Montes Taurus J. Pure Appl. Math. 4 (1), 59–76, 2022

Montes Taurus Journal of Pure and Applied Mathematics

https://www.mtjpamjournal.com

MTJPAM
ISSN: 2687-4814

On combinatorial formulation of Fermat quotients and generalization

Mouloud Goubi [a]

[a]*Department of Mathematics, University of UMMTO Tizi-Ouzou 15000, Algeria Algebra and Number Theory Laboratory, USTHB, Algiers*

Abstract

In this work we revisit the Fermat quotients to give their combinatorial formulae and study the corresponding vanishing congruences. The obtained results are used to resolve some problems encountered in the literature. To do this, we use the generating functions and Bell polynomials. In the final section, we introduce the convolved Fermat quotients and we give its recursive and combinatorial formulae.

Keywords: Fermat quotients, Fermat functions, congruences, p-adic numbers, Bell numbers, Bell polynomials

2010 MSC: 11A07, 11D41, 11B73

1. Introduction

Throughout this paper we consider $p \geq 3$ a prime number and a a positive integer. For $p \nmid a$, the Fermat quotient of p to base a is denoted by

$$q_p(a) = \left(a^{p-1} - 1\right)/p.$$

Fermat quotients played an important role in number theory. As for the study of cyclotomic fields and Fermat Last Theorem. There are numerous results in the literature relating Fermat quotients to congruence equations, one can see (*cf.* [2, 10, 11, 18, 27, 28]) and references therein. The Fermat quotient to base 2 is wildly studied (*cf.* [16] and [19]) and some authors are interested by different powers of $q_p(2)$ (*cf.* [1, 5, 6, 15]). In the literature some questions concerning the vanishing of the Fermat quotients are asked (*cf.* [28]): can one say exactly when $q_p(a)$ is congruent to zero modulo p? Can one give the exact power of p dividing $q_p(a)$? Are there infinitely many pairs (a, p) so that $q_p(a) \equiv 0 \pmod{p}$? If a is fixed, is there a finite or infinite number of p's such that $q_p(a) \equiv 0 \pmod{p}$. Our purpose in this work is to give several combinatorial formulae and arithmetic properties of $q_p(a)$ in order to study the vanishing congruence of $q_p(a)$ to construct infinitely many pairs (p, a) solutions of the congruence $q_p(a) \equiv 0 \pmod{p^k}$, and find combinatorial numbers multiples of p. Using Mathematica 4 some results are illustrated in tables and numerical examples. The method used contributes to the literature in the study of special numbers and polynomials including their generating functions (*cf.* [3, 17, 23]).

†*Article ID:* MTJPAM-D-21-00032

Email address: mouloud.goubi@ummto.dz (Mouloud Goubi)

Received:16 May 2021, Accepted:7 October 2021, Published:7 November 2021

⋆*Corresponding Author:* Mouloud Goubi

1.1. Preliminaries

The natural extension of Fermat quotients to all integers a, m is defined by

$$Q_m(a) = \frac{a^{m-1} - 1}{m}$$

and lies to $\mathbb{Q}$. The study of the Fermat quotient needs the introduction of Fermat functions on $\mathbb{Z}^2$.

Definition 1.1. The Fermat functions f_n^+ and f_n^- from $\mathbb{Z}^2$ to $\mathbb{Z}$ are given respectively by the relations

$$f_n^+(a,b) = a^n + b^n, \text{ and } f_n^-(a,b) = a^n - b^n. \tag{1.1}$$

Among others, the function f_n^+, f_n^- so defined satisfy the identities

$$f_n^+(a+b,0) = f_n^+(a,b) + \sum_{j=1}^{n-1} \binom{n}{j} f_j^+(a,0)\, f_{n-j}^+(b,0), \tag{1.2}$$

$$f_{p-1}^+(a,b) = p\left(Q_p(a) + Q_p(b)\right) + 2. \tag{1.3}$$

and $f_{m-1}^-(a,-1) = mQ_m(a)$. Fermat functions appears in Wieferich's Theorem (*cf.* [2]): If a, b, c are integers not divisible by p, satisfying the equation $f_p(a,b) + f_p(c,0) = 0$. Then $2^{p-1} - 1 \equiv 0 \pmod{p}$. Odd primes satisfying this congruence are called Wieferich primes (*cf.* [5]).

The well-known exponential partial Bell polynomials (*cf.* [4]): $B_{n,k} := B_{n,k}(x_1, \cdots, x_{n-k+1})$ are defined by the generating function

$$\frac{1}{k!}\left(\sum_{m\geq 1} x_m \frac{t^m}{m!}\right) = \sum_{n\geq k} B_{n,k} \frac{t^n}{n!} \tag{1.4}$$

and admit for explicit formula the expression

$$B_{n,k} = \frac{n!}{k!} \sum_{s_n(k)} \binom{k}{k_1, \cdots, k_{n-k+1}} \prod_{r=1}^{n-k+1} \left(\frac{x_r}{r!}\right)^{k_r}, \tag{1.5}$$

where $s_n(k)$ is the set of all $k_1, k_2, \cdots, k_{n-k+1}$ for which $k_1 + k_2 + \cdots + k_{n-k+1} = k$ and $k_1 + 2k_2 + \cdots + nk_{n-k+1} = n$, and

$$\binom{k}{k_1, \cdots, k_{n-k+1}} = \frac{k!}{k_1! \cdots k_{n-k+1}!}.$$

Bell polynomials play an important role in generating functions theory, let $f(t) = \sum_{n\geq 0} a_n t^n$ and $g(t) = \sum_{n\geq 0} b_n t^n$ be two generating functions and consider the sequence $x_j = j! b_j$. The series expansion of $f \circ g$ is given by the expression (*cf.* [12]):

$$f \circ g(t) = f(b_0) + \sum_{n\geq 1} \sum_{k=1}^{n} B_{n,k} f^{(k)}(b_0) \frac{t^n}{n!}. \tag{1.6}$$

Consequently for $b_0 = 0$ we have $f(0) = a_0$, $f^{(k)}(b_0) = k! a_k$ and

$$f \circ g(t) = a_0 + \sum_{n\geq 1} \sum_{k=1}^{n} k! a_k B_{n,k} \frac{t^n}{n!}. \tag{1.7}$$

In the case $f(t) = t^\alpha$, where α a complex number and $b_0 \neq 0$. The identity (1.6) transforms to the expression (*cf.* [14])

$$g^\alpha(t) = b_0^\alpha + \sum_{n\geq 1} \sum_{k=1}^{n} (\alpha)_k b_0^{\alpha-k} B_{n,k} \frac{t^n}{n!}. \tag{1.8}$$

