Hermitian canonical forms of integer matrices, and p-adic values of a multidimensional continued fraction (Analytic Number Theory: Expectations for the 21st Century)

Author(s)
Tamura, Jun-ichi

Citation
数理解析研究所講究録 1219: 77-90

Issue Date
2001-07

URL
http://hdl.handle.net/2433/41261

Type
Departmental Bulletin Paper

Textversion
publisher

Kyoto University
Hermitian canonical forms of integer matrices, and p-adic values of a multidimensional continued fraction

Jun-ichi TAMURA (野村淳一)

3-3-7-307 AZAMINO AOBA-KU YOKOHAMA 225-0011 JAPAN

ABSTRACT: All the components of the first row of the hermitian canonical form of the n-th power of the adjugate matrix of the companion matrix of a monic polynomial \( f \in \mathbb{Z}[x] \) converge to numbers \( \neq 0 \) in the p-adic sense, as \( n \) tends to infinity, for some prime numbers \( p \) under a minor condition on \( f \), cf. Theorem 1. Using this fact, for any given monic polynomial \( f \in \mathbb{Z}[x] \) of degree \( s+1 \) \((s \geq 1)\) satisfying \( |f(0)| > 1 \), and \( \text{GCD}(f(0), f'(0)) = 1 \), we can construct a periodic continued fraction of dimension \( s \) that converges, with respect to the p-adic topology for all the prime factors \( p \) of \( f(0) \), to a vector consisting of \( s \) numbers belonging to a field \( \mathbb{Q}(\ell) \), where \( \ell \in \mathbb{Z} \), is a root of \( f \), cf. Theorem 2.

§0. Introduction. Throughout the paper, \( s \) denotes a fixed positive integer, \(|*|_s \) the p-adic absolute value for prime \( p < \infty \), \(|*|_\infty \) the ordinal absolute value \(|*|_\infty \). For a given monic polynomial

\[ f = x^{s+1} - c_s x^s - \cdots - c_1 x - c_0 \in \mathbb{Z}[x], \]

we mean by \( C \) the matrix

\[
C = C(f) := \begin{bmatrix}
\tau & 0 & c_0 \\
E_s & 0 & c_1 & \cdots & c_s \\
0 & \cdots & 0 & \cdots & 0
\end{bmatrix}, \quad c = (c_1, \ldots, c_s),
\]

where \( E_s \) is the \( s \times s \) unit matrix, \("\tau" \) indicates the transpose of a matrix. The matrix \( C \), the so called companion matrix of \( f \), which is one of the matrices having \( f \) as its characteristic polynomial. Let us suppose

\[ d := |c_0| > 1, \quad \text{GCD}(c_0, c_1) = 1. \quad (1) \]

Then, Hensel's lemma, \([1]\) tells us that there exists a unique p-adic integer \( \lambda, \in \mathbb{Z} \), satisfying

\[ f(\lambda) = 0, \quad |\lambda|_p < 1, \quad p \in \text{Prime}(d), \]

where \( \text{Prime}(d) \) denotes the set of the prime factors of \( d \), see any standard text for p-adic numbers. In what follows, we assume (1) unless otherwise mentioned.
In Section 1, we give a theorem which disclose a link between the numbers \( \lambda \), \( p \in \text{Prime}(d) \) and the hermitian canonical forms of the powers of the adjugate matrix

\[
\tilde{C} = (\det C)C^{-1}
\]

of the companion matrix \( C \) of \( f \), cf. Theorem 1. We give some lemmas for the proof of Theorem 1 in Section 2. In Sections 3, 4, we construct a continued fraction of dimension \( s \) that converges in \( Q \), with respect to the \( p \)-adic metric, for any \( p \in \text{Prime}(d) \), to a vector consisting of \( s \) components belonging to the field \( Q(\lambda,)[x] \subset Q \), cf. Theorem 2. We give some \( p \)-adic results related to a homogeneous form coming Theorem 1 in connection with a certain partition of the lattice \( Z \) in Section 5.

In this report, we are not intending to give proofs of our theorems, and lemmas. But we refer to some lemmas, since they seem to have their own interest. Some of the results can be extended to matrices with entries in \( Z \), by taking \( f \in Z, [x] \subset Z[x] \), but we do not extend them, since we are mainly interested in matrices with integer entries.

