Hokkaido Mathematical Journal Vol. 28 (1999) p. 71–85

A p-adic property of the Taylor series of $\exp(x + x^p/p)$

Hiroyuki OCHIAI

(Received October 22, 1997)

Abstract. The p-adic norms of the Taylor coefficients of the function $\exp(x + x^p/p)$ are expressed in terms of a p-adic analytic function for $p \leq 23$.

Key words: p-adic, Tate algebra, exponential function.

Introduction

Let us fix a prime $p \geq 2$. Consider a series $\{a(n) \mid n \in \mathbf{Z}_{\geq 0}\}$ defined by the recursion:

$$\begin{aligned} &a(n+1) = a(n) + n(n-1)\cdots(n-p+2)a(n-p+1), \\ &a(0) = a(1) = \cdots = a(p-1) = 1. \end{aligned} \tag{0.1}$$

In other words, $\{a(n)\}$ is the coefficients of the Taylor series expansion of the function $\exp(x + x^p/p)$,

$$\exp\left(x + \frac{x^p}{p}\right) = \sum_{n=0}^{\infty} a(n)\frac{x^n}{n!}.$$

As another interpretation, a_n is the number of group homomorphisms from the cyclic group $\mathbf{Z}/p\mathbf{Z}$ of order p to the symmetric group S_n of n letters [Y]. In this paper we discuss the p-adic valuation $\nu_p(a(n))$ of $a(n)$.

Throughout the paper, we assume that the prime p satisfies the following condition. The conditions concern with the p-adic behaviour of the transfer matrix $T(x)$, which is defined in §1.

Condition A *We define the following condition on the transfer matrix* $T(x)$.

(A1) $T(x) \in M(p, \mathbf{Z}[x])$.

(A2) *If we denote the first row of* $T(x)$ *by*

$$\mathbf{t}(x)^T := (T(x)_{11}, \ldots, T(x)_{1p}) \in M(1, p, \mathbf{Z}[x]),$$

then $T(x) \equiv \mathbf{e} \cdot \mathbf{t}(x)^T \bmod p$.

1991 Mathematics Subject Classification : Primary 11B39; Secondary 19A22, 30G06, 11B50, 12J25.

(A3) $\mathrm{tr}(T(x)) \bmod p$ *is in* $(\mathbf{Z}/p\mathbf{Z})^{\times}$.

Here $\mathrm{tr}(\cdot)$ means the trace of a matrix. Under these conditions, we have the main theorem of the paper.

Theorem B *Suppose p to be a prime satisfying Condition* A. *Then there exist p-adic analytic functions $\lambda(x) \in \mathbf{Z}\langle x \rangle$ and $f_i(x) \in \mathbf{Z}\langle x \rangle$ for $i = 0, 1, \ldots, p^2 - 1$ convergent on $\{x \mid \nu_p(x) \geq 0\}$ such that*

$$a(p^2m + i) = f_i(m)p^{(p-1)m} \prod_{j=1}^{m} \lambda(j) \quad \text{for any} \quad m \in \mathbf{Z}_{\geq 0}.$$

In particular, the asymptotic behaviour of $\nu_p(a(p^2m + i))$ for large m is described by that of $\nu_p(f_i(m))$.

Corollary C *With the notation in Theorem* B, *we have the following results.*

(i) $\nu_p(a(p^2m + i)) = (p - 1)m + \nu_p(f_i(m))$ *for* $i = 0, 1, \ldots, p^2 - 1$.

(ii) $\nu_p(f_i(m)) \geq [i/p]$ *for* $i = 0, 1, \ldots, p^2 - 1$.

(iii) $\nu_p(f_i(m)) = 0$ *for* $i = 0, 1, \ldots, p - 1$.

The proof of Theorem B and Corollary C is given in Section 2. In Section 3, we prove that Condition A holds for $p \leq 23$. It seems true that Condition A would hold for all p though we have not yet proved it. We also give examples of $f_i(x)$.

The author would like to thank Professor T. Yoshida and a referee for valuable comments. He also thanks Professor K. Conrad for helpful suggestions on an earlier version of the paper.

Notation

We denote the ring of p-adic integers by $\mathbf{Z}_p$. The cyclic group of order p is denoted by $\mathbf{Z}/p\mathbf{Z}$. Let $\nu_p : \mathbf{Z}_p \to \mathbf{Z} \cup \{\infty\}$ be the p-adic valuation. If $p^b || a$, then we define $\nu_p(a) := b$. Here $p^b || a$ means that $p^b | a$ and $p^{b+1} \nmid a$. Namely, $\nu_p(a)$ is the highest power of p dividing a.

