COMPOSITIO MATHEMATICA

MATTHIJS COSTER

Congruence properties of coefficients of certain algebraic power series

Compositio Mathematica, tome 68, nº 1 (1988), p. 41-57

<http://www.numdam.org/item?id=CM_1988__68_1_41_0>

Compositio Mathematica 68: 41–57 (1988)

Congruence properties of coefficients of certain algebraic power series

MATTHIJS COSTER
Department of Mathematics and Computer Science, University of Leiden, Niels Bohrweg 1, P.O. Box 9512, 2300 RA Leiden, The Netherlands

Received 4 September 1987; accepted in revised form 17 March 1988

Abstract. Let $\Sigma_{i=1}^{\infty} u_n X^n$ denote the power series expansion around $X = 0$ of the algebraic function $(1 + \Sigma_{i=1}^{e} \alpha_i X^i)^{-1/e}$. In this paper we show some congruences for the coefficients u_n. Furthermore we give some lower bounds for the number of factors of an arbitrary prime $p \geqslant 3$ in u_n, if $p \equiv 1 \bmod e$ and $p|\alpha_j$ for at least one j.

1. Introduction

Let $f(X) = \Sigma_{n=0}^{\infty} u_n X^n$ be a power series with rational coefficients which satisfies an equation of the form

$$P(X, f(X)) = 0 \quad \text{where } P(X, Y) \in \mathbb{Z}[X, Y] \text{ and } P(X, Y) \not\equiv 0.$$

Such power series are called algebraic power series. It follows from a theorem of Eisenstein that the set of primes which divide the denominator of some coefficients, is finite. Let us call this set of primes S.

Let p be a prime, $p \notin S$. Christol, Kamae, Mendès-France and Rauzy [1] showed that the sequence $\{u_n \bmod p\}_{n=0}^{\infty}$ is p-recognisable. This means that the sequence $\{u_n \bmod p\}_{n=0}^{\infty}$ can be generated by a p-automaton. Denef and Lipshitz [2] showed that the sequence $\{u_n \bmod p^s\}_{n=0}^{\infty}$ is p^s-recognisable for each $s \in \mathbb{N}$. They reformulate this property in the following way:

$\forall s \in \mathbb{N}, \exists r \in \mathbb{N}, \forall i \in \mathbb{Z}$ with $0 \leqslant i < p^r$ we can find
$r' \in \mathbb{N}$ with $r' < r$ and $i' \in \mathbb{Z}$ with $0 \leqslant i' < p^{r'}$
such that $\forall m \in \mathbb{N}$ we have $u_{mp^r+i} \equiv u_{mp^{r'}+i'} \bmod p^s$.

In special cases this congruence takes on a simple form. In this paper we consider algebraic power series of a special form

$$\left(1 + \sum_{i=1}^{e} \alpha_i X^i\right)^{-1/e} = \sum_{n=0}^{\infty} u_n X^n, \quad \text{where } e \geqslant 2, \alpha_i \in \mathbb{Z}, \text{ for } i = 1, 2, \ldots, e. \tag{1}$$

One of the results in this paper is

THEOREM A. *Let p be a prime, $p \equiv 1$ mod e. Then we have*

$$u_{mp^r} \equiv u_{mp^{r-1}} \bmod p^r \text{ for all } m, r \in \mathbb{N}.$$

The second result in this paper is quite different. It provides a lower bound for the number of factors p in u_n in the case $e = p - 1$. It is based on the following identity mod p which is known as Frobenius factorisation (cf. [3]).

$$\left(1 + \sum_{i=1}^{p-1} \alpha_i X^i\right)^{1/(1-p)} \equiv \left(1 + \sum_{i=1}^{p-1} \alpha_i X^i\right)^{1+p+p^2+\cdots} \equiv \prod_{j=0}^{\infty} \left(1 + \sum_{i=1}^{p-1} \alpha_i X^i\right)^{p^j}$$

$$\equiv \prod_{j=0}^{\infty} \left(1 + \sum_{i=1}^{p-1} \alpha_i X^{ip^j}\right) \bmod p.$$

It follows from a simple calculation that

$$u_n \equiv \prod_i \alpha_{n_i} \bmod p,$$

where $n = n_0 + n_1 p + \cdots + n_t p^t$, $0 \leqslant n_i < p$ is the p-adic representation of n. In particular we have $u_n \equiv 0 \bmod p$ if $p | \alpha_j$ and $n_i = j$ for some i. The following theorem gives a stronger law.

THEOREM B. *Let p be a prime, $p \geqslant 3$. Let $\Sigma_{n=0}^{\infty} u_n X^n$ be the power series expansion of $(1 + \Sigma_{i=1}^{p-1} \alpha_i X^i)^{-1/(p-1)}$ where $\alpha_i \in \mathbb{Z}$ for $i = 1, \ldots, p-1$. Let n be a positive integer with p-adic representation $\Sigma_{i=0}^{t} n_i p^i$. Let $J = \{1 \leqslant j \leqslant p - 1: p | \alpha_j\}$ and $S = \{k \in \mathbb{N}: n_k \in J\}$. Then*

$$\operatorname{ord}_p u_n \geqslant [\tfrac{1}{2}(|S| + 1)].$$

This phenomenon appears also in the case that the Taylor series does not represent an algebraic function, but satisfies a linear differential equation. We finish the introduction with a conjecture of F. Beukers.

