MATTHIJS COSTER

Congruence properties of coefficients of certain algebraic power series


<http://www.numdam.org/item?id=CM_1988__68_1_41_0>
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 $\sum_{n=0}^{\infty} u_n x^n$ denote the power series expansion around $X = 0$ of the algebraic function $(1 + \sum_{i=1}^{e} a_i x^i)^{-1/e}$. 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 $p \geq 3$ in $u_n$, if $p \equiv 1 \mod e$ and $p | a_j$ for at least one $j$.

1. Introduction

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

$$P(X, f(X)) = 0$$

where $P(X, Y) \in \mathbb{Z}[X, Y]$ and $P(X, Y) \neq 0$.

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 $\{u_n \mod p\}_{n=0}^{\infty}$ is $p$-recognisable. This means that the sequence $\{u_n \mod p\}_{n=0}^{\infty}$ can be generated by a $p$-automaton. Denef and Lipshitz [2] showed that the sequence $\{u_n \mod p^s\}_{n=0}^{\infty}$ is $p^s$-recognisable for each $s \in \mathbb{N}$. They reformulate this property in the following way:

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

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

$$\left(1 + \sum_{i=1}^{e} a_i x^i\right)^{-1/e} = \sum_{n=0}^{\infty} u_n x^n, \text{ where } e \geq 2, a_i \in \mathbb{Z}, \text{ for } i = 1, 2, \ldots, e.$$ 

(1)

One of the results in this paper is
THEOREM A. Let $p$ be a prime, $p \equiv 1 \mod e$. Then we have

$$u_{mpr} \equiv u_{mpr-1} \mod p^r$$ 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]).

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

It follows from a simple calculation that

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

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

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

$$\text{ord}_p u_n \geq \left\lfloor \frac{1}{2} (|S| + 1) \right\rfloor.$$

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

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

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, \( p \geq 3 \),
- \( \text{ord}_p(r) = \) multiplicity of the prime factor \( p \) in \( r \), for \( r \in \mathbb{Z}\setminus\{0\} \),
- \( r^* = r \cdot p^{\text{ord}_p(r)} \) is the \( p \)-free part of the rational number \( r \neq 0 \),
- for \( \alpha \in \mathbb{Q} \), \( m_1, \ldots, m_n \in \mathbb{Z}_{\geq 0} \) we define the multinomial coefficient

\[
\binom{\alpha}{m_1 \ldots m_n} = \frac{\alpha(\alpha - 1) \ldots (\alpha + 1 - \sum_{i=1}^{n} m_i)}{m_1!m_2! \ldots m_n!}.
\]

- 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 \( \sum_{n=0}^{\infty} a_n p^n \) with \( a_n \in \mathbb{Z} \) and \( 0 \leq a_n < p \) for all \( n \). For \( k \in \mathbb{N} \) we denote its truncation \( \sum_{n=0}^{k-1} a_n p^n \) by \([\alpha]_k\).

- Let \( n \) be a positive integer. Let \( \{b_1, \ldots, b_e\} \) be any partition of non-negative integers such that

\[
\sum_{i=1}^{e} ib_i = n. \quad (2)
\]

We denote the \( p \)-adic representation of \( b_i \) by

\[
b_i = b_{i0} + b_{i1}p + \cdots + b_{ip^i} \quad (i = 1, \ldots, e). \quad (3)
\]

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

\[
c_k = \sum_{i=1}^{e} b_{ik}, \quad (4)
\]

\[
d_k = p \sum_{i=1}^{e} \left\{ \frac{b_i}{p^{k+1}} \right\} \quad \text{for} \ k \geq 0, \ \text{and} \ d_{-1} = d_{-2} = 0, \quad (5)
\]

\[
T_k = \sum_{i=0}^{k} \sum_{i=1}^{e} ib_{ij} p^i. \quad (6)
\]
LEMMA 2.1. Let $n \in \mathbb{Z}_{\geq 0}$ and $\alpha \in \mathbb{Z}_p$. Then

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

Proof. We have

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

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

$$\text{ord}_p \left( \frac{\alpha}{n} \right) = \sum_{k=1}^{\infty} \left( u_k - \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

