

Transcendence of binomial and Lucas' formal power series

J.-P. Allouche, D. Gouyou-Beauchamps
CNRS and Université Paris-Sud
LRI, Bâtiment 490
F-91405 Orsay Cedex (France)
allouche@lri.fr dgb@lri.fr

G. Skordev
CEVIS, Universität Bremen
Universitätsallee 29
D-28359 Bremen (Germany)
skordev@cevis.uni-bremen.de

Abstract

The formal power series $\sum_{n \geq 0} \binom{2n}{n}^t X^n$ is transcendental over $\mathbb{Q}(X)$ when t is an integer ≥ 2 . This is due to Stanley for t even, and independently to Flajolet and to Woodcock and Sharif for the general case. While Stanley and Flajolet used analytic methods and studied the asymptotics of the coefficients of this series, Woodcock and Sharif gave a purely algebraic proof. Their basic idea is to reduce this series modulo prime numbers p , and to use the *p-Lucas property*: if $n = \sum n_i p^i$ is the base p expansion of the integer n , then $\binom{2n}{n} \equiv \prod \binom{2n_i}{n_i} \pmod{p}$. The series reduced modulo p is then proved algebraic over $\mathbb{F}_p(X)$, the field of rational functions over the Galois field \mathbb{F}_p , but its degree is not a bounded function of p . We generalize this method to characterize all formal power series that have the p -Lucas property for “many” prime numbers p , and that are furthermore algebraic over $\mathbb{Q}(X)$.

Keywords: Transcendence of formal power series, binomial coefficients, Lucas' property, Legendre polynomials.

1 Introduction

In 1980 R. P. Stanley [21] noted that the series $F_t(X) = \sum_{n=0}^{\infty} \binom{2n}{n}^t X^n$ is transcendental over $\mathbb{C}(X)$ for t any even integer > 1 , and he asked whether the series $F_t(X)$ is transcendental over $\mathbb{C}(X)$ for any integer $t > 1$. The transcendence for all integer values of $t > 1$ was proved by Flajolet [8, p. 294] who studied the asymptotic behavior of the coefficients, and by Woodcock and Sharif [24]. The argument of Woodcock and Sharif, for proving the transcendence of

the series $F_t(X)$ over $K(X)$, where K is a (commutative) field of characteristic zero, consists in reducing the series modulo prime numbers: if the series $F_t(X)$ were algebraic of degree d over, say, $\mathbb{Q}(X)$, then, its reduction modulo any prime number p would be algebraic of degree d_p over $\mathbb{F}_p(X)$, the field of rational functions with coefficients in the Galois field \mathbb{F}_p , and $d_p \leq d$. It then suffices to exhibit a sequence of prime numbers p for which $F_t(X) \bmod p$ is algebraic of degree d_p over $\mathbb{F}_p(X)$, such that d_p is not bounded. Woodcock and Sharif also indicate their method works for proving the transcendence of the multinomial series $\sum_{n=0}^{\infty} \binom{kn}{n, n, \dots, n}^t X^n$, where $t \geq 1$ and $k \geq 3$. (Note that the case $k = 3, t = 1$ is addressed in [8].)

Let us be more precise. The series $F_1(X)$ satisfies $F_1(X) = (1-4X)^{-1/2}$, when considered as a series with, say, rational coefficients. Hence $(1-4X)F_1^2(X) - 1 = 0$: since F_1 has integer coefficients, this proves that $F_1(X) \bmod p$ is algebraic over $\mathbb{F}_p(X)$ for any prime number p . This implies that the series $F_t(X) \bmod p$ is algebraic over $\mathbb{F}_p(X)$, since this is the Hadamard product of algebraic series over a field of positive characteristic (see [9, 6, 20, 13, 1]). To compute its degree, Woodcock and Sharif note, using Lucas' Theorem [18], that

$$F_t^{p-1}(X) \equiv \left(\sum_{i=0}^{(p-1)/2} \binom{2i}{i}^t X^i \right)^{-1} \bmod p.$$

Their last step is to prove there exists δ_p such that all irreducible factors of the polynomial $T^{p-1} - \left(\sum_{i=0}^{(p-1)/2} \binom{2i}{i}^t X^i \right)^{-1} \in \mathbb{F}_p(X)[T]$ have degree $\geq \delta_p$, and that δ_p is not bounded.

In what follows we replace the series $F_t(X)$ by the series $G(X) = \sum_{n=0}^{\infty} u(n)X^n$ where $(u(n))_{n \geq 0}$ is a sequence of rational numbers that has the p -Lucas property (see [19]) for “many” prime numbers p . We say that the sequence $(u(n))_{n \geq 0} \in \mathbb{Q}^{\mathbb{N}}$ has the p -Lucas property if the denominators of the u_n 's are not divisible by p , and if

$$\forall n \geq 0, \forall i, j \in [0, p-1], u(pn + j) \equiv u(n)u(j) \bmod p.$$