Let $b_n = \Sigma_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$. Let $J_5 = \{1, 3\}$ and $J_{11} = \{5\}$. Let $S_5 = \{k \in \mathbb{N} \,|\, n_k \in J_5$, where $\Sigma_j n_j 5^j$ is the 5-adic representation of $n\}$ and $S_{11} = \{k \in \mathbb{N} \,|\, n_k \in J_{11}$, where $\Sigma_j n_j 11^j$ is the 11-adic representation of $n\}$. Beukers conjectures that

(i) $\operatorname{ord}_5(b_n) \geqslant |S_5|$,
(ii) $\operatorname{ord}_{11}(b_n) \geqslant |S_{11}|$,

cf. [4] and [5].

2. Some preliminaries

We use the following *notation*:
- For a finite set S we denote the cardinality of S by $|S|$,
- $[X]$ is the largest integer not exceeding X, $\{X\} = X - [X]$,
- p is a fixed prime, $p \geqslant 3$,
- $\mathrm{ord}_p(r)$ = multiplicity of the prime factor p in r, for $r \in \mathbb{Z}\backslash\{0\}$,
- $r^* = r \cdot p^{-\mathrm{ord}_p(r)}$ is the p-free part of the rational number $r \neq 0$,
- for $\alpha \in \mathbb{Q}$, $m_1, \ldots, m_n \in \mathbb{Z}_{\geqslant 0}$ we define the multinomial coefficient

$$\binom{\alpha}{m_1 \ldots m_n} \text{ by } \frac{\alpha(\alpha - 1) \ldots \left(\alpha + 1 - \sum_{i=1}^{n} m_i\right)}{m_1! m_2! \ldots m_n!}.$$

- We denote by $\mathbb{Z}_p$ the set of p-adic integers.

For any $\alpha \in \mathbb{Z}_p$ we have its p-adic representation $\Sigma_{n=0}^{\infty} a_n p^n$ with $a_n \in \mathbb{Z}$ and $0 \leqslant a_n < p$ for all n. For $k \in \mathbb{N}$ we denote its truncation $\Sigma_{n=0}^{k-1} a_n p^n$ by $[\alpha]_k$.
- Let n be a positive integer. Let $\{b_1, \ldots, b_e\}$ be any partition of non-negative integers such that

$$\sum_{i=1}^{e} i b_i = n. \tag{2}$$

We denote the p-adic representation of b_i by

$$b_i = b_{i0} + b_{i1} p + \cdots + b_{it} p^t \quad (i = 1, \ldots e). \tag{3}$$

Further we define integers c_k, T_k and rationals d_k for $k = 0, \ldots, t$ by

$$c_k = \sum_{i=1}^{e} b_{ik}, \tag{4}$$

$$d_k = p \sum_{i=1}^{e} \left\{ \frac{b_i}{p^{k+1}} \right\} \quad \text{for } k \geqslant 0, \text{ and } d_{-1} = d_{-2} = 0, \tag{5}$$

$$T_k = \sum_{j=0}^{k} \sum_{i=1}^{e} i b_{ij} p^j. \tag{6}$$

LEMMA 2.1. *Let $n \in \mathbb{Z}_{\geqslant 0}$ and $\alpha \in \mathbb{Z}_p$. Then*

$$\operatorname{ord}_p \binom{\alpha}{n} = \sum_{k=1}^{\infty} \left(- \left[\frac{[\alpha]_k}{p^k} - \left\{ \frac{n}{p^k} \right\} \right] \right).$$

Proof. We have

$$\binom{\alpha}{n} = \frac{1}{n!} \cdot \alpha(\alpha - 1)(\alpha - 2) \ldots (\alpha - n + 1).$$

We define u_k as the number of the factors among $\alpha, \alpha - 1, \ldots, \alpha - n + 1$ which are divisible by p^k. Then

$$\operatorname{ord}_p \binom{\alpha}{n} = \sum_{k=1}^{\infty} \left(u_k - \left[\frac{n}{p^k} \right] \right).$$

We have to calculate u_k. To do so, we define v_k as the largest integer not exceeding 0 such that $\operatorname{ord}_p(\alpha + v_k) \geqslant k$ and w_k as the largest integer not exceeding $-n$ such that $\operatorname{ord}_p(\alpha + w_k) \geqslant k$. Then $u_k = (v_k - w_k)/p^k$. It is clear that $v_k = -[\alpha]_k$ and $w_k = -[\alpha]_k + [([\alpha]_k - n)p^k] \cdot p^k$. Hence $u_k = -[([\alpha]_k - n)/p^k] \cdot p^k$. By $n/p^k = [n/p^k] + \{n/p^k\}$, we have

$$\begin{aligned} \operatorname{ord}_p \binom{\alpha}{n} &= \sum_{k=1}^{\infty} \left(u_k - \left[\frac{n}{p^k} \right] \right) \\ &= \sum_{k=1}^{\infty} \left(- \left[\frac{[\alpha]_k}{p^k} - \left[\frac{n}{p^k} \right] - \left\{ \frac{n}{p^k} \right\} \right] - \left[\frac{n}{p^k} \right] \right). \end{aligned}$$