For the proof we refer to [13] and references therein. The n-th derivative of $f \circ g$ and fg are computed respectively by Faà di Bruno formula [9] and Leibniz formula. Letting $D^n f$ the n-th derivative of f then we have

$$D^n f\left(g(t)\right) = \sum_{k=0}^{n} \left(D^k f\right)\left(g\left(t\right)\right) B_{n,k}\left(D^1 g(t), D^2 g(t), \cdots\right) \tag{1.9}$$

and

$$D^n fg(t) = \sum_{k=0}^{n} \binom{n}{k} D^k f(t) D^{n-k} g(t). \tag{1.10}$$

The Leibniz formula is easy to check but for Faà di Bruno formula we refer to (*cf.* [24]) for a detailed proof. For a good understanding of this article, we recall some elementary notions in number theory; let $(\mathbb{Z}, +, .)$ the ring of integer and $(\mathbb{Z}/p\mathbb{Z}, +)$ the additive quotient group obtained via the equivalence relation

$$a \equiv b \pmod{p} \Leftrightarrow a - b \in p\mathbb{Z}.$$

We denote $\bar{a}$ the inverse of a modulo. The Fermat last theorem states that $a^{p-1} - 1 \equiv 0 \pmod{p}$ for a coprime to p and then $\bar{a} = a^{p-2}$. Finally we consider $\left(\mathbb{Z}_p, +, .\right)$ the ring of p-adic integers and $\mathbb{Z}_p$ the additive group of $\left(\mathbb{Z}_p, +, .\right)$, and one can extend the vanishing congruences to $\mathbb{Z}_p$. This is our subject in section 3.

2. Explicit formula of Fermat functions and Fermat quotients

The generating function of the sequence $f_n^+(a,b)$ and $f_n^-(a,b)$ are given respectively by the relations

$$\frac{2 - (a+b)z}{(1-az)(1-bz)} = \sum_{n\geq 0} f_n^+(a,b) z^n \tag{2.1}$$

and

$$\frac{(a-b)z}{(1-az)(1-bz)} = \sum_{n\geq 0} f_n^-(a,b) z^n. \tag{2.2}$$

For n odd, it is obvious to remark that $f_n^+(a,b) = f_n^-(a,-b)$. Letting $F_n(a,b)$ the numbers defined by means of the generating function

$$\frac{1}{1 - (a+b)z + abz^2} = \sum_{n\geq 0} F_n(a,b) z^n. \tag{2.3}$$

Then

$$(2 - (a+b)z) \sum_{n\geq 0} F_n(a,b) z^n = \sum_{n\geq 0} f_n^+(a,b) z^n.$$

Thus $f_0^+(a,b) = 2$ and

$$f_n^+(a,b) = 2F_n(a,b) - (a+b) F_{n-1}(a,b). \tag{2.4}$$

But for $f_n^-(a,b)$ it is easy to show that

$$f_0^-(a,b) = 0 \text{ and } f_n^-(a,b) = (a-b)F_{n-1}(a,b).$$

Thereafter we have

$$f_n^+(a,b) = \frac{2}{a-b} f_{n+1}^-(a,b) - \frac{a+b}{a-b} f_n^-(a,b). \tag{2.5}$$

The explicit formula of the numbers $F_n(a,b)$ is given by the following lemma.

Lemma 2.1.

$$F_n(a,b) = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j} (a+b)^{n-2j} (-ab)^j . \tag{2.6}$$

Proof. Let the polynomial

$$g(z) = 1 - (a+b)z + abz^2.$$

Then $g(z) = \sum_{j\geq 0} a_j z^j$ with $a_0 = 1, a_1 = -a-b, a_2 = -ab$ and others are zero. Letting $x_j = j!a_j$ and applying relation (1.8) to g and $\alpha = -1$, to obtain

$$\frac{1}{1-(a+b)z+abz^2} = 1 + \sum_{n\geq 1} \sum_{j=1}^{n} (-1)^j j! B_{n,j} \frac{z^n}{n!}.$$

Thus $F_0(a,b) = 1$ and

$$F_n(a,b) = \frac{1}{n!} \sum_{j=1}^{n} (-1)^j j! B_{n,j}.$$

But

$$B_{n,j} = \frac{n!}{j!} \sum_{\substack{j_1+j_2=j \\ j_1+2j_2=n}} \binom{j}{j_1} (a+b)^{j_1} (-ab)^{j_2}.$$

The system

$$\begin{cases} j_1 + j_2 = j \\ j_1 + 2j_2 = n \end{cases}$$

admit zero or one solution. $B_{n,j}$ vanishes if their is no solution for the system. For example if $n < 2$ we have $B_{n,j} = 0$ for $j \neq n$. The solution if exist, is of the form $(j-i, i)$ with $n = j + i$. In this case we have

$$B_{n,j} = \frac{n!}{j!} \binom{j}{i} (a+b)^{j-i} (-ab)^i$$

and

$$F_n(a,b) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-j}{j} (a+b)^{n-2j} (-ab)^j .$$

□

According to parity of n, the explicit formula of f_n^+ is given by the following theorem.

Theorem 2.2.

$$f_{2n}^+(a,b) = 2(ab)^{2n} + \sum_{j=0}^{n-1} \frac{n}{n-j} \binom{2n-1-j}{j} (-ab)^j (a+b)^{2n-2j} \tag{2.7}$$

and

$$f_{2n+1}^+(a,b) = \sum_{j=0}^{n} \frac{2n+1}{2n-2j+1} \binom{2n-j}{j} (-ab)^j (a+b)^{2n-2j+1} . \tag{2.8}$$

Proof. The proof consists to use the well-known identity

$$\binom{n}{j} = \frac{n}{n-j}\binom{n-1}{j}$$

and the fact that

$$f_{2n}^{+}(a,b) = 2(-ab)^{2n} + \sum_{j=0}^{n}\left(2\binom{2n-j}{j} - \binom{2n-1-j}{j}\right)(-ab)^{j}(a+b)^{2n-2j}$$

and

$$f_{2n+1}^{+}(a,b) = \sum_{j=0}^{n}\left[2\binom{2n-j+1}{j} - \binom{2n-j}{j}\right](-ab)^{j}(a+b)^{2n-2j+1}.$$

□

Consequently for $a+b \neq 0$, $(a+b)^{2n}$ admits the following combinatorial evaluations

$$(a+b)^{2n} = (a^n - (-b)^n)^2 - \sum_{j=1}^{n-1}\frac{n}{j}\binom{n+j-1}{2j-1}(-ab)^{n-j}(a+b)^{2j}$$

and

$$(a+b)^{2n} = \frac{a^{2n+1}+b^{2n+1}}{a+b} - \sum_{j=0}^{n-1}\frac{2n+1}{2j+1}\binom{n+j}{2j}(-ab)^{n-j}(a+b)^{2j}.$$

These identities imply that

$$Q_n\left((a+b)^2\right) = \frac{1}{n}\left(-1 + \left(\frac{a^n-(-b)^n}{a+b}\right)^2\right) - \sum_{j=1}^{n-1}\frac{1}{j}\binom{n+j-1}{2j-1}(-ab)^{n-j}(a+b)^{2j-2} \tag{2.9}$$

and

$$Q_{2n+1}(a+b) = \frac{1}{2n+1}\left(-1 + \frac{a^{2n+1}+b^{2n+1}}{a+b}\right) - \sum_{j=0}^{n-1}\frac{1}{2j+1}\binom{n+j}{2j}(-ab)^{n-j}(a+b)^{2j}. \tag{2.10}$$