If the coefficients of the formal power series $G(X)$ have the p -Lucas property for all large primes p , there are two (easy) cases where $G(X)$ is algebraic over $\mathbb{Q}(X)$, one is the case where $G(X) = F_1(X)$, the other corresponds to $u(n)$ being the value of Legendre polynomials at some point. These cases are essentially the only cases of algebraicity: we prove that, *if the sequence $(u(n))_{n \geq 0}$ has the p -Lucas property for all large primes p , then, the series $G(X) = \sum_{n=0}^{\infty} u(n)X^n$ is transcendental if and only if the sequence $(u(n))_{n \geq 0}$ is neither equal to the sequence $(\alpha^n \binom{2n}{n})_{n \geq 0}$ for some $\alpha \in \mathbb{Q}$, nor to the sequence $(\gamma^n P_n(\lambda))_{n \geq 0}$, where $P_n(X)$ is the sequence of Legendre polynomials, for some γ and λ , where $\gamma^2 \in \mathbb{Q}$ and $\gamma\lambda \in \mathbb{Q}$.*

Actually we prove more: *Let s be an even integer ≥ 2 . A formal power series $F(X)$ with coefficients in \mathbb{Q} has the p -Lucas property for all large primes $p \equiv 1 \pmod{s}$ and is algebraic over $\mathbb{Q}(X)$ if and only if there exists a polynomial $P(X) \in \mathbb{Q}(X)$ of degree $\leq s$ such that $F(X) = P(X)^{-1/s}$.* Of course the restriction s even is not really a loss of generality: if an odd prime number is congruent to 1 modulo $2b+1$, it is necessarily congruent to 1 modulo $2(2b+1)$.

Note that transcendence results for power series are useful in different domains. Roughly speaking, a formal power series is algebraic if the object it represents has a strong underlying structure:

- In number theory. See, among many examples, [5] where the first step towards proving the transcendence of the Thue-Morse real number is to prove that a power series is transcendental.
- In group theory. See for example the survey [12] on growth functions of finitely generated groups.
- In theoretical computer science. The Chomsky-Schützenberger Theorem [4] asserts that *the generating series of a non-ambiguous context-free language is algebraic over $\mathbb{Q}(X)$* . For more information about generating series of languages, the reader can read [15] for example, and for a systematic survey of (analytic) methods for proving the transcendence of generating series, the reader is referred to [8].

2 Sequences and power series with Lucas' property

A well-known result of Lucas [18] asserts that, if p is a prime number and if $0 \leq i, j \leq p - 1$, then, for all $m, n \geq 0$,

$$\binom{pm + i}{pn + j} \equiv \binom{m}{n} \binom{i}{j} \pmod{p}.$$

McIntosh proposed in [19] the following definition. A function $u : \mathbb{N} \rightarrow \mathbb{Z}$ is said to have *the Lucas property* if $u(0) = 1$, and, for every prime p , every i in $[0, p - 1]$, and every $n \geq 0$, the equality $u(pn + i) \equiv u(n)u(i) \pmod{p}$ holds. Of course this definition is equivalent to saying that, for n having base- p expansion $n = \sum n_k p^k$ (where $0 \leq n_k \leq p - 1$ and only a finite number of n_k 's are non-zero) we have $u(n) \equiv \prod u(n_k) \pmod{p}$. An analogous definition (*double Lucas property*) is given in [19] for a function $u : \mathbb{N}^2 \rightarrow \mathbb{Z}$ with the extra condition that $u(n, k) = 0$ for $n < k$. We give here the following definition.

Definition *Let p be a prime number. A sequence $u = (u(n))_{n \geq 0} \in \mathbb{Q}^{\mathbb{N}}$ is said to have the p -Lucas property if the denominators of the u_n 's are not divisible by p , and if*

$$\forall i \in [0, p - 1], \forall n \geq 0, u(pn + i) \equiv u(n)u(i) \pmod{p}.$$

Remarks 1

- Note that a sequence with the p -Lucas property satisfies $u(0) \equiv 0 \pmod{p}$ or $u(0) \equiv 1 \pmod{p}$. Furthermore, if $u(0) \equiv 0 \pmod{p}$, then $u(j) \equiv 0 \pmod{p}$ for all $j \in [0, p - 1]$, hence, the sequence $(u(n))_{n \geq 0}$ is zero modulo p .

- In what follows we will consider sequences that are p -Lucas for infinitely many primes. What precedes implies that such a sequence either satisfies $u(n) = 0$ for all $n \geq 0$, or $u(0) = 1$.

3 Condition of algebraicity for Lucas' formal power series. The main Theorem

Inspired by the method of [24], with slight modifications, we give in this section a necessary and sufficient condition for a formal power series with rational coefficients to both have the p -Lucas property for “many” primes p and to be algebraic over $\mathbb{Q}(X)$. (Note that [20, Theorem 6.1] implies that a formal power series with rational coefficients is algebraic over $\mathbb{Q}(X)$ if and only if it is algebraic over $K(X)$, where K is any commutative field of characteristic zero.) We start with three useful lemmas: the first one is a generalization of a lemma of [24], the second one is given in [24] for integer coefficients.

Lemma 1 *Let s be a given even integer ≥ 2 . Let a be a large integer. Then, there exist infinitely many prime numbers p such that*

- $p \equiv 1 \pmod{s}$,
- any divisor of $p - 1$ either divides s or is larger than a .

Proof.