□

COROLLARY 2.2. *Let $M, N, r \in \mathbb{Z}_{\geqslant 0}$, $N \leqslant M < p^{t+1}$ and let e be an integer, $e \geqslant 2$, which divides $p - 1$. Put $N_k = \{N/p^k\}$, $M_k = \{M/p^k\}$, and let $b_1, \ldots, b_e, d_k$ be defined as in* (2) *and* (5). *Then*

(i) $$\operatorname{ord}_p \binom{Mp^r}{Np^r} = \operatorname{ord}_p \binom{M}{N} = \sum_{k=1}^{t+1} -[M_k - N_k],$$

(ii) $$\begin{aligned} \operatorname{ord}_p \binom{-1/e}{Np^r} &= \sum_{k=1}^{t+1} \left[N_k + \frac{e-1}{e} \right] \\ &= \sum_{k=1}^{t+1} \left(\left[\frac{N}{p^k} + \frac{e-1}{e} \right] - \left[\frac{N}{p^k} \right] \right), \end{aligned}$$

(iii) $\operatorname{ord}_p \begin{pmatrix} -1/e \\ b_1 p^r \ldots b_e p^r \end{pmatrix} = \sum_{k=0}^{t} \left[\frac{d_k}{p} + \frac{e-1}{e} \right].$

Proof. (i) The first equality follows by induction on r. Apply Lemma 2.1 with $\alpha = M$ for proving the case $r = 0$.

(ii) Let $a = (p-1)/e$. Then $-1/e = a/(1-p) = a + ap + ap^2 + \cdots \in \mathbb{Z}_p$. We use Lemma 2.1 with $\alpha = -1/e$. Since

$$[\alpha]_k = \sum_{j=0}^{k-1} ap^j = a \cdot \frac{p^k - 1}{p - 1} = \frac{p^k - 1}{e}$$

and

$$\left[\frac{p^l - 1}{ep^l} - \left\{ \frac{Np^r}{p^l} \right\} \right] = 0 \text{ for } 0 \leqslant l \leqslant r,$$

we have

$$\operatorname{ord}_p \binom{-1/e}{Np^r} = \sum_{l=1}^{r+t+1} \left(-\left[\frac{p^l - 1}{ep^l} - \left\{ \frac{Np^r}{p^l} \right\} \right] \right)$$

$$= \sum_{k=1}^{t+1} \left(-\left[\frac{p^k - 1}{ep^k} - \left\{ \frac{N}{p^k} \right\} \right] \right).$$

Since for any rational integer f

$$\left[\frac{1}{e} - \frac{1}{ep^k} + \frac{f}{p^k} \right] = \left[\frac{1}{e} + \frac{f}{p^k} \right],$$

we obtain

$$\operatorname{ord}_p \binom{-1/e}{Np^r} = \sum_{k=1}^{t+1} -\left[\frac{1}{e} - N_k \right].$$

A simple calculation shows that

$$-[1/e - N_k] = \left[\frac{e-1}{e} + N_k \right].$$

(iii) Put $N = \Sigma_{i1}^{e} b_i$. We have

$$\binom{-1/e}{b_1 p^r \ldots b_e p^r} = \binom{-1/e}{Np^r} \cdot \binom{Np^r}{b_1 p^r \ldots b_e p^r}.$$

Hence

$$\operatorname{ord}_p \binom{-1/e}{b_1 p^r \ldots b_e p^r} = \operatorname{ord}_p \binom{-1/e}{Np^r} + \operatorname{ord}_p \binom{Np^r}{b_1 p^r \ldots b_e p^r}.$$

Since

$$\operatorname{ord}_p \binom{-1/e}{Np^r} = \sum_{k=1}^{t+1} \left[N_k + \frac{e-1}{e} \right],$$

$$\operatorname{ord}_p \binom{Np^r}{b_1 p^r \ldots b_e p^r} = \operatorname{ord}_p \binom{N}{b_1 \ldots b_e} = \sum_{k=1}^{t+1} \left(\left[\frac{N}{p^k} \right] - \left[\frac{b_1}{p^k} \right] - \cdots - \left[\frac{b_e}{p^k} \right] \right) = \sum_{k=1}^{t+1} \left(\frac{N}{p^k} - N_k - \sum_{i=1}^{e} \left[\frac{b_i}{p^k} \right] \right)$$

and

$$\sum_{i=1}^{e} \left[\frac{b_i}{p^k} \right] = \sum_{i=1}^{e} \left(\frac{b_i}{p^k} - \left\{ \frac{b_i}{p^k} \right\} \right) = \frac{N}{p^k} - \frac{d_{k-1}}{p},$$

we obtain

$$\operatorname{ord}_p \binom{-1/e}{b_1 p^r \ldots b_e p^r} = \sum_{k=1}^{t+1} \left[N_k + \frac{e-1}{e} \right] + \frac{d_{k-1}}{p} - N_k.$$

Now (iii) follows by noting that $d_{k-1}/p - N_k$ is an integer. □

LEMMA 2.3. *Let $n \in \mathbb{Z}_{\geqslant 0}$ and $n = n_0 + n_1 p + \cdots + n_t p^t$ its p-adic representation. Let $\{b_1, \ldots, b_e\}$ be an arbitrary partition, as in* (2). *Then we have with the notation of* (3)–(6)

(i) $T_k \equiv n \bmod p^{k+1}$ *for* $k \geqslant 0$,

(ii) $c_m p^m \leqslant T_k \leqslant ed_k p^k$ *for* $0 \leqslant m \leqslant k$,

(iii) $T_k = T_{k-1} + \sum_{i=1}^{e} ib_{ik}p^k$ *for* $k \geqslant 1$.