§1. Hermitian canonical forms We denote by \( M(s;Q) \) (resp. \( M(s;Z) \)) the set of \( s \times s \) matrices with rational entries (resp. integer entries), and by \( M_0(s;Q) \) (resp. \( M_0(s;Z) \)) the set of matrices \( X \in M(s;Q) \) (resp. \( X \in M(s;Z) \)) such that \( \det X \neq 0 \). \( GL(s;Z) \) is the set of matrices \( X \in M(s;Z) \) with \(|\det X|=1\), which are the units of \( M(s;Z) \). For two matrices \( A, B \in M(s+1;Q) \), we write

\[ A \sim B \]

iff there exists a matrix \( P \in GL(s+1;Z) \) such that \( A=PB \). The relation \( \sim \) is an equivalence relation on \( M(s+1;Q) \), in particular, so is on \( M_0(s+1;Z) \). For a given matrix \( X \in M_0(s+1;Z) \), there exists a unique upper triangular matrix \( H(X) \) satisfying

\[
X \sim H(X) = (h_{ij})_{0 \leq i, j \leq s} \in M_0(s+1;Z),
\]

\[
h_{ij} = 0, 0 \leq h_{ii} < h_{ii} (0 \leq j < i \leq s), h_{ii} = 0 (0 \leq j < i < s).
\]

\( H(X) \) is the so called hermitian canonical form of \( X \), which can be obtained by elementary transformations, i.e., it can be found by multiplying \( X \) by elementary matrices \( E \in GL(s+1;Z) \) from the left.

We denote by \( H_*(X) \) the hermitian canonical form of \( \tilde{X}^* \).
\[ H_n(X) := H(\tilde{X}^n) = H((\det X^{-1})^n), \quad X \in M_0(s+1; \mathbb{Z}). \]

**Theorem 1.** Let \( f := x^{s+1} - c_1 x^s - \cdots - c_n x - c_0 \in \mathbb{Z}[x] \) be a polynomial satisfying (1), and let \( C = C(f) \) be its companion matrix. Let \( e(p) \) be numbers determined by
\[
d := |c_0| = \prod_{p \in \text{Prime}(d)} p^{e(p)}, \quad e(p) \geq 1 \quad (p \in \text{Prime}(d)),
\]
and \( \lambda_p \in \mathbb{Z} \), the number satisfying
\[ f(\lambda_p) = 0, \quad |\lambda_p| < 1 \quad (p \in \text{Prime}(d)). \]

Then the following statements \((i, ii)\) hold.

1. The hermitian canonical forms \( H_n(C) \) are of the shape
\[
H_n(C) = \begin{bmatrix}
1 & T h_n \\
0 & d^* E
\end{bmatrix} \in M_0(s; \mathbb{Z}), \quad h_n = \tau(h_n^{(1)}, \ldots, h_n^{(s)}), \quad 0 < h_n^{(1)} < d^*
\]
for all \( n \geq 1 \). \( 1 \leq j \leq s > 1 \).

2. \( |\lambda_p| - x_n^{(j)} \leq p^{-e(p)} \) holds for all \( n \geq 1 \), \( 1 \leq j \leq s \), \( p \in \text{Prime}(d) \).

We denote by \( a_0, a_1, a_2, \ldots (p) \) the \( p \)-adic expansion of a number in \( \mathbb{Z} \), with canonical representatives:
\[
a_0, a_1, a_2, \ldots (p) := \sum_{s \geq 0} a_s p^s, \quad a_s \in \{0, 1, \ldots, p-1\}.
\]

**Remark 1.** When \(|f(0)| = dp^s \) \((p: \text{prime, } e \geq 1)\), then \( h_n^{(1)} \) coincides with an integer coming from the truncation of the \( p \)-adic expansion of \( \lambda_p \), i.e., \( \lambda_p = a_0, a_1, a_2, \ldots (p) \) implies \( h_n^{(1)} = a_0, a_1, a_2, \ldots a_{s-1} (p) \), and vice versa. Note that \( a_0 = 0 \) since \(|\lambda_p| < 1 \). In particular, if \( \lambda_p \not\in \mathbb{Q} \), then \( a_s \neq 0 \) for infinitely many \( n \geq 1 \), so that in the statement \((i)\), the equality holds infinitely often. In this sense, the approximation \((i)\) is best possible.

**Remark 2.** Since \( f \in \mathbb{Z}[x] \) is monic, \( \lambda_p \not\in \mathbb{Z} \) implies \( \lambda_p \not\in \mathbb{Q} \), so that the \( p \)-adic expansion of \( \lambda_p \) is periodic, and in particular, the expansion diverges with respect to the archimedean norm \(|*|_\infty \). Hence, the sequence \( \{h_n^{(1)}\}_{n=1}^{\infty} \) is unbounded for all \( 1 \leq j \leq s \) (with respect to the usual topology) if there exists a prime \( p \in \text{Prime}(d) \) such that \( \lambda_p \not\in \mathbb{Z} \). (Note that the converse is not valid.) In particular, if \( f \) has no linear factors in \( \mathbb{Z}[x] \), then \( \{h_n^{(1)}\}_{n=1}^{\infty} \) is unbounded; if \( f \) is irreducible over \( \mathbb{Q}[x] \), then
Remark 3. In general, the minimal polynomial \( f \), in \( \mathbb{Z}[x] \) of \( \lambda \), depends on \( p \). If \( f \in \mathbb{Z}[x] \) is irreducible over \( \mathbb{Q}[x] \), and \( \text{Prime}(d)>1 \) then the assertion (i) with \( j=1 \) gives simultaneous diophantine approximations by a rational integer \( x^*(1) \) for roots \( \lambda \), \( \in \text{Prime}(d) \) having an identical minimal polynomial.