We denote the polynomial ring over $\mathbf{Z}$ with the variable x by $\mathbf{Z}[x]$, the ring of formal power series with coefficients in $\mathbf{Z}_p$ by $\mathbf{Z}_p[[x]]$. The Tate algebra $\mathbf{Z}\langle x \rangle$ is defined by (see [BGR])

$$\mathbf{Z}\langle x \rangle = \left\{ \sum_{n=0}^{\infty} b_n x^n \mid \lim_{n \to \infty} \nu_p(b_n) = +\infty \right\}.$$

For $f(x) = \sum b_n x^n \in \mathbf{Z}[x]$, $\mathbf{Z}_p[x]$, or $\mathbf{Z}_p[[x]]$, we define

$$\nu_p(f(x)) := \min_n \{\nu_p(b_n)\}$$

and

$$f(x) \equiv g(x) \mod p^k \overset{\text{def}}{\iff} \nu_p(f(x) - g(x)) \geq k.$$

Remark that $f(x) \equiv 0 \mod p^k$ is equivalent to $f(x+1) \equiv 0 \mod p^k$. For a vector or a matrix, this means that all entries satisfy the condition.

We denote the set of all $m \times n$ matrices with coefficients in R by $M(m, n, R)$.

1. Transfer matrix $T(x)$

Define a $p \times p$ matrix $C(x) \in M(p, \mathbf{Z}[x])$ by

$$C(x)_{ij} := \begin{cases} (x+1)(x+2)\cdots(x+p-1) & \text{for } i = p,\ j = 1, \\ 1 & \text{for } j = i+1, \text{ or } i = j = p, \\ 0 & \text{otherwise.} \end{cases}$$

Namely,

$$C(x) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ * & 0 & 0 & 1 \end{pmatrix},$$

where the lower-left entry is $(p-1)!\binom{x+p-1}{p-1} = (x+1)(x+2)\cdots(x+p-1)$.

From the series (0.1), we define a column vector $\mathbf{a}(n) \in M(p, 1, \mathbf{Z})$ by

$$\mathbf{a}(n) = (a(n), a(n+1), \ldots, a(n+p-1))^T,$$

here T means the transpose. The initial condition is given by

$$\mathbf{a}(0) = \mathbf{e}$$

where

$$\mathbf{e} := (1, 1, \ldots, 1)^T \in M(p, 1, \mathbf{Z}).$$

The recursion relation is written as

$$\mathbf{a}(n+1) = C(n)\mathbf{a}(n) \qquad n \in \mathbf{Z}_{\geq 0}.$$

We define a *transfer matrix* $T(x)$ by

$$T(x) := C(p^2x + p^2 - 1) \cdots C(p^2x + 1)C(p^2x)/p^{p-1}.$$

Then we have

$$\mathbf{a}(p^2m + p^2) = p^{p-1}T(m)\mathbf{a}(p^2m). \tag{1.1}$$

Lemma 1.1 *All row vectors of* $T(-1)$ *are identical; that is,* $T(-1) = \mathbf{e} \cdot (*, *, \ldots, *)$.

Proof. Since $C(-1) = C(-2) = \cdots = C(-p+1)$ and the lower left-most entry of $C(-1)$ is zero, we have

$$C(-1)C(-2) \cdots C(-p+1) = C(-1)^{p-1} = \mathbf{e} \cdot (0, \ldots, 0, 1).$$

This proves the lemma. □

The condition (A1) is equivalent to the condition that every entry $T(x)_{ij}$ belongs to $\mathbf{Z}[x]$. The condition (A2) is equivalent to the condition that

$$T(x)_{ij} - T(x)_{i'j}$$

can be divided by p. The condition (A3) is equivalent to the equality $\mathbf{t}(x)^T\mathbf{e} = \sum_{j=1}^{p} T(x)_{1j} \in (\mathbf{Z}/p\mathbf{Z})^\times$.

2. Main theorem

The following proposition is a key to the main theorem, Theorem B.

Proposition 2.1 (i) *Suppose* p *satisfies Condition* A. *Fix a positive integer* k. *Then there exist polynomials*

$$\mathbf{f}^{(k)}(x) = (f_0^{(k)}(x), f_1^{(k)}(x), \ldots, f_{p-1}^{(k)}(x))^T \in M(p, 1, \mathbf{Z}[x]),$$
$$\text{and} \quad \lambda^{(k)}(x) \in \mathbf{Z}[x]$$

satisfying the following condition:

(1) $f_0^{(k)}(x) = 1$.
(2) $\mathbf{f}^{(k)}(0) = \mathbf{e}$.
(3) $\mathbf{f}^{(k)} \equiv \mathbf{e} \bmod p$.
(4) $\lambda^{(k)}(x) \bmod p$ *is in* $(\mathbf{Z}/p\mathbf{Z})^\times$.
(5) $T(x-1)\mathbf{f}^{(k)}(x-1) \equiv \lambda^{(k)}(x)\mathbf{f}^{(k)}(x) \bmod p^k$.

(ii) *Such* $\mathbf{f}^{(k)}(x)$ *and* $\lambda^{(k)}(x)$ *are unique modulo* p^k.

Proof. (i) This is proved by induction on k. In particular, we construct $\mathbf{f}^{(k)}(x)$ and $\lambda^{(k)}(x)$ inductively. The argument is similar to that used in the Hensel lemma.