Proof. (i) We have, by using the definition of b_i, T_k and b_{ij},

$$n = \sum_{i=1}^{e} ib_i = \sum_{i=1}^{e}\sum_{j=0}^{t} ib_{ij}p^j \equiv \sum_{i=1}^{e}\sum_{j=0}^{k} ib_{ij}p^j = T_k \bmod p^{k+1}.$$

(ii) We prove the left inequality by

$$c_m p^m = \sum_{i=1}^{e} b_{im}p^m \leqslant \sum_{i=1}^{e} ib_{im}p^m \leqslant \sum_{i=1}^{e}\sum_{j=0}^{k} ib_{ij}p^j = T_k.$$

For the right inequality notice that

$$T_k = \sum_{i=1}^{e}\sum_{j=0}^{k} ib_{ij}p^j \leqslant \sum_{i=1}^{e}\sum_{j=0}^{k} eb_{ij}p^j = ed_k p^k.$$

(iii) follows immediately from definition (5). □

LEMMA 2.4. *Let* $\alpha_i \in \mathbb{Q}$, $e \in \mathbb{N}$. *Then*

$$\left(1 + \sum_{i=1}^{e} \alpha_i X^i\right)^{-1/e} = \sum_{n=0}^{\infty} u_n X^n,$$

where

$$u_n = \sum^{0} \binom{-1/e}{b_1 \ldots b_e} \prod_{i=1}^{e} \alpha_i^{b_i}$$

and 0 *indicates that the sum is taken over all partitions* $\{b_1, \ldots, b_e\}$ *such that* $\Sigma_{i=1}^{e} ib_i = n$.

Proof. We have

$$\left(1 + \sum_{i=1}^{e} \alpha_i X^i\right)^{-1/e} = \sum_{m=0}^{\infty} \binom{-1/e}{m} \cdot \left(\sum_{i} \alpha_i X^i\right)^m$$

$$= \sum_{m=0}^{\infty} \binom{-1/e}{m} \cdot \sum^{0} \binom{m}{b_1 \ldots b_e} \cdot \prod_i \alpha_i^{b_i} \cdot X^{(\Sigma_i ib_i)}$$

$$= \sum_{n=0}^{\infty} \sum^{0} \binom{-1/e}{b_1 + \cdots + b_e} \cdot \binom{b_1 + \cdots + b_e}{b_1 \ldots b_e} \cdot \prod_i \alpha_i^{b_i} \cdot X^n.$$

LEMMA 2.5. *Let* $n = np^r$ *and let* $\{b_1 \ldots b_e\}$ *be an arbitrary partition as in* (2). *For any non-negative integer* j *such that* $c_j > 0$ *we have*

$$\operatorname{ord}_p \binom{-1/e}{b_1 p^r \ldots b_e p^r} \geqslant r - j.$$

Proof. From Corollary 2.2 (iii) it follows that

$$\operatorname{ord}_p \binom{-1/e}{b_i p_1^r \ldots b_l p_e^r} = \sum_{k=0}^{t} \left[\frac{d_k}{p} + \frac{e-1}{e} \right].$$

It suffices to prove that

$$\left[\frac{d_k}{p} + \frac{e-1}{e} \right] \geqslant 1 \quad \text{for } j \leqslant k < r.$$

Suppose that

$$\left[\frac{d_k}{p} + \frac{e-1}{e} \right] = 0 \quad \text{for some } j \leqslant k < r.$$

Then $d_k < p/e$. From Lemma 2.3(ii) it follows that $T_k < p^{k+1}$. By using Lemma 2.3(i) we conclude that $T_k = 0$. But Lemma 2.3(ii) implies $c_j p^j \leqslant T_k$. Hence $c_j = 0$ which contradicts $c_j > 0$. □

LEMMA 2.6. *Let* $e \geqslant 2$ *be an integer which divides* $p - 1$. *Let* $r \geqslant 1$ *be an integer. Then*

$$\binom{-1/e}{b_1 p^r \ldots b_e p^r}^* \equiv \binom{-1/e}{b_1 p^{r-1} \ldots b_e p^{r-1}}^* \bmod p^r.$$

Proof. Put $m = \Sigma_{i=1}^{e} b_i$. Then we have

$$\binom{-1/e}{b_1 p^r \ldots b_e p^r} = (-1/e)^{mp^r} \cdot \frac{1 \cdot (1+e) \ldots (1 + mep^r - e)}{(b_1 p^r)! \cdot (b_2 p^r)! \ldots (b_e p^r)!}$$

$$= (-1/e)^{mp^r} \cdot \frac{p \cdot (p + ep) \ldots (p + mep^r - ep)}{(p \cdot 2p \ldots b_1 p^r) \ldots (p \cdot 2p \ldots b_e p^r)}$$

$$\times \frac{1 \cdot (1+e) \ldots (1 + mep^r - e)}{p \cdot (p + ep) \ldots (p + mep^r - ep)}$$

$$\times \frac{(p \cdot 2p \ldots b_1 p^r) \ldots (p \cdot 2p \ldots b_e p^r)}{(b_1 p^r)! \cdot (b_2 p^r)! \ldots (b_e p^r)!}$$

$$= (-1/e)^{mp^r - mp^{r-1}} \cdot \binom{-1/e}{b_1 p^{r-1} \ldots b_e p^{r-1}}$$

$$\times \frac{1 \cdot (1+e) \ldots (1 + mep^r - e)}{p \cdot (p + ep) \ldots (p + mep^r - ep)}$$

$$\times \frac{(p \cdot 2p \ldots b_1 p^r) \ldots (p \cdot 2p \ldots b_e p^r)}{(b_1 p^r)! \cdot (b_2 p^r)! \ldots (b_e p^r)!}.$$