We have to calculate $u_k$. To do so, we define $v_k$ as the largest integer not exceeding 0 such that $\text{ord}_p(\alpha + v_k) \geq k$ and $w_k$ as the largest integer not exceeding $-n$ such that $\text{ord}_p(\alpha + w_k) \geq k$. 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 $n/p^k = \lfloor n/p^k \rfloor + \{n/p^k\}$, we have

$$\text{ord}_p \left( \frac{\alpha}{n} \right) = \sum_{k=1}^{\infty} \left( u_k - \left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

$$= \sum_{k=1}^{\infty} \left( - \left[ \frac{\alpha}{p^k} \right] - \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

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

(i) $\text{ord}_p \left( \frac{Mp^r}{Np^r} \right) = \text{ord}_p \left( \frac{M}{N} \right) = \sum_{k=1}^{r+1} -[M_k - N_k],$

(ii) $\text{ord}_p \left( \frac{-1/e}{Np^r} \right) = \sum_{k=1}^{r+1} \left[ N_k + \frac{e - 1}{e} \right]$

$$= \sum_{k=1}^{r+1} \left( \left[ \frac{N}{p^k} + \frac{e - 1}{e} \right] - \left[ \frac{N}{p^k} \right] \right).$$
Proof. (i) The first equality follows by induction on $r$. Apply Lemma 2.1 with $x = M$ 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 $x = -1/e$. Since

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

and

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

we have

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

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

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

$$\text{ord}_p\left( \frac{-1/e}{Np^l} \right) = \sum_{k=1}^{r+1} - \left[ \frac{1}{e} - N_k \right].$$

A simple calculation shows that

$$-[1/e - N_k] = \left[ \frac{e - 1}{e} + N_k \right].$$
(iii) Put $N = \sum_i b_i$. We have
\[
\left(\begin{array}{c}
-1/e \\
b_1p' \ldots b_\epsilon p'
\end{array}\right) = \left(\begin{array}{c}
-1/e \\
Np'
\end{array}\right) \cdot \left(\begin{array}{c}
Np' \\
b_1p' \ldots b_\epsilon p'
\end{array}\right).
\]
Hence
\[
\text{ord}_p\left(\begin{array}{c}
-1/e \\
b_1p' \ldots b_\epsilon p'
\end{array}\right) = \text{ord}_p\left(\begin{array}{c}
-1/e \\
Np'
\end{array}\right) + \text{ord}_p\left(\begin{array}{c}
Np' \\
b_1p' \ldots b_\epsilon p'
\end{array}\right).
\]
Since
\[
\text{ord}_p\left(\begin{array}{c}
-1/e \\
Np'
\end{array}\right) = \sum_{k=1}^{\epsilon+1} \left\lfloor N_k + \frac{e - 1}{e} \right\rfloor,
\]
\[
\text{ord}_p\left(\begin{array}{c}
Np' \\
b_1p' \ldots b_\epsilon p'
\end{array}\right) = \sum_{k=1}^{\epsilon+1} \left\lfloor \frac{N}{p^k} \right\rfloor
\]
\[
- \left\lfloor \frac{b_1}{p^k} \right\rfloor - \ldots - \left\lfloor \frac{b_\epsilon}{p^k} \right\rfloor = \sum_{k=1}^{\epsilon+1} \left( \frac{N}{p^k} - N_k - \sum_{i=1}^{\epsilon} \left\lfloor \frac{b_i}{p^k} \right\rfloor \right)
\]
and
\[
\sum_{i=1}^{\epsilon} \left\lfloor \frac{b_i}{p^k} \right\rfloor = \sum_{i=1}^{\epsilon} \left( \frac{b_i}{p^k} - \left\{ \frac{b_i}{p^k} \right\} \right) = \frac{N}{p^k} - \frac{d_{k-1}}{p},
\]
we obtain
\[
\text{ord}_p\left(\begin{array}{c}
-1/e \\
b_1p' \ldots b_\epsilon p'
\end{array}\right) = \sum_{k=1}^{\epsilon+1} \left\lfloor N_k + \frac{e - 1}{e} \right\rfloor + \frac{d_{k-1}}{p} - N_k.
\]
Now (iii) follows by noting that $d_{k-1}/p - N_k$ is an integer. \qed