Let $s = \prod_{i=1}^k p_i^{\alpha_i}$ be the decomposition of s into primes, with $p_1 = 2 < p_2 < \dots < p_k$. It suffices to prove the lemma for a prime $> \max p_j$. Define $\bar{\omega} = \prod_{p \text{ prime}, p \leq a, p \nmid s} p$. Note that $\bar{\omega}$ is odd. The solutions of the system of congruences

$$\begin{cases} x \equiv p_j^{\alpha_j} + 1 \pmod{p_j^{\alpha_j+1}}, & j = 1, 2, \dots, k, \\ x \equiv 2 \pmod{\bar{\omega}}, \end{cases}$$

are the numbers $x \equiv c \pmod{\bar{\omega} \prod_{j=1}^k p_j^{\alpha_j+1}}$, for some $c \in \mathbb{Z}$, since $\bar{\omega}$ and $\prod_{j=1}^k p_j^{\alpha_j+1}$ are coprime. Furthermore c and $\bar{\omega} \prod_{j=1}^k p_j^{\alpha_j+1}$ are coprime, since $p_j^{\alpha_j} + 1$ and $p_j^{\alpha_j+1}$ are coprime, and $\bar{\omega}$ is odd. Hence, by Dirichlet's Theorem on primes in arithmetic progressions, there exist infinitely many primes p satisfying

$$\begin{cases} p \equiv p_j^{\alpha_j} + 1 \pmod{p_j^{\alpha_j+1}}, & j = 1, 2, \dots, k, \\ p \equiv 2 \pmod{\bar{\omega}}. \end{cases}$$

For such a prime, we have $p \equiv 1 \pmod{s}$, and

$$\begin{cases} p - 1 \equiv p_j^{\alpha_j} \pmod{p_j^{\alpha_j+1}}, & j = 1, 2, \dots, k, \\ p - 1 \equiv 1 \pmod{\bar{\omega}}. \end{cases}$$

Now let $\delta | (p - 1)$. The prime factors of δ cannot divide $\bar{\omega}$. Those that belong to $\{p_1, \dots, p_k\}$ occur in δ with an exponent at most equal to the one they have in s . Any other prime divisor of δ is $> a$. Hence, either $\delta | s$ or $\delta > a$. \square

Lemma 2 (see [24]) *Let $H(X) = \sum_{n=0}^{\infty} h_n X^n$ a formal power series with rational coefficients. If $H(X)$ is algebraic of degree d over $\mathbb{Q}(X)$, then, for any prime number p that does not divide any of the denominators of the coefficients of $H(X)$, the formal power series $\sum_{n=0}^{\infty} (h_n \bmod p) X^n$ is algebraic over $\mathbb{F}_p(X)$, and its degree is $\leq d$.*

The proof is straightforward: it consists in projecting modulo p the minimal polynomial of $H(X)$.

Lemma 3 *Let $G(X) = \sum_{n \geq 0} b_n X^n$ be a formal power series with coefficients in the finite field \mathbb{F}_p . If $G(0) = 1$ and $G(X)^{p-1} = 1$, then $G(X) = 1$.*

Proof.

Since $G(X)^{p-1} = 1$, we have $G(X)^p - G(X) = 0$. Now, in the field $K = \mathbb{F}_p(X)$, as in any commutative field of characteristic p , the solutions of $Z^p - Z = 0$ are $Z = 0, 1, \dots, p-1$. \square

We are now ready for our main Theorem.

Theorem 1 *Let s be an integer ≥ 2 . Define $s' = s$ if s is even, and $s' = 2s$ if s is odd. Let $F(X) = \sum_{n=0}^{\infty} a_n X^n$ be a nonzero formal power series with coefficients in \mathbb{Q} . Then, the following conditions are equivalent:*

- (i) *The sequence $(a_n)_{n \geq 0}$ has the p -Lucas property, for all large $p \equiv 1 \pmod{s}$, and the formal power series $F(X)$ is algebraic over $\mathbb{Q}(X)$;*
- (ii) *There exists a polynomial P with coefficients in \mathbb{Q} , of degree $\leq s'$, with $P(0) = 1$, such that $F(X) = (P(X))^{-1/s'}$.*

If s is odd, and if the number s' is replaced by s in the statement (ii), we still have (ii) implies (i), but the converse is not necessarily true.

Proof.

We first suppose that s is even, hence $s' = s$. Suppose that the formal power series $F(X) = \sum_{n \geq 0} a_n X^n$ is algebraic over $\mathbb{Q}(X)$, and that its coefficients have the p -Lucas property for all large primes p congruent to 1 modulo s . For such a p we have

$$\begin{aligned}
F(X) &= \sum_{n=0}^{\infty} a_n X^n = \sum_{j=0}^{p-1} \sum_{n=0}^{\infty} a_{pn+j} X^{pn+j} \\
&\equiv \sum_{j=0}^{p-1} \sum_{n=0}^{\infty} a_n a_j X^{pn} X^j \pmod{p} \\
&\equiv \sum_{j=0}^{p-1} a_j X^j \sum_{n=0}^{\infty} a_n X^{pn} \pmod{p} \\
&\equiv \left(\sum_{j=0}^{p-1} a_j X^j \right) \left(\sum_{n=0}^{\infty} a_n X^n \right)^p \pmod{p} \\
&\equiv \left(\sum_{j=0}^{p-1} a_j X^j \right) F^p(X) \pmod{p}
\end{aligned}$$

