Title	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 (2001), 1219: 77-90
Issue Date	2001-07
URL	http://hdl.handle.net/2433/41261
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1219 巻 2001 年 77-90

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

Jun-ichi TAMURA (田村 純一)

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 $f\in\mathbf{Z}[x]$ 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 $f\in\mathbf{Z}[x]$ of degree s+1 ($s\geq 1$) satisfying $|f(0)|>1$, and GCD(f(0),f′(0))=1, we can construct a periodic continued fraction of dinmension 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 $\mathbf{Q}(\lambda_p)$, where $\lambda_p\in\mathbf{Z}_p$ is a root of f, cf. Theorem 2.

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

$$f:=x^{s+1}-c_s x^s-\cdots-c_1x-c_0\in\mathbf{Z}[x],$$

we mean by C the matrix

$$C=C(f):=\begin{bmatrix} {}^T\underline{0} & c_0 \\ E_s & \underline{c} \end{bmatrix},\quad \underline{c}={}^T(c_1,\ldots,c_s),$$

where E_s is the s×s unit matrix, "T" 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

$$d:=|c_0|>1,\ \mathrm{GCD}(c_0,c_1)=1. \tag{1}$$

Then, Hensel's lemma, [1] tells us that there exists a unique p-adic integer $\lambda_p\in\mathbf{Z}_p$ satisfying

$$f(\lambda_p)=0,\quad |\lambda_p|_p<1,\quad p\in\mathrm{Prime}(d),$$

where 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 mensioned.

In Section 1, we give a theorem which disclose a link between the numbers λ_p ($p\in\mathrm{Prime}(d)$) 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 $\mathbf{Q}_p$ with respect to the p-adic metric, for any $p\in\mathrm{Prime}(d)$, to a vector consisting of s components belonging to the field $\mathbf{Q}(\lambda_p)\subset\mathbf{Q}_p$, 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 $\mathbf{Z}^s$ 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 $\mathbf{Z}_p$ by taking $f\in\mathbf{Z}_p[x]\supset\mathbf{Z}[x]$, but we do not extend them, since we are mainly interested in matrices with integer entries.

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

$$A\sim B$$

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

$$X\sim H(X)=(h_{ij})_{0\leqq i,j\leqq s}\in M_0(s+1;\mathbf{Z}),$$

$$h_{00}>0,\ 0\leqq h_{ij}<h_{jj}\ (0\leqq i<j\leqq s),\ h_{ij}=0\ (0\leqq j<i\leqq s).$$

$H(X)$ 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$\in GL(s+1;\mathbf{Z})$ from the left.

We denote by $H_n(X)$ the hermitian canonical form of $\tilde{X}^n$

$$H_n(X):=H(\tilde{X}^n)=H((\det X\cdot X^{-1})^n),\ X\in M_0(s+1;\mathbf{Z}).$$

Theorem 1. Let $f:=x^{s+1}-c_s x^s-\cdots-c_1x-c_0\in\mathbf{Z}[x]$ be a polynomial satisfying (1), and let $C=C(f)$ be its companion matrix. Let $e(p)$ be numbers determined by

$$d:=|c_0|=\prod_{p\in \mathrm{Prime}(d)} p^{e(p)},\ e(p)\geqq 1\ (p\in\mathrm{Prime}(d)),$$

and $\lambda_p\in\mathbf{Z}_p$ the number satisfying

$$f(\lambda_p)=0,\ |\lambda_p|_p<1\quad (p\in\mathrm{Prime}(d))$$

Then the following statements (i, ii) hold.

(i) The hermitian canonical forms $H_n(C)$ are of the shape

$$H_n(C)=\begin{bmatrix} 1 & {}^T\underline{h}_n \\ \underline{0} & d^nE \end{bmatrix}\in M_0(s;\mathbf{Z}),\ \underline{h}_n={}^T(h_n^{(1)},\ldots,h_n^{(s)}),\ 0\leqq h_n^{(j)}<d^n$$

for all $n\geqq 1$, $1\leqq j\leqq s$.

(ii) $|\lambda_p^j-x_n^{(j)}|\leqq p^{-e(p)n}$ holds for all $n\geqq 1$, $1\leqq j\leqq s$, $p\in\mathrm{Prime}(d)$.

We denote by $a_0.a_1a_2\cdots(p)$ the p-adic expansion of a number in $\mathbf{Z}_p$ with canonical representatives:

$$a_0.a_1a_2\cdots(p):=\sum_{n\geq 0}a_np^n,\ a_n\in\{0,1,\ldots,p-1\}.$$

Remark 1. When $|f(0)|=d=p^e$ (p: prime, $e\geqq 1$), then $h_n^{(j)}$ coincides with an integer coming from the truncation of the p-adic expansion of λ_p^j, i.e., $\lambda_p^j=a_0.a_1a_2\ldots a_{en-1}\ldots(p)$ implies $h_n^{(j)}=a_0.a_1a_2\ldots a_{en-1}(p)$, and vice versa. Note that $a_0=0$ since $|\lambda_p|_p<1$. In particular, if $\lambda_p^j\notin\mathbf{Z}_{>0}$, then $a_n\neq 0$ for infinitely many $n\geqq 1$, so that in the statement (ii), the equality holds infinitely often. In this sense, the approximation (ii) is best possible.