Remark 4. (cf. the Chinese remainder theorem) Let \( f(0) \) be an integer having \( s+1 \) distinct prime factors, and let
\[
f = \prod_{p \in \text{Prime}(f(0))} (x-p^*(p)).
\]
Then \( \gcd(f(0), f'(0))=1 \), i.e., (1) is valid. In this case, \( \lambda^* = p^*(p) \) holds, and Theorem 1 implies
\[
x^*(1) \equiv p^*(p) \pmod{p^*(p)^s} \quad \text{for all } n \geq 1, 1 \leq j \leq s, p \in \text{Prime}(f(0)).
\]

Remark 5. In general, the assertion (i) does not hold even for the case where \( f \) is irreducible over \( \mathbb{Q}[x] \) if the condition (1) does not hold. For instance, take an irreducible polynomial \( f = x^5 - 13x^4 - 7x^3 + 5x^2 - 3x - 3 \) with its companion matrix \( C \). Then the \((2,4)\)-entry of \( H_4(C) = 54 \neq 0 \), and the \((1,2)\)-entry of \( H_4(C) \) is identically zero for \( 1 \leq n \leq 16 \). Consequently, the assertions (i) is not valid.

§2. Lemmas for Theorem 1. We can prove the following assertion (i)*:

Lemma 1. For \( C = C(f) \) satisfying (1),
\[
(i)^* \quad H_s(C) = \begin{bmatrix} 1 & T_{h^*} \\ 0 & d^*E_s \end{bmatrix} \in \mathbb{M}(s+1; \mathbb{Z}), h^* = \left(h^*(1), \ldots, h^*(s)\right)
\]
with \( 0 < h^*(i) < d^* \), \( h^*(i) \in \mathbb{Z} \) \( (1 \leq j \leq s) \) holds for all \( n \geq 1 \).

It is clear that Lemma 1 implies Theorem 1, (i). Notice that (i) and (i) in Theorem 1 imply (i)*. We need the following Lemmas 2-4 for the proof of Theorem (i). We denote by \( e_j \) \( (1 \leq j \leq s) \) the \( j \)-th fundamental vector \( (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}^s \).

Lemma 2. For \( 1 \leq j \leq s \)
\[d^{-n}H_n(C) = \begin{bmatrix} h_{n+1}^{(1)} \\ -e_j \end{bmatrix} = \begin{bmatrix} (h_{n+1}^{(1)} - h_{n}^{(1)})/d^n \\ -e_j \end{bmatrix} \in \mathbb{Z}^{*+}.\]

**Lemma 3.**

\[
\begin{bmatrix} 1 & \tau h_n \\ 0 & d^nE_* \end{bmatrix} \begin{bmatrix} -c_{0E_*} \\ h_{n+1}^{(1)} \end{bmatrix} = \begin{bmatrix} -c_d \\ \vdots \\ -c_d \\ c_0d^nE_{s-1} \end{bmatrix} \begin{bmatrix} h_{n+1}^{(1)} \\ -e_j \end{bmatrix}
\]

for all \(n \geq 1, 1 \leq i \leq s\), where \(d_*\) is the integer (2).

**Lemma 4.** \(|\lambda - h| = |f(h)|\) for any \(h \in \mathbb{P} \mathbb{Z}_s, p \in \text{Prime}(f(0)).\)

## §3. A continued fraction of dimension \(s\)

Let \(K\) be any field. By \(K(x)\), we denote the field of rational functions of \(s\) variables \(x := (x_1, \ldots, x_s)\) over \(K\), and by \(T(x)\) the \(s\)-tuple of rational functions defined by

\[T(x) := (1/x_s, x_1/x_s, \ldots, x_{s-1}/x_s) \in K(x)^s.\]

We write

\[
\frac{x_0^{-1}}{x} := x_0^{-1}T(x) \in K(x) = K(x), \quad \vec{x} := (x_0, \ldots, x_s).
\]

Then, we can consider an \(s\)-tuple of rational functions

\[
\Xi = \Xi(x_0, \ldots, x_s) := T(\xi_1(x_0, \ldots, x_s), \ldots, \xi_s(x_0, \ldots, x_s))
\]

where

\[
\begin{align*}
& (x_0^{(0)})^{-1}x_0 + \frac{(x_1^{(0)})^{-1}}{(x_2^{(0)})^{-1}x_2 + \ldots + (x_{s-1}^{(0)})^{-1}} + (x_n^{(0)})^{-1}x_n \\
& (x_1^{(0)})^{-1}x_1 + \frac{(x_2^{(0)})^{-1}}{(x_3^{(0)})^{-1}x_3 + \ldots + (x_{s-1}^{(0)})^{-1}} + (x_n^{(0)})^{-1}x_n \\
& \vdots \\
& (x_{s-1}^{(0)})^{-1}x_{s-1} + \frac{(x_s^{(0)})^{-1}}{x_n} \\
\end{align*}
\]
\[ \epsilon K(x_0, \ldots, x_n)^*, \ x_m = ^T(x_m^{(1)}, \ldots, x_m^{(s)}), \ x_m = ^T(x_m^{(0)}, \ldots, x_m^{(s)}) \] (0 \leq m \leq n).$

