\neq 2$, then

$$2q(2)=-\sum_{\nu=0}^{\infty}\left(\sum_{\substack{\frac{p^{\nu}}{2}<x<\frac{p^{\nu+1}}{2}\\ p\nmid x}}\frac{1}{x}\right),\ 3q(2)=-\sum_{\nu=0}^{\infty}\left(\sum_{\substack{\frac{p^{\nu}}{4}<x<\frac{p^{\nu+1}}{4}\\ p\nmid x}}\frac{1}{x}\right).$$

(b) If $p\neq 3$, then

$$3q(3)=-2\sum_{\nu=0}^{\infty}\left(\sum_{\frac{p^{\nu}}{3}<x<\frac{p^{\nu+1}}{3}}\frac{1}{x}\right).$$

(c) If $p\geq 5$, then

$$q(2^4\cdot 3^3)=4q(2)+3q(3)=-2\sum_{\nu=0}^{\infty}\left(\sum_{\substack{\frac{p^{\nu}}{6}<x<\frac{p^{\nu+1}}{6}\\ p\nmid x}}\frac{1}{x}\right).$$

5. Wilson Quotients for the p-Adic Case

Definition 5.1. Let $m \geq 2$ be an integer and $\varepsilon_m = -1$ if $m = 2, 4, p^\alpha$ or $2p^\alpha$ (p an odd prime and α a positive integer) and $\varepsilon_m = 1$ otherwise.

The integer

$$W(m) = \frac{1}{m}\,\Big[\prod_{\substack{j=1\\(j,m)=1}}^{m} j - \varepsilon_m\Big]$$

is called the *generalized Wilson quotient of* m (see [ADS2], Definition 2.1).

According to [ADS2], Propositions 3.1 and 3.2, we have

$$W(p^{n+1}) \equiv W(p^n) \pmod{p^{n-1}}, \tag{5.1}$$

hence there exists $\lim\limits_{n\to\infty} W(p^n)$.

Definition 5.2. Set

$$W = W_p = \lim_{n\to\infty} W(p^n)$$

and call the p-adic integer W_p the *Wilson quotient for the p-adic case*, or simply *p-adic Wilson quotient.*

Proposition 5.1. $v(W - W(p^n)) \geq n - 1$.

Proof. According to (5.1) we get for each integer $m > n$ the inequality $v(W(p^m) - W(p^n)) \geq n - 1$. There exists an integer $m > n$ such that $v(W - W(p^m)) \geq n - 1$, therefore

$$\begin{aligned} v(W - W(p^n)) &= v((W - W(p^m)) + (W(p^m) - W(p^n)) \geq \\ &\geq \min\{v(W - W(p^m)), v(W(p^m) - W(p^n)) \geq n - 1 \end{aligned}$$

and we are done. □

Notation. For an integer $m \geq 2$ set

$$\sigma_1(m) = \sum_{\substack{a=1\\(a,m)=1}}^{m} q(a,m),\ \ \sigma_2(m) = \sum_{\substack{a=1\\(a,m)=1}}^{m}\ \sum_{\substack{b=a+1\\(b,m)=1}}^{m} q(a,m)q(b,m).$$

Further let

$$\bar{\varepsilon}_p = \begin{cases} -1 & \text{if } p \text{ is odd} \\ \ \ 1 & \text{if } p = 2 \end{cases} \qquad (= \varepsilon_{p^3}) \text{ and } c(n) = \varphi(p^n) = p^{n-1}(p-1).$$

As usual the *n-th Bernoulli number* will be denoted by B_n ($B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, \ldots$).

In the following proposition the congruence mod m in Proposition 2.1 of [ADS2] is extended to mod m^2 using the same method of the proof.