For $k = 1$, we can take

$$\mathbf{f}^{(1)}(x) := \mathbf{e} \quad \text{and} \quad \lambda^{(1)}(x) := \mathrm{tr}(T(x-1)).$$

The conditions (1), (2), (3) are clear. The condition (4) is equivalent to the condition (A3). The condition (5) follows from the condition (A2).

Now we assume that Proposition 2.1 (i) holds for a $k \geq 1$. We will prove Proposition 2.1 (i) for $k+1$. By the induction assumption (4), there exists an element $(\lambda^{(k)}(x))^{-1} \in \mathbf{Z}[x]$ such that

$$\lambda^{(k)}(x)(\lambda^{(k)}(x))^{-1} \equiv 1 \mod p^{k+1}.$$

Although such an element is not unique, we pick up such an element in what follows.

Let us define

$$\mathbf{g}(x) := (\lambda^{(k)}(x))^{-1} T(x-1)\mathbf{f}^{(k)}(x-1) - \mathbf{f}^{(k)}(x) \in M(p, 1, \mathbf{Z}[x]).$$

Although this should be denoted by $\mathbf{g}^{(k)}(x)$, we use $\mathbf{g}(x)$ for brevity. By the induction assumption (5),

$$\mathbf{g}(x) \equiv 0 \mod p^k. \tag{2.1}$$

By the induction assumption (2) together with Lemma 1.1, we see that $\mathbf{g}(0)$ is a multiple of $\mathbf{e}$. In other words,

$$\mathbf{g}(0) = g_0(0)\mathbf{e}. \tag{2.2}$$

We define

$$\mathbf{f}^{(k+1)}(x) := \mathbf{f}^{(k)}(x) + \mathbf{g}(x) - g_0(x)\mathbf{e},$$
$$\lambda^{(k+1)}(x) := \lambda^{(k)}(x)(1 + g_0(x)) + \mathbf{t}(x-1)^T(\mathbf{g}(x-1) - g_0(x-1)\mathbf{e}).$$

By definition, we have

$$f_0^{(k+1)}(x) = f_0^{(k)}(x).$$

By (2.2), we have

$$\mathbf{f}^{(k+1)}(0) = \mathbf{f}^{(k)}(0).$$

By (2.1), we have

$$\mathbf{f}^{(k+1)}(x) \equiv \mathbf{f}^{(k)}(x) \mod p^k,$$
$$\lambda^{(k+1)}(x) \equiv \lambda^{(k)}(x) \mod p^k.$$

Then the induction assumption (1), (2), (3), (4) implies the corresponding required condition for $k+1$.

Finally, we prove the condition (5). For the quantity in question,

$$\begin{aligned} &T(x-1)\mathbf{f}^{(k+1)}(x-1) \\ &\quad \equiv \lambda^{(k)}(x)(\mathbf{f}^{(k)}(x)+\mathbf{g}(x)) + T(x-1)(\mathbf{g}(x-1)-g_0(x-1)\mathbf{e}) \\ &\quad = \lambda^{(k)}(x)(\mathbf{f}^{(k+1)}(x)+g_0(x)\mathbf{e}) \\ &\qquad\qquad + T(x-1)(\mathbf{g}(x-1)-g_0(x-1)\mathbf{e}) \mod p^{k+1}. \end{aligned}$$

In order to prove the condition (5)

$$T(x-1)\mathbf{f}^{(k+1)}(x-1) \equiv \mathbf{f}^{(k+1)}(x)\lambda^{(k+1)}(x) \mod p^{k+1},$$

it is enough to prove that

$$\begin{aligned} &\lambda^{(k)}(x)g_0(x)\mathbf{e} \equiv \lambda^{(k)}(x)g_0(x)\mathbf{f}^{(k+1)}(x), \quad \text{and} \\ &T(x-1)(\mathbf{g}(x-1)-g_0(x-1)\mathbf{e}) \\ &\qquad \equiv \mathbf{f}^{(k+1)}(x)\mathbf{t}(x-1)^T(\mathbf{g}(x-1)-g_0(x-1)\mathbf{e}) \end{aligned}$$

modulo p^{k+1}. The first equality follows from (2.1) and the condition (3). Similarly, the right hand side of the second equality is equivalent to

$$\equiv \mathbf{e}\cdot\mathbf{t}(x-1)^T(\mathbf{g}(x-1)-g_0(x-1)\mathbf{e}) \mod p^{k+1}.$$

Then the second equality is guaranteed by (2.1) and (A2). This proves (i).

(ii) This is also proved by induction on k. For $k=1$, we see that $\mathbf{f}^{(1)}$ is uniquely determined by the condition (3) modulo p^1. Then the condition (5) and the assumption (A2) imply that $\mathrm{tr}(T(x-1)) = \lambda^{(1)}(x)$ modulo p^1. Hence we have (ii) for $k=1$.