If the denominators of \( t_i \) do not vanish at \( x_0 = c_0, \ldots, x_n = c_n \in K^{**1} \), then we can consider the value \( \Xi(c_0, \ldots, c_n) \in K^* \). In such a case, we say that the continued fraction \( \Xi(c_0, \ldots, c_n) \) is well-defined. Setting \( K = \mathbb{Q} \), we may consider an infinite continued fraction \( \Xi(c_0, \ldots, c_n, \ldots) \), which is defined to be the limit of \( n \)-th convergent \( \Xi(c_0, \ldots, c_n) \) with respect to the \( p \)-adic topology provided that \( \Xi(c_0, \ldots, c_n) \) is well-defined for all \( n \), and the limit exists. In particular, if \( c_m^{(0)} = 1 \) for all \( m \), then the continued fraction \( \Xi(c_0, \ldots, c_n, \ldots) \) turns out to be of the form coming from the Jacobi-Perron algorithm (possibly non-admissible), which is denoted by

\[
\left[ c_0 ; c_1, c_2, c_3, \ldots \right] = \begin{bmatrix}
  c_0^{(1)}; c_1^{(1)}, c_2^{(1)}, c_3^{(1)}, \ldots \\
  c_0^{(2)}; c_1^{(2)}, c_2^{(2)}, c_3^{(2)}, \ldots \\
  \vdots & \vdots & \vdots & \vdots \\
  c_0^{(s)}; c_1^{(s)}, c_2^{(s)}, c_3^{(s)}, \ldots \\
\end{bmatrix}
\]

\( c_n = ^T(c_n^{(1)}), c_n^{(2)}, \ldots, c_n^{(s)}) \), \( n \geq 0 \).

If we take \( s = 1 \), then

\[
\Xi(c_0, \ldots, c_n, \ldots) = (c_0^{(0)})^{-1} c_0^{(1)} + \frac{(c_0^{(0)})^{-1}}{(c_1^{(0)})^{-1} c_1^{(1)} + \frac{(c_1^{(0)})^{-1}}{(c_2^{(0)})^{-1} c_2^{(1)} + \frac{(c_2^{(0)})^{-1}}{(c_3^{(0)})^{-1} c_3^{(1)} + \ldots}}}
\]

so that

\[
c_0^{(0)} \Xi(c_0, \ldots, c_n, \ldots) = c_0^{(1)} + \frac{c_1^{(0)}}{c_1^{(1)} + \frac{c_2^{(0)}}{c_2^{(1)} + \frac{c_3^{(0)}}{c_3^{(1)} + \ldots}}}
\]

**Theorem 2.** Let \( f := x^{**1} - c_1 x^{* - \cdots - c_1 x - c_0} \in \mathbb{Z}[x], \ l, \in \mathbb{Z}_+, \ e(p) \) (\( p \) \( \epsilon \) \text{Prime}(d)) b
as in Theorem 1. Let $\Theta = \tau(\theta^{(1)}, \ldots, \theta^{(s)}) \in Q^*(\subset Q_+)$ be the $n$-th convergent of the following periodic continued fraction:

$\begin{align*}
\Theta &= a_0 - \frac{1}{a_1 - \frac{1}{a_2 - \frac{1}{\ddots - \frac{1}{a_s}}}} \\
&= a_0 - \frac{1}{\ddots - \frac{1}{a_s}}
\end{align*}$

where

$\begin{align*}
c_0^* &= \tau(0, \ldots, 0, a_0, a_1, \ldots, a_s) \in \mathbb{Z}^s, \\
c^*_j &= c_j.
\end{align*}$

Let $r_n = (r_n^{(0)}, \ldots, r_n^{(s)}) \in \mathbb{Z}^s$ be the final column vector of a matrix $J_0 J_1 \cdots J_n$

where

$J_n := \begin{bmatrix} 0 & c_0^* \\ E & -c_m^* \end{bmatrix}$ (0 ≤ m ≤ s), $J_m := J_s$ (m > s),

$C_0^* := \tau(0, \ldots, 0) \in \mathbb{Z}^s$.