2.1. Combinatorial formula of Fermat quotients

For $p \nmid a+b$, the identities (2.9) and (2.10) become

$$q_p\left((a+b)^2\right) = \frac{1}{p}\left(\left(\frac{f_p^{+}(a,b)}{a+b}\right)^2 - 1\right) - \sum_{j=1}^{p-1}\frac{1}{j}\binom{p+j-1}{2j-1}(-ab)^{p-j}(a+b)^{2j-2}$$

and

$$q_p(a+b) = \frac{1}{p}\left(-1 + \frac{f_p^{+}(a,b)}{a+b}\right) - \sum_{j=0}^{(p-3)/2}\frac{1}{2j+1}\binom{(p-1)/2+j}{2j}(a+b)^{2j}(-ab)^{(p-1)/2-j}.$$

A variety of relations are deduced, for example let $b = ma$ and $c = m+1$. Then we have

$$q_p\left(c^2a^2\right) = \frac{1}{p}\left(\left(\frac{f_p^{+}(c-1,1)\,a^{p-1}}{c}\right)^2 - 1\right) - a^{2p-2}\sum_{j=1}^{p-1}\frac{1}{j}\binom{p+j-1}{2j-1}c^{2j-2}(1-c)^{p-j}$$

and

$$q_p(ca) = \frac{1}{p}\left(-1 + \frac{f_p^{+}(c-1,1)\,a^{p-1}}{c}\right) - a^{p-1}\sum_{j=0}^{(p-3)/2}\frac{1}{2j+1}\binom{(p-1)/2+j}{2j}c^{2j}(1-c)^{(p-1)/2-j}.$$

By taking $a = 1$ in the last identities, we have already proved the following theorem.

Theorem 2.3. *For $p \nmid c$ we have*

$$q_p\left(c^2\right) = \frac{1}{p}\left(\left(\frac{1+(c-1)^p}{c}\right)^2 - 1\right) - \sum_{j=1}^{p-1} \frac{1}{j}\binom{p+j-1}{2j-1} c^{2j-2}(1-c)^{p-j} \tag{2.11}$$

and

$$q_p(c) = \frac{1}{p}\left(\frac{1+(c-1)^p}{c} - 1\right) - \sum_{j=0}^{(p-3)/2} \frac{1}{2j+1}\binom{(p-1)/2+j}{2j} c^{2j}(1-c)^{(p-1)/2-j}. \tag{2.12}$$

The combination of the expressions of $q_p(c)$ and $q_p(ca)$ yields the following corollary.

Corollary 2.4. *Let a, c two integers such that $(c,p) = (a,p) = 1$. Then*

$$q_p(ca) = q_p(a) + a^{p-1} q_p(c). \tag{2.13}$$

Since $a^{p-1} \equiv 1 \pmod{p}$, we get another proof of the well-known identity

$$q_p(ca) \equiv q_p(c) + q_p(a) \pmod{p}. \tag{2.14}$$

For simplifying notations, we use the sum

$$S(p,c) = \sum_{j=0}^{(p-3)/2} \frac{1}{2j+1}\binom{(p-1)/2+j}{2j} c^{2j}(1-c)^{(p-1)/2-j}$$

to obtain the identity $cq_p(c) = (c-1)Q_p(c-1) - cS(p,c)$, and for $(c-1,p) = 1$ we have

$$cq_p(c) = (c-1)q_p(c-1) - cS(p,c). \tag{2.15}$$

By recursion we prove that

$$q_p(c) = \frac{2}{c} q_p(2) + \frac{1}{c}\sum_{j=3}^{c} jS(p,j),\ 3 \le c \le p-1. \tag{2.16}$$

On general, with the Euclidean algorithm $c = ip + k$ we deduce that

$$q_p(ip+k) = \frac{2}{ip+k} q_p(ip+2) + \frac{1}{k}\sum_{j=3}^{k} jS(p, ip+j). \tag{2.17}$$

2.2. Fermat quotient of p to base 2

Spivey (*cf.* [25]) proved that

$$\frac{2^{n+1}-1}{n+1} = \sum_{j=0}^{n} \frac{1}{j+1}\binom{n}{j}. \tag{2.18}$$

Another proof of this result is given by Meštrović (*cf.* [19]). Let $p = n+1$ then

$$q_p(2) = \frac{1}{2}\sum_{j=0}^{p-2} \frac{1}{j+1}\binom{p-1}{j}.$$

According to identity

$$\frac{1}{j+1}\binom{p-1}{j} = \frac{1}{p}\binom{p}{j+1},$$

we have

$$q_p(2) = \frac{1}{2p}\sum_{j=1}^{p-1}\binom{p}{j}. \tag{2.19}$$

Thank's to Theorem 2.3 a new combinatorial formulations of $q_p(2)$ and $q_p(4)$ are given by the following proposition.

Proposition 2.5.

$$q_p(2) = -\sum_{j=0}^{(p-3)/2}\frac{(-1)^{(p-1)/2-j}2^{2j}}{2j+1}\binom{(p-1)/2+j}{2j} \tag{2.20}$$

and

$$q_p(4) = \sum_{j=1}^{p-1}\frac{(-1)^j 4^{j-1}}{j}\binom{p+j-1}{2j-1}. \tag{2.21}$$

Proof. The results are obtained by taking $c = 2$ in the identities (2.12) and (2.11). □

A classical congruence of Eisenstein (*cf.* [7]) asserts that

$$q_p(2) \equiv \frac{1}{2}\sum_{j=1}^{p-1}\frac{(-1)^{j-1}}{j} \pmod p,$$

which was extended by Sylvester (*cf.* [26]) and Glaisher (*cf.* [11]) as

$$q_p(2) \equiv \frac{1}{2}\sum_{j=1}^{(p-1)/2}\frac{1}{j} \pmod p.$$

It is obvious that $q_p(4) = \left(1+2^{p-1}\right)q_p(2)$. Then we have

$$q_p(2) = \frac{1}{1+2^{p-1}}\sum_{j=1}^{p-1}\frac{(-1)^j 4^{j-1}}{j}\binom{p+j-1}{2j-1}$$

and another congruence follows:

$$q_p(2) \equiv \frac{1}{2}\sum_{j=1}^{p-1}\frac{(-1)^j 4^{j-1}}{j}\binom{p+j-1}{2j-1} \pmod p.$$

Since $q_p(2)^2 = \frac{1}{p}\left(q_p(4) - 2q_p(2)\right)$, then as for congruences (*cf.* [10] and [15]) the following corollary holds true.