Remark 2. Since $f\in\mathbf{Z}[x]$ is monic, $\lambda_p\notin\mathbf{Z}$ implies $\lambda_p\notin\mathbf{Q}$, so that the p-adic expansion of $\lambda_p^j\notin\mathbf{Z}$ can not be periodic, and in particular, the expansion diverges with respect to the archimedian norm $|*|_\infty$. Hence, the sequence $\{h_n^{(j)}\}_{n=1,2,\ldots}$ is unbounded for all $1\leqq j\leqq s$ (with respect to the usual topology) if there exists a prime $p\in\mathrm{Prime}(d)$ such that $\lambda_p\notin\mathbf{Z}$. (Note that the converse is not valid.) In particular, if f has no linear factors in $\mathbf{Z}[x]$, then $\{h_n^{(1)}\}_{n=1,2,\ldots}$ is unbounded; if f is irreducible over $\mathbf{Q}[x]$, then

$\{h_n^{(j)}\}_{n=1,2,...}$ is unbounded for all $1 \leqq j \leqq s$.

Remark 3. In general, the minimal polynomial f_p in $\mathbf{Z}[x]$ of λ_p depends on p. If $f \in \mathbf{Z}[x]$ is irreducible over $\mathbf{Q}[x]$, and $\sharp\mathrm{Prime}(d)>1$ then the assertion (ii) with $j=1$ gives simultaneous diophantine approximations by a rational integer $x_n^{(1)}$ for roots λ_p ($p \in \mathrm{Prime}(d)$) 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

$$f = \prod_{p \in \mathrm{Prime}(f(0))} (x-p^{e(p)}).$$

Then $\mathrm{GCD}(f(0),f'(0))=1$, i.e., (1) is valid. In this case, $\lambda_p=p^{e(p)}$ holds, and Theorem 1 implies

$$x_n^{(j)} \equiv p^{e(p)j} \pmod{p^{e(p)n}} \text{ for all } n \geqq 1,\ 1 \leqq j \leqq s,\ p \in \mathrm{Prime}(f(0)).$$

Remark 5. In general, the assertion (i) does not holds even for the case where f is irreducible over $\mathbf{Q}[x]$ 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 $H_n(C)$ is identically zero for $1 \leqq n \leqq 16$. 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),

$$\text{(i)* } \quad H_n(C) = \begin{bmatrix} 1 & {}^T\underline{h}_n \\ \underline{0} & d^n E_s \end{bmatrix} \in M(s+1;\mathbf{Z}),\ \underline{h}_n={}^T(h_n^{(1)},\dots,h_n^{(s)})$$

with $0 \leqq h_n^{(j)} < d^n$, $h_n^{(j)} \in d^j\mathbf{Z}$ $(1 \leqq j \leqq s)$ holds for all $n \geqq 1$.

It is clear that Lemma 1 implies Theorem 1, (i). Notice that (i) and (ii) in Theorem 1 imply (i)*. We need the following Lemmas 2-4 for the proof of Theore (ii). We denote by $\underline{e}_j$ $(1 \leqq j \leqq s)$ the j-th fundamental vector $(0,\dots,0,1,0,\dots,0) \in \mathbf{Z}^s$.

Lemma 2. For $1 \leqq j \leqq s$

$$d^{-n}H_n(C)\begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix} = \begin{bmatrix} (h_{n+1}^{(j)}-h_n^{(j)})/d^n \\ -\underline{e}_j \end{bmatrix} \in \mathbf{Z}^{s+1}.$$

<u>Lemma 3</u>.

$$\mathbf{Z}^{s+1} \ni d^{-n}\begin{bmatrix} 1 & {}^T\underline{h}_n \\ \underline{0} & d^nE_s \end{bmatrix}\begin{bmatrix} -\underline{c} & c_0E_s \\ 1 & {}^T\underline{0} \end{bmatrix}\begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix}$$

$$= d^{-n}\left[\begin{array}{c|c|cccc} -d_n & c_0 & c_0h_n^{(1)} & c_0h_n^{(2)} & \cdots & c_0h_n^{(s-1)} \\ \cline{2-6} -c_2d^n & & & & & \\ \vdots & \underline{0} & \multicolumn{4}{c}{c_0d^nE_{s-1}} \\ -c_sd^n & & & & & \\ \cline{3-6} d^n & & \multicolumn{4}{c}{{}^T\underline{0}} \end{array}\right]\begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix}$$

for all $n \geqq 1$, $1 \leqq j \leqq s$, where d_n is the integer (2).

<u>Lemma 4</u>. $|\lambda_p - h|_p = |f(h)|_p$ for any $h \in p\mathbf{Z}_p$, $p \in \mathrm{Prime}(f(0))$.