Now we suppose that Proposition 2.1 (ii) holds for $k \geq 1$ and prove that it also holds for $k+1$. Suppose that $\mathbf{f}^{(k+1)}(x)$ and $\lambda^{(k+1)}(x)$ satisfy the conditions (1) to (5). By the uniqueness for k, which is the induction assumption, we have

$$\mathbf{f}^{(k+1)}(x) \equiv \mathbf{f}^{(k)}(x),\ \lambda^{(k+1)}(x) \equiv \lambda^{(k)}(x) \mod p^k. \tag{2.3}$$

Now let us suppose that $\tilde{\mathbf{f}}^{(k+1)}(x)$ and $\tilde{\lambda}^{(k+1)}(x)$ also satisfy the conditions (1) to (5) for $k+1$. We define

$$\begin{aligned}\mathbf{F}(x) &:= (\tilde{\mathbf{f}}^{(k+1)}(x) - \mathbf{f}^{(k+1)}(x))/p^k,\\ \Lambda(x) &:= (\tilde{\lambda}^{(k+1)}(x) - \lambda^{(k+1)}(x))/p^k.\end{aligned}$$

Note that these are in $\mathbf{Z}[x]$.

The condition (5),

$$\begin{aligned}T(x-1)\mathbf{f}^{(k+1)}(x-1) &\equiv \lambda^{(k+1)}(x)\mathbf{f}^{(k+1)}(x) \mod p^{k+1},\\ T(x-1)\tilde{\mathbf{f}}^{(k+1)}(x-1) &\equiv \tilde{\lambda}^{(k+1)}(x)\tilde{\mathbf{f}}^{(k+1)}(x) \mod p^{k+1},\end{aligned}$$

implies

$$T(x-1)\mathbf{F}(x-1) \equiv \Lambda(x)\mathbf{f}^{(k+1)}(x) + \tilde{\lambda}^{(k+1)}(x)\mathbf{F}(x) \mod p.$$

By the assumption (A2) and the condition (3), we have

$$\begin{aligned}\lambda^{(1)}(x)\mathbf{F}(x) &\equiv \mathbf{e}\cdot\mathbf{t}(x-1)^T\mathbf{F}(x-1) - \Lambda(x)\mathbf{e}\\ &= (\mathbf{t}(x-1)^T\mathbf{F}(x-1) - \Lambda(x))\mathbf{e} \mod p.\end{aligned}$$

In particular, each entry of $\lambda^{(1)}(x)\mathbf{F}(x)$ satisfies

$$\begin{aligned}\lambda^{(1)}(x)F_0(x) \equiv \cdots &\equiv \lambda^{(1)}(x)F_{p-1}(x)\\ &\equiv (\mathbf{t}(x-1)^T\mathbf{F}(x-1) - \Lambda(x))\mathbf{e} \mod p.\end{aligned}$$

The condition (1),

$$f_0^{(k+1)}(x) = 1, \quad \tilde{f}_0^{(k+1)}(x) = 1$$

implies $F_0(x) = 0$. Together with the condition (4), we see that $\mathbf{F}(x)$ and $\Lambda(x)$ are zero modulo p. This proves the uniqueness for $k+1$. □

As a limit "$k \to \infty$", we have the following theorem.

Theorem 2.2 *Suppose p satisfies Condition* A. *Then there exist unique p-adic analytic functions*

$$\mathbf{f}(x) = (f_0(x), \ldots, f_{p-1}(x))^T \in M(p, 1, \mathbf{Z}\langle x\rangle), \quad \textit{and} \quad \lambda(x) \in \mathbf{Z}\langle x\rangle$$

defined on $\mathbf{Z}_p$ such that

(1) $f_0(x) = 1$.

(2) $\mathbf{f}(0) = \mathbf{e}$.

(3) $\mathbf{f}(x) \equiv \mathbf{e} \bmod p$.
(4) $\lambda(x) \in (\mathbf{Z}\langle x \rangle)^{\times}$.
(5) $T(x-1)\mathbf{f}(x-1) = \lambda(x)\mathbf{f}(x)$.

Proof. From the proof of Proposition 2.1, we can take

$$\begin{aligned} \mathbf{f}^{(k+1)}(x) &\equiv \mathbf{f}^{(k)}(x) \mod p^k \\ \lambda^{(k+1)}(x) &\equiv \lambda^{(k)}(x) \mod p^k. \end{aligned}$$

This implies that $\{f^{(k)}(x)\}_{k=1}^{\infty}$ and $\{\lambda^{(k)}(x)\}_{k=1}^{\infty}$ are Cauchy sequences in $\mathbf{Z}\langle x \rangle$, that is, $\nu_p(\lambda^{(k)}(x) - \lambda^{(k')}(x)) \geq \min(k, k') \to \infty$ as $k, k' \to \infty$. As limits, we obtain the required functions. For example, the value at $n \in \mathbf{Z}$ is given by a convergent series in $\mathbf{Z}_p$:

$$\lambda(n) := \lim_{k \to \infty} \lambda^{(k)}(n).$$

The properties (1)–(5) follow from the corresponding conditions in Proposition 2.1. The uniqueness follows from Proposition 2.1 (ii). □

As a corollary, we obtain an expression of the general term $\mathbf{a}(p^2m)$.