**Lemma 2.3.** Let $n \in \mathbb{Z}_{\geq 0}$ and $n = n_0 + n_1p + \ldots + n_\epsilon p'$ its $p$-adic representation. Let $\{b_1, \ldots, b_{\epsilon}\}$ be an arbitrary partition, as in (2). Then we have with the notation of (3)-(6)

(i) $T_k \equiv n \mod p^{k+1}$ for $k \geq 0$, 
(ii) \( c_m p^m \leq T_k \leq e d_k p^k \) for \( 0 \leq m \leq k \),

(iii) \( T_k = T_{k-1} + \sum_{i=1}^{e} i b_{ik} p^k \) for \( k \geq 1 \).

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

\[
n = \sum_{i=1}^{e} i b_i = \sum_{i=1}^{e} \sum_{j=0}^{i} i b_{ij} p^i = \sum_{i=1}^{e} \sum_{j=0}^{k} i b_{ij} p^i = T_k \mod p^{k+1}.
\]

(ii) We prove the left inequality by

\[
c_m p^m = \sum_{i=1}^{e} b_{im} p^m \leq \sum_{i=1}^{e} i b_{ij} p^i \leq \sum_{i=1}^{e} \sum_{j=0}^{k} i b_{ij} p^i = T_k.
\]

For the right inequality notice that

\[
T_k = \sum_{i=1}^{e} \sum_{j=0}^{k} i b_{ij} p^j \leq \sum_{i=1}^{e} \sum_{j=0}^{k} e b_{ij} p^j = e d_k p^k.
\]

(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

\[
u_n = \sum_{b_1 \ldots b_e} \left( -\frac{1}{e} \right)^{\prod_{i=1}^{e} \alpha_i^{b_i}}
\]

and 0 indicates that the sum is taken over all partitions \( \{b_1, \ldots, b_e\} \) such that \( \sum_{i=1}^{e} i b_i = n \).

**Proof.** We have

\[
\left( 1 + \sum_{i=1}^{e} \alpha_i X^i \right)^{-1/e} = \sum_{m=0}^{\infty} \left( -\frac{1}{e} \right)^{m} \left( \sum_{i=1}^{e} \alpha_i X^i \right)^m
\]
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

$$\text{ord}_p \left( \frac{-1/e}{b_1 p^r \cdots b_e p^r} \right) \geq r - j.$$  

Proof. From Corollary 2.2 (iii) it follows that

$$\text{ord}_p \left( \frac{-1/e}{b_1 p^r \cdots b_e p^r} \right) = \sum_{k=0}^{r} \left[ \frac{d_k}{p} + \frac{e - 1}{e} \right].$$

It suffices to prove that

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

Suppose that

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

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 $c_j p^r \leq T_k$. Hence $c_j = 0$ which contradicts $c_j > 0$.  

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

$$\begin{pmatrix} -1/e \\ b_1 p^r \cdots b_e p^r \end{pmatrix}^* \equiv \begin{pmatrix} -1/e \\ b_1 p^{r-1} \cdots b_e p^{r-1} \end{pmatrix}^* \mod p^r.$$
Proof. Put \( m = \Sigma_{i=1}^{e} b_i \). Then we have

\[
\left( \frac{-1/e}{b_1 p' \ldots b_e p'} \right) = (-1/e)^{mp'} \cdot \frac{1 \cdot (1 + e) \ldots (1 + mp' - e)}{(b_1 p')! \cdot (b_2 p')! \ldots (b_e p')!}
\]

\[
= (-1/e)^{mp'} \cdot \frac{p \cdot (p + ep) \ldots (p + mp' - ep)}{(p \cdot 2p \ldots b_1 p') \ldots (p \cdot 2p \ldots b_e p')}
\]

\[
\times \frac{1 \cdot (1 + e) \ldots (1 + mp' - e)}{p \cdot (p + ep) \ldots (p + mp' - ep)}
\]

\[
\times \frac{(p \cdot 2p \ldots b_1 p') \ldots (p \cdot 2p \ldots b_e p')}{(b_1 p')! \cdot (b_2 p')! \ldots (b_e p')!}
\]

\[
= (-1/e)^{mp' - mp' - 1} \cdot \left( \frac{-1/e}{b_1 p'^{-1} \ldots b_e p'^{-1}} \right)
\]

\[
\times \frac{1 \cdot (1 + e) \ldots (1 + mp' - e)}{p \cdot (p + ep) \ldots (p + mp' - ep)}
\]

\[
\times \frac{(p \cdot 2p \ldots b_1 p') \ldots (p \cdot 2p \ldots b_e p')}{(b_1 p')! \cdot (b_2 p')! \ldots (b_e p')!}.
\]