Hence $F(X)$ satisfies

$$F^{p-1}(X) \equiv \left(\sum_{j=0}^{p-1} a_j X^j \right)^{-1} \pmod{p}.$$

Since $F^{p-1}(X)$ belongs to $\mathbb{F}_p(X)$, and since $\mathbb{F}_p(X)$ contains a primitive $(p-1)$ -th root of unity (any generator of the cyclic group \mathbb{F}_p^\times), we know (see for example [16, p. 207]) that the minimal polynomial of $F(X)$ over $\mathbb{F}_p(X)$ is of the form $T^{d_p} - F^{d_p}$, where $d_p | (p-1)$. In particular F^{d_p} belongs to $\mathbb{Q}(X)$. If the degree d_p were not a divisor of s , this would imply from Lemma 1 the inequality $d_p > a$. Taking a to be the degree of $F(X)$ over $\mathbb{Q}(X)$, and using Lemma 2, we would obtain a contradiction. Hence, the degree d_p of $(F(X) \bmod p)$ over $\mathbb{F}_p(X)$ divides s . Hence, $(F(X)^s \bmod p)$ belongs to $\mathbb{F}_p(X)$. Let $F(X)^s \equiv U_p(X)/V_p(X) \bmod p$ where U_p and V_p are polynomials (depending on p) in $\mathbb{Z}[X]$ such that $(U_p \bmod p)$ and $(V_p \bmod p)$ are coprime. Then, since $p \equiv 1 \pmod{s}$,

$$1 / \left(\sum_{j=0}^{p-1} a_j X^j \right) \equiv F(X)^{p-1} \equiv (F(X)^s)^{(p-1)/s} \equiv (U_p(X)/V_p(X))^{(p-1)/s} \pmod{p}.$$

This implies

$$\left(\sum_{j=0}^{p-1} a_j X^j \right) U_p^{(p-1)/s}(X) \equiv V_p^{(p-1)/s}(X) \pmod{p}.$$

Since $(U_p \bmod p)$ and $(V_p \bmod p)$ are coprime, we have that $(U_p(X)^{(p-1)/s} \bmod p)$ is a constant c_p . This implies

$$c_p \left(\sum_{j=0}^{p-1} a_j X^j \right) \equiv V_p(X)^{(p-1)/s} \pmod{p}.$$

Hence, the degree of $(V_p(X) \bmod p)$ is at most s , and we have

$$\frac{c_p}{F(X)^{p-1}} \equiv V_p(X)^{(p-1)/s} \pmod{p}.$$

Taking $X = 0$ proves that

$$c_p \equiv F(0)^{p-1} V_p(0)^{(p-1)/s} \equiv a_0^{p-1} V_p(0)^{(p-1)/s} \equiv V_p(0)^{(p-1)/s} \pmod{p}.$$

Hence, by defining $W_p(X) = V_p(X)/V_p(0)$, we have

$$\frac{1}{F(X)^{p-1}} \equiv W_p(X)^{(p-1)/s} \pmod{p},$$

where the degree of $(W_p(X) \bmod p)$ is at most s . But this congruence implies

$$(F(X)^s W_p(X))^{p-1} \equiv 1 \pmod{p}.$$

This implies, using Lemma 3, the congruence

$$F(X)^s W_p(X) \equiv 1 \pmod{p},$$

i.e.,

$$\frac{1}{F(X)^s} \equiv W_p(X) \pmod{p}.$$

The formal power series $1/F(X)^s$, reduced modulo p , is a polynomial of degree bounded by s , for infinitely many primes p . Hence, this formal power series is a polynomial P of degree at most s in $\mathbb{Q}(X)$. Hence $F(X) = P(X)^{-1/s}$. Of course $P(0) = 1$ since $a_0 = 1$.

The case where s is odd is addressed by noting that: an odd prime number congruent to 1 modulo s , with s odd, is also congruent to 1 modulo $2s$.

Suppose conversely that there exists a polynomial $P(X)$ in $\mathbb{Q}(X)$, of degree less than or equal to s (s is not necessarily even), with $P(0) = 1$, such that $F(X) = P(X)^{-1/s}$. The formal power series $F(X)$ is clearly algebraic over $\mathbb{Q}(X)$. To prove that its coefficients have the p -Lucas property for all large primes $p \equiv 1 \pmod{s}$, we mimic a proof that can be found for example in [2] for the generating function of Legendre's polynomials. Let p be a prime number such that $p = 1 + \lambda s$. We take p large enough so that none of the coefficients of the polynomial $P(X)$ has its denominator divisible by p . Then $F(X)^{p-1} = F(X)^{\lambda s} = P(X)^{-\lambda}$. Hence

$$F(X) = \frac{F(X)^p}{F(X)^{p-1}} = F(X)^p P(X)^\lambda.$$

Now the degree of the polynomial $P(X)^\lambda$ is at most $\lambda s = p - 1$. Hence, writing $P(X)^\lambda = \sum_{j=0}^{p-1} c_j X^j$, and $F(X) = \sum_{n=0}^{\infty} a_n X^n$, we have

$$\sum_{n=0}^{\infty} a_n X^n \equiv \sum_{n=0}^{\infty} a_n X^{pn} \sum_{j=0}^{p-1} c_j X^j \pmod{p}.$$

We easily deduce that, for each $j \in [0, p-1]$, and all $n \geq 0$,

$$a_{pn+j} \equiv a_n c_j \pmod{p}.$$

Taking $n = 0$ proves that $c_j = a_j$, since $a_0 = P(0) = 1$. Hence, the sequence $(a_n)_{n \geq 0}$ has the p -Lucas property.