Proposition 2.3 *Suppose there are p-adic analytic functions* $\mathbf{f}(x)$ *and* $\lambda(x)$ *on* $\mathbf{Z}_p$ *satisfying the conditions* (1) *to* (5) *in Theorem* 2.2. *Let us regard the vector* $\mathbf{a}(p^2m) \in M(p, 1, \mathbf{Z})$ *defined in* §1 *as an element of* $M(p, 1, \mathbf{Z}_p)$. *Then we have the equality*

$$\mathbf{a}(p^2m) = \mathbf{f}(m)p^{(p-1)m} \prod_{j=1}^{m} \lambda(j) \quad \textit{for any} \quad m \in \mathbf{Z}_{\geq 0}.$$

Proof. By (1.1), we have

$$\begin{aligned} \mathbf{a}(p^2m)/p^{(p-1)m} &= T(m-1)\cdots T(1)T(0)\mathbf{a}(0) \\ &= T(m-1)\cdots T(1)T(0)\mathbf{e} \end{aligned}$$

On the other hand, Theorem 2.2 tells us

$$\begin{aligned} &T(m-1)T(m-2)\cdots T(1)T(0)\mathbf{e} \\ &\quad = T(m-1)T(m-2)\cdots T(1)T(0)\mathbf{f}(0) \\ &\quad = \mathbf{f}(m)\lambda(m)\lambda(m-1)\cdots\lambda(2)\lambda(1). \end{aligned}$$

□

Now we are ready to prove the main theorem.

Proof of Theorem B. For $i = 0, 1, \ldots, p-1$, it has already been proved in Proposition 2.3. Recall the relation

$$\mathbf{a}(n+1) = C(n)\mathbf{a}(n).$$

Then, for example, we have

$$\mathbf{a}(p^2m+1) = C(p^2m)\mathbf{a}(p^2m) = C(p^2m)\mathbf{f}(m)p^{(p-1)m}\prod_{j=1}^{m}\lambda(j).$$

The last entry of this equality means that it is enough to take

$$f_p(x) = (0, 0, \ldots, 0, 1)C(p^2x)\mathbf{f}(x).$$

In general, we can take

$$f_i(x) = (0, 0, \ldots, 0, 1)C(p^2x + i - p)\ldots C(p^2m+1)C(p^2m)\mathbf{f}(x).$$

for $p \leq i < p^2$. □

Proof of Corollary C. Assertion (i) is immediate from Theorem B. Assertion (ii) is proved in [Y]. Assertion (iii) follows from the property (3) in Theorem 2.2. □

In particular, the asymptotic behaviour of $\nu_p(a(p^2m+i))$ for large m is described by that of $\nu_p(f_i(m))$. In practical applications, we can expect that $\nu_p(f_i(m))$ has a simpler behaviour.

The following is a special case of the Weierstrass preparation theorem [BGR], [G].

Lemma 2.4 *Any element* $h(x) \in \mathbf{Z}\langle x\rangle$ *is a unique product of a power of* p, *a monic polynomial* $k(x) \in \mathbf{Z}_p[x]$, *and a unit* $u(x) \in (\mathbf{Z}\langle x\rangle)^\times$:

$$h(x) = p^e k(x)u(x).$$

Here, the order N *of the polynomial* $k(x)$ *is given by*

$$N = \max\left\{n \in \mathbf{Z}_+ \mid \nu_p(h_n) = \min_{n' \geq 0}\nu_p(h_{n'})\right\} \quad \textit{for} \quad h(x) = \sum_{n=0}^{\infty} h_n x^n.$$

Also, for any $x \in \mathbf{Z}_p$,

$$\nu_p(h(x)) = e + \nu_p(k(x)).$$

Lemma 2.5 *Let* $h(x) \in \mathbf{Z}\langle x \rangle$.

(i) *If*

$$h(x) \equiv cp^e \mod p^{e+1},$$

with some $e \in \mathbf{Z}$ *and* $c \in (\mathbf{Z}/p\mathbf{Z})^\times$, *then* $\nu_p(h(m)) = e$. *In particular, if* $h(x) = f_i(x)$, *then*

$$\nu_p(a(p^2m + i)) = (p-1)m + e.$$

(ii) *If*

$$h(x) \equiv cp^e(x - b^{(1)}) \mod p^{d+1},$$

with some $e \in \mathbf{Z}$, $c \in (\mathbf{Z}/p\mathbf{Z})^\times$, *and* $b^{(1)} \in \mathbf{Z}/p\mathbf{Z}$, *then the equation* $h(x) = 0$ *has a unique solution* $x = b \in \mathbf{Z}_p$ *such that* $b \equiv b^{(1)} \mod p$. *Using this solution,* $\nu_p(h(m)) = e + \nu_p(m - b)$. *In particular, if* $h(x) = f_i(x)$, *then*

$$\nu_p(a(p^2m + i)) = (p-1)m + e + \nu_p(m - b).$$

Proof. We use the notation in Lemma 2.4.