By Corollary 2.2(iii) we have

$$\operatorname{ord}_p \binom{-1/e}{b_1 p^r \ldots b_e p^r} = \operatorname{ord}_p \binom{-1/e}{b_1 p^{r-1} \ldots b_e p^{r-1}}.$$

Hence we have mod p^r

$$\binom{-1/e}{b_1 p^r \ldots b_e p^r}^* \equiv \binom{-1/e}{b_1 p^{r-1} \ldots b_e p^{r-1}}^* \cdot (-1/e)^{mp^r - mp^{r-1}}.$$

$$\times \frac{1 \cdot (1+e) \ldots (1 + mep^r - e)}{p \cdot (p + ep) \ldots (p + mep^r - ep)}$$

$$\times \frac{(p \cdot 2p \ldots b_1 p^r) \ldots (p \cdot 2p \ldots b_e p^r)}{(b_1 p^r)! \cdot (b_2 p^r)! \ldots (b_e p^r)!}. \tag{7}$$

Note that $(-1/e)^{mp^r} \equiv (-1/e)^{mp^{r-1}} \bmod p^r$ by a theorem of Fermat–Euler. Furthermore by $e|(p-1)$,

$$\left(\frac{1\cdot(1+e)\ldots(1+mep^r-e)}{p\cdot(p+ep)\ldots(p+mep^r-ep)}\right)$$

$$\text{and}\quad\left(\frac{(b_1p^r)!\cdot(b_2p^r)!\ldots(b_ep^r)!}{(p\cdot 2p\ldots(p\cdot 2p\ldots b_ep^r)}\right)$$

are rational integers. It now follows that

$$\left(\frac{1\cdot(1+e)\ldots(1+mep^r-e)}{p\cdot(p+ep)\ldots(p+mep^r-ep)}\right)^* \equiv \left(\sum_{a=1,\,p\nmid a}^{p^r} a\right)^m \tag{8}$$

$$\equiv \left(\frac{(b_1p^r)!\cdot(b_2p^r)!\ldots(b_ep^r)!}{(p\cdot 2p\ldots b_1p^r)\ldots(p\cdot 2p\ldots b_ep^r)}\right)^* \bmod p^r.$$

The substitution of these congruences in (7) completes the proof of the lemma. □

COROLLARY 2.7. *With r and e as in Lemma 2.6 we have*

$$\binom{-1/e}{b_1p^r\ldots b_ep^r} \equiv \binom{-1/e}{b_1p^{r-1}\ldots b_ep^{r-1}} \bmod p^{r+\mu}$$

$$\textit{where } \mu = \operatorname{ord}_p\binom{-1/e}{b_1\ldots b_e}.$$

Proof. This is obvious since

$$\binom{-1/e}{b_1p^m\ldots b_ep^m} = \binom{-1/e}{b_1p^m\ldots b_ep^m}^*\cdot p^\mu \quad \text{for all } m \geqslant 0.$$ □

3. Congruences

THEOREM A. *Let*

$$\left(1+\sum_{i=1}^{e}\alpha_iX^i\right)^{-1/e} = \sum_{n=0}^{\infty}u_nX^n, \quad \textit{where } \alpha_i\in\mathbb{Z} \textit{ for } i=1\ldots e \textit{ and } e\in\mathbb{Z},\ e\geqslant 2.$$

Let p be a prime such that $p \equiv 1 \bmod e$. *Let* $r, m \in \mathbb{N}$. *Then*

$$u_{mp^r} \equiv u_{mp^{r-1}} \bmod p^r.$$

Proof. Put $n = mp^r$. We may assume $p \nmid m$. Take an arbitrary partition $\{b_1 \ldots b_e\}$ as defined in (2). Define j with $0 \leqslant j \leqslant r$ by $c_0 = c_1 = \cdots = c_{j-1} = 0$, $c_j > 0$. If $j = 0$ then Lemma 2.5 implies that

$$\binom{-1/e}{b_1 \ldots b_e} \equiv 0 \bmod p^r. \tag{9}$$

Now suppose that $j > 0$. Since $c_k = \Sigma_{i=1}^{e} b_{ik}$, $b_{ik} \geqslant 0$ and $c_k = 0$ for $k < j$, we have $p^j | b_i$ for $i = 1 \ldots e$. Substitute $b = b_i' p_i^j$. By Lemma 2.6 we have

$$\binom{-1/e}{b_1'p^j \ldots b_e'p^j}^* \equiv \binom{-1/e}{b_1'p^{j-1} \ldots b_e'p^{j-1}}^* \bmod p^j.$$

