NEW PROPERTIES FOR A COMPOSITION OF SOME GENERATING FUNCTIONS FOR PRIMES

DMITRY V. KRUCHININ, YURIY V. SHABLYA

ABSTRACT. In this paper, we consider properties of coefficients of a generating functions composition, where the outer function is a logarithmic generating function and the inner function is an ordinary generating function with integer coefficients. Using notions of composita and composition of generating functions, we get new properties for this composition. The properties can be used for distinguishing prime numbers from composite numbers. As an application, obtained results can be used to obtain new primality criteria. We obtain primality criteria for the Mersenne numbers, the Lucas numbers, the Pell-Lucas numbers, the Jacobsthal-Lucas numbers, and the Lucas sequences.

KEYWORDS AND PHRASES: generating function, composition of generating function, composita, primality criterion.

1. INTRODUCTION

There are many authors who have studied generating functions and their properties (for instance, Comtet [2], Flajolet [3], Graham [4], Robert [9], Stanley [12], Wilf [14]). Generating functions are a powerful tool for solving problems in number theory, combinatorics, algebra, probability theory, and in other fields of mathematics. One of the advantages of generating functions is that an infinite number sequence can be represented in the form of single expression.

Definition 1.1. *The ordinary generating function of a sequence $\{a_n\}$ is the following formal power series*

$$A(x) = a_0 + a_1 x + a_2 x^2 + \ldots = \sum_{n \geq 0} a_n x^n.$$

There exist many operations on generating functions, such as addition, multiplication, integration, differentiation, and composition. In this paper, we consider properties of a composition of generating functions, where the outer function is a logarithmic generating function and the inner function is an ordinary generating function with integer coefficients.

The article structure is presented as follows:

- In section 2, we show basic rules for calculating the coefficients of the composition of generating functions and we give necessary mathematical notions.
- In section 3 we get the main results and give them in Theorem 3.1, Theorem 3.2 and Corollary 3.1.
- In section 4 we consider an application of obtained results.

2. COMPOSITION OF GENERATING FUNCTIONS

According to Stanley [13], the composition of generating functions is defined as follows:

Definition 2.1. *Suppose $R(x) = \sum_{n \geq 0} r_n x^n$ and $F(x) = \sum_{n > 0} f_n x^n$ are formal power series. Then the composition $G(x) = R(F(x)) = \sum_{n \geq 0} r_n F(x)^n$ is a well-defined formal power series.*

We consider a composition of generating functions $R(F(x))$, where the outer function $R(x)$ is a logarithmic generating function and the inner function $F(x)$ is an ordinary generating function with integer coefficients.

According to Robert [9], the logarithmic generating function is defined as follows:

Definition 2.2. *The logarithmic generating function is the generating function in the form*

$$R(x) = \sum_{n > 0} r_n x^n = \sum_{n > 0} \frac{a_n}{n} x^n.$$

To calculate the coefficients of the composition of generating functions, we use the mathematical notion of the composita of a given generating function, which was introduced by Kruchinin [6].

Definition 2.3. *The composita of the generating function $F(x) = \sum_{n > 0} f_n x^n$ is the function of two variables*

$$(1) \qquad F^{\Delta}(n, k) = \sum_{\pi_k \in C_n} f_{\lambda_1} f_{\lambda_2} \dots f_{\lambda_k},$$

where C_n is a set of all compositions of an integer n, π_k is the composition n into k parts such that $\sum_{i=1}^{k} \lambda_i = n$.

Also we can write the following condition

$$(F(x))^k = \sum_{n \geq k} F^{\Delta}(n, k) x^n.$$

Using the notion of the composita (1), we can obtain the coefficients of the composition of generating functions [6].

Lemma 2.1. *Suppose $F(x) = \sum_{n > 0} f_n x^n$ and $R(x) = \sum_{n \geq 0} r_n x^n$ are generating functions, and $F^{\Delta}(n, k)$ is the composita of $F(x)$. Then for the composition of the generating functions $G(x) = R(F(x))$ the coefficients of the generating function $G(x) = \sum_{n \geq 0} g_n x^n$ are*

$$(2) \qquad g_n = \begin{cases} r_0, & \text{if } n = 0; \\ \sum_{k=1}^{n} F^{\Delta}(n, k) r_k, & \text{if } n > 0. \end{cases}$$

3. MAIN RESULTS

We show the main results of this paper in the following theorems and their corollaries.