<u>§3. A continued fraction of dimension s</u>. Let K be any field. By $K(\underline{x})$, we denotes the field of rational functions of s variables $\underline{x} := {}^T(x_1,\dots,x_s)$ over K, and by $T(\underline{x})$ the s-tuple of rational functions defined by

$$T(\underline{x}) := {}^T(1/x_s, x_1/x_s, \dots, x_{s-1}/x_s) \in K(\underline{x})^s.$$

We write

$$\frac{x_0^{-1}}{\underline{x}} := x_0^{-1}T(\underline{x}) \in K(x_0,\underline{x})^s = K(\underline{\underline{x}}),\ \underline{\underline{x}} = {}^T(x_0,\dots,x_s).$$

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

$$\Xi = \Xi(\underline{\underline{x}}_0,\dots,\underline{\underline{x}}_n) = {}^T(\xi_1(\underline{\underline{x}}_0,\dots,\underline{\underline{x}}_n),\dots,\xi_s(\underline{\underline{x}}_0,\dots,\underline{\underline{x}}_n))$$

$$:= (x_0^{(0)})^{-1}\underline{x}_0 + \cfrac{(x_0^{(0)})^{-1}}{(x_1^{(0)})^{-1}\underline{x}_1 + \cfrac{(x_1^{(0)})^{-1}}{(x_2^{(0)})^{-1}\underline{x}_2 + \cdot \cdot \cdot + \cfrac{(x_{n-1}^{(0)})^{-1}}{(x_n^{(0)})^{-1}\underline{x}_n}}}$$

$\in K(\underline{\underline{x}}_0,\ldots,\underline{\underline{x}}_n)^s$, $\underline{x}_m={}^T(x_m^{(1)},\ldots,x_m^{(s)})$, $\underline{\underline{x}}_m={}^T(x_m^{(0)},\ldots,x_m^{(s)})$ $(0\leqq m\leqq n)$.

If the denominators of ξ_j do not vanish at $\underline{\underline{x}}_0=\underline{\underline{c}}_0$, ..., $\underline{\underline{x}}_n=\underline{\underline{c}}_n\in K^{s+1}$, then we can consider the value $\Xi(\underline{\underline{c}}_0,\ldots,\underline{\underline{c}}_n)\in K^s$. In such a case, we say that the continued fraction $\Xi(\underline{\underline{c}}_0,\ldots,\underline{\underline{c}}_n)$ is well-defined. Setting $K=\mathbf{Q}_p$, we may consider an infinite continued fraction $\Xi(\underline{\underline{c}}_0,\ldots,\underline{\underline{c}}_n,\ldots)$, which is defined to be the limit of n-th convergent $\Xi(\underline{\underline{c}}_0,\ldots,\underline{\underline{c}}_n)$ with respect the p-adic topology provided that $\Xi(\underline{\underline{c}}_0,\ldots,\underline{\underline{c}}_n)$ is well-defined for all n, and the limit exists. In particular, if $c_m^{(0)}=1$ for all m, then the continued fraction $\Xi(\underline{\underline{c}}_0,\ldots,\underline{\underline{c}}_n,\ldots)$ turns out to be of the form coming from the Jacobi-Perron algorithm (possibly non-admissible), which is denoted by

$$[\ \underline{c}_0;\ \underline{c}_1,\ \underline{c}_2,\ \underline{c}_3,\ \ldots] =$$

$$\left[\begin{array}{l} c_0^{(1)};\ c_1^{(1)},\ c_2^{(1)},\ c_3^{(1)},\ \ldots \\ c_0^{(2)};\ c_1^{(2)},\ c_2^{(2)},\ c_3^{(2)},\ \ldots \\ \ \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ c_0^{(s)};\ c_1^{(s)},\ c_2^{(s)},\ c_3^{(s)},\ \ldots \end{array}\right],$$

$$\underline{c}_n={}^T(c_n^{(1)},\ c_n^{(2)},\ \ldots,\ c_n^{(s)}),\ n\geqq 0.$$

If we take s=1, then

$$\Xi(\underline{\underline{c}}_0,\ldots,\underline{\underline{c}}_n,\ldots)$$
$$=(c_0^{(0)})^{-1}c_0^{(1)}+\cfrac{(c_0^{(0)})^{-1}}{(c_1^{(0)})^{-1}c_1^{(1)}+\cfrac{(c_1^{(0)})^{-1}}{(c_2^{(0)})^{-1}c_2^{(1)}+\cfrac{(c_2^{(0)})^{-1}}{(c_3^{(0)})^{-1}c_3^{(1)}+\cdot\,\cdot\,\cdot}}},$$

so that

$$c_0^{(0)}\,\Xi(\underline{\underline{c}}_0,\ldots,\underline{\underline{c}}_n,\ldots)=c_0^{(1)}+\cfrac{c_1^{(0)}}{c_1^{(1)}+\cfrac{c_2^{(0)}}{c_2^{(1)}+\cfrac{c_3^{(0)}}{c_3^{(1)}+\cdot\,\cdot\,\cdot}}}.$$