Corollary 2.6.

$$q_p(2)^2 = \frac{1}{p}\sum_{j=1}^{p-1}\frac{(-1)^j 4^{j-1}}{j}\binom{p+j-1}{2j-1} + \frac{2}{p}\sum_{j=0}^{(p-3)/2}\frac{(-1)^{(p-1)/2-j}2^{2j}}{2j+1}\binom{(p-1)/2+j}{2j}.$$

3. Vanishing congruences of Fermat quotient

First we consider Fermat quotients to base 2^k where $k \geq 2$. In this case we have

$$q_p(2^k) = q_p(2) + 2^{p-1} q_p(2^{k-1}).$$

By recursion we prove that

$$q_p\left(2^k\right) = q_p(2) \sum_{j=0}^{k-1} 2^{j(p-1)}.$$

Then for $(a, p) = 1$;

$$q_p\left(2^k a\right) = q_p(a) + a^{p-1} q_p(2) \sum_{j=0}^{k-1} 2^{j(p-1)}. \tag{3.1}$$

Letting $k = p$ and $a = 1$ in the identity (3.1) to obtain $q_p(2^p) \equiv 0 \pmod{p}$. This result justifies that there are infinitely many pairs (p, a) satisfying the congruence $a^{p-1} \equiv 1 \pmod{p}$. On general we have the following characterization.

Theorem 3.1. *Let $q_p(a) \equiv r \pmod{p}$ and $q_p(2) \equiv v \pmod{p}$ then*

$$q_p\left(2^k a\right) \equiv 0 \pmod{p} \text{ if and only if } p \mid r + kv.$$

Let p a Wieferich prime, then $q_p(2^k a) \equiv 0 \pmod{p}$ if and only if $q_p(a) \equiv 0 \pmod{p}$. Otherwise the congruence $r + kv \equiv 0 \pmod{p}$ as an equation on k admits infinitely many solutions $k \equiv p - r\bar{v} \pmod{p}$. Let $p = 3$, then $q_3(2) = 1$ and $q_3\left(2^k a\right) \equiv q_3(a) + k \pmod 3$. If $q_3(a) \equiv r \pmod 3$, then $q_3\left(2^{3m-r} a\right) \equiv 0 \pmod 3$, for $m \geq 1$. Consequently there is infinitely many pairs $(c, 3)$ solutions of $q_3(c) \equiv 0 \pmod 3$. From the Table 1 of Montgomery (*cf.* [20]) the even numbers solutions of the congruence $x^2 \equiv 1 \pmod 9$ are $10, 26, 28, 44, 46, 62, 80, 82, 98$. We add to this list the numbers $8, 64, 100, 116, 136, 152, 172, 224$ and 296. More relevant examples are given in the Table 1.

p	$q_p(2)$	$c, c^{p-1} - 1 \equiv 0 \pmod{p^2}$
5	3	32, 96, 128
7	2	128, 48, 80
11	5	40, 2048, 6144, 4194304
13	3	8192, 192, 7168, 80, 36864
17	13	131072, 6144, 40

Table 1. Few solutions of $c^{p-1} - 1 \equiv 0 \pmod{p^2}$

According to Theorem 2.3 if $p \mid c$ then $q_p(1 + c) \equiv 0 \pmod{p}$ and $q_p\left((1 + c)^2\right) \equiv 0 \pmod{p}$. Let $a = 1 + c$ with $c = p_1 \cdots p_r$ the decomposition of c on product of primes. Then $q_{p_j}(a) \equiv 0 \pmod{p_j}$ for $1 \leq j \leq r$, which gives a partial answer to the question asked by Vandiver (*cf.* [28]) concerning the number of primes p satisfying $q_p(a) \equiv 0 \pmod{p}$. Otherwise we construct infinitely many solutions of $q_p(c) \equiv 0 \pmod{p^k}$ in the set of integers. Let us considering $c = 1 + md^k$ with $p \mid d$. Then $p^k \mid d^k$ and

$$q_p\left(1 + md^{k+1}\right) \equiv 0 \pmod{p^k}$$

and

$$q_p\left(1 + 2md^{k+1} + m^2 d^{2(k+1)}\right) \equiv 0 \pmod{p^k}.$$

Consequently, for every odd prime p we have

$$q_p\left(1 + p^{k+1}\right) \equiv 0 \pmod{p^k}$$

and

$$q_p\left(1+2p^{k+1}+2p^{2(k+1)}\right)\equiv 0 \pmod{p^k}.$$

Few solution of the congruence $q_p(c)\equiv 0 \pmod{p^{20}}$ are given in the following table.

p	$c, c^{p-1}-1\equiv 0 \pmod{p^{20}}$
5	95367431640626
7	79792266297612002
11	672749994932560009202
13	19004963774880799438802
17	406423140664757252240 1602
19	37589973457545958193355602
23	17161558313345863429238952 02

Table 2. Few solutions of $c^{p-1}-1\equiv 0 \pmod{p^{20}}$

For large numbers we have for example

$$q_7\left(1+15\times 7^{10}\right)=7^9 \times 826669502240218393002873522590375641255075783649276498$$
$$50520485640905414437747854201052965987433417681439215$$

and

$$q_7\left(\left(1+720\times 7^5\right)^2\right)=7^4 \times 586654746257352540693726886304133680208 80$$
$$263715142615951158266037864090406286944 0.$$

Let $\omega_a=a+a_1p+a_2p^2+\cdots\in\mathbb{Z}_p$ be a p-adic integer $(p-1)$st root of unity congruent to a modulo p. Ernvall et al. (*cf.* [8]) proved for any integer $k\geq 1$ that $\omega_a\equiv a \pmod{p^{k+1}}$ if and only if $q_p(a)\equiv 0 \pmod{p^k}$. Computation of ω_a still an open problem. Recursively we prove that

$$q_p\left(\left(1+p^{k+1}\right)^{2^n}\right)\equiv 0 \pmod{p^k}.$$

The limit in p-adic sense gives

$$\omega_1=\lim_{n\to\infty}\sum_{i=0}^{2^n}\binom{2^n}{i}p^{i(k+1)}.$$

4. Arithmetical properties of Fermat quotients

The image of $(a,-1)$ by the Fermat function f_n^- is $f_n^-(a,-1)=a^n-(-1)^n$ and we have $pQ_p(a)=f_{p-1}^-(a,-1)$. Letting $f_n^-(a):=f_n^-(a,-1)$, from the identity (2.2) we have

$$\frac{(a+1)z}{(1-az)(1+z)}=\sum_{n\geq 0}f_n^-(a)z^n,\ |z|<1. \tag{4.1}$$

But

$$\frac{(a+1)z}{(1-az)(1+z)}=(a+1)\sum_{n\geq 1}F_{n-1}(a)z^n.$$

Then $f_0^-(a)=0$ and

$$f_n^-(a)=(a+1)\sum_{j=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n-j-1}{j}(a-1)^{n-2j-1}a^j.$$

We have already proved the following theorem.