By Corollary 2.2(iii) we have

\[
\text{ord}_p\left( \frac{-1/e}{b_1 p' \ldots b_e p'} \right) = \text{ord}_p\left( \frac{-1/e}{b_1 p'^{-1} \ldots b_e p'^{-1}} \right).
\]

Hence we have \( \text{mod } p' \)

\[
\left( \frac{-1/e}{b_1 p' \ldots b_e p'} \right)^* \equiv \left( \frac{-1/e}{b_1 p'^{-1} \ldots b_e p'^{-1}} \right)^* \cdot (-1/e)^{mp' - mp' - 1}.
\]

\[
\times \frac{1 \cdot (1 + e) \ldots (1 + mp' - e)}{p \cdot (p + ep) \ldots (p + mp' - ep)}
\]

\[
\times \frac{(p \cdot 2p \ldots b_1 p') \ldots (p \cdot 2p \ldots b_e p')}{(b_1 p')! \cdot (b_2 p')! \ldots (b_e p')!}.
\]

\[ (7) \]
Note that \((-1/e)^{mp^r} \equiv (-1/e)^{mp^{r-1}} \mod p'\) by a theorem of Fermat–Euler. Furthermore by \(e|(p - 1)\),
\[
\left( \frac{1 \cdot (1 + e) \ldots (1 + mep' - e)}{p \cdot (p + ep) \ldots (p + mep' - ep)} \right)
\]
and
\[
\frac{(b_1p')! \cdot (b_2p')! \ldots (b_e p')!}{(p \cdot 2p \ldots (p \cdot 2p \ldots b_e p')}\]
are rational integers. It now follows that
\[
\left( \frac{1 \cdot (1 + e) \ldots (1 + mep' - e)}{p \cdot (p + ep) \ldots (p + mep' - ep)} \right)^* \equiv \left( \sum_{a=1, p \not| a}^{\xi} a \right)^m
\]
\[
\equiv \left( \frac{(b_1p')! \cdot (b_2p')! \ldots (b_e p')!}{(p \cdot 2p \ldots b_1p') \ldots (p \cdot 2p \ldots b_e p')} \right)^* \mod p'.
\]
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
\[
\left( \frac{-1/e}{b_1p' \ldots b_e p'} \right) \equiv \left( \frac{-1/e}{b_1p^{r-1} \ldots b_e p^{r-1}} \right) \mod p^{r+\mu}
\]
where \(\mu = \text{ord}_p\left( \frac{-1/e}{b_1 \ldots b_e} \right)\).

**Proof.** This is obvious since
\[
\left( \frac{-1/e}{b_1p^m \ldots b_e p^m} \right) = \left( \frac{-1/e}{b_1p^{r-1} \ldots b_e p^{r-1}} \right)^* \cdot p^\mu \text{ for all } m \geq 0.
\]

3. Congruences

**Theorem A.** Let
\[
\left( 1 + \sum_{i=1}^{e} \alpha_i X^i \right)^{-1/e} = \sum_{n=0}^{\infty} u_n X^n, \text{ where } \alpha_i \in \mathbb{Z} \text{ for } i = 1 \ldots e \text{ and } e \in \mathbb{Z}, e \geq 2.
\]
Let \( p \) be a prime such that \( p \equiv 1 \mod e \). Let \( r, m \in \mathbb{N} \). Then

\[ u_{m'r} \equiv u_{m'r-1} \mod p'. \]

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

\[ \left( \begin{array}{c} -1/e \\ b_1 \ldots b_e \end{array} \right) \equiv 0 \mod p'. \]  

(9)