<u>Theorem 2</u>. Let $f:=x^{s+1}-c_sx^s-\cdots-c_1x-c_0\in\mathbf{Z}[x]$, $\lambda_p\in\mathbf{Z}_p$, e(p) (p∈Prime(d)) b

as in Theorem 1. Let $\Theta_n={}^T(\theta_n^{(1)},\ldots,\theta_n^{(s)})\in\mathbf{Q}^s(\subset\mathbf{Q}_p^s)$ be the n-th convergent of the following periodic continued fraction:

$$\cfrac{c_0^{-s}}{-c_0^{-s}\underline{c}_1^*+\cfrac{c_0^{-s}}{-c_0^{-s}\underline{c}_2^*+\cdots+\cfrac{c_0^{-s}}{-c_0^{-1}\underline{c}_{s-1}^*+\cfrac{c_0^{-s}}{-c_0^{-s}\underline{c}^*+\cdots+\cfrac{c_0^{-s}}{-c_0^{-s}\underline{c}^*+\cdots}}}}},$$

where

$$\underline{c}_m^*:={}^T(0,\ldots 0,c_0^{m-1}c_m,c_0^{m-2}c_{m-1},\ldots,c_0c_2,c_1)\in\mathbf{Z}^s\ (1\leqq m\leqq s),$$

$$\underline{c}^*:=\underline{c}_s^*.$$

Let $\underline{\underline{r}}_n:={}^T(r_n^{(0)},\ldots,r_n^{(s)})\in\mathbf{Z}^s$ be the final column vector of a matrix $J_0J_1\cdots J_n$ where

$$J_m:=\begin{bmatrix} {}^T\underline{0} & c_0^s \\ E_s & -\underline{c}_m^* \end{bmatrix}\quad(0\leqq m\leqq s),\quad J_m:=J_s\quad(m>s),$$

$$\underline{c}_0^*:={}^T(0,\ldots 0)\in\mathbf{Z}^s.$$

Then

(i) $\theta_n^{(j)}=r_n^{(j)}/r_n^{(0)}$, $n\geqq 0$, $1\leqq j\leqq s$,

and

(ii) $|\theta_n^{(j)}-c_0^{-j}\lambda_p^j|_p\leqq p^{-e(p)n+j}$, $n\geqq 0$, $1\leqq j\leqq s$, and $p\in\mathrm{Prime}(d)$.

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

$$\Theta:={}^T(c_0^{-1}\lambda_p,\ c_0^{-2}\lambda_p^2,\ \ldots,\ c_0^{-s}\lambda_p^s)\in\mathbf{Z}_p.$$

Corollary 1. A periodic continued fraction $[\underline{0};\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_{s-1},\overset{*}{\underline{a}_s},\underline{a}_{s+1},\ldots,\overset{*}{\underline{a}_{2s}}]$ has the same convergents as that in Theorem 2, so that it converges to Θ, where $\underline{a}_s,\underline{a}_{s+1},\ldots,\underline{a}_{2s}$ is a period, $\underline{0}\in\mathbf{Z}^s$, and

$$\begin{array}{lllllllll}
\underline{a}_1 & ={}^T(0 & ,\ 0 & ,\ 0 & ,\ \ldots, & 0 & ,\ 0 & , & -c_1), \\
\underline{a}_2 & ={}^T(0 & ,\ 0 & ,\ 0 & ,\ \ldots, & 0 & ,\ -c_0c_2, & & -c_1), \\
\underline{a}_3 & ={}^T(0 & ,\ 0 & ,\ 0 & ,\ \ldots, & -c_0{}^2c_3, & -c_0c_2, & & -c_1), \\
\cdots & & \cdots & & \cdots & & & & \cdots \\
\underline{a}_{s-2} & ={}^T(0 & ,\ 0 & ,-c_0{}^{s-3}c_{s-2}, & \ldots, & -c_0{}^2c_3, & -c_0c_2, & & -c_1), \\
\underline{a}_{s-1} & ={}^T(0 & ,-c_0{}^{s-2}c_{s-1}, & -c_0{}^{s-3}c_{s-2}, & \ldots, & -c_0{}^2c_3, & -c_0c_2, & & -c_1), \\
\underline{a}_s & ={}^T(-c_0{}^{s-1}c_s, & -c_0{}^{s-2}c_{s-1}, & -c_0{}^{s-3}c_{s-2}, & \ldots, & -c_0{}^2c_3, & -c_0c_2, & & -c_1), \\
\underline{a}_{s+1} & ={}^T(-c_0{}^{-1}c_s, & -c_0{}^{s-2}c_{s-1}, & -c_0{}^{s-3}c_{s-2}, & \ldots, & -c_0{}^2c_3, & -c_0c_2, & & -c_1), \\
\underline{a}_{s+2} & ={}^T(-c_0{}^{-1}c_s, & -c_0{}^{-2}c_{s-1}, & -c_0{}^{s-3}c_{s-2}, & \ldots, & -c_0{}^2c_3, & -c_0c_2, & & -c_1), \\
\cdots & & \cdots & & \cdots & & & & \cdots \\
\underline{a}_{2s-2} & ={}^T(-c_0{}^{-1}c_s, & -c_0{}^{-2}c_{s-1}, & -c_0{}^{-3}c_{s-2}, & \ldots, & -c_0{}^{-s+2}c_3, & -c_0c_2, & & -c_1), \\
\underline{a}_{2s-1} & ={}^T(-c_0{}^{-1}c_s, & -c_0{}^{-2}c_{s-1}, & -c_0{}^{-3}c_{s-2}, & \ldots, & -c_0{}^{-s+2}c_3, & -c_0{}^{-s+1}c_2, & & -c_1), \\
\underline{a}_{2s} & ={}^T(-c_0{}^{-1}c_s, & -c_0{}^{-2}c_{s-1}, & -c_0{}^{-3}c_{s-2}, & \ldots, & -c_0{}^{-s+2}c_3, & -c_0{}^{-s+1}c_2, & & -c_0{}^{-s}c_1).
\end{array}$$