Then

(i) $\theta_n^{(j)} = r_n^{(j)} / r_n^{(0)}, n \geq 0, 1 \leq j \leq s$, and

(ii) $|\theta_n^{(j)} - C_0^{-j} a_j |_p \leq \tau^{p^{n+\tau(s)}} a_j$, $n \geq 0, 1 \leq j \leq s$, and $p \in \text{Prime}(d)$.

are valid. In particular, the $p$-adic value of the continued fraction $\Theta_n$ converges to

$\Theta = \tau(C_0^{-1} a_0, C_0^{-2} a_1, \ldots, C_0^{-s} a_s) \in \mathbb{Z}_p$.

**Corollary 1.** A periodic continued fraction

$[0; a_1, a_2, \ldots, a_s, a_1, a_2, \ldots, a_s]$ has the same convergents as that in Theorem 2, so that it converges to $\Theta$, where $a_1, a_2, \ldots, a_s$ is a period, $0 \in \mathbb{Z}^+$, and
Remark 6. Lemma 9. (i) given below implies that \( q_* (n) \neq 0 \) for all \( n \geq 0 \). so that any convergent \( \Theta_* (n \geq 0) \) of the continued fraction given in Theorem 2 is well-defined.

Remark 7. In general, the continued fractions in Theorem 2, and Corollary 1 do not converge in \( \mathbb{R} \) with respect to the metric coming from \( |*| = |*|_{\infty} \). These continued fractions always diverge when \( f \in \mathbb{Z}[x] \) is of totally imaginary.

§4. Lemmas for Theorem 2, and Corollary 1. We can prove Lemmas 5-11 for the proof of Theorem 2, and its Corollary.

Let \( A \in (a_{ij})_{0 \leq i \leq s, 0 \leq j \leq s+1; K} \). Then \( A \) defines a linear map on \( K^{**1} \), which will be also denoted by \( A \). For elements \( \underline{y}, \underline{w} \in K^{**1 \setminus \{ \underline{0} \}} \), iff there exists \( c \in K \) such that \( c \underline{y} = \underline{w} \), we write \( \underline{y} \sim \underline{w} \), which defines an equivalence relation on \( K^{**1 \setminus \{ \underline{0} \}} \). We denote by \( \pi \) the map

\[ \pi : K^{**1} \rightarrow P^*(K) := (K^{**1 \setminus \{ \underline{0} \}})/\sim, \]

\[ \pi(\underline{y}) := \{ \underline{w} \in K^{**1 \setminus \{ \underline{0} \}} : \underline{w} \sim \underline{y} \} \ (\underline{y} \neq \underline{0}), \]

where the broken arrow \( \rightarrow \) indicates a "map" with some exceptional elements for which the map is not defined. Since \( \pi(\underline{y}) = \pi(\underline{w}) \) implies \( \pi \underline{y} = \pi \underline{w} \), so that the linear map \( A \) induces a map \( A_* : P^*(K) \rightarrow P^*(K) \). We define a projection \( \pi \), and an injection \( \iota \) by
$\mathfrak{I} : P^*(K) \rightarrow K^*$,
$\mathfrak{I}(v) := (v_1/v_0, v_2/v_0, \ldots, v_*/v_0)$. $v^T = (v_0, v_1, \ldots, v_*).$ 

$\mathfrak{K} : K^* \rightarrow P^*(K)$,
$\mathfrak{K}(v) := \mathfrak{I}(1, v_1, v_2, \ldots, v_*)$. $v^T = (v_1, v_2, \ldots, v_*) \in K^*.$

We set $A_* = \mathfrak{I} \circ A_* \circ \mathfrak{K}.$ Then, Lemma 5 given below can be easily seen.

**Lemma 5.** The following diagram is commutative:

\[
\begin{array}{ccc}
K^{**} & \longrightarrow & P^*(K) \\
\downarrow A & & \downarrow \mathfrak{I} \\
K^{*+1} & \longrightarrow & K^*
\end{array}
\]

Using Lemma 5, we get the following

**Lemma 6.** Let $X_m$ be a matrix with $s+1$ variables $x_m^T(x_m^{(0)}, \ldots, x_m^{(*)})$:

\[
X_m := \\
\begin{bmatrix}
T & x_m^{(0)} \\
0 & x_m \\
E_0 & x_m
\end{bmatrix}, \quad x_m^T := (x_m^{(1)}, \ldots, x_m^{(*)}), \quad 0 \leq m \leq n.
\]

and let $p_j^{(*)}$ be polynomials

\[
p_j^{(*)} = p_j^{(*)}(x_0, \ldots, x_*) \in \mathbb{Z}[x_0, \ldots, x_*] \quad (-s \leq j \leq n, 0 \leq j \leq s)
\]

defined by $s+1$ recurrences

\[
p_m^{(*)} = x_m^{(*)}p_m^{(*)} + \sum_{j=0}^{s} x_m^{(j)}p_m^{(*)} - p_m^{(*)}p_{m-1}^{(*)}
\]

with an initial condition

\[
P_{-1} = E_{s+1},
\]

where

\[
P_m := (p_m^{(*)})_{0 \leq i \leq s, 0 \leq j \leq s}.
\]

Then the following formulae are valid for all $0 \leq m \leq n$.