Proposition 5.2. *For integers $m \geq 3$ we have*

$$\varepsilon_m \varphi(m) W(m) + \binom{\varphi(m)}{2} m W(m)^2 \equiv \sigma_1(m) + m\sigma_2(m) \pmod{m^2}.$$

Proof. The result follows from observing that

$$\left(\prod_{\substack{j=1 \\ (j,m)=1}}^{m} j \right)^{\varphi(m)} = (\varepsilon_m + mW(m))^{\varphi(m)} \equiv \varepsilon_m^{\varphi(m)} + \varphi(m)\varepsilon_m^{\varphi(m)-1} mW(m) +$$

$$+ \binom{\varphi(m)}{2} \varepsilon_m^{\varphi(m)-2} m^2 W(m)^2 \pmod{m^3} =$$

$$= 1 + \varepsilon_m \varphi(m) m W(m) + \binom{\varphi(m)}{2} m^2 (W(m))^2$$

and also,by the definition of $q(a, m)$,

$$\left(\prod_{\substack{j=1 \\ (j,m)=1}}^{m} j \right)^{\varphi(m)} = \prod_{\substack{a=1 \\ (a,m)=1}}^{m} (1 + mq(a, m)) \equiv$$

$$\equiv 1 + m\sigma_1(m) + m^2 \sigma_2(m) \pmod{m^3}.$$ □

Proposition 5.3. $\lim_{n \to \infty} \sigma_1(p^n) = 0$.

Proof. Using Proposition 5.2 we get $v(\sigma_1(p^n)) \geq n - 1$ and the result follows. □

Theorem 5.4. $\sum_{\nu=1}^{\infty} \left(\sum_{\substack{a=p^{\nu-1}+1 \\ p \nmid a}}^{p^\nu} q(a) \right) = 0$.

Proof. Let $n \geq 2$. According to Theorem 3.3 (a) we have for each integer a ($p \nmid a$) $v(q(a) - q(a, p^n)) \geq n$, therefore

$$v \left(\sum_{\substack{a=1 \\ p \nmid a}}^{p^n} q(a) - \sigma_1(p^n) \right) = v \left(\sum_{\substack{a=1 \\ p \nmid a}}^{p^n} [q(a) - q(a, p^n)] \right) \geq$$

$$\geq \min\{v(q(a) - q(a, p^n)) : 1 \leq a \leq p^n, a \in \mathbf{Z}, p \nmid a\} \geq n.$$

The result follows from Proposition 5.3. □

Proposition 5.5.

$$W_p = \bar{\varepsilon}_p \frac{p}{p-1} \lim_{n \to \infty} \left(\frac{\sigma_1(p^n)}{p^n} + \sigma_2(p^n) \right) = \frac{\bar{\varepsilon}_p}{p-1} \lim_{n \to \infty} \left(\frac{\sigma_1(p^n)}{p^{n-1}} + p\sigma_2(p^n) \right).$$

Proof. If we substitute for m the power p^n ($n \geq 3$) in the congruence of Proposition 5.2, we get

$$\bar{\varepsilon}_p (p-1) W(p^n) \equiv \frac{\sigma_1(p^n)}{p^{n-1}} + p\sigma_2(p^n) \pmod{p^{n-1}}.$$

Using Proposition 5.1 we get the result. □

For the proof of Theorem 5.7 we will need the following lemma:

Lemma 5.6. *Let t be a positive integer and $n \geq 5$. Then*

$$\sum_{\substack{a=1 \\ p \nmid a}}^{p^n} a^{tc(n)} \equiv B_{tc(n)} p^n \ (mod\ p^{3n-1}).$$

Proof. For the sake of simplicity put $c = c(n)$ and $m = p^n$. Then by a well-known identity for Bernulli numbers,

$$\sum_{a=1}^{m-1} a^{tc} = \frac{1}{tc+1} \sum_{k=0}^{tc} \binom{tc+1}{k} B_k m^{tc+1-k}.$$

Since for $0 \leq k \leq tc - 2$ the inequality $v(B_k m^{tc+1-k}) \geq 3n - 1$ is satisfied by the von Staudt-Clausen theorem, we get

$$\sum_{a=1}^{m-1} a^{tc} \equiv \frac{1}{tc+1} \left(\binom{tc+1}{1} B_{tc} p^n + \binom{tc+1}{2} B_{tc-1} p^{2n} \right) \pmod{p^{3n-1}}.$$

The integer $tc - 1$ is odd and greater than 3, hence $B_{tc-1} = 0$. If a is an integer divisible by p, then $v(a^{tc}) \geq tc \geq 2^{n-1} \geq 3n + 1$. The result follows. □

Theorem 5.7.

$$W_p = -\bar{\varepsilon}_p \frac{p}{2(p-1)} \lim_{n\to\infty} \frac{1}{p^n} \left(B_{2c(n)} - 4B_{c(n)} + \frac{3(p-1)}{p} \right).$$