Since $\alpha_i^{p^j} \equiv \alpha_i^{p^{j-1}} \bmod p^j$, by Fermat–Euler, we have

$$\binom{-1/e}{b_1'p^j \ldots b_e'p^j}^* \prod_i \alpha_i^{b_i'p^j} \equiv \binom{-1/e}{b_1'p^{j-1} \ldots b_e'p^{j-1}}^* \prod_i \alpha_i^{b_i'p^{j-1}} \bmod p^j.$$

Since $c_j > 0$ we find, using Corollary 2.2(iii) and Lemma 2.5,

$$\binom{-1/e}{b_1'p^j \ldots b_e'p^j} \prod_i \alpha_i^{b_i'p^j} \equiv \binom{-1/e}{b_1'p^{j-1} \ldots b_e'p^{j-1}} \prod_i \alpha_i^{b_i'p^{j-1}} \bmod p^r. \tag{10}$$

We recall Lemma 2.4,

$$u_n = \sum^{0} \binom{-1/e}{b_1 \ldots b_e} \cdot \prod_{i=1}^{e} \alpha_i^{b_i}.$$

For $n = mp^r$ we split this sum into two parts: One part for which $p \nmid b_i$ for some i, the other part for which $p | b_i$ for all i. Congruence (9) implies that the first part vanishes mod p^r. Hence

$$u_{mp^r} \equiv \sum^{\wedge} \binom{-1/e}{b_1 \ldots b_e} \cdot \prod_{i=1}^{e} \alpha_i^{b_i} \bmod p^r,$$

where $\hat{}$ denotes the sum taken over all partitions $\{b_1, \ldots, b_e\}$ such that $\Sigma_{i=1}^{e} ib_i = mp^r$ and $p|b_i$ for $i = 1, \ldots, e$. According to (10) the right side of this congruence equals

$$\sum^{0} \binom{-1/e}{b_1 \ldots b_e} \cdot \prod_{i=1}^{e} \alpha_i^{b_i} \equiv u_{mp^{r-1}} \bmod p^r,$$

here 0 denotes the sum is taken over all partitions $\{b_1, \ldots, b_e\}$ such that $\Sigma_{i=1}^{e} ib_i = mp^{r-1}$. □

4. Prime factors p of the algebraic power series $(1 + \Sigma_{i=1}^{p-1} \alpha_i X^i)^{-1/(p-1)}$

THEOREM B. *Let p be a prime, $p \geqslant 3$, and $\alpha_i \in \mathbb{Z}$ for $i = 1, \ldots, p - 1$. Put*

$$\left(1 + \sum_{i=1}^{p-1} \alpha_i X^i\right)^{-1/(p-1)} = \sum_{n=0}^{\infty} u_n X^n.$$

Let n be a positive integer with p-adic representation $n_0 + n_1 p + \cdots + n_t p^t$. Let $J = \{1 \leqslant j \leqslant p - 1: p|\alpha_j\}$, $S = \{k \in \mathbb{N}: n_k \in J\}$ and let R be a subset of S such that for each pair of successive numbers m and $m + 1$, at most one of the numbers n_m and n_{m+1} belongs to R. Put $\sigma = |S|$ and $\varrho = |R|$. Then

(i) $\mathrm{ord}_p u_n \geqslant \varrho$,

(ii) $\mathrm{ord}_p u_n \geqslant [(\sigma + 1)/2]$,

(iii) *if $J = \{p - s, p - s + 1, \ldots, p - 1\}$ for some s, then* $\mathrm{ord}_p u_n \geqslant \sigma$.

Proof. Let $\{b_1 \ldots b_e\}$ be an arbitrary partition, as defined in (2). We need the following notation in this proof:

$$B = \left\{k \in \mathbb{N}: \sum_{j \in J} b_{jk} > 0\right\},$$

$$K_i = \left\{k \in \mathbb{N}: \left[\frac{d_k}{p} + \frac{p-2}{p-1}\right] = i\right\}, \quad \text{for } i = 0, 1, 2, \ldots.$$

$$\bar{K}_i = \{k + j: k \in K_i, 0 \leqslant j \leqslant i - 1\},$$

$$\bar{K} = \bigcup_{i=1}^{\infty} \bar{K}_i,$$

$$\beta = |B|, \quad \tau = \sum_{k=0}^{t} \left[\frac{d_k}{p} + \frac{p-2}{p-1}\right].$$

Notice that

$$\tau = \sum_{k=0}^{t} \left[\frac{d_k}{p} + \frac{p-2}{p-1} \right] = \sum_{i=1}^{t} i \cdot |K_i| \geqslant |\bar{K}|.$$

We prove the theorem by use of the two following lemmas.