Remark 6. Lemma 9, (i) given below implies that $q_n{}^{(0)}\neq 0$ for all $n\geqq 0$, so that any convergent Θ_n $(n\geqq 0)$ 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 $\mathbf{R}$ with respect to the metric coming from $|*|=|*|_\infty$. These continued fractions always doverge when $f\in\mathbf{Z}[x]$ 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 $A\in(a_{ij})_{0\leq i\leq s,\,0\leq j\leq s}\in M_0(s+1;K)$. Then A defines a linear map on K^{s+1}, which will be also denoted by A. For elements $\underline{v}$, $\underline{w}\in K^{s+1}\backslash\{\underline{0}\}$, iff there exists $c\in K$ such that $c\underline{v}=\underline{w}$, we write $\underline{v}\sim\underline{w}$, which defines an equivalence relation on $K^{s+1}\backslash\{\underline{0}\}$. We denote by κ the map

$$\kappa:\ K^{s+1} \dashrightarrow P^s(K):=(K^{s+1}\backslash\{\underline{0}\})/\sim,$$
$$\kappa(\underline{v}):=\{\underline{w}\in K^{s+1}\backslash\{\underline{0}\};\ \underline{w}\sim\underline{v}\}\ \ (\underline{v}\neq\underline{0}),$$

where the broken arrow $\dashrightarrow$ indicates a "map" with some exceptional elements for which the the map is not defined. Since $\kappa(\underline{v})=\kappa(\underline{w})$ implies $\kappa A\underline{v}=\kappa A\underline{w}$, so that the linear map A induces a map A_*: $P^s(K)\longrightarrow P^s(K)$. We define a projection π, and an injection ι by

$$\pi : P^s(K) \longrightarrow K^s,$$

$$\pi(\kappa(\underline{\underline{v}})) := (v_1/v_0 . v_2/v_0, \dots, v_s/v_0),\ \underline{\underline{v}} = {}^T(v_0, v_1, \dots, v_s) \in K^{s+1};$$

$$\iota : K^s \longrightarrow P^s(K),$$

$$\iota(\underline{v}) := \kappa(1, v_1, v_2, \dots, v_s),\ \underline{v} = {}^T(v_1, v_2, \dots, v_s) \in K^s.$$

We set $A_\# = \pi \circ A_* \circ \iota$. Then, Lemma 5 given below can be easily seen.

Lemma 5. The following diagram is commutative:

$$\begin{tikzcd}
K^{s+1} \arrow[r] \arrow[d, "A"'] & P^s(K) \arrow[r, shift left, "\pi"] \arrow[d, "A_*"] & K^s \arrow[l, shift left, "\iota"] \arrow[d, "A_\#"] \\
K^{s+1} \arrow[r] & P^s(K) \arrow[r, shift left, "\pi"] & K^s \arrow[l, shift left, "\iota"]
\end{tikzcd}$$

Using Lemma 5, we get the following

Lemma 6. Let X_m be a matrix with s+1 variables $\underline{\underline{x}}_m = {}^T(x_m^{(0)}, \dots, x_m^{(s)})$;

$$X_m := \begin{bmatrix} {}^T\underline{0} & x_m^{(0)} \\ E_s & \underline{x}_m \end{bmatrix},\ \underline{x}_m := {}^T(x_m^{(1)}, \dots, x_m^{(s)}),\ 0 \leqq m \leqq n.$$

and let $p_i^{(j)}$ be polynomials

$$p_i^{(j)} = p_i^{(j)}(\underline{\underline{x}}_0, \dots, \underline{\underline{x}}_n)^s \in \mathbf{Z}[\underline{\underline{x}}_0, \dots, \underline{\underline{x}}_n]\ (-s-1 \leqq i \leqq n,\ 0 \leqq j \leqq s)$$

defined by s+1 recurrences

$$p_m^{(j)} = x_m^{(0)} p_{m-s-1}^{(j)} + x_m^{(1)} p_{m-s}^{(j)} + \cdots + x_m^{(s)} p_{m-1}^{(j)}\ (0 \leqq m \leqq n,\ 0 \leqq j \leqq s)$$

with an initial condition

$$P_{-1} = E_{s+1},$$

where

$$P_m := (p_{m-s+i}^{(j)})_{0 \leqq i \leqq s,\ 0 \leqq j \leqq s}.$$

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

(i) $P_m = X_0 X_1 \cdots X_m \in M(s+1; \mathbf{Z}[\underline{\underline{x}}_0, \dots, \underline{\underline{x}}_m])$.

(ii) $\Xi(\underline{\underline{x}}_0, \dots, \underline{\underline{x}}_m) = (p_m^{(0)})^{-1}\ {}^T(p_m^{(1)}, \dots, p_m^{(s)}) \in \mathbf{Q}(\underline{\underline{x}}_0, \dots, \underline{\underline{x}}_m)^s$.