Theorem 4.1.

$$q_p(a) = \frac{3Q_3(a)}{p} \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} a^j (a-1)^{p-2j-3}. \tag{4.2}$$

$q_p(a)$ is a polynomial on a and $a-1$, for example we have $q_p(p+1) \equiv -1 \pmod p$. According to the identity (4.2) we have $a+1 \mid q_p(a)$ and

$$p \mid \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} a^j (a-1)^{p-2j-2}$$

for $a \neq p-1$. But if $p \neq 3$ and $p \nmid Q_3(p)$ we have

$$p \mid \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} a^j (a-1)^{p-2j-3}.$$

Only from the identity (4.2) we have $a+1 \mid pq_p(a)$ which is conform with the identity

$$a^{p-1} - 1 = (a^2-1) \sum_{k=0}^{\frac{p-3}{2}} a^{2k}.$$

Let $(3,a) = 1$ and $p \neq 3$, the last elementary identity shows that $q_3(a) \mid q_p(a)$. In the case $p = 3$ we just have the simple identity $3q_3(a) = (a+1)(a-1)$. Let r be the remainder obtained when n is divided into p, we write $a = kp + r$ and it is easily checked that

$$k = \left\lfloor \frac{a}{p} \right\rfloor \text{ and } r = a - p\left\lfloor \frac{a}{p} \right\rfloor.$$

Then in the case $a \equiv 1 \pmod p$ we can show that

$$q_p(a) \equiv \frac{(a+1)(p-1)}{2} a^{(p-3)/2} \left\lfloor \frac{a}{p} \right\rfloor \pmod p,$$

which can be reduced to

$$q_p(a) \equiv (p-1)\left\lfloor \frac{a}{p} \right\rfloor \pmod p. \tag{4.3}$$

Another proof is given by

$$q_p(kp+1) = \frac{(2p+1)^{p-1} - 1}{p} = \sum_{j=1}^{p-1} \binom{p-1}{j} k^j p^{j-1} \equiv (p-1)k \pmod p.$$

For $0 \leq k \leq p-1$ it is obvious that $q_p(a) = p - k \pmod p$. For example we have

$$q_{11}(3 \times 11 + 1) = 187670704914525 \equiv 11 - 3 \pmod{11}.$$

The following combinatorial reformulation of the Fermat quotient to base 2 is deduced.

Corollary 4.2. *Another combinatorial reformulation of $q_p(2)$ is given by the following expression*

$$q_p(2) = \frac{3}{p} \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} 2^j. \tag{4.4}$$

If $p = 3$, it is obvious that $q_3(2) = 1$. But for $p \neq 3$ we conclude that

$$p \mid \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} 2^j.$$

For example we have $1 + 8 \times 2 + \binom{7}{2}2^2 + \binom{6}{3}2^3 + \binom{5}{4}2^4 = 341 = 31 \times 11$. The identity (4.2) goes alone to establish the following congruence.

Theorem 4.3. *For $p \geq 5$ and $a = kp + r$ with $r \neq 0$ we have*

$$\begin{aligned} q_p(a) &\equiv \frac{a^2-1}{p} \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} r^j (r-1)^{p-2j-3} \\ &+ (a^2-1) \sum_{j=1}^{\frac{p-3}{2}} \binom{p-j-2}{j} jkr^{j-1}(r-1)^{p-2j-3} \\ &+ (a^2-1) \sum_{j=0}^{\frac{p-5}{2}} \binom{p-j-2}{j} (p-2j-3)kr^j(r-1)^{p-2j-4} \pmod{p}. \end{aligned}$$

Proof. We substitute the identities

$$(a-1)^{p-2j-3} = \sum_{u=0}^{p-2j-3} \binom{p-2j-3}{u} (r-1)^{p-2j-3-u} k^u p^u$$

and

$$a^j = \sum_{\ell=0}^{j} \binom{j}{\ell} r^{j-\ell} k^\ell p^\ell$$

in the identity (4.2) to get

$$\frac{q_p(a)}{a^2-1} = \sum_{j=0}^{\frac{p-3}{2}} \sum_{u=0}^{p-2j-3} \sum_{\ell=0}^{j} \binom{p-j-2}{j} \binom{p-2j-3}{u} \binom{j}{\ell} k^{u+\ell} (r-1)^{p-2j-3-u} r^{j-\ell} p^{u+\ell-1}.$$

We carry out the terms which are multiples of p to reduce the last sum to

$$q_p(a) \equiv \frac{a^2-1}{p} \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} (r-1)^{p-2j-3} r^j$$

$$+(a^2-1) \sum_{j=0}^{\frac{p-3}{2}} \sum_{\substack{u+\ell=1 \\ \ell \leq j, u \leq p-2j-3}} \binom{p-j-2}{j} \binom{p-2j-3}{u} \binom{j}{\ell} k (r-1)^{p-2j-3-u} r^{j-\ell} \pmod{p}.$$

Let S be the sum

$$\sum_{\substack{u+\ell=1 \\ \ell \leq j, u \leq p-2j-3}} \binom{p-j-2}{j} \binom{p-2j-3}{u} \binom{j}{\ell} k (r-1)^{p-2j-3-u} r^{j-\ell},$$

then

$$S = \binom{p-j-2}{j} \binom{j}{1} k (r-1)^{p-2j-3} r^{j-1} + \binom{p-j-2}{j} \binom{p-2j-3}{1} k (r-1)^{p-2j-4} r^j$$

and

$$\sum_{j=0}^{\frac{p-3}{2}} \sum_{\substack{u+\ell=1 \\ \ell\le j, u\le p-2j-2}} \binom{p-j-2}{j}\binom{p-2j-2}{u}\binom{j}{\ell} k(r-1)^{p-2j-3-u} r^{j-\ell} = \sum_{j=1}^{\frac{p-3}{2}} \binom{p-j-2}{j} jk(r-1)^{p-2j-3} r^{j-1}$$
$$+ \sum_{j=0}^{\frac{p-5}{2}} \binom{p-j-2}{j} (p-2j-3)k(r-1)^{p-2j-4} r^j,$$

and the result follows. □

For $a = kp + 2$ the previous formula is written under the form

$$\begin{aligned} q_p(a) &\equiv \frac{a^2-1}{p} \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} 2^j \\ &+ (a^2-1) \sum_{j=1}^{\frac{p-3}{2}} \binom{p-j-2}{j} jk2^{j-1} \\ &+ (a^2-1) \sum_{j=0}^{\frac{p-5}{2}} \binom{p-j-2}{j} (p-2j-3)k2^j \pmod p. \end{aligned}$$

Corollary 4.4. *We have $p \mid a^2 - 1$ or*

$$p \mid \sum_{j=0}^{\frac{p-3}{2}} \binom{p-j-2}{j} \left(a - p\left\lfloor \frac{a}{p} \right\rfloor\right)^j \left(a - p\left\lfloor \frac{a}{p} \right\rfloor - 1\right)^{p-2j-3}.$$

In the case $k = 0$, we have $a = r$ and we return back to Theorem 4.1. The relation

$$(1-az)\sum_{n\ge 0} f_n^-(a) z^n = 1 - (1-az)\sum_{n\ge 0} (-1)^n z^n$$

helps us to write

$$\sum_{n\ge 1} \left(f_n^-(a) - a f_{n-1}^-(a)\right) z^n = (a+1)\sum_{n\ge 1} (-1)^{n-1} z^n.$$

Thereafter we have

$$f_n^-(a) - a f_{n-1}^-(a) = (-1)^{n-1}(a+1),$$

which implies that $pq_p(a) = a\left(f_{p-2}^-(a) - 2\right) + a - 1$ and one obtains $pq_p(a) \equiv (a-1) \pmod a$. It also stems from the relationship $a^{p-1} - 1 = a - 1 + (a-1)(1 + \cdots + a^{p-3})a$.