To finish the proof, let us prove our last assertion, by giving for each odd s an example of a sequence $(a_n)_{n \geq 0}$ that has the p -Lucas property for all large primes $p \equiv 1 \pmod{s}$, but such that the formal power series $F(X) = \sum a_n X^n$, though algebraic, is *not* of the form $F(X) = P(X)^{-1/s}$ for some polynomial $P(X)$ of degree at most s . Namely, let $a_n = \binom{2n}{n}$. Hence $F(X) = \sum a_n X^n = (1 - 4X)^{-1/2}$. We know that the sequence $(a_n)_{n \geq 0}$ has the p -Lucas property for all primes p , hence, for all primes $p \equiv 1 \pmod{s}$, where s is any odd integer ≥ 2 . We claim that $F(X)$ cannot be equal to $P(X)^{-1/s}$, where P is any polynomial: if $(1 - 4X)^{-1/2} = P(X)^{-1/s}$, then $P(X)^2 = (1 - 4X)^s$. Decomposing $P(X)$ into factors of degree 1 in $\mathbb{C}(X)$ yields the desired contradiction. \square

When the number s is equal to 2, our Theorem 1 above can be made more precise.

Theorem 2 *Let $(a_n)_{n \geq 0}$ be a nonzero sequence of rational numbers. Then, the following conditions are equivalent.*

- (i) *The sequence $(a_n)_{n \geq 0}$ has the p -Lucas property for all large primes p , and the series $\sum_{n=0}^{\infty} a_n X^n$ is algebraic over $\mathbb{Q}(X)$.*
- (ii) *There exists a polynomial in $\mathbb{Q}[X]$, of degree at most 2, with $P(0) = 1$, such that $\sum_{n \geq 0} a_n X^n = P(X)^{-1/2}$.*
- (iii) *The sequence $(a_n)_{n \geq 0}$ satisfies $a_0 = 1$ and the recursion*

$$\forall n \geq 1, (n+1)a_{n+1} - a_1(2n+1)a_n + (3a_1^2 - 2a_2)na_{n-1} = 0.$$

- (iv) *The sequence $(a_n)_{n \geq 0}$ satisfies the equalities (with the usual convention $0^0 = 1$)*

$$\forall n \geq 0, a_n = \frac{1}{2^n} \sum_{v=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^v \binom{n}{v} \binom{2n-2v}{n-2v} (3a_1^2 - 2a_2)^v a_1^{n-2v}.$$

- (v) *The sequence $(a_n)_{n \geq 0}$ satisfies*

– *either*

$$\forall n \geq 0, a_n = \binom{2n}{n} \left(\frac{a_1}{2}\right)^n;$$

this is equivalent to saying that

$$\sum_{n=0}^{\infty} a_n X^n = (1 - 2a_1 X)^{-1/2};$$

– *or*

$$\forall n \geq 0, a_n = \gamma^n P_n(a_1/\gamma),$$

where $\gamma^2 = 3a_1^2 - 2a_2$, and $P_n(X)$ is the n -th Legendre polynomial; this is equivalent to saying that

$$\sum_{n=0}^{\infty} a_n X^n = (1 - 2a_1 X + (3a_1^2 - 2a_2)X^2)^{-1/2}.$$

Proof.

The equivalence between (i) and (ii) is Theorem 1 above for $s = 2$. Let us prove the equivalence between (ii) and (iii). If $F(X) = \sum_{n \geq 0} a_n X^n = P(X)^{-1/2}$, where $P(X)$ is a polynomial of degree at most 2, satisfying $P(0) = 1$, let $P(X) = 1 + AX + BX^2$. We clearly have $a_0 = 1$, and

$$\frac{F'(X)}{F(X)} = -\frac{A + 2BX}{2(1 + AX + BX^2)}.$$

Hence

$$-2(1 + AX + BX^2) \sum_{n \geq 1} na_n X^{n-1} = (A + 2BX) \sum_{n \geq 0} a_n X^n.$$

This gives $A = -2a_1$, $B = 3a_1^2 - 2a_2$, and

$$\forall n \geq 1, -2(n+1)a_{n+1} - a_n A(2n+1) - 2Bna_{n-1} = 0,$$

i.e.,

$$\forall n \geq 1, (n+1)a_{n+1} - a_1(2n+1)a_n + (3a_1^2 - 2a_2)na_{n-1} = 0.$$

If conversely the sequence $(a_n)_{n \geq 0}$ satisfies: $a_0 = 1$, and $\forall n \geq 1$,

$$(n+1)a_{n+1} - a_1(2n+1)a_n + (3a_1^2 - 2a_2)na_{n-1} = 0,$$

then, the above computation proves that

$$F(X) = (1 - 2a_1X + (3a_1^2 - 2a_2)X^2)^{-1/2}.$$

Let us prove that (iii) implies (v). Suppose that the sequence $(a_n)_{n \geq 0}$ satisfies $a_0 = 1$, and

$$\forall n \geq 1, (n+1)a_{n+1} - a_1(2n+1)a_n + (3a_1^2 - 2a_2)na_{n-1} = 0.$$

- If $3a_1^2 - 2a_2 = 0$, then, we have $a_0 = 1$, and

$$\forall n \geq 1, a_{n+1} = \frac{2n+1}{n+1} a_1 a_n,$$

which easily implies

$$\forall n \geq 0, a_n = \binom{2n}{n} \left(\frac{a_1}{2}\right)^n.$$

This is exactly saying that $F(X) = (1 - 2a_1X)^{-1/2}$.