For (i), we see that $N = 0$, and that $k(x) = 1$.

For (ii), we see that $N = 1$, and that $k(x) = x - b$. □

Lemma 2.5 may not apply to all situations, but its assumptions are satisfied in most cases. In fact, Lemma 2.5 covers all cases for $p \leq 11$, as is seen in §3.

3. Example

In this section, we deal with the case for a small p.

3.1. On Condition A

We will see that Condition A is true for $p = 2, 3, 5, 7, 11, 13, 17, 19, 23$.

Proposition 3.1 *For* $p \leq 23$, *every entry of the matrix*

$$C(p^2x + p^2 - 1) \cdots C(p^2x + 1)C(p^2x)$$

can be divided by p^{p-1}.

In other words, $T(x) \in M(p, \mathbf{Z}[x])$. Let us define

$$\tilde{T}(x) := (T(x) \mod p) \in M(p, (\mathbf{Z}/p\mathbf{Z})[x]).$$

Proposition 3.2 *For* $p \leq 23$, *we have*

(a) *The matrix* $\tilde{T}(x)$ *does not contain the variable* x.

(b) *All row vectors of* $\tilde{T}(x)$ *are identical.*

(c) $\mathrm{tr}(\tilde{T}(x)) = -1 \bmod p$.

In particular, Condition A holds for $p \leq 23$. Both propositions are proved with the help of Mathematica. The explicit form of $\tilde{T}(x)$ is given as follows:

$$T(x) \equiv \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \mathbf{e} \cdot (0,1) \mod 2.$$

$$T(x) \equiv \mathbf{e} \cdot (0,2,0) \mod 3.$$

$$T(x) \equiv \mathbf{e} \cdot (2,1,3,2,1) \mod 5.$$

$$T(x) \equiv \mathbf{e} \cdot (6,3,5,0,4,3,6) \mod 7.$$

$$T(x) \equiv \mathbf{e} \cdot (0,2,3,3,9,2,4,0,7,7,6) \mod 11.$$

$$T(x) \equiv \mathbf{e} \cdot (9,0,9,5,2,1,1,10,3,2,7,6,9) \mod 13.$$

$$T(x) \equiv \mathbf{e} \cdot (10,7,16,5,15,9,8,7,14,5,5,14,9,13,15,0,0) \mod 17.$$

$$T(x) \equiv \mathbf{e} \cdot (9,2,13,5,18,7,11,13,2,6,13,15,13,13,7,6,12,5,0) \mod 19.$$

$$T(x) \equiv \mathbf{e} \cdot (8,10,8,12,14,9,20,2,9,6,1,18,0,11,9,21,10,15,19, 3,15,17,15) \mod 23.$$

In what follows, we calculate $f_i(x)$ for $p \leq 11$. This enables us to express the series $\nu_p(a(m))$ explicitly.

3.2. $p = 2$

We use the algorithm given in the proof of Proposition 2.1. We easily obtain, for example,

$$f_0(x) \equiv 1 \mod p^5$$
$$f_1(x) \equiv 1 + 24x + 16x^2 \mod p^5.$$

This, with the help of the proof of Theorem B, implies that

$$f_2(x) \equiv 2(1 + 14x + 8x^2) \mod p^5$$
$$f_3(x) \equiv 4(1 + 2x^2) \mod p^5.$$

Then it is summarized as

$$f_0(x) \equiv 1,\ f_1(x) \equiv 1,\ f_2(x) \equiv p(1 + px),\ f_3(x) \equiv p^2 \mod p^3.$$

All of these are of the form in Lemma 2.5 (i). Hence, we have

$$\begin{aligned}
&\nu_p(f_0(m)) = 0, \quad \nu_p(f_1(m)) = 0,\\
&\nu_p(f_2(m)) = 1, \quad \nu_p(f_3(m)) = 2, \quad \text{and}\\
&\nu_2(a(4m)) = m, \quad \nu_2(a(4m+1)) = m,\\
&\nu_2(a(4m+2)) = m+1, \quad \nu_2(a(4m+3)) = m+2.
\end{aligned}$$

3.3. $p = 3$

It is enough to calculate $\mathbf{f}(x)$ mod p^5, although this fact cannot be recognized before the calculation. The result is

$$\begin{aligned}
f_0(x) &\equiv 1 \mod p^5\\
f_1(x) &\equiv 1 + 108x + 81x^2 \mod p^5\\
f_2(x) &\equiv 1 + 117x + 81x \mod p^5\\
f_3(x) &\equiv p(1 + 48x + 54x^2) \mod p^5.\\
f_4(x) &\equiv p^2(1 + 12x) \mod p^5\\
f_5(x) &\equiv p(7 + 39x + 54x^2) \mod p^5\\
f_6(x) &\equiv p^4(1 + x) \mod p^5\\
f_7(x) &\equiv p^3(4 + 3x) \mod p^5\\
f_8(x) &\equiv p^2(2 + 18x + 9x^2) \mod p^5.
\end{aligned}$$