4.1. Further identities

Identities satisfied by the sequence $f_n^-(a)$ depend in the way we write its generating function. For $|z| < 1$ we have

$$\frac{1}{1-(a-1)z - az^2} = \sum_{j\ge 0} (a - 1 + az)^j z^j.$$

Then

$$\frac{1}{1-(a-1)z - az^2} = \sum_{j\ge 0} \sum_{k=0}^{j} \binom{j}{k} a^k (a-1)^{j-k} z^{j+k}$$

and

$$\frac{1}{1-(a-1)z-az^2}=\sum_{j\geq 0}\sum_{\ell=j}^{2j}\binom{j}{\ell-j}a^{\ell-j}(a-1)^{2j-\ell}z^{\ell}.$$

Furthermore

$$\frac{1}{1-(a-1)z-az^2}=\sum_{n\geq 0}\left(\sum_{n/2\leq j\leq n}\binom{j}{n-j}a^{n-j}(a-1)^{2j-n}\right)z^n.$$

Thus

$$F_n(a,-1)=\sum_{n/2\leq j\leq n}\binom{j}{n-j}a^{n-j}(a-1)^{2j-n}.$$

Numbers $F_n(a,-1)$ are connected to Fibonacci-type polynomials in two variables $\mathcal{G}_n(x,y;k,m,j)$ (see [21, 22]) by the relations $F_n(a,-1)=\mathcal{G}_n(a-1,a;1,1,1)$ or $F_n(a,-1)=\mathcal{G}_n\left(a-1,\sqrt{a};1,2,0\right)$. According to the expression of $\mathcal{G}_n(x,y;k,m,j)$ in [21]; we can write

$$F_n(a,-1)=\sum_{j=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n-j}{j}a^{j}(a-1)^{n-2j}.$$

From the relation $f_n^{-}(a)=(a+1)F_{n-1}(a,-1)$ we deduce that

$$f_n^{-}(a)=(a^2-1)\sum_{(n-1)/2\leq j\leq n-1}\binom{j}{n-j-1}(a-1)^{2j-n}a^{n-j-1},$$

and the following theorem is true.

Theorem 4.5. *For p and odd prime we have*

$$pq_p(a)=3q_3(a)\sum_{(p-2)/2\leq j\leq p-2}\binom{j}{p-j-2}(a-1)^{2j-p+1}a^{p-j-2}. \tag{4.5}$$

Since we have

$$\sum_{(p-1)/2\leq j\leq p-2}\binom{j}{p-j-2}a^{p-j-2}(a-1)^{2j-p+1}=\sum_{n=0}^{(p-3)/2}\binom{p-n-2}{n}a^{n}(a-1)^{p-2n-3},$$

thus Theorem 4.5 is another reformulation of Theorem 4.3. As a consequence; if $p\nmid q_3(a)$ we have p a divisor of the sum

$$\sum_{(p-1)/2\leq n\leq p-2}\binom{n}{p-n-2}a^{p-n-2}(a-1)^{2n-p+1}.$$

According to the Euclidean algorithm we write $a=kp+r$ and

$$q_p(a)=3q_3(a)\sum_{(p-1)/2\leq n\leq p-2}\sum_{u=0}^{2n-p+1}\sum_{\ell=0}^{p-n-2}\binom{n}{p-n-2}\binom{2n-p+1}{u}\binom{p-n-2}{\ell}(r-1)^{2n-p+1-u}r^{p-n-\ell-2}k^{u+\ell}p^{u+\ell-1}.$$

Thus the following theorem holds true.

Theorem 4.6. *For $p\geq 5$ and $a=kp+r$ we have*

$$\begin{aligned}
q_p(a) &\equiv \frac{3Q_3(a)}{p}\sum_{(p-1)/2\leq n\leq p-2}\binom{n}{p-n-2}r^{p-n-2}(r-1)^{2n-p+1}\\
&+ 3Q_3(a)\sum_{(p+1)/2\leq n\leq p-2}\binom{n}{p-n-2}(2n-p+1)kr^{p-n-2}(r-1)^{2n-p}\\
&+ 3Q_3(a)\sum_{(p-1)/2\leq n\leq p-2}\binom{n}{p-n-2}(p-n-2)kr^{p-n-3}(r-1)^{2n-p+1}\pmod{p}.
\end{aligned}$$

Thereafter if $p \nmid q_3(a)$ and $r \in \{2, \cdots, p-2\}$, we conclude that p divides the sum

$$\sum_{(p-2)/2 \leq n \leq p-2} \binom{n}{p-n-2} r^{p-n-2}(r-1)^{2n-p+1}.$$

For example if we consider $a = 4$ and $p = 11$, then we have $11 \nmid q_{11}(4) = 95325$ and the above sum becomes

$$\sum_{5 \leq n \leq 9} \binom{n}{9-n} 9^{n-5} 4^{9-n} = 69905 = 6355 \times 11.$$

The identity

$$(1-(a-1)z-az)\sum_{n\geq 0} f_n^-(a) z^n = (a+1)z$$

implies that

$$f_n^-(a) - (a-1)f_{n-1}^-(a) - af_{n-2}^-(a) = 0, \ n \geq 2.$$

In the Fermat quotients language we have

$$pq_p(a) - (a-1)f_{p-2}^- - af_{p-3}^-(a) = 0.$$

In the case $(p, p-2)$ are twice primes we conclude that

$$pq_p(a) - (a-1)f_{p-2}^-(a,-1) - a(p-2)q_{p-2}(a) = 0,$$

which follows too from the obvious identity

$$a^{p-1} - 1 - (a-1)(a^{p-2}+1) - a(a^{p-3}-1).$$

But it stills important to get the following congruence.

Theorem 4.7. *For $(p, p-2)$ twice primes we have*

$$pq_p(a) - (p-2)q_{p-2}(a) \equiv 0 \pmod{a-1} \tag{4.6}$$

for every a coprime to p and $p-2$. Thereafter

$$a^{p-1} - a^{p-3} \equiv 0 \pmod{a-1}.$$

For the twice primes $(p, p-2)$, a numerical illustration of this result is given in the Table 3.