(i) $P_m = x_0 x_1 \cdots x_m \in M(s+1; \mathbb{Z}[x_0, \ldots, x_m]).$

(ii) $\exists (x_0, \ldots, x_*) = (p_m^{(*)})^{-1} \tau (p_m^{(*)} \cdots p_0^{(*)}) \in Q(x_0, \ldots, x_*).$

**Remark 8.** In general, the formula (i) holds for $x_0, \ldots, x_* \in K^{*+1}$ for any field $K$ even for the case of $\text{char}(K) \neq 0$ provided that $p_m^{(*)}(x_0, \ldots, x_*)$ differs from $0$ as an element of $K$. 

In what follows, we mean by $H_n = H_n(C)$ and $J_n$ be matrices as in Theorem 1. Recall that we are assuming (1).

We put

$$K_n := \begin{bmatrix} d^* & -^T h_n \\ 0 & E_n \end{bmatrix}, \quad J_n := J_n = \begin{bmatrix} 0 & c^n \\ E_n & -c^* \end{bmatrix}$$

$c^* = (c_0^{n-1}, c_0^{n-2} c_{n-1}, \ldots, c_0 C_{n-1}, C_n)$,

where $h_n \in Z_n$ is a vector in Theorem 1, (i). We define integers $q_n^{(1,1)}$ by

$$Q_n := (q_n^{(1,1)})_{0 \leq j \leq s} (n \geq 0).$$

where

$$Q := \begin{bmatrix} -c & c_0 E_n \\ 1 & 0 \end{bmatrix}.$$  

Note that

$$Q = c_0 C^{-1} = (-1)^* \tilde{C}, \quad C = C(f).$$

We mean by $X \equiv Y \pmod{m}$ that all the entries of $X - Y$ are divisible by $m \in Z$.

**Lemma 7.** $q_n^{(0,1)} h_n^{(1)} \equiv q_n^{(1,1)} \pmod{d^*}$ for all $0 \leq j \leq s$, $1 \leq j \leq s$, $n \geq 0$.

We set

$$Q_n := (q_{n-s+1}^{(1,0)})_{0 \leq j \leq s} (n \geq s).$$

**Lemma 8.** $Q_n = Q_n J_n^{-} n \geq s$ for all $n \geq s$.

**Lemma 9.** (i) $q_n^{(0)} \equiv (-c_1)^* \pmod{d}$,

(ii) $|h_n^{(1)} - q_n^{(1,0)}| / q_n^{(0,0)} \leq \delta^{-(\sigma^*) n}$ for all $n \geq 0$, $1 \leq j \leq s$, and $p \in \text{Prime}(d)$.

Let $J_n$ be as in Theorem 2. We denote by $O_{t \times u}$ the zero matrix of size $t \times u$, by $Q_n$ the matrix $Q_n$, and by $D(a_0, a_2, \ldots, a_s)$ the diagonal matrix with $a_0, a_2, \ldots, a_s$ as its diagonal components. For $n \geq 0$, we put
\[ Q_\star := GJ_1 \cdots J_\star, \quad (21) \]
\[ G_{n+1} := D(c_0^{-n}, c_{n+1}^{-1}, \ldots, c_{n+1}^{-1}, 1), \]
\[ G := G_{n+1}. \]

\[ \Lambda_{n+1} := \begin{bmatrix} q_0^{(0)} & q_1^{(0)} & \cdots & q_n^{(0)} \\ q_1^{(1)} & q_0^{(0)} & \cdots & q_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ q_n^{(n)} & \cdots & \cdots & q_n^{(n)} \end{bmatrix}, \]

where
\[ q_n^{(1)} := q_n^{(1,0)} \quad (0 \leq i \leq s, n \geq 0) \]

with \( q_n^{(j,0)} \) defined by (15). We put
\[ g := (q_n^{(0)}, \ldots, q_n^{(s)}) \in \mathbb{Z}^{s+1} (n \geq 0). \]

**Lemma 10.**
(i) \[ g_0 = (1, 0, \ldots, 0), \]
\[ g_n = (-c_1q_{n-1}^{(0)} - c_2q_{n-1}^{(1)} - \ldots - c_nq_{n-1}^{(n-1)}, c_0q_{n-1}^{(0)}, c_0q_{n-1}^{(1)}, \ldots, c_0q_{n-1}^{(n-1)}, T_{n,s}) \quad (1 \leq n \leq s). \]
(ii) \[ Q_\star := \begin{bmatrix} 0_{n+1 \times n} & \Lambda_{n+1} \\ D_{s-n} & O_{s-n \times n+1} \end{bmatrix} (0 \leq n < s), \quad Q_\star = Q_{n}. \]