LEMMA 4.1.

$$\mathrm{Ord}_p(u_n) \geqslant \min_{\Sigma i b_i = n} (\beta + \tau).$$

Proof. Lemma 2.4 implies that

$$u_n = \sum^{0} \binom{-1/(p-1)}{b_1 \ldots b_{p-1}} \cdot \prod_{i=1}^{p-1} \alpha_i^{b_i}.$$

Hence

$$\mathrm{ord}_p(u_n) \geqslant \min_{\Sigma i b_i = n} \left(\sum_{i=1}^{p-1} b_i \cdot \mathrm{ord}_p(\alpha_i) + \mathrm{ord}_p \binom{-1/(p-1)}{b_1 \ldots b_{p-1}} \right).$$

It now follows from Corollary 2.2 that

$$\mathrm{ord}_p(u_n \geqslant \min_{\Sigma i b_i = n} \left(\sum_{i=1}^{p-1} b_i \cdot \mathrm{ord}_p(\alpha_i) + \sum_{k=0}^{t} \left[\frac{d_k}{p} + \frac{p-2}{p-1} \right] \right).$$

Since

$$\sum_{i=1}^{p-1} b_i \cdot \mathrm{ord}_p(\alpha_i) \geqslant \sum_{i \in J} b_i \cdot \mathrm{ord}_p(\alpha_i) \geqslant |B| = \beta$$

and

$$\sum_{k=0}^{t} \left[\frac{d_k}{p} + \frac{p-2}{p-1} \right] = \tau,$$

the lemma is proved. □

LEMMA 4.2. *If* $d_{k-1} < p/(p-1)$ *and* $d_k < p/(p-1)$ *then either*

$$c_k = n_k = 0$$

or

$$c_k = 1, n_k = j, b_{jk} = 1 \textit{ for some } j \in \{1, \ldots, p-1\} \textit{ and } b_{ik} = 0 \textit{ for all } i \neq j.$$

Proof. By Lemma 2.3(ii) the conditions $d_{k-1} < p/(p-1)$ and $d_k < p/(p-1)$ imply that $T_{k-1} < p^k$ and $T_k < p^{k+1}$. Furthermore we have, by Lemma 2.3(iii), $T_k = T_{k-1} + \Sigma_i\, ib_{ik}p^k$ and finally we have, by Lemma 2.3(i), $T_k \equiv n \bmod p^{k+1}$. By combining this we obtain $n_k = \Sigma_i\, ib_{ik}$. Note that $d_k < p/(p-1)$ implies $c_k \leqslant 1$. Hence either $c_k = 0$ or $c_k = 1$. If $c_k = 0$ then $\Sigma_i\, ib_{ik} = 0$ and $n_k = 0$. If $c_k = 0$. If $c_k = 1$ then $\Sigma_i\, b_{ik} = 1$. Hence there exists a j such that $b_{jk} = 1$ and $b_{ik} = 0$ for all $i \neq j$. Here we conclude $n_k = j$. □

Proof of Theorem B (i). Let $\{b_1 \ldots b_{p-1}\}$ be an arbitrary partition, as defined in (2). We will construct a set $K \subset \mathbb{Z}_{\geqslant 0}$ with the properties:

(i) $|K| \leqslant \tau$,
(ii) $R \subset B \cup K$.

For any such set K we have

$$\beta + \tau = |B| + |K| \geqslant |B \cup K| \geqslant |R| = \varrho.$$

We can complete the proof of Theorem B(i) by applying Lemma 4.1 which yields

$$\operatorname{ord}_p(u_n) \geqslant \min(\beta + \tau) \geqslant \varrho.$$

We shall now construct K satisfying properties (i) and (ii). Let M be the set of all k such that $k \in \bar{K}$, $k+1 \notin \bar{K}$ and $k \notin R$. Put $N = \{k+1 : k \in M\}$ and take $K = (\bar{K} \backslash M) \cup N$. Then K satisfies property (i) because $|K| \leqslant |\bar{K}| \leqslant \tau$. We shall prove property (ii) by showing that $k \in R$, $k \notin B \cup K$ leads to a contradiction. Note that $k \notin K$ implies $k \notin K_i$ for any $i \geqslant 1$. Hence

$$\left[\frac{d_k}{p} + \frac{p-2}{p-1}\right] = 0.$$

We conclude that $d_k < p/(p-1)$. By definition of R, we have $k-1 \notin R$. If $k-1 \in \bar{K}$ then our construction of K would imply $k \in K$, which contradicts the supposition that $k \notin B \cup K$. Hence $k-1 \notin K_i$ for any $i \geqslant 1$. This implies $d_{k-1} < p/(p-1)$. Thus by Lemma 4.2 we have either $n_k = 0$ or $n_k = j$ and $b_{jk} = 1$ for some j. Since $n_k = 0$ implies $k \notin R$, the first case of Lemma 4.2 is excluded. However $k \in R$ implies $j = n_k \in J$. The second case therefore implies $k \in B$, which is also excluded. This yields the desired contradiction.

Proof of Theorem B(ii). Choose $R \subset S$ such that ϱ is maximal. Then at least $\varrho \geqslant \frac{1}{2}\sigma$.

Proof of Theorem B(iii). Let $\{b_1 \ldots b_{p-1}\}$ be an arbitrary partition, as defined in (2). We will construct a set $K \subset Z_{\geqslant 0}$ with the properties:

(i) $|K| \leqslant \tau$,
(ii) $S \subset B \cup K$.