Now we introduce the notation

$$f(x) \sim cp^d \overset{\text{def}}{\iff} f(x) \equiv cp^d \mod p^{d+1}$$

for short. Then the result above can be written

$$\begin{aligned}
&f_0(x) \sim 1p^0, && f_1(x) \sim 1p^0, && f_2(x) \sim 1p^0\\
&f_3(x) \sim 1p^1, && f_4(x) \sim 1p^2, && f_5(x) \sim 1p^1\\
&f_6(x) \sim (1+x)p^4, && f_7(x) \sim 1p^3, && f_8(x) \sim 2p^2.
\end{aligned}$$

For $\nu_3(f_i(m))$ and $\nu_3(a_{9m+i})$, we can apply Lemma 2.5. For example,

$$\begin{aligned}
&\nu_3(a(9m)) = 2m, && \nu_3(a(9m+1)) = 2m,\\
&\nu_3(a(9m+2)) = 2m, && \nu_3(a(9m+3)) = 2m+1,\\
&\nu_3(a(9m+4)) = 2m+2, && \nu_3(a(9m+5)) = 2m+1,\\
&\nu_3(a(9m+6)) \geq 2m+4, && \nu_3(a(9m+7)) = 2m+3,\\
&\nu_3(a(9m+8)) = 2m+2.
\end{aligned}$$

For $f_6(x)$, we can apply Lemma 2.5 (ii). In particular, we have

$$\nu_3(a(9m+6)) = 2m + 4 + \nu_3(m-b)$$

with some $b \in \mathbf{Z}_3$. Its approximation is

$$b \equiv -1 + 3 + 3^2 - 3^7 - 3^8 + 3^9 - 3^{10} + 3^{14} - 3^{15} - 3^{16} + 3^{17} + 3^{18} - 3^{19} + 3^{20} \mod 3^{21}.$$

3.4. $p = 5$

It is enough to calculate $\mathbf{f}(x)$ mod p^5. The result is

$$\begin{pmatrix} f_0(x) & f_1(x) & \dots & f_{p-1}(x) \\ f_p(x) & f_{p+1}(x) & \dots & f_{2p-1}(x) \\ \dots & \dots & \dots & \dots \\ f_{p^2-p}(x) & \dots & \dots & f_{p^2-1}(x) \end{pmatrix} \sim \begin{pmatrix} 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 \\ 1p^2 & 4p^1 & 1p^1 & 4p^1 & 1p^2 \\ 4p^3 & 2p^2 & 1p^2 & 1p^3 & 3p^3 \\ 4p^3 & 3p^3 & 4p^3 & 4p^3 & 4p^3 \\ 3p^4 & 1p^4 & 3p^4 & 1p^4 & 2p^4 \end{pmatrix}$$

This set of relations is read entry-wise, as in §3.3.

As is above, this completely determines $\nu_5(f_i(m))$ and $\nu_5(a(m))$ by Lemma 2.5 (i). Remark that no 'exception' arises for $p = 5$.

3.5. $p = 7$

It is enough to calculate $\mathbf{f}(x)$ mod p^9. We find

$$\begin{pmatrix} f_0(x) & f_1(x) & \dots & f_{p-1}(x) \\ f_p(x) & f_{p+1}(x) & \dots & f_{2p-1}(x) \\ \dots & \dots & \dots & \dots \\ f_{p^2-p}(x) & \dots & \dots & f_{p^2-1}(x) \end{pmatrix} \sim$$

$$\begin{pmatrix} 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 \\ 5p^1 & 4p^1 & 4p^2 & 2p^1 & 5p^2 & 4p^1 & 5p^1 \\ 4p^2 & 3p^2 & 3p^2 & 4p^2 & 4p^2 & 1p^2 & 4p^2 \\ 1p^3 & 6p^3 & 5p^3 & 1p^3 & 5p^3 & 3p^3 & 1p^3 \\ * & 4p^4 & 1p^4 & 2p^4 & 4p^4 & 3p^4 & 4p^5 \\ 4p^5 & 5p^5 & 6p^5 & 5p^5 & 3p^6 & 4p^5 & 4p^5 \\ 1p^6 & 6p^6 & 2p^6 & 6p^6 & 6p^6 & 4p^6 & 1p^8 \end{pmatrix}$$

Here the missing entry $* = (6+6x)p^6$. Slightly more precisely,

$$\begin{aligned} f_{28}(x) \equiv\ & p^6(186476807 + 166348020x + 226514421x^2 \\ & + 112502285x^3 + 83692x^4 + 241874339x^5 \\ & + 97295723x^6 + 132590423x^7 \mod p^{16}. \end{aligned}$$