$(p, p-2)$	$4^{p-1} - 4^{p-3}$
$(5, 3)$	3×80
$(7, 5)$	3×1280
$(13, 11)$	3×5242880
$(19, 17)$	3×21474836480

Table 3. Few values for $a = 4$

5. Convolved Fermat quotients

We consider the sequence $f_{n,m}^-(a)$ defined by the generating function

$$\frac{(a+1)^m z^m}{(1-(a-1)z-az^2)^m} = \sum_{n\geq 0} f_{n,m}^-(a) z^n, \ |z| < 1. \tag{5.1}$$

Definition 5.1. The convolved Fermat quotient $q_p^{(m)}(a)$ is given by the expression

$$q_p^{(m)}(a) = \frac{f_{p-1,m}^{-}(a)}{p} \text{ and } q_p^{(1)}(a) = q_p(a). \tag{5.2}$$

According to the identity

$$\frac{(a+1)^m z^m}{(1-(a-1)z-az^2)^m} = \left(\sum_{n\geq 0} f_n^{-}(a) z^n\right)\left(\sum_{n\geq 0} f_{n,m-1}^{-}(a) z^n\right),$$

a recursive formula of $f_{m,n}^{-}(a)$ is given as follows

$$f_{n,m}^{-}(a) = \sum_{k=0}^{n} f_{n-k,m-1}^{-}(a) f_k^{-}(a,-1).$$

It is obvious to remark that $f_{n,m}^{-}(a) = 0$ for $n < m$, thereafter for $n \geq m$ we have

$$f_{n,m}^{-}(a) = \sum_{k=m}^{n} f_{n-k,m-1}^{-}(a) f_k^{-}(a). \tag{5.3}$$

Equivalent recursive formula of $q_p^{(m)}(a)$ is

$$q_p^{(m)}(a) = \begin{cases} 0 & \text{if } p-1 < m, \\ \sum\limits_{k=m}^{p-1} f_{p-1-k,m}^{-}(a) f_{k,m}^{-}(a) & \text{if } p-1 \geq m. \end{cases}$$

The development of the quantity $\left(1-(a-1)z-az^2\right)^m$ conducts to

$$\left(1-(a-1)z-az^2\right)^m = \sum_{k=0}^{m}\sum_{j=0}^{k}\binom{m}{k}\binom{k}{j}(-1)^k a^j (a-1)^{k-j} z^{k+j}$$

and then

$$\left(1-(a-1)z-az^2\right)^m = \sum_{n=0}^{2m}\sum_{k=0}^{m}\binom{m}{k}\binom{k}{n-k}(-1)^k a^{n-k} (a-1)^{2k-n} z^n.$$

Letting

$$a_m(n) = \sum_{k=0}^{m}\binom{m}{k}\binom{k}{n-k}(-1)^k a^{n-k} (a-1)^{2k-n}.$$

Thus

$$\left(\sum_{n=0}^{2m} a_m(n) z^n\right)\left(\sum_{n\geq 0} f_{n,m}^{-}(a) z^n\right) = (a+1)^m z^m$$

and

$$\sum_{k=0}^{m} a_m(m-k) f_{k,m}^{-}(a) = (a+1)^m$$

and for $n \neq m$ we have

$$\sum_{k=0}^{n} a_m(n-k) f_{k,m}^{-}(a) = 0.$$

Furthermore $f_{m,m}^{-}(a) = (a+1)^m$ and for $n > m$ we have

$$\sum_{k=m}^{n} a_m(n-k) f_{k,m}^{-}(a) = 0.$$

The formula of $pq_p(a)$ by means of the sequence $f_{j,k}^{-}$ is given by the following theorem.

Theorem 5.2.

$$\begin{aligned}(p-1)_n pq_p(a) &= \sum_{k=0}^{n-1}(-1)^k\left(\frac{1}{a+1}\right)^{k+1}k!\left(B_{n,k}f^-_{k+p-1,k+1}(a)+nB_{n-1,k}f^-_{k+p,k+1}(a)\right)\\ &+ (-1)^n\left(\frac{1}{a+1}\right)^{n+1}n!B_{n,n}f^-_{n+p-1,n+1}(a).\end{aligned}$$

Proof. For $m=1$ we have $g(t)=z^{-1}$ and

$$D^n g\left(h(z)\right)=\sum_{k=0}^{n}(-1)^k k!\frac{B_{n,k}\left(1-a-2az,-2a,0,0\cdots\right)}{\left(1-(a-1)t-at^2\right)^{1+k}}.$$

But it is easily checked that

$$D^n\left(zg(h(z))\right)=zD^n g(h(z))+nD^{n-1}g(h(z))$$

and then

$$D^n\left(zg(h(z))\right)=\sum_{k=0}^{n}(-1)^k k!\frac{B_{n,k}\left(1-a-2az,-2a,0,0\cdots\right)z}{\left(1-(a-1)z-az^2\right)^{1+k}}+n\sum_{k=0}^{n-1}(-1)^k k!\frac{B_{n-1,k}\left(1-a-2az,-2a,0,0\cdots\right)}{\left(1-(a-1)z-az^2\right)^{1+k}}.$$

But we have

$$\frac{1}{\left(1-(a-1)z-az^2\right)^{1+k}}=\frac{(a+1)^{-k-1}}{z^{1+k}}\sum_{\ell\geq 0}f^-_{\ell,1+k}(a)z^\ell$$

then

$$\begin{aligned}\sum_{k=0}^{n}(-1)^k k!\frac{B_{n,k}z}{\left(1-(a-1)z-az^2\right)^{1+k}} &= \sum_{k=0}^{n}(-1)^k k!B_{n,k}\frac{(a+1)^{-1-k}}{z^k}\sum_{\ell\geq 0}f^-_{\ell,k+1}(a)z^\ell\\ &= \sum_{u\geq 0}\sum_{k=0}^{n}(-1)^k\left(\frac{1}{a+1}\right)^{k+1}k!B_{n,k}f^-_{k+u,k+1}(a)z^u\end{aligned}$$

and

$$\sum_{k=0}^{n-1}(-1)^k k!\frac{B_{n-1,k}}{\left(1-(a-1)z-az^2\right)^{1+k}} = \sum_{u\geq 0}\sum_{k=0}^{n-1}(-1)^k\left(\frac{1}{a+1}\right)^{k+1}k!B_{n-1,k}f^-_{k+u+1,k+1}(a)z^u.$$

Furthermore

$$D^n(zg(h(t)))=\sum_{u\geq 0}\sum_{k=0}^{n}(-1)^k\left(\frac{1}{a+1}\right)^{k+1}k!B_{n,k}f^-_{k+u,k+1}(a)z^u+n\sum_{u\geq 0}\sum_{k=0}^{n-1}(-1)^k\left(\frac{1}{a+1}\right)^{k+1}k!B_{n-1,k}f^-_{k+u+1,k+1}(a)z^u.$$

Then

$$(u)_n f^-_u(a,-1)=\sum_{k=0}^{n}(-1)^k\left(\frac{1}{a+1}\right)^{k+1}k!\left(B_{n,k}f^-_{k+u,k+1}(a)+nB_{n-1,k}f^-_{k+u+1,k+1}(a)\right)+(-1)^n\left(\frac{1}{a+1}\right)^{n+1}k!B_{n,n}f^-_{k+u,k+1}(a).$$

Substituting $u=p-1$ to get the desired result. □

Explicit formula of $q_p^{(m)}(a)$ is established in the following theorem.