Using Lemmas 1-10, we can show Theorem 1. We denote by \([r] \in \mathbb{R}, [\omega] := \omega\) the largest integer not exceeding \( r \). We put
\[ t(n) := [n/(s+1)], \quad r(n) := n-(s+1)t(n) (n \in \mathbb{Z}). \]

It is clear that \( n=(s+1)t(n)+r(n) \), \( 0 \leq r(n) \leq s \) holds. We can show the following

**Lemma 11.** Let \( X_n \in M(s+1; Z \{x_n\}), x_n = (x_n^{(0)}, x_n^{(1)}, \ldots, x_n^{(s)}), 0 \leq m < n \) be as in Lemma 6. Let
\[ x_m := x_n X_{n-m-1} \cdots X_{r(m)} (0 \leq m < n), \quad x_m := 1 \quad (m < 0); \]
\[ x_n^\star := (x_n^{(0)}, \ldots, x_n^{(s)}) \quad (m < 0); \]
\[ x_n^\star := (x_n^{(0)}, x_n^{(1)}, \ldots, x_n^{(s)}) \quad (0 \leq m < n); \]
\[ x_n^\star := (x_n^{(0)}, x_n^{(1)}, \ldots, x_n^{(s)}) \quad (n \leq m). \]

where \( x_m = x_m^{(0)} \). Then the following formula holds:
\[
(x_0(0))^{-1}x_0 + \frac{(x_0(0))^{-1}}{(x_1(0))^{-1}x_1 + \frac{(x_1(0))^{-1}}{(x_2(0))^{-1}x_2 + \cdots + \frac{(x_{m-2}(0))^{-1}}{(x_{m-1}(0))^{-1}x_{m-1} + \frac{(x_{m-1}(0))^{-1}}{(x_{m}(0))^{-1}x_m}}}
= [x_0^m; x_1^m, \ldots, x_m^m] \in \mathcal{Q}[x_0, x_1, \ldots, x_m]^m. \quad \text{0} \leq m \leq n.
\]

In view of Lemma 11, we get Corollary 1 from Theorem 1.

**5. A form \( \Upsilon(x; f) \)** We denote by \( \mathcal{Q}^{*11} \subset \mathbb{C} \) (resp. \( \mathcal{Q}_*^{*11} \subset \mathcal{Q}_* \)) the algebraic closure of \( \mathcal{Q} \) (resp. \( \mathcal{Q}_* \)). Let \( f \in \mathcal{Z}[x] \) be a monic polynomial of degree \( s+1 \), \( \mathcal{C} = \mathcal{C}(f) \in \mathcal{M}_0(s+1; \mathcal{Z}) \) the companion matrix of \( f \), \( e(p) \) \( (p \in \text{Prime}(|f(0)|)) \) the number as in Section 0. We denote by

\( \Phi(x; A) \) the characteristic polynomial of a matrix \( A \in \mathcal{M}(s+1; \mathcal{Q}_*) \).

We define a form \( \Upsilon(x; f) \) with \( s+1 \) indeterminates by

\[
\Upsilon(x; f) = \Upsilon(x_0, x_1, \ldots, x_s; f) := \det(\sum_{0 \leq j \leq s} x_j \mathcal{C}(f)^j).
\]

We remark that

\[
\Upsilon(x; f) = \frac{1}{f(a)} \prod_{a \in \mathcal{Q}_*^{*11}} \left( \sum_{0 \leq j \leq s} a^j x_j \right) = \frac{1}{f(a)} \prod_{a \in \mathcal{Q}_*^{*11}} \left( \sum_{0 \leq j \leq s} a^j x_j \right)
\]

holds, where the former (resp. the latter) product is taken over all the roots \( a \) of \( f \) in the field \( \mathcal{Q}^{*11} \) (resp. \( \mathcal{Q}_*^{*11} \)) with their multiplicity. For \( f \) being irreducible over \( \mathcal{Z}[x] \), \( \Upsilon(x; f) \) becomes a norm form in the usual sense.

For a given matrix \( A \in \mathcal{M}_0(s+1; \mathcal{Z}) \), we write \( A \in \text{Bdd} \) if \( A \) satisfies the following condition (Bdd):

\( \text{(Bdd)} \) The set \( \{n \geq 0; \; \forall a \in \mathcal{Z}^{*+1} \} \) is bounded for any \( a \in \mathcal{Z}^{*+1} \backslash \{0\} \).

We can show that if \( A \in \text{Bdd} \), then \( A \in \mathcal{M}(s+1; \mathcal{Z}) \) has no units \( (\in \mathcal{Q}_*^{*11}) \) as its eigenvalues in \( \mathcal{Q}_*^{*11} \); and if

\[
A = U^{-1} \begin{bmatrix} A_1 & \star \\ \vdots & \iddots \\ 0 & A_1 \end{bmatrix} U \quad \text{or} \quad U^{-1} \begin{bmatrix} A_1 & \circ \\ \vdots & \iddots \\ \star & A_1 \end{bmatrix} U, \quad U \in \text{GL}(s+1; \mathcal{Z})
\]
such that $|\det A_i| > 1$, and $\Phi(x; A_i)$ is irreducible over $\mathbb{Z}[x]$ for all $i$. In particular, if $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}[x]$, and $|f(0)| > 1$, then $C(f) \in (\text{Bdd})$, cf. Theorem 2 in [3], see also [2].