Proof. Put $\gamma(n) = \sum_{\substack{a=1 \\ p \nmid a}}^{p^n} q(a,p^n)^2$ and $c = c(n)$. According to Lemma 5.6 we have for $n \geq 5$

$$\gamma(n) = \frac{1}{p^{2n}} \sum_{\substack{a=1 \\ p \nmid a}}^{p^n} (a^{2c} - 2a^c + 1) = \frac{1}{p^n} \left(B_{2c} - 2B_c + \frac{p-1}{p} \right) + x_n p^{n-1}$$

and

$$\sigma_1(p^n) = \frac{1}{p^n} \sum_{\substack{a=1 \\ p \nmid a}}^{p^n} (a^c - 1) = B_c - \frac{p-1}{p} + y_n p^{2n-1},$$

where x_n and y_n are (rational) integers.

Further

$$\sigma_1(p^n)^2 = \gamma(n) + 2\sigma_2(p^n),$$

therefore

$$\frac{\sigma_1(p^n)}{p^n} + \sigma_2(p^n) = \frac{1}{p^n} \left(B_c - \frac{p-1}{p} \right) + y_n p^{n-1} + \frac{\sigma_1(p^n)^2}{2} - \frac{\gamma(n)}{2} =$$

$$= \frac{1}{2p^n} \left(2B_c - \frac{2(p-1)}{p} - B_{2c} + 2B_c - \frac{p-1}{p} \right) + (y_n - \frac{x_n}{2}) p^{n-1} + \frac{\sigma_1(p^n)^2}{2} =$$

$$= \frac{-1}{2p^n} \left(B_{2c} - 4B_c + \frac{3(p-1)}{p} \right) + (y_n - \frac{x_n}{2}) p^{n-1} + \frac{\sigma_1(p^n)^2}{2}.$$

Since $\lim_{n\to\infty} (y_n - x_n) p^{n-1} = 0$ and $\lim_{n\to\infty} \frac{\sigma_1(p^n)^2}{2} = 0$ (by Proposition 5.3), the proof is complete according to Proposition 5.5. □

6. Friedmann-Tamarkine Congruence

In their paper [FT] (1909) *Friedmann* and *Tamarkine* proved for an odd prime p and an integer m ($3 \leq m \leq p-2$) the following congruence:

$$\text{(FT)} \qquad \sum_{a=1}^{p-1} a^m q(a,p) \equiv -\frac{1}{m} B_m \pmod{p}.$$

Note that the congruences of this kind were given by *Lerch* ([Lr1], 1905) for special m.

$$(4),\quad m=0: \qquad \sum_{a=1}^{p-1} q(a,p) \equiv W(p) \pmod{p},$$

$$(17),\quad m=1: \qquad \sum_{a=1}^{p-1} aq(a,p) \equiv \frac{1}{2} \pmod{p},$$

$$(24),\quad m=2: \qquad \sum_{a=1}^{p-1} a^2 q(a,p) \equiv -\frac{1}{12} \pmod{p}, (p \neq 3),$$

$$(18),\quad m=\tfrac{p-1}{2}: \qquad \sum_{a=1}^{p-1} (\frac{a}{p}) a(a,p) \equiv 0 \pmod{p}, (p \equiv 3 \pmod{4}),$$

$$(21),\quad m=\tfrac{p-1}{2}: \qquad \sum_{a=1}^{p-1} (\frac{a}{p}) q(a,p) \equiv 2B_{\frac{p-1}{2}} \pmod{p}, (p \equiv 1 \pmod{4}),$$

$$(22^1),\quad m=\tfrac{p+1}{2}: \qquad \sum_{a=1}^{p-1} (\frac{a}{p}) aq(a,p) \equiv 0 \pmod{p}, (p \equiv 1 \pmod{4}),$$

$$(22^2),\quad m=\tfrac{p+1}{2}: \qquad \sum_{a=1}^{p-1} (\frac{a}{p}) aq(a,p) \equiv C\ell(-p) \pmod{p}, (p \equiv 3 \pmod{4}),$$

where $C\ell(-p)$ is the number of divisor classes of the quadratic field $\mathbf{Q}(\sqrt{-p})$ and $C\ell(-p) \equiv -2B_{\frac{p+1}{2}} \pmod{p}$ for $p > 3$ ([BS], Chap. 5, Sec. 8, Problem 4).