Remark 8. In general, the formula (ii) holds for $\underline{\underline{x}}_0, \dots, \underline{\underline{x}}_m \in K^{s+1}$ for ar field K even for the case of char(K)≠0 provided that $p_m^{(0)}(\underline{\underline{x}}_0, \dots, \underline{\underline{x}}_m)$ dif 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

$$K_n := \begin{bmatrix} d^n & -{}^T\underline{h}_n \\ \underline{0} & E_s \end{bmatrix}, \quad J := J_s = \begin{bmatrix} {}^T\underline{0} & c_0{}^s \\ E_s & -\underline{c}^* \end{bmatrix}$$

$$\underline{c}^*={}^T(c_0{}^{s-1}c_s, c_0{}^{s-2}c_{s-1}, \dots, c_0c_2, c_1),$$

where $\underline{h}_n \in \mathbf{Z}^s$ is a vector in Theorem 1, (i). We define integers $q_n{}^{(j,i)}$ by

$$Q^n =: (q_n{}^{(j,i)})_{0\leq i\leq s,\, 0\leq j\leq s} \quad (n\geqq 0), \tag{15}$$

where

$$Q := \begin{bmatrix} -\underline{c} & c_0E_s \\ 1 & {}^T\underline{0} \end{bmatrix}.$$

Note that

$$Q=c_0C^{-1}=(-1)^s\tilde{C}, \quad C=C(f).$$

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

<u>Lemma 7</u>. $q_n{}^{(0,i)}h_n{}^{(j)}\equiv q_n{}^{(j,i)} \pmod{d^n}$ for all $0\leqq i\leqq s$, $1\leqq j\leqq s$, $n\geqq 0$.

We set

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

<u>Lemma 8</u>. $Q_n=Q_sJ^{n-s}$ for all $n\geqq s$.

<u>Lemma 9</u>. (i) $q_n{}^{(0)}\equiv(-c_1)^n \pmod{d}$,

(ii) $|h_n{}^{(j)}-q_n{}^{(j,0)}/q_n{}^{(0,0)}|_p\leqq p^{-e(p)n}$ for all $n\geqq 0$, $1\leqq j\leqq s$, and $p\in\mathrm{Prime}(d)$.

Let J_m, be as in Theorem 2. We denote by $O_{t,u}$ the zero matrix of size t×u, by $\underline{0}_m$ the matrix $O_{m,1}$, and by $D(a_0,a_2,\dots,a_s)$ the diagonal matrix with $a_0,a_2,\dots,a_s$ as its diagonal components. For $m\geqq 0$, we put

$$Q_m^* := GJ_0J_1\cdots J_m, \tag{21}$$

$$G_{m+1} := D(c_0^{-m}, c_0^{-m+1}, \dots, c_0^{-1}, 1),$$

$$G := G_{s+1},$$

$$\Delta_{m+1} := \begin{bmatrix} q_0^{(0)} & q_1^{(0)} & \cdots & q_m^{(0)} \\ & q_1^{(1)} & \cdots & q_m^{(1)} \\ & & & \\ & & \ddots & \vdots \\ \bigcirc & & & q_m^{(m)} \end{bmatrix},$$

where

$$q_n^{(i)} := q_n^{(i.0)} \quad (0\leqq i\leqq s,\ n\geqq 0)$$

with $q_n^{(j.0)}$ defined by (15). We put

$$\underline{\underline{q}}_n := {}^T(q_n^{(0)}, \dots, q_n^{(s)}) \in \mathbf{Z}^{s+1} \quad (n\geqq 0).$$

<u>Lemma 10</u>.

(i) $\underline{\underline{q}}_0 = {}^T(1,0,\dots,0)$,

$$\begin{aligned} \underline{\underline{q}}_n = {}^T(&-c_1q_{n-1}^{(0)} - c_2q_{n-1}^{(1)} - \dots - c_nq_{n-1}^{(n-1)}, \\ &c_0q_{n-1}^{(0)}, c_0q_{n-1}^{(1)}, \dots, c_0q_{n-1}^{(n-1)}, {}^T\underline{0}_{s-n}) \quad (1\leqq n\leqq s). \end{aligned} \tag{22}$$

(ii) $Q_n^* = \begin{bmatrix} O_{n+1,\,s-n} & \Delta_{n+1} \\ & \\ D_{s-n} & O_{s-n,\,n+1} \end{bmatrix}$ $(0\leqq n< s)$, $Q_s^* = Q_s$.