Now suppose that \( j > 0 \). Since \( c_k = \sum_{i=1}^{e} b_k, b_k \geq 0 \) and \( c_k = 0 \) for \( k < j \), we have \( p' \mid b_i \) for \( i = 1, \ldots, e \). Substitute \( b = b'p' \). By Lemma 2.6 we have

\[ \left( \begin{array}{c} -1/e \\ b'_1p' \ldots b'_ep' \end{array} \right) \equiv \left( \begin{array}{c} -1/e \\ b'_1p'^{-1} \ldots b'_ep'^{-1} \end{array} \right) \mod p'. \]

Since \( \alpha_i^{p'} \equiv \alpha_i^{p'^{-1}} \mod p' \), by Fermat–Euler, we have

\[ \left( \begin{array}{c} -1/e \\ b'_1p' \ldots b'_ep' \end{array} \right) \prod_i \alpha_i^{b'p'} \equiv \left( \begin{array}{c} -1/e \\ b'_1p'^{-1} \ldots b'_ep'^{-1} \end{array} \right) \prod_i \alpha_i^{b'^{p'^{-1}}} \mod p'. \]

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

\[ \left( \begin{array}{c} -1/e \\ b'_1p' \ldots b'_ep' \end{array} \right) \prod_i \alpha_i^{b'p'} \equiv \left( \begin{array}{c} -1/e \\ b'_1p'^{-1} \ldots b'_ep'^{-1} \end{array} \right) \prod_i \alpha_i^{b'^{p'^{-1}}} \mod p'. \]  

(10)

We recall Lemma 2.4,

\[ u_n = \sum_{i=0}^{e} \left( \begin{array}{c} -1/e \\ b_1 \ldots b_e \end{array} \right) \cdot \prod_{i=1}^{e} \alpha_i^{b_i}. \]

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

\[ u_{m'r} \equiv \sum \left( \begin{array}{c} -1/e \\ b_1 \ldots b_e \end{array} \right) \cdot \prod_{i=1}^{e} \alpha_i^{b_i} \mod p', \]
where \( \wedge \) denotes the sum taken over all partitions \( \{b_1, \ldots, b_e\} \) such that 
\[
\Sigma_{i=1}^e ib_i = mp \quad \text{and} \quad p | b_i \quad \text{for} \quad i = 1, \ldots, e.
\] According to (10) the right side of this congruence equals
\[
\sum_0^e \left( -\frac{1}{e} \right) \cdot \prod_{i=1}^e \alpha_i^{b_i} \equiv \, \text{u}_{m^{e-1}} \mod p',
\]
here 0 denotes the sum is taken over all partitions \( \{b_1, \ldots, b_e\} \) such that 
\[
\Sigma_{i=1}^e ib_i = mp^{e-1}.
\]

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

**THEOREM B.** Let \( p \) be a prime, \( p \geq 3 \), 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 \( J = \{1 \leq j \leq p - 1 : p | x_j\} \), \( S = \{k \in \mathbb{N} : n_k \in J\} \) 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 \( q = |R| \). Then
(i) \( \text{ord}_p u_n \geq \sigma \),
(ii) \( \text{ord}_p u_n \geq [(\sigma + 1)/2] \),
(iii) if \( J = \{p - s, p - s + 1, \ldots, p - 1\} \) for some \( s \), then \( \text{ord}_p u_n \geq \sigma \).

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

\[
B = \left\{ k \in \mathbb{N} : \sum_{j \neq i} b_{jk} > 0 \right\},
\]

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

\[
\bar{K}_i = \{k + j : k \in K_i, 0 \leq j \leq i - 1\},
\]

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

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

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

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

**Lemma 4.1.**

\[ \text{Ord}_p(u_n) \geq \min_{\Sigma b_i = n} (\beta + \tau). \]

**Proof.** Lemma 2.4 implies that

\[
u_n = \sum_{i=1}^{n} \left( -\frac{1}{p - 1} \right) \cdot \prod_{i=1}^{p-1} \alpha_i^{h_i}.
\]

Hence

\[
\text{ord}_p(u_n) \geq \min_{\Sigma b_i = n} \left( \sum_{i=1}^{p-1} b_i \cdot \text{ord}_p(\alpha_i) + \text{ord}_p\left( -\frac{1}{p - 1} \right) \right).
\]