The aim of this section is to transfer the congruence (FT) to the p-adic case for the Fermat quotient q. For $m = 0$ the modified relation was expressed by Theorem 5.4.

Further we will assume that p is an odd prime and for a positive integer N set

$$S_N(n) = 1^N + 2^N + \cdots + (n-1)^N.$$

To prove the main theorem of this section we will state some lemmas.

Lemma 6.1. *If μ, ν are positive integers, $\nu \geq v(\mu+1)$, then*

$$S_\mu(p^\nu) \equiv B_\mu p^\nu \ (mod\ p^{2\nu-1}).$$

Proof. Put $x = v(\mu+1)$. Since $v(B_k) \geq -1$ by the von Staudt-Clausen theorem, we have for $0 \leq k \leq \mu-2$ (k an integer):

$$v\left(\frac{1}{\mu+1}\binom{\mu+1}{k}B_k p^{\nu(\mu+1-k)}\right) \geq -x-1+3\nu \geq 2\nu-1,$$

therefore, as in the proof of Lemma 5.6,

$$S_\mu(p^\nu) = \frac{1}{\mu+1}\sum_{k=0}^{\mu}\binom{\mu+1}{k}B_k p^{\nu(\mu+1-k)}) \equiv$$
$$\equiv \frac{1}{\mu+1}\left(\binom{\mu+1}{\mu}B_\mu p^\nu + \binom{\mu+1}{\mu-1}B_{\mu-1}p^{2\nu}\right) \ (\mathrm{mod}\ p^{2\nu-1}) \equiv$$
$$\equiv B_\mu p^\nu \ (\mathrm{mod}\ p^{2\nu-1}).$$

□

In Lemmas 6.2 and 6.3 we assume that m is a positive integer, $m \not\equiv 0 \ (\mathrm{mod}\ p-1)$, ν is an integer, $\nu \geq v(m+1)+2$ and $M = m + p^{\nu-1}(p-1)$.

Lemma 6.2. $\frac{1}{p^\nu}(S_M(p^\nu) - S_m(p^\nu)) \equiv -p^{m-1}B_m \ (mod\ p^{\nu-1})$.

Note that $\nu \geq v(m+1) = v(M+1)$, hence the numbers $\frac{1}{p^\nu}S_M(p^\nu)$ and $\frac{1}{p^\nu}S_m(p^\nu)$ are integers by Lemma 6.1.

Proof. We will use Kummer's congruence for the Bernoulli numbers modulo a prime power ([W], Corollary 12.3, p. 241):

If $m \equiv M \ (\mathrm{mod}\ p^{\nu-1}(p-1))$, and $m \not\equiv 0 \ (\mathrm{mod}\ p-1)$, then

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{M-1})\frac{B_M}{M} \ (\mathrm{mod}\ p^\nu).$$

Since $M-1 \geq p^{\nu-1}(p-1) \geq 3^{\nu-1}\cdot 2 \geq \nu$, we have $(1-p^{n-1})\frac{B_m}{m} \equiv \frac{B_M}{m} \ (\mathrm{mod}\ p^{\nu-1})$, therefore

$$B_M \equiv (1-p^{m-1})B_m \ (\mathrm{mod}\ p^{\nu-1}).$$

Using Lemma 6.1 we get

$$\frac{1}{p^\nu}(S_M(p^\nu) - S_m(p^\nu)) \equiv B_M - B_m \equiv -p^{m-1}B_m \ (\mathrm{mod}\ p^{\nu-1}).$$ □

Lemma 6.3.

$$\sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^m q(a,p^\nu) \equiv 0 \ (mod\ p^{\nu-2}).$$

Proof. For an integer a divisible by p we have $v(a^M) \geq M > p^{\nu-1}(p-1) \geq 3^{\nu-1}\cdot 2 \geq 2\nu$, hence

$$\sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^M \equiv S_M(p^\nu) \pmod{p^{2\nu}}$$

and there exists $A \in \mathbf{Z}$ such that

$$\sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^M = S_M(p^\nu) + A\cdot p^{2\nu}. \tag{6.1}$$