- If $3a_1^2 - 2a_2 \neq 0$, let γ be a (complex) number such that $\gamma^2 = 3a_1^2 - 2a_2$. Define the sequence $(b_n)_{n \geq 0}$ by $b_n = a_n \gamma^{-n}$. Then $(b_n)_{n \geq 0}$ satisfies $b_0 = 1$, and

$$\forall n \geq 1, (n+1)b_{n+1} - b_1(2n+1)b_n + nb_{n-1} = 0.$$

But, denoting by $(P_n(X))_{n \geq 0}$ the sequence of Legendre polynomials, we have (see for example [17, p. 46]) $P_0(X) = 1$, $P_1(X) = X$, and

$$\forall n \geq 1, (n+1)P_{n+1}(X) - X(2n+1)P_n(X) + nP_{n-1}(X) = 0.$$

Hence, our sequence $(b_n)_{n \geq 0}$ satisfies

$$\forall n \geq 0, b_n = P_n(b_1).$$

Hence, the sequence $(a_n)_{n \geq 0}$ satisfies

$$\forall n \geq 0, a_n = \gamma^n P_n\left(\frac{a_1}{\gamma}\right),$$

where $\gamma^2 = 3a_1^2 - 2a_2$.

This is exactly saying that $F(X) = (1 - 2a_1X + (3a_1^2 - 2a_2)X^2)^{-1/2}$, since the Legendre polynomials $P_n(Z)$ satisfy $\sum_{n \geq 0} P_n(Z)X^n = (1 - 2ZX + X^2)^{-1/2}$ (see for example [17, p. 45]).

The n -th Legendre polynomial has the following explicit expression (see for example [17, p. 44])

$$P_n(X) = \frac{1}{2^n} \sum_{v=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^v \binom{n}{v} \binom{2n-2v}{n-2v} X^{n-2v}.$$

Hence, if the sequence $(a_n)_{n \geq 0}$ satisfies $a_0 = 1$ and $a_n = \gamma^n P_n(a_1/\gamma)$, with $\gamma^2 = 3a_1^2 - 2a_2$, then

$$\begin{aligned} \forall n \geq 0, a_n &= \gamma^n \frac{1}{2^n} \sum_{v=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^v \binom{n}{v} \binom{2n-2v}{n-2v} \left(\frac{a_1}{\gamma}\right)^{n-2v} \\ &= \frac{1}{2^n} \sum_{v=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^v \binom{n}{v} \binom{2n-2v}{n-2v} \gamma^{2v} a_1^{n-2v} \\ &= \frac{1}{2^n} \sum_{v=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^v \binom{n}{v} \binom{2n-2v}{n-2v} (3a_1^2 - 2a_2)^v a_1^{n-2v}. \end{aligned}$$

If $3a_1^2 - 2a_2 = 0$, we note that this formula gives, with the usual convention $0^0 = 1$, the equality $a_n = \left(\frac{a_1}{2}\right)^n \binom{2n}{n}$. This proves the equivalence between (v) and (iv).

To prove that (v) implies (i), we compute in closed form the series $\sum_{n=0}^{\infty} a_n X^n$ when $(a_n)_{n \geq 0}$ has the above form: this easily gives the algebraicity. Furthermore such a sequence $(a_n)_{n \geq 0}$ has the p -Lucas property:

- in the case $\gamma = 0$, we use the remark in [19, p. 236] with $m = 1$; the sequence $b(n, k) = \binom{n+k}{k}$ has the “double Lucas property”. Hence, the sequence $b(n, n) = \binom{2n}{n}$ has the p -Lucas property for all primes p . This clearly implies that the sequence $\left(\binom{2n}{n} \left(\frac{a_1}{2}\right)^n\right)_{n \geq 0}$ has the p -Lucas property for all odd primes p that do not divide a_1 .
- in the case $\gamma \neq 0$, this comes from the p -Lucas property, for all odd primes p , for the Legendre polynomials (see [22], see also [2]; note that in [19] the Legendre polynomials are shifted):

$$\forall p \text{ odd prime, } \forall n \geq 0, \forall j \in [0, p-1], P_{pn+j}(X) \equiv P_n(X)^p P_j(X) \pmod{p}.$$

□

4 Corollaries

Corollary 1 *Let $m \geq 1$, and let r_1, r_2, \dots, r_m be integers ≥ 1 . Then, the series*

$$\sum_{n=0}^{\infty} \binom{2n}{n}^{r_1} \binom{3n}{n}^{r_2} \cdots \binom{(m+1)n}{n}^{r_m} X^n$$

is transcendental over $\mathbb{Q}(X)$ if $m = 1$ and $r_1 \geq 2$, or if $m \geq 2$.