Theorem 5.3. *The combinatorial formula of convolved Fermat quotient for $p\geq m+1$ is given by the relation*

$$q_p^{(m)}(a)=\frac{(a+1)^m m!}{p(p-1)!}\sum_{j=0}^{p-1-m}\binom{p-1}{p-1-m}(-m)_j B_{p-1-m,j}. \tag{5.4}$$

Proof. First we consider the functions

$$g(z) = z^{-m} \text{ and } h(z) = 1 - (a-1)z - az^2.$$

Since we have

$$D^k g(z) = (-m)_k z^{-m-k},$$

then using Faà di Bruno formula to show that

$$D^n g\left(h(z)\right) = \sum_{k=0}^{n} (-m)_k h^{-m-k}(z) B_{n,k}\left(1 - a - 2az, -2a, 0, 0 \cdots\right).$$

The application of Leibniz identity to the function $z^m g \circ h(z)$ conducts to

$$D^n\left(z^m g \circ h(z)\right) = \sum_{k=0}^{n} \sum_{j=0}^{k} \binom{n}{k} (m)_{n-k} (-m)_j z^{m-n+k} h^{-m-j}(z) B_{k,j}$$

and then

$$D^n\left(z^m g \circ h(z)\right)|_{z=0} = \sum_{j=0}^{n-m} \binom{n}{n-m} m!(-m)_j B_{n-m,j}.$$

But we have

$$(a+1)^m D^n\left(z^m g \circ h(z)\right) = \sum_{\ell \geq 0} (\ell)_n f^{-}_{\ell,m}(a) z^{\ell-n},$$

and then

$$n! f^{-}_{n,m}(a) = (a+1)^m \sum_{j=0}^{n-m} \binom{n}{n-m} m!(-m)_j B_{n-m,j}.$$

Substituting $n = p - 1$ to get the desired result. □

In the case $m = 1$ we have

$$q_p(a) = \frac{(a+1)}{p(p-2)!} \sum_{j=0}^{p-2} (-1)^j j! B_{p-2,j},$$

which is identical with the identity (4.5) of Theorem 4.5, by remarking that

$$B_{p-2,j} = \frac{(p-2)!}{j!} (-1)^j \binom{j}{p-2-j} (a-1)^{2j-p+2} a^{p-2-j}.$$

However all the problem concerning Fermat quotients can be extended to convolved Fermat quotients and obtained new open problems. The most important one is the Fermat last theorem. We know that $pq_p^{(1)}(a) \equiv 0 \pmod{p}$, are their others values of m for which the congruence stills true?

6. Conclusion

In the literature the Fermat quotients are the object of several works, especially the vanishing congruences. In this work we gave their generating functions; which allowed us to find several combinatorial formulas. This study permits to resolve some congruence problems and state new divisibility properties. We propose, as a perspective for this work to study the arithmetical properties of convolved Fermat quotients.

References

[1] T. Agoh and L. Skula, *The fourth power of the Fermat quotient*, J. Number Theory **128**, 2865–2873, 2008.
[2] T. Agoh, K. Dilcher and L. Skula, *Fermat quotients for composite moduli*, J. Number Theory **66**, 29–50, 1997.
[3] T. T. Bai and Q. M. Luo, *A simple proof of a binomial identity with applications*, Montes Taurus J. Pure Appl. Math. **1 (2)**, 13–20, 2019; Article ID: MTJPAM-D-19-00008.
[4] L. Comtet, *Advanced combinatorics*, Reidel, Boston, 1974.
[5] R. Crandall, K. Dilcher and C. Pomerance, *A search for Weileferich and Wilson primes*, Mathematics of Computation **66 (217)**, 433–449, 1997.
[6] K. Dilcher and L. Skula, *The cube of the fermat quotient*, Integers: Electronic J. of Combinatorial Number Theory **6**, #A24, 2006.
[7] G. Eisenstein, *Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert*, werden. Bericht. K. Preuss. Akad.Wiss. Berlin **15** , 36–42, 1850.
[8] R. Ernvall and T. Metsänkylä, *On the p-divisibilty of Fermats quotients*, Mathematics of Computation **66 (219)**, 1353–1365, 1997.
[9] F. Faà di Bruno, *Sullo Sviluppo delle funzioni*, Annali di Scienze e Matematiche fisiche **6**, 479–480, 1855.
[10] J. W. L. Glaisher, *On the residues of the sums of the inverse powers of numbers in arithmetical progression*, Quart. J. Math. **32**, 271–288, 1900.
[11] J. W. L. Glaisher, *On the residues of* r^{p-1} *to modulus* p^2*,* p^3*, etc.*, Quart. J. **32**, 1–27, 1900.
[12] M. Goubi *On composition of generating functions*, CJMS. **9 (2)**, 256–265, 2020.
[13] M. Goubi, *Explicit formula of a new class of q-Hermite-based Apostol-type polynomials and generalization*, Notes Numb. Theory Discr. Math. **26**, 93–102, 2020.
[14] M. Goubi, *On a generalized family of Euler-Genocchi polynomials*, Integers **21**, # 48, 2021.
[15] A. Granville, *The square of the Fermat quotient*, Integers: Electronic J. of Combinatorial Number Theory **4**, #A22, 2004.
[16] H. Ichimura, *Note on a congruence for the Fermat quotient with base* 2, Kyushu J. Math. **73**, 115–121, 2019.
[17] D. V. Kruchinin and M. Y. Perminova, *About solving some functional equations related to the Lagrange inversion theorem*, Montes Taurus J. Pure Appl. Math. **3 (1)**, 62–69, 2021; Article ID: MTJPAM-D-20-00011.
[18] L. Lianfei and M. Wenping *Almost perfect sequence pairs derived from Fermat quotient*, Electronics letters **55 (10)**, 599–601, 2019.
[19] R. Meštrović, *An elementary proof of a congruence by Skula and Granville*, Archivum Mathematicum **48**, 113–120, 2012.
[20] P. L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61**, 361–363, 1993.
[21] G. Ozdemir and Y. Simsek, *Generating functions for two-variable polynomials related to a family of Fibonacci type polynomials and numbers*, Filomat **30 (4)**, 969–975 2016.
[22] G. Ozdemir, Y. Simsek and G. V. Milovanović, *Generating functions for special polynomials and numbers including Apostol-type and Humbert-type polynomials*, Mediterr. J. Math. **14 (117)**, 1–17, 2017.
[23] F. Qi and B. N. Guo, Sums of infinite power series whose coefficients involve products of the Catalan-Qi numbers, Montes Taurus J. Pure Appl. Math. **1 (2)**, 1–12, 2019; Article ID: MTJPAM-D-19-00007.
[24] S. Roman, *The Formula of Faà di Bruno*, Amer. Math. Monthly **87 (10)**, 805–809, 1980.
[25] M. Z. Spivey, *Combinatorial sums and finite differences*, Discrete Math. **307**, 3130–3146, 2007.
[26] J. J. Sylvester, *Sur une propriété des nombres premiers qui se ratache au théorème de Fermat*, C. R. Acad. Sci. Paris **52**, 161–163, 1861.
[27] N. Terai, *Generalization of Lucas' Theorem for Fermat's Quotient II*, Tokyo J. Math. **13 (2)**, 278–287, 1990.
[28] H. S. Vandiver, *Fermat's quotient and related arithmetic functions*, Mathematics **31**, 55–60, 1945.