Theorem 3.1. *Suppose $F(x) = \sum_{n>0} f_n x^n$ is an ordinary generating function, $R(x) = \sum_{n>0} r_n x^n = \sum_{n>0} \frac{a_n}{n} x^n$ is a logarithmic generating function, $\{f_n\}$ and $\{a_n\}$ are integer sequences, $G(x) = \sum_{n>0} g_n x^n$ is a generating function, which is the composition of the generating functions $G(x) = R(F(x))$. Then the value of*

$$(3) \qquad ng_n = n \sum_{k=1}^{n} F^{\Delta}(n,k) r_k = n \sum_{k=1}^{n} \frac{F^{\Delta}(n,k) a_k}{k}$$

is integer for $n \in \mathbb{N}$.

Proof. According to (2), the coefficients of the generating function $G(x)$ are

$$(4) \qquad g_n = \sum_{k=1}^{n} F^{\Delta}(n,k) r_k = \sum_{k=1}^{n} \frac{F^{\Delta}(n,k) a_k}{k}.$$

The derivative of the generating function $G(x) = \sum_{n>0} g_n x^n$ (see [7]) is the function

$$G'(x) = g_1 + 2g_2 x^2 + 3g_3 x^2 + \ldots + ng_n x^{n-1} + \ldots = \sum_{n>0} ng_n x^{n-1}.$$

Also, we can obtain the derivative of the generating function $G(x)$

$$G'(x) = (R(F(x)))' = F'(x) R'(F(x)).$$

Since $\{nf_n\}$ is an integer sequence, then the coefficients of the generating function $F'(x) = \sum_{n>0} nf_n x^{n-1}$ are integer.

Since $\{a_n\}$ is an integer sequence, then the coefficients of the generating function $R'(x) = \sum_{n>0} nr_n x^{n-1} = \sum_{n>0} a_n x^{n-1}$ are integer.

Since $F(x)$ and $R'(x)$ are generating functions with integer coefficients, then the coefficients of the composition of the generating functions $R'(F(x))$ are also integer.

The coefficients of the product of generating functions with integer coefficients are also integer, so $G'(x) = F'(x) R'(F(x)) = \sum_{n>0} ng_n x^{n-1}$ is the generating function with integer coefficients.

Therefore, $\{ng_n\}$ is an integer sequence.

The theorem is proved: the value of the expression (3) is integer. $\qquad \square$

From Theorem 3.1 we obtain a new important property of the coefficients of the generating functions composition:

Corollary 3.1. *The value of the coefficients function (4) without the n-th term*

$$(5) \qquad \sum_{k=1}^{n-1} \frac{F^{\Delta}(n,k) a_k}{k} = \frac{ng_n - a_n f_1^n}{n}$$

is integer for every prime n. The converse is not true.

Proof. Let us consider the expression (3). The value of the n-th term in the sum (3) is equal to the integer expression

$$n \frac{F^{\Delta}(n,n) a_n}{n} = a_n f_1^n.$$

Then the value of the expression

$$ng_n - a_n f_1^n = n \sum_{k=1}^{n-1} \frac{F^\Delta(n,k)a_k}{k}$$

is integer.

The coefficients of the generating function $F(x) = \sum_{n>0} f_n x^{n-1}$ are integer. Then the values of the composita $F^\Delta(n,k)$ are integer.

Since n is a prime, $n > k$, $F^\Delta(n,k)$ and a_k are integer, then the expression (5) is integer. $\qquad\square$

The expression (5) is integer for every prime n. It can be used for distinguishing prime numbers from composite numbers. For composite numbers n the value of the expression (5) can be integer or not integer. But if the value of the expression (5) is not integer, then n is determinately a composite number.

We note that an integral of the generating function $B(x) = \sum_{n\geq 0} b_n x^n$ through term by term integration of power series (see [7]) is the function

$$(6) \qquad \int B(x) = b_0 x + b_1 \frac{x^2}{2} + b_2 \frac{x^3}{3} + \ldots + b_n \frac{x^{n+1}}{n+1} + \ldots = \sum_{n>0} \frac{b_{n-1}}{n} x^n.$$

Then Theorem 3.1 takes the following form:

Theorem 3.2. *Suppose $B(x) = \sum_{n\geq 0} b_n x^n$ and $F(x) = \sum_{n>0} f_n x^n$ are ordinary generating functions with integer coefficients, $G(x) = \sum_{n>0} g_n x^n$ is a generating function, that is the composition of the generating functions $G(x) = R(F(x))$, where $R(x) = \int B(x)$. Then the value of*

$$ng_n = n \sum_{k=1}^{n} \frac{F^\Delta(n,k)b_{k-1}}{k}$$

is integer for $n \in \mathbb{N}$.