The construction of K is more complicated than in the first part. Put

$$M_1 = \{k \in \bar{K}: k \notin S,\ k+1 \notin \bar{K}\}, \quad N_1 = \{k+1 \in \mathbb{N}: k \in M_1\},$$

$$M_2 = \{k \in \bar{K}: k \in \bar{K}_i \cap \bar{K}_j \text{ for some distinct positive integers } i, j\},$$

$$N_2 = \{k+1 \in \mathbb{N}: k \in M_2\},$$

$$M_3 = \{k \in \bar{K} \cap B\}, \quad N_3 = \{k+1 \in \mathbb{N}: k \in M_3\}.$$

Take $K = (\bar{K}\backslash(M_1 \cup M_3)) \cup N_1 \cup N_2 \cup N_3$. Note that $|M_i| = |N_i|$ for $i = 1, 2, 3$, and $|M_1 \cup M_3| = |N_1 \cup N_3|$ and $|\bar{K}| + |N_2| \leqslant \Sigma_i |\bar{K}_i|$. We conclude $|K| \leqslant \Sigma_i |\bar{K}_i| \leqslant \tau$ and K satisfies property (i). K also satisfies property (ii). to see this, suppose $k \in S$ and $k \notin B \cup K$. This will lead to a contradiction. $k \in \bar{K}$ implies that $k \in M_1 \cup M_3$, since $k \notin K$. But $k \in M_1$ implies $k \notin S$ which contradicts $k \in S$, while $k \in M_3$ implies $k \in B$ which contradicts $k \notin B \cup K$. Therefore $k \notin \bar{K}$, hence

$$d_k < \frac{p}{p-1} \quad \text{and} \quad d_{k-1} < \frac{p^2}{p-1}.$$

We distinguish five cases:

(a) $d_{k-1} < p/(p-1)$. This leads to a contradiction, just as in the proof Theorem B(i).
(b) $d_{k-1} \geqslant p/(p-1)$ and $k-1 \notin S$. These imply that $k-1 \in \bar{K}$. Hence $k \in N_1$, contradicting $k \notin K$.

(c) $d_{k-1} \geqslant p/(p-1)$ and $d_{k-2} \geqslant p^2/(p-1)$. These imply that $k-1 \in K_i$ for some $i \geqslant 1$, and $k-2 \in K_j$ for some $j \geqslant 2$. Hence $k-1 \in \bar{K}_i \cap \bar{K}_j$. If $i \neq j$ then $k \in N_2$, which contradicts $k \notin K$. If $i = j$ then $i \geqslant 2$. This implies $k \in \bar{K}_i$, which also contradicts $k \notin K$.

(d) $d_{k-1} \geqslant p/(p-1)$ and $k-1 \in B$. These imply that $k-1 \in \bar{K} \cap B$. Hence $k \in N_3$, contradicting $k \notin K$.

(e) The remaining case reads

$$d_k < \frac{p}{p-1} \leqslant d_{k-1} < \frac{p^2}{p-1}, \quad d_{k-2} < \frac{p^2}{p-1}, \quad k-1 \in S, \quad k-1 \notin B.$$

Then $d_{k-2} < p^2/(p-1)$ implies that $T_{k-2} < p^k$ by Lemma 2.3(ii). Further $d_{k-1} < p^2/(p-1)$ implies that $c_{k-1} \leqslant p+1$. Since $k-1 \notin B$, we have

$$\sum_{i=1}^{p-1} ib_{i(k-1)} = \sum_{i=1}^{p-s-1} ib_{i(k-1)} \leqslant (p-s-1)\cdot c_{k-1} \leqslant (p-s-1)\cdot(p+1).$$

These arguments imply that

$$\begin{aligned} T_{k-1} &= T_{k-2} + \sum_i ib_{i(k-1)}p^{k-1} < p^k + (p+1)\cdot(p-s-1)\cdot p^{k-1} \\ &= p^{k+1} - (s-1)\cdot p^k - (s+1)\cdot p^{k-1} \\ &= (p-s)\cdot p^k + (p-s-1)\cdot p^{k-1}. \end{aligned}$$

Since $d_k < p/(p-1)$, $d_k = c_k + d_{k-1}/p$ and $p/(p-1) \leqslant d_{k-1}$, we have $c_k = 0$. Hence by use of Lemma 2.3(iii) we have

$$T_k = T_{k-1} < (p-s)\cdot p^k + (p-s-1)\cdot p^{k-1}. \tag{11}$$

On the other hand we have $k, k-1 \in S$, which implies $n_k \geqslant p-s$ and $n_{k-1} \geqslant p-s$ and thus

$$\begin{aligned} T_k &= \sum_{j=0}^{k}\sum_{i=1}^{e} ib_{ij}p^j \geqslant \sum_{j=0}^{k} n_j p^j \geqslant n_{k-1}p^{k-1} + n_k p^k \\ &\geqslant (p-s)p^k + (p-s)p^{k-1}, \end{aligned}$$

which contradicts (11). □

References

1. G. Christol, T. Kamae, M. Mendès-France and G. Rauzy: Suites algébriques, automates et substitutions. *Bull. Soc. Math. France* 108 (1980) 401–419.
2. J. Denef and L. Lipshitz: Algebraic power series and diagonals. *J. Number Theory* 26 (1987) 46–67.
3. M. Mendès-France and A.J. van der Poorten: Automata and the arithmetic of formal power series. *Publ. Math. Orsay*, 86-1, Univ. Paris XI, Orsay (1986).
4. S. Chowla, J. Cowles and M. Cowles: Congruence properties of Apéry numbers, *J. Number Theory* 12 (1980) 188–190.
5. I. Gessel: Some congruences for Apéry numbers. *J. Number Theory* 14 (1982) 362–368.