Proof.

The remark in [19, p. 236] proves that the sequence

$$b(n, k) = \binom{n+k}{k}^{r_1} \binom{n+2k}{k}^{r_2} \cdots \binom{n+mk}{k}^{r_m},$$

where m, r_1, \dots, r_m are as above, has the double Lucas property. Hence $b(n, n)$ has the p -Lucas property for all primes p . It then suffices to check that the sequence $(b(n, n))_{n \geq 0}$ is not of the form given in Theorem 1. \square

Remarks 2

- This corollary contains the results of [24], (see also [8]):

- the series $\sum_n \binom{2n}{n}^t X^n$ is transcendental over $\mathbb{Q}(X)$, for $t \geq 2$.
- the series $\sum_n \binom{kn}{n, n, \dots, n}^t X^n$ is transcendental for $t \geq 1, k \geq 3$. We namely have

$$\binom{kn}{n, n, \dots, n}^t = \prod_{i=2}^k \binom{in}{n}^t.$$

- Note that the series $\sum_n \binom{2n}{n}^2 X^n$ is the usual example proving that the Hadamard product of two algebraic series with rational coefficients is not necessarily algebraic. What precedes proves that this gives, for all $A > 0$, the existence of a prime number p , and of a formal power series over \mathbb{F}_p , that is both algebraic of degree $> A$ over $\mathbb{F}_p(X)$, and is the Hadamard product of two quadratic series. Note also that this series is frequently encountered in combinatorial problems (for but one example, see [11]).

Corollary 2 *Let $(a_n)_{n \geq 0}$ be the Apéry numbers. They are defined by*

$$a_n = \sum_{j=0}^n \binom{n}{j}^2 \binom{n+j}{j}^2.$$

Then, the formal power series $\sum_n a_n X^n$ is transcendental over $\mathbb{Q}(X)$.

Proof.

It has been proved by Gessel [10] that Apéry's numbers have the p -Lucas property for all primes p . \square

Corollary 3 *Let $J_0(z)$ be the Bessel function of index 0. Define the sequence $(\omega(n))_{n \geq 0}$ by*

$$\frac{1}{J_0(2z^{1/2})} = \sum_{n \geq 0} \omega(n) \frac{z^n}{(n!)^2}.$$

Then, the formal power series $\sum_n \omega(n)X^n$ is transcendental over $\mathbb{Q}(X)$.

Proof.

It has been proved by Carlitz [3] that the sequence $(\omega(n))_{n \geq 0}$ has the p -Lucas property for all primes p . \square

We end this section with four remarks.

Remarks 3

- In Theorem 1 and Theorem 2 above, some hypotheses are actually redundant. Namely when we suppose that $F(X) = \sum a_n X^n$ is both algebraic and has the p -Lucas property for “many” primes p , this implies in particular, from our definition of the p -Lucas property, that the denominators of the a_n 's are not divisible by these primes. But this is also a consequence of Eisenstein's theorem (announced by Eisenstein in [7], and proved by Heine in [14]): *if a formal power series with rational coefficients is algebraic over $\mathbb{Q}(X)$, then, the set of prime numbers that divide the denominator of at least one coefficient a_n is finite.*

- The above results can be generalized to N -dimensional sequences.

- Theorem 1 still holds if the field \mathbb{Q} is replaced by $\mathbb{Q}(Z)$, and if p -Lucas sequences are replaced by p -Carlitz sequences of polynomials: a sequence of polynomials $(P_n(Z))_{n \geq 0}$ is called a p -Carlitz sequence of polynomials if, for all $n \geq 0$, and for all $j \in [0, p-1]$, we have $P_{pn+j}(Z) \equiv P_n(Z^p)P_j(Z) \pmod{p}$ (see [3]; see also [2], where the reader can find algebraicity results modulo p for these sequences of polynomials).

- The last remark we make here was suggested by one of the referees. The series mentioned above, namely $\sum_{n \geq 0} \binom{2n}{n}^t X^n$, $\sum_{n=0}^{\infty} \binom{2n}{n}^{r_1} \binom{3n}{n}^{r_2} \dots \binom{(m+1)n}{n}^{r_m} X^n$ and $\sum_{n \geq 0} a_n X^n$, where $(a_n)_{n \geq 0}$ are the Apéry numbers, are not only algebraic modulo p for all primes p , but also algebraic modulo p^k , for all primes p , and all $k \geq 1$. More precisely, for each of these series, say $F(X)$, for each prime number p , and each integer $k \geq 1$, there exists a series $G(X)$ in $\mathbb{Q}[[X]]$, algebraic over $\mathbb{Q}(X)$, such that $F(X) \equiv G(X) \pmod{p^k}$. This is an easy consequence of a result of Denef and Lipschitz [6, Theorem 5.2]. For example, the formal power series $\sum_{n \geq 0} \binom{2n}{n}^2 X^n$ is the diagonal of the series $\sum_{m, n \geq 0} \binom{2m}{m} \binom{2n}{n} X^m Y^n$ which is algebraic over $\mathbb{Q}(X, Y)$ (it is equal to $(1 - 4X - 4Y + 16XY)^{-1/2}$), and [6, Theorem 5.2] readily applies.