Proof. If in (6) we consider a sequence $\{a_n\}$, where $a_n = b_{n-1}$ for every integer $n = 1, 2, \ldots$, then we obtain the logarithmic generating function

$$\int B(x) = \sum_{n>0} \frac{b_{n-1}}{n} x^n = \sum_{n>0} \frac{a_n}{n} x^n = \sum_{n>0} r_n x^n = R(x).$$

According to Theorem 3.1, the value of the expression

$$ng_n = n \sum_{k=1}^{n} \frac{F^\Delta(n,k)a_k}{k} = n \sum_{k=1}^{n} \frac{F^\Delta(n,k)b_{k-1}}{k}$$

is integer for $n \in \mathbb{N}$. $\qquad\square$

Also, the value of the expression

$$\sum_{k=1}^{n-1} \frac{F^\Delta(n,k)b_{k-1}}{k} = \frac{ng_n - b_{n-1}f_1^n}{n}$$

is integer for every prime n. The converse is not true.

4. APPLICATION

The obtained results can be used in public-key cryptography [11]. The obtained properties of the composition of generating functions can be used in constructing new primality criteria. The primality criterion is a statement that necessarily must be satisfied for primes. Such criteria may be used as the basis for the probabilistic primality tests. If the number does not satisfy the conditions of tests, then probabilistic primality tests can exactly detect that the number n is composite. If the number satisfies all conditions, then n is a prime with a certain probability. Often repeating the test with different parameters can reduce the probability of error. Using the obtained properties of the composition of generating functions, we consider several examples of construction of primality criteria.

Example 4.1. Let us consider the following composition of the generating functions $G(x) = R\left(F(x)\right)$, where

$$(7) \qquad F(x) = \frac{bx}{1 - ax} = \sum_{n>0} ba^{n-1}x^n$$

is a generating function with integer coefficients, b and a are integer;

$$R(x) = \ln\left(\frac{1}{1-x}\right) = \sum_{n>0} \frac{1}{n}x^n$$

is a logarithmic generating function.

Since the composita of the generating function (7) is (see [5])

$$F^\Delta(n, k, a, b) = \binom{n-1}{k-1}a^{n-k}b^k,$$

then the coefficients of the composition $G(x) = R\left(F(x)\right)$ are given by

$$(8) \qquad g_n = \sum_{k=1}^{n} \binom{n-1}{k-1}\frac{a^{n-k}b^k}{k}.$$

Using (5), we get the primality criterion: the value of expression

$$\sum_{k=1}^{n-1} \binom{n-1}{k-1}\frac{a^{n-k}b^k}{k} = \frac{(a+b)^n - a^n - b^n}{n}.$$

is integer for every prime n.

After some transformations, we obtain the following primality criterion: if n is prime, then

$$(9) \qquad (a+b)^n - a^n - b^n \equiv 0 \mod n.$$

Obtained expression is similar to the Fermat's little theorem [1].

Since the following condition

$$a^n \equiv a \mod n$$

holds true for every prime n and integer a, then we transform (9) into the following primality criterion: if n is prime, then

$$(10) \qquad (a+b)^n \equiv a+b \mod n.$$

Substituting c for $(a + b)$ in (10), we get the Fermat's little theorem: if n is prime, then for every $c \in \{1, 2, \ldots, n - 1\}$

$$c^{n-1} \equiv 1 \mod n.$$

The Fermat's little theorem has had a great influence in algorithmic number theory as it has been the basis for some of the most well-known primality tests: Fermat primality test, Solovay-Strassen primality test, Miller-Rabin primality test, AKS primality test, etc. (see [1]). The first three are probabilistic polynomial time algorithms and are widely used in practice, the fourth one is the only known deterministic polynomial time algorithm.

If we set $a = 1$ and $b = 1$ in (8), then we obtain

$$ng_n = \{1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, \ldots\} = 2^n - 1 = M_n,$$

where M_n is the Mersenne number (the sequence A000225 in The On-Line Encyclopedia of Integer Sequences [10]).

Therefore, using Corollary 3.1, we obtain the primality criterion: if n is prime, then

$$M_n \equiv 1 \mod n.$$

Example 4.2. Let us consider the following composition of generating functions $G(x) = R(F(x))$, where

(11) $$F(x) = ax + bx^2$$

is a generating function with integer coefficients, b and a are integer;

$$R(x) = \ln\left(\frac{1}{1-x}\right) = \sum_{n>0} \frac{1}{n} x^n$$

is a logarithmic generating function.