Using Lemmas 1-10, we can show Theorem 1. We denote by $\lfloor r\rfloor$ $(r\in\mathbf{R},\ \lfloor\infty\rfloor:=\infty)$ the largest integer not exceeding r. We put

$$t(n) := \lfloor n/(s+1)\rfloor,\quad r(n) := n-(s+1)t(n) \quad (n\in\mathbf{Z}).$$

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

<u>Lemma 11</u>. Let $X_m\in M(s+1;\mathbf{Z}[\underline{\underline{x}}_m])$, $\underline{\underline{x}}_m = {}^T(x_m^{(0)}, x_m^{(1)}, \dots, x_m^{(s)})$, $0\leqq m\leqq n$ be as in Lemma 6. Let

$$x_m^\# := x_mx_{m-s-1}x_{m-2(s+1)}\cdots x_{r(m)} \quad (0\leqq m\leqq n),\quad x_m^\# := 1 \quad (m<0);$$

$$\begin{aligned} \underline{x}_m^* &= {}^T(x_m^{*(0)}, x_m^{*(1)}, \dots, x_m^{*(s)}) \\ &:= (x_m^\#)^{-1}\cdot{}^T(x_{m-s}^\#\cdot x_m^{(1)}, x_{m-s+1}^\#\cdot x_m^{(2)}, \dots, x_{m-1}^\#\cdot x_m^{(s)}), \end{aligned}$$

where $x_m = x_m^{(0)}$. Then the folowing formula holds:

$$(x_0^{(0)})^{-1}\underline{x}_0 + \cfrac{(x_0^{(0)})^{-1}}{(x_1^{(0)})^{-1}\underline{x}_1 + \cfrac{(x_1^{(0)})^{-1}}{(x_2^{(0)})^{-1}\underline{x}_2 + \cdot \cdot + \cfrac{(x_{m-2}^{(0)})^{-1}}{(x_{m-1}^{(0)})^{-1}\underline{x}_n + \cfrac{(x_{m-1}^{(0)})^{-1}}{(x_m^{(0)})^{-1}\underline{x}_m}}}}$$

$$= [\underline{x}_0{}^*;\underline{x}_1{}^*,\dots,\underline{x}_m{}^*] \in (\mathbf{Q}[\underline{x}_0,\underline{x}_1,\dots,\underline{x}_m])^*,\ 0 \leqq m \leqq n.$$

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

§5. A form $\Upsilon(\underline{x};f)$ We denote by $\mathbf{Q}^{alg} \subset \mathbf{C}$ (resp. $\mathbf{Q}_p^{alg} \subset \Omega_p$) the algebraic closure of $\mathbf{Q}$ (resp. $\mathbf{Q}_p$). Let $f \in \mathbf{Z}[x]$ be a monic polynomial of degree $s+1$, $C=C(f) \in M_0(s+1;\mathbf{Z})$ the companion matrix of f, $e(p)$ ($p \in \mathrm{Prime}(|f(0)|)$) the number as in Section 0. We denote by $\Phi(x;A)$ the characteristic polynomial of a matrix $A \in M(s+1;\mathbf{Q})$.

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

$$\Upsilon(\underline{x};f)=\Upsilon(x_0,x_1,\dots,x_s;f) := \det\Big(\sum_{0 \leqq j \leqq s} x_j C(f)^j\Big).$$

We remark that

$$\Upsilon(\underline{x};f)= \prod_{f(\alpha)=0\ (\alpha \in \mathbf{Q}^{alg})} \Big(\sum_{0 \leqq j \leqq s} \alpha^j x_j\Big)$$
$$= \prod_{f(\alpha)=0\ (\alpha \in \mathbf{Q}_p^{alg})} \Big(\sum_{0 \leqq j \leqq s} \alpha^j x_j\Big)$$

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

For a given matrix $A \in M_0(s+1;\mathbf{Z})$, we write $A \in (\mathrm{Bdd})$ if A satisfies the following condition (Bdd):

(Bdd) The set $\{n \geqq 0;\ A^{-n}\underline{x} \in \mathbf{Z}^{s+1}\}$ is bounded for any $\underline{x} \in \mathbf{Z}^{s+1} \setminus \{\underline{0}\}$.

We can show that if $A \in (\mathrm{Bdd})$, then $A \in M(s+1;\mathbf{Z})$ has no units ($\in \mathbf{Q}^{alg}$) as its eigenvalues in $\mathbf{Q}^{alg}$; and if

$$A = U^{-1}\begin{bmatrix} A_1 & \ast \\ & \ddots & \\ \bigcirc & & A_t \end{bmatrix} U \quad \left(\text{or } U^{-1}\begin{bmatrix} A_1 & \bigcirc \\ & \ddots & \\ \ast & & A_t \end{bmatrix} U\right),\ U \in GL(s+1;\mathbf{Z})$$

such that $|\det A_k|>1$, and $\Phi(x;A_k)$ is irreducible over $\mathbf{Z}[x]$ for all $1\leqq k\leqq t$, th $C(f)\in(\mathrm{Bdd})$. In particular, if $f\in\mathbf{Z}[x]$ is irreducible over $\mathbf{Z}[x]$, and $|f(0)|>1$, then $C(f)\in(\mathrm{Bdd})$, cf. Theorem 2 in [3], see also [2].