It now follows from Corollary 2.2 that

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

Since

\[
\sum_{i=1}^{p-1} b_i \cdot \text{ord}_p(\alpha_i) \geq \sum_{i \in J} b_i \cdot \text{ord}_p(\alpha_i) \geq |B| = \beta
\]

and

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

the lemma is proved. \qed
LEMMA 4.2. If $d_{k-1} < p/(p - 1)$ and $d_k < p/(p - 1)$ then either

$$c_k = n_k = 0$$

or

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

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), $T_k = T_{k-1} + \Sigma_i b_{ik} p^k$ and finally we have, by Lemma 2.3(i), $T_k \equiv n \mod p^{k+1}$. By combining this we obtain $n_k = \Sigma_i b_{ik}$. 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 $\Sigma_i b_{ik} = 0$ and $n_k = 0$. 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

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

We shall now construct $K$ satisfying properties (i) and (ii). Let $M$ be the set of all $k$ such that $k \in \tilde{K}, k + 1 \notin \tilde{K}$ and $k \notin R$. Put $N = \{k + 1 : k \in M\}$ and take $K = (\tilde{K} \setminus M) \cup N$. Then $K$ satisfies property (i) because $|K| \leqslant |\tilde{K}| \leqslant \tau$. 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 \( d_k < \frac{p}{p-1} \). 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 \( i \geq 1 \). This implies \( d_{k-1} < \frac{p}{p-1} \). 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 \( \varrho \) is maximal. Then at least \( \varrho \geq \frac{1}{2} \sigma \).

**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 \( K \subset \mathbb{Z}_{\geq 0} \) with the properties:

(i) \( |K| \leq \tau \),
(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 \( K = (\bar{K} \setminus (M_1 \cup M_3)) \cup N_1 \cup N_2 \cup N_3 \). Note that \( |M_i| = |N_i| \) for \( i = 1, 2, 3 \), and \( |M_1 \cup M_3| = |N_1 \cup N_3| \) and \( |\bar{K}| + |N_2| \leq \Sigma|\bar{K}| \). We conclude \( |K| \leq \Sigma|\bar{K}| \leq \tau \) 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) \( d_{k-1} < \frac{p}{p-1} \). This leads to a contradiction, just as in the proof of Theorem B(i).

(b) \( d_{k-1} \geq \frac{p}{p-1} \) and \( k - 1 \notin S \). These imply that \( k - 1 \in \bar{K} \). Hence \( k \in N_1 \), contradicting \( k \notin K \).
(c) $d_{k-1} \geq p/(p - 1)$ and $d_{k-2} \geq p^2/(p - 1)$. These imply that $k - 1 \in K_i$ for some $i \geq 1$, and $k - 2 \in K_j$ for some $j \geq 2$. 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 $i \geq 2$. This implies $k \in \bar{K}_i$, which also contradicts $k \notin K$.

(d) $d_{k-1} \geq p/(p - 1)$ 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

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

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 $c_{k-1} \leq p + 1$. Since $k - 1 \notin B$, we have

$$\sum_{i=1}^{p-1} \bar{b}_{(k-1)} \leq \sum_{i=1}^{p-s-1} \bar{b}_{(k-1)} \leq (p - s - 1) \cdot c_{k-1} \leq (p - s - 1) \cdot (p + 1).$$

These arguments imply that

$$T_{k-1} = T_{k-2} + \sum_i \bar{b}_{(k-1)}p^{k-1} < p^k + (p + 1) \cdot (p - s - 1) \cdot p^{k-1}$$

$$= p^{k+1} - (s - 1) \cdot p^k + (s + 1) \cdot p^{k-1}$$

$$= (p - s) \cdot p^k + (p - s - 1) \cdot p^{k-1}.$$ 

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

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

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

$$T_k = \sum_{j=0}^k \sum_{i=1}^e \bar{b}_{ij}p^i \geq \sum_{j=0}^k n_j p^i \geq n_{k-1} p^{k-1} + n_k p^k$$

$$\geq (p - s) p^k + (p - s) p^{k-1},$$

which contradicts (11).
References