By Lemma 2.5, this completely determines $\nu_7(f_i(m))$ and $\nu_7(a(49m+i))$, except for the case $i = 28$. The approximation of the solution $x = b$ for the equation $f_{28}(x) = 0$ is given by

$$b \equiv -1 - p + 3p^2 + 3p^4 - p^5 + 2p^6 - p^8 \mod p^{10}.$$

3.6. $p = 11$

$$\begin{pmatrix} f_0(x) & f_1(x) & \dots & f_{p-1}(x) \\ f_p(x) & f_{p+1}(x) & \dots & f_{2p-1}(x) \\ \dots & \dots & \dots & \dots \\ f_{p^2-p}(x) & \dots & \dots & f_{p^2-1}(x) \end{pmatrix} \sim$$

$$\begin{pmatrix} 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 & 1p^0 \\ 1p^1 & 5p^2 & 5p^1 & 1p^1 & 9p^1 & 2p^2 & 9p^1 & 1p^1 & 5p^1 & 3p^2 & 1p^1 \\ 1p^2 & 1p^2 & 7p^2 & 10p^2 & 9p^3 & 6p^3 & 8p^2 & 3p^2 & 10p^2 & 10p^2 & 1p^2 \\ 7p^4 & 8p^3 & 3p^3 & 4p^3 & 4p^3 & 4p^3 & 7p^4 & 5p^3 & 4p^3 & 8p^3 & 4p^4 \\ 8p^4 & 9p^4 & 3p^4 & 5p^4 & 1p^4 & ** & 10p^5 & 5p^4 & 3p^4 & 8p^4 & 8p^4 \\ 4p^5 & 3p^5 & 1p^5 & *** & 7p^5 & 7p^5 & 7p^5 & 5p^5 & 10p^5 & 8p^5 & 4p^5 \\ 3p^6 & 7p^6 & 4p^6 & 4p^6 & 10p^6 & 6p^6 & 10p^6 & 1p^6 & 10p^6 & 1p^6 & 3p^6 \\ 7p^7 & 2p^7 & 10p^7 & 8p^7 & 7p^7 & 3p^7 & 6p^7 & 5p^7 & 10p^7 & 8p^7 & 7p^7 \\ 9p^8 & 4p^8 & 8p^8 & 5p^8 & 2p^8 & 6p^8 & 9p^8 & 8p^8 & 9p^8 & 8p^8 & 9p^8 \\ 9p^9 & 6p^9 & 3p^9 & 10p^9 & 4p^{10} & 9p^9 & 1p^9 & 8p^9 & 2p^9 & 5p^9 & 9p^9 \\ 10p^{11} & 6p^{10} & 2p^{10} & 9p^{10} & 9p^{10} & 2p^{10} & 4p^{10} & 2p^{10} & 5p^{10} & 8p^{10} & 10p^{10} \end{pmatrix}$$

Here, $** = (3+3x)p^6 \sim f_{49}(x)$ and $*** = (10+9x)p^7 \sim f_{58}(x)$. More precisely, modulo p^{12}, we have

$$\begin{aligned} f_{49}(x) \equiv\ & p^6(338968 + 472706x + 807653x^2 + 741730x^3 \\ & + 766656x^4 + 263538x^5) \end{aligned}$$

$$f_{58}(x) \equiv p^7(66439 + 76074x + 39666x^2 + 19844x^3 + 35937x^4 + 117128x^5).$$

This table completely determines $\nu_{11}(f_i(m))$ and $\nu_{11}(a(121m+i))$ for $i \neq 49, 58$ by Lemma 2.5 (i). For $i = 49, 58$, we can apply Lemma 2.5 (ii). An approximation of the solution is given by

$$b \equiv -1 - 2p - p^3 + 5p^4 - 3p^5 \mod p^6 \quad \text{for } f_{49}(b) = 0.$$
$$b' \equiv 5 + 6p + 4p^2 + 5p^3 + 4p^4 \mod p^5 \quad \text{for } f_{58}(b') = 0.$$

References

[BGR] Bosch S., Güntzer U. and Remmert R., *Non-Archimedean Analysis.* Springer, Grund. **261**, 1984.

[G] Gouvêa F.Q., *p-adic Numbers.* Springer, Universitext, 2nd. ed., 1997.

[K] Koblitz N., *p-adic numbers, p-adic analysis, and zeta functions.* Springer, Graduate Text in Math. **58**, 1977.

[O] Ochiai H., *A three-adic property of Taylor series of* $\exp(x+x^3/3)$. (1997), preprint.

[S] Stanley R., *Enumerative combinatorics.* Vol. 1, Wadsworth & Brooks/Cole Mathematics Series, 1986, reprinted from Cambridge Studies in Advanced Mathematics. **49** (1997).

[Y] Yoshida T., *Groups and generating functions.* in 'Groups and Combinatorics', Proceeding of Symp. RIMS **794** (1992), 18–29.

Department of Mathematics, Rikkyo University
Nishi-ikebukuro, Tokyo 171-8501, Japan

Current Address:
Deparment of Mathematics, Kyushu University
Fukuoka 812-0053, Japan
E-mail: ochiai@rkmath.rikkyo.ac.jp
ochiai@math.kyushu-u.ac.jp