Let us suppose $A\in(\mathrm{Bdd})$, and consider a map ind_A defined by

$$\mathrm{ind}_A:\ \mathbf{Z}^{s+1}\longrightarrow \mathbf{N}\cup\{\infty\}$$

$$\mathrm{ind}_A(\underline{x}):=\max\{n\geqq 0:\ A^{-n}\underline{x}\in\mathbf{Z}^{s+1}\}\ (\underline{x}\neq\underline{0}),\ \mathrm{ind}_A(\underline{0}):=\infty,$$

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

$$\bigcup_{0\leqq j<c} A^j\Gamma=\mathbf{Z}^{s+1}\backslash\{\underline{0}\}\ \text{(disjoint)}$$

of the set $\mathbf{Z}^{s+1}\backslash\{\underline{0}\}$ into c ($2\leqq c\leqq\infty$) parts iff $A\in(\mathrm{Bdd})$, and

$$\Gamma=\{\underline{x}\in\mathbf{Z}^{s+1}\backslash\{\underline{0}\};\ \mathrm{ind}_A(\underline{x})\equiv 0\ (\mathrm{mod}\ c)\}\quad (c\neq\infty),$$

$$\Gamma=\{\underline{x}\in\mathbf{Z}^{s+1}\backslash\{\underline{0}\};\ \mathrm{ind}_A(\underline{x})=0\}\quad (c=\infty)$$

holds, cf. Theorem 1 in [3].

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

Corollary 2. Let $f\in\mathbf{Z}[x]$ be a monic polynomial satisfying (1) such that $C(f)\in(\mathrm{Bdd})$. Let $\lambda_p\in\mathbf{Z}_p$ ($p\in\mathrm{Prime}(f(0))$ be as in Theorem 1. Then

$$\mathrm{ind}_{C(f)}(\underline{x})=\min_{p\in\mathrm{Prime}(|f(0)|)}\left(\lfloor v_p\Big(\sum_{0\leqq j\leqq s}\lambda_p{}^j x_j\Big)\Big)/v_p(f(0))\rfloor\right)$$

holds for all $\underline{x}={}^T(x_0,x_1,\ldots,x_s)\in\mathbf{Z}^{s+1}$.

Recalling

$$\Upsilon(\underline{x};f)=\prod_{f(\alpha)=0\ (\alpha\in\mathbf{Q}_p{}^{alg})}\Big(\sum_{0\leqq j\leqq s}\alpha^j x_j\Big),$$

we see that Corollary 2 immediately implies the following

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

$$\min_{p\in\mathrm{Prime}(|f(0)|)}\left(\lfloor v_p(\Upsilon(\underline{x};f))/v_p(f(0))\rfloor\right)\leqq\mathrm{ind}_{C(f)}(\underline{x}),\quad \underline{x}\in\mathbf{Z}^{s+1}.$$

In particular, the equality holds if $x_j\not\equiv 0$ (mod p) for exactly one $0\leqq j\leqq s$.

Corollary 3 is of somewhat trivial, but it may be of interest by two reason first, the assertion is stated within the set $\mathbf{Z}$; secondly, the form $\Upsilon(\underline{x};f)$ i 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) $s=1$, $f=x^2-bx-a$,

$\Upsilon(x,y;f)=x^2+bxy-ay^2$.

(ii) $s=2$, $f=x^3-cx^2-bx-a$,

$\Upsilon(x,y,z;f)=x^3+cx^2y+(2b+c^2)x^2z-bxy^2-(3a+bc)xyz+(b^2-2ac)xz^2+ay^3+acy^2z-abyz^2$
$+a^2z^3$

(iii) $s=3$, $f=x^4-dx^3-cx^2-bx-a$,

$\Upsilon(x,y,z,w;f)=x^4+dx^3y+(2c+d^2)x^3z+(3b+3cd+d^3)x^3w-cx^2y^2-(3b+cd)x^2yz$
$-(4a+bd+2c^2+cd^2)x^2yw-(2a+2bd-c^2)x^2z^2-(5ad-bc+2bd^2-c^2d)x^2zw$
$-(3ac+3ad^2-3b^2-3bcd+c^3)x^2w^2+bxy^3+(4a+bd)xy^2z+(ad+bd^2+2bc)xy^2w+(3ad-bc)xyz^2$
$+(4ac+3ad^2-3b^2-bcd)xyzw-(5ab+acd+2b^2d-bc^2)xyw^2-(2ac-b^2)xz^3+(ab-2acd+b^2d)xz^2w$
$+(4a^2+2ac^2+abd-b^2c)xzw^2+(3a^2d-3abc+b^3)xw^3-ay^4-ady^3z-(2ac+ad^2)y^3w+acy^2z^2$
$+(3ab+acd)y^2zw+(2a^2+2abd-ac^2)y^2w^2-abyz^3-(4a^2+abd)yz^2w-(3a^2d-abc)yzw^2$
$+(2a^2c-ab^2)yw^3+a^2z^4+a^2dz^3w-a^2cz^2w^2+a^2bzw^3-a^3w^4$

In general, $\Upsilon(x_0,x_1,\ldots,x_s;f)$ consists of $(2s+1)!/((s+1)!s!)$ terms as a polynomial in x_0, x_1, $\ldots,x_s$.

References

[1] N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-functions, Springer-Verlag, New York, Heidelberg, Berlin, 1977.

[2] J. Tamura, Certain partition of a lattice, in From Crystal to Chaos, Proceedings of the conference in honor of Gérard Rauzy on his 60 th birthday, ed. J.-M. Gambaudo, P. Hubert, P. Tisseur and S. Vaienti, World Scientific, 18 pages, to appear.

[3] ________, Certain words, tilings, their nonperiodcity, 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.