5 D-finiteness and p -Lucas property

Many of the formal power series given above that have the p -Lucas property for many primes p , are D -finite, i.e., they satisfy a linear differential equation with coefficients in $\mathbb{Q}(X)$ (see [21]). On the other hand M. Bousquet-Mélou suggested to us that the series $\sum_{n \geq 0} \omega(n)X^n$ is not D -finite, where $(\omega(n))_{n \geq 0}$ has been defined in Corollary 3 above. Namely, if $\sum_{n \geq 0} \omega(n)X^n$ were D -finite, the sequence of its coefficients $(\omega(n))_{n \geq 0}$ would be P -recursive [21], hence, so would be the sequence $(\frac{\omega(n)}{(n!)^2})_{n \geq 0}$. In other words the power series

$$\sum_{n \geq 0} \omega(n) \frac{z^n}{(n!)^2} = \frac{1}{J_0(2z^{1/2})}$$

would be D -finite. This is not the case, since $J_0(z)$, the Bessel function of index 0, has infinitely many real zeros (see for example [23, p. 478]), hence $\frac{1}{J_0(2z^{1/2})}$ has infinitely many poles.

It thus would be interesting to give a characterization of the formal power series that are both D -finite and have the p -Lucas property for “many” primes p .

Acknowledgments

Part of this work was done when the first author visited the University of Genève, supported by a grant of the “Fonds National Suisse de la Recherche Scientifique”. The first author wants to thank P. de la Harpe and R. Grigorchuk for very interesting discussions. The article came to its present form during two of the stays of the first author at the University of Bremen, with the always enthusiastic and very friendly colleagues from Cevis and Mevis. Finally the authors want to thank the referees for valuable suggestions.

References

- [1] J.-P. Allouche, *Note sur un article de Sharif et Woodcock*, Sémin. Théorie des Nombres, Bordeaux, Série II **1** (1989), 163–187.
- [2] J.-P. Allouche, G. Skordev, *Schur congruences, Carlitz sequences of polynomials and automaticity*, Preprint, Inst. Dyn. Syst., Univ. Bremen, Rep. 399 (1997).
- [3] L. Carlitz, *The coefficients of the reciprocal of $J_0(X)$* , Arch. Math. **6** (1955), 121–127.
- [4] N. Chomsky, M. P. Schützenberger, *The algebraic theory of context-free languages*, in: Computer programming and formal languages, P. Braffort and D. Hirschbert eds., North Holland, Amsterdam, 1963, pp. 118–161.
- [5] F. M. Dekking, *Transcendance du nombre de Thue-Morse*, C. R. Acad. Sci. Paris, Sér. I **285** (1977), 157–160.

- [6] J. Denef, L. Lipschitz, *Algebraic power series and diagonals*, J. Number Theory **26** (1987), 46–67.
- [7] G. Eisenstein, *Über eine allgemeine Eigenschaft der Reihenentwicklungen aller algebraischen Funktionen*, Berlin. Sitzber. (1852), 441–443.
- [8] P. Flajolet, *Analytic models and ambiguity of context-free languages*, Theoret. Comput. Sci. **49** (1987), 283–309.
- [9] H. Furstenberg, *Algebraic functions over finite fields*, J. Algebra **7** (1967), 271–277.
- [10] I. Gessel, *Some congruence for Apéry numbers*, J. Number Theory **14** (1982), 362–368.
- [11] D. Gouyou-Beauchamps, *Standard Young tableaux of height 4 and 5*, Eur. J. Comb. **10** (1989), 69–82.
- [12] R. Grigorchuk, P. de la Harpe, *On problems related to growth, entropy and spectrum in group theory*, J. of Dynamical and Control Systems **3** (1997), 51–89.
- [13] T. Harase, *Algebraic elements in formal power series rings*, Israel J. Math. **63** (1988), 281–288.
- [14] E. Heine, *Der Eisensteinsche Satz über Reihen-Entwicklung algebraischer Functionen*, J. Reine Angew. Math. **45** (1853), 285–302.
- [15] J. E. Hopcroft, J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley, 1979.
- [16] G. Karpilovsky, *Field theory. Classical foundations and multiplicative groups*, Dekker, New York, 1988.
- [17] N. Lebedev, *Special functions and their applications*, Prentice Hall Inc., Englewood Cliffs, N. J., 1965.
- [18] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1878), 49–54.
- [19] R. J. McIntosh, *A generalization of a congruential property of Lucas*, Amer. Math. Monthly **99** (1992), 231–238.
- [20] H. Sharif, C. F. Woodcock, *Algebraic functions over a field of positive characteristic and Hadamard products*, J. Lond. Math. Soc. **37** (1988), 395–403.
- [21] R. P. Stanley, *Differentiably finite power series*, Eur. J. Comb. **1** (1980), 175–188.
- [22] J. Wahab, *New cases of irreducibility for Legendre polynomials*, Duke Math. J. **19** (1952), 165–176.

- [23] G. N. Watson, *Treatise on the theory of Bessel functions*, 2nd ed., Cambridge Univ. Press, Cambridge, 1966, reprinted 1980.
- [24] C. F. Woodcock, H. Sharif, *On the transcendence of certain series*, J. Algebra **121** (1989), 364–369.