Since the composita of the generating function (11) is (see [5])

$$F^{\Delta}(n, k, a, b) = \binom{k}{n-k} a^{2k-n} b^{n-k},$$

then the coefficients of the composition $G(x) = R(F(x))$ are given by

(12) $$g_n = \sum_{k=1}^{n} \binom{k}{n-k} \frac{a^{2k-n} b^{n-k}}{k}.$$

Using (5), we get the new primality criterion: the value of expression

(13) $$\sum_{k=1}^{n-1} \binom{n-1}{k-1} \frac{a^{n-k} b^k}{k} = \frac{\left(\frac{a+\sqrt{a^2+4b}}{2}\right)^n + \left(\frac{a-\sqrt{a^2+4b}}{2}\right)^n - a^n}{n}$$

is integer for every prime n.

We consider special cases of a and b.

Set $a = 1$ and $b = 1$ in (12), then we obtain

$$ng_n = \{1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots\} = \left(\frac{1 + \sqrt{5}}{2}\right)^n + \left(\frac{1 - \sqrt{5}}{2}\right)^n = L_n,$$

where L_n is the Lucas number (the sequence A000032 in The On-Line Encyclopedia of Integer Sequences [10]).

Therefore, the primality criterion: if n is prime, then

$$L_n \equiv 1 \mod n.$$

Set $a = 2$ and $b = 1$ in (12), then we obtain

$$ng_n = \{2, 6, 14, 34, 82, 198, 478, 1154, 2786, \ldots\} = (1+\sqrt{2})^n + (1-\sqrt{2})^n = Q_n,$$

where Q_n is the Pell-Lucas number (the sequence A002203 in The On-Line Encyclopedia of Integer Sequences [10]).

Therefore, the primality criterion: if n is prime, then

$$Q_n \equiv 2 \mod n.$$

Set $a = 1$ and $b = 2$ in (12), then we obtain

$$ng_n = \{1, 5, 7, 17, 31, 65, 127, 257, 511, 1025, \ldots\} = 2^n + (-1)^n = j_n,$$

where j_n is the Jacobsthal-Lucas number (the sequence A014551 in The On-Line Encyclopedia of Integer Sequences [10]).

Therefore, the primality criterion: if n is prime, then

$$j_n \equiv 1 \mod n.$$

Next we consider the Lucas sequence [8]

$$V_n(P, Q) = \left(\frac{P + \sqrt{P^2 - 4Q}}{2} \right)^n + \left(\frac{P - \sqrt{P^2 - 4Q}}{2} \right)^n,$$

and set $a = P$, $b = -Q$ in expression (13), then we obtain the primality criterion: the value of expression

$$\frac{V_n(P, Q) - P^n}{n}$$

is integer for every prime n.

After some transformations, we obtain the following primality criterion: if n is prime, then

$$V_n(P, Q) \equiv P \mod n.$$

REFERENCES

[1] M. AGRAWAL: *Primality tests based on Fermat's little theorem*. Distributed Computing and Networking, 2006, 288–293.
[2] L. COMTET: *Advanced combinatorics*. D. Reidel Publishing Company, 1974.
[3] P. FLAJOLET, R. SEDGEWICK: *Analytic combinatorics*, Cambridge University Press, 2009.
[4] R. L. GRAHAM, D. E. KNUTH, O. PATASHNIK: *Concrete mathematics*, Addison-Wesley, 1989.
[5] D. V. KRUCHININ, V. V. KRUCHININ: *Application of a composition of generating functions for obtaining explicit formulas of polynomials*, Journal of Mathematical Analysis and Applications, **404** (2013), 161–171.
[6] V. V. KRUCHININ, D. V. KRUCHININ: *Composita and its properties*, Journal of Analysis and Number Theory, **2** (2014), 37–44.
[7] S. K. LANDO: *Lectures on generating functions*, American Mathematical Society, 2003.
[8] P. RIBENBOIM: *The little book of bigger primes*, New York: Springer-Verlag, 2004, 44–62.

[9] A. M. ROBERT: *A course in p-adic analysis*, Springer, 2000.

[10] N. J. A. SLOANE: *The on-line encyclopedia of integer sequences*, http://oeis.org.

[11] Y. SONG: *Primality testing and integer factorization in public-key cryptography*, Springer, 2009.

[12] R. P. STANLEY: *Generating functions*, in Studies in Combinatorics, Mathematical Association of America, 1978, 100–141.

[13] R. P. STANLEY: *Enumerative combinatorics, Volume 2*, Cambridge University Press, 1999, 1–158

[14] H. S. WILF: *Generatingfunctionology*, New York: Academic Press, 1994.

TOMSK STATE UNIVERSITY OF CONTROL SYSTEMS AND RADIOELECTRONICS, TOMSK, RUSSIA

E-mail address: kruchininDm@gmail.com