Let us suppose $A \in (\text{Bdd})$, and consider a map $\text{ind}_A$ defined by

$$\text{ind}_A : \mathbb{Z}^{*+} \rightarrow \mathbb{N} \cup \{\infty\}$$

$$\text{ind}_A(x) := \max\{n \geq 0 : A^n x \in \mathbb{Z}^{*+}\} \ (x \neq 0), \ \text{ind}_A(0) := \infty.$$  

where $\mathbb{N} := \{0, 1, 2, \ldots\}$. We remark that there exists a unique partition

$$\bigcup_{0 \leq j < c} A^j \Gamma = \mathbb{Z}^{*+} \setminus \{0\} \ (\text{disjoint})$$

of the set $\mathbb{Z}^{*+} \setminus \{0\}$ into $c$ ($2 \leq c < \omega$) parts iff $A \in (\text{Bdd})$, and

$$\Gamma = \{x \in \mathbb{Z}^{*+} \setminus \{0\} : \text{ind}_A(x) \equiv 0 \ (\text{mod } c)\} \ (c \neq \omega),$$

$$\Gamma = \{x \in \mathbb{Z}^{*+} \setminus \{0\} : \text{ind}_A(x) = 0\} \ (c = \omega)$$

holds, cf. Theorem 1 in [3].

We mean by $v_p=\text{ord}_p$, the $p$-adic valuation, i.e., the additive version of $|\cdot|$, Then Theorem 1 implies the following:

**Corollary 2.** Let $f \in \mathbb{Z}[x]$ be a monic polynomial satisfying (1) such that $C(f) \in \text{Bdd}$. Let $\lambda_0 \in \mathbb{Z}$, $(p \in \text{Prime}(f(0)))$ be as in Theorem 1. Then

$$\text{ind}_{0(\Gamma)}(x) = \min_{p \in \text{P} \setminus \{f(0)\}} \{v_p(\sum_{0 \leq j < s} \lambda_p^j x_j)/v_p(f(0))\}$$

holds for all $x = (x_0, x_1, \ldots, x_s) \in \mathbb{Z}^{*+}$. 

Recalling

$$\tau(x; f) = \prod_{f(a) = 0} (d \in \mathbb{Q}_p^{*+}) \ (\sum_{0 \leq j < s} a^j x_j),$$

we see that Corollary 2 immediately implies the following

**Corollary 3.** Let $f$ be as in Corollary 2. Then

$$\min_{p \in \text{P} \setminus \{f(0)\}} \{v_p(\tau(x; f))/v_p(f(0))\} \leq \text{ind}_{0(\Gamma)}(x), \ x \in \mathbb{Z}^{*+}.$$ 

In particular, the equality holds if $x_j \equiv 0 \ (\text{mod } p)$ for exactly one $0 \leq j < s$. 

Corollary 3 is of somewhat trivial, but it may be of interest by two reasons: first, the assertion is stated within the set $\mathbb{Z}$; secondly, the form $\tau(x; f)$ is not so simple when $s$ is large. We give some examples, using $a, b, c, d$ (resp. $y, z, w$) instead of $c_0, c_1, c_2, c_3$ (resp. $x_0, x_1, x_2, x_3$):
\( i \) s=1, \( f=x^2-bx-a \),
\( \gamma_{(x,y,j)}(f) = x^2+bx-ay \).

\( i \) s=2, \( f=x^3-cx^2-bx-a \),
\( \gamma_{(x,y,j)}(f) = x^3+cxy-(3a+bc)xz+ay^2+acyz-abyz \).

\( i \) s=3, \( f=x^4-dx^3-cx^2-bx-a \),
\( \gamma_{(x,y,j)}(f) = x^4+dx^3y+(2c+d^2)x^2z-(3b+3cd)x^2w-cx^2y^2-(3b+cd)x^2yz \).

In general, \( \gamma_{(x_o,x_1,\ldots,x_n)}(f) \) consists of \( (2s+1)!(s+1)!s! \) terms as a polynomial in \( x_o, x_1, \ldots, x_n \).

References


[3] ________, Certain words, tilings, their nonperiodicity, and substitutions of high dimension, Analytic Number Theory, the joint Proceedings of the China-Japan Number Theory Conference (Beijing, September 1999) and the RIMS Analytic Number Theory Conference (Kyoto, November-December 1999), ed. Ch. Jia and K. Matsumoto, 41 pages, accepted to publication.