Since $S_m(p^\nu) = \sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^m + p^m \sum_{a=1}^{p^{\nu-1}-1} a^m$, we have

$$\sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^m = S_m(p^\nu) - p^m S_m(p^{\nu-1}), \tag{6.2}$$

and using Lemma 6.1 we get $S_m(p^{\nu-1}) \equiv B_m p^{\nu-1} \pmod{p^{2\nu-3}}$. Therefore there exists a p-adic integer C such that

$$p^m S_m(p^{\nu-1}) = p^{m+\nu-1}B_m + p^{m+2\nu-3}C. \tag{6.3}$$

Summarizing (6.1) - (6.3) we obtain

$$\sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^m q(a,p^\nu) = \frac{1}{p^\nu}\left(\sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^M - \sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^m\right) =$$

$$= \frac{1}{p^\nu}(S_M(p^\nu) + Ap^{2\nu} - S_m(p^\nu) + p^{m+\nu-1}B_m + p^{m+2\nu-3}C) \equiv$$

$$\equiv \frac{1}{p^\nu}(S_M(p^\nu) - S_m(p^\nu)) + p^{m-1}B_m \pmod{p^{\nu-2}} \equiv$$

$$\equiv 0 \pmod{p^{\nu-2}}$$

according to Lemma 6.2. □

Theorem 6.4. *If p is an odd prime and m a positive integer, $m \not\equiv 0 \pmod{p-1}$, then*

$$\sum_{\nu=1}^{\infty}\left(\sum_{\substack{a=p^{\nu-1}+1\\ p\nmid a}}^{p^\nu} a^m q(a)\right) = 0.$$

Proof. For a positive integer ν put

$$A(\nu) = \sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^m q(a) \text{ and } B(\nu) = \sum_{\substack{a=1\\ p\nmid a}}^{p^\nu} a^m q(a,p^\nu).$$

According to Theorem 3.3 (a) we have $v(A(\nu) - B(\nu)) \geq \nu$.

If $\nu \geq v(m+1) + 2$, then by Lemma 6.3 $v(B(\nu)) \geq \nu - 2$, therefore $v(A(\nu)) = v(A(\nu)-B(\nu)+B(\nu)) \geq \min\{v(A(\nu)-B(\nu)), v(B(\nu))\} \geq \nu-2$ (for $\nu \geq v(m+1)+2$).

This proves $\lim_{\nu\to\infty} A(\nu) = 0$ and the proof is complete. □

Acknowledgement

The author is grateful to Tauno Metsänkylä for the advice on Leopoldt's formula and the paper [Lp].

References

[ADS1] T. Agoh, K. Dilcher, and L. Skula, *Fermat quotients for composite moduli*, J. Number Theory **66** (1997), 29–50.

[ADS2] T. Agoh, K. Dilcher, and L. Skula, *Wilson quotients for composite moduli*, Math. Comp. **67**, No. 222(1998), 843–861.

[BS] Z. I. Borevich, I. R. Shafarevich, *"Number Theory"*, Academic Press, Orlando, 1966.

[E] G. Eisenstein, *Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden*, Bericht über die zur Bekanntmachung geeigenten Verhandlungen der Königl. Preuss. Akademie der Wissenschaften zu Berlin (1850), 36–42 (p.41). "Math. Werke, Gotthold Eisenstein", Band II, Chelsea, New York, 2nd ed. 1989, 705–711 (p. 7–10).

[FT] A. Friedmann, J. Tamarkine, *Quelques formules concernant la théorie de la fonction $[x]$ et des nombres de Bernoulli*, J. Reine Angew. Math. **135** (1909), 146–156.

[K] H. Koch, *"Galoissche Theorie der p-Erweiterungen"*, Berlin 1970.

[Lp] H.-W. Leopoldt, *Zur Approximation des p-adischen Logarithmus*, Abh. Math. Sem. Univ. Hamburg **25** (1961), 77–81.

[Lr1] M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1}-1)/p = q(a)$, Math. Ann. **60** (1905), 471–490.

[Lr2] M. Lerch, *Sur les théorèmes de Sylvester concernant le quotient de Fermat*, C. R. Acad. Sci. Paris **142** (1906), 35–38.

[W] L. C. Washington, *"Introduction to Cyclotomic Fields"*, Second Edition, Springer, 1997.

Author's address: Department of Mathematics, Faculty of Science, Masaryk University, 662 95 Brno, Czech Republic
E-mail address: skula @ math.muni.cz

Received: January 28, 1998