International Journal of Pure and Applied Mathematics
Volume 87 No. 3 2013, 421-430
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v87i3.6

COMPLETE RESIDUE SYSTEMS IN THE RING OF MATRICES OVER EUCLIDEAN DOMAINS AND A GREATEST COMMON DIVISOR OF MATRICES

Santad Damkaew[1], Supawadee Prugsapitak[2] §
[1,2]Department of Mathematics and Statistics
Faculty of Science
Prince of Songkla University
Hatyai, Songkla, 90112, THAILAND

Abstract: In this paper, we construct a complete residue system in the ring of 2×2 matrices over a Euclidean domain and use it to provide a division algorithm for matrices in order to obtain a greatest common divisor of two matrices over some Euclidean domains.

AMS Subject Classification: 11A05, 15A99
Key Words: complete residue system, greatest common divisor

1. Introduction

In 1978, J.S. Shiue and C.P. Hwang [3] characterized the complete residue system modulo G where G is any nonsingular $n \times n$ matrix over the ring of integers. Since the ring of integers is a Euclidean domain, it is natural to generalize their results to Euclidean domains. This motivates the author to extend their results. Furthermore we know that in the set of integers, one can find a greatest common divisor by applying a Euclidean algorithm. In the last section, we discuss how one can construct a division algorithm to obtain a greatest common divisor of two matrices over some Euclidean domains.

Received: May 4, 2013

§Correspondence author

2. Complete Residue Systems in the Ring of 2×2 Matrices over Euclidean Domains and its Application

In this section, we generalized J.S. Shiue and C.P. Hwang's results [3] to find a complete residue system in the ring of 2×2 matrices over a Euclidean domains. Throughout D is a Euclidean domain. For any matrices $A, B \in \mathrm{Mat}_n D$ where A is nonsingular, $A \mid B$ means that there exists $C \in \mathrm{Mat}_n D$ such that $B = CA$. We denote a complete residue system modulo g by $\mathrm{C.R.S.}(g)$ for a nonzero element g. Similarly we denote a complete residue system modulo $G \in \mathrm{Mat}_n(D)$ by $\mathrm{C.R.S.}(G)$ for a nonsingular matrix G. By modifying the proof in [3], we obtain a complete residue system for any diagonal matrix over a Euclidean domain as follows:

Lemma 1. *Let* $G = \begin{pmatrix} g_1 & 0 & \cdots & 0 \\ 0 & g_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_n \end{pmatrix} \in \mathrm{Mat}_n(D)$ *with* $g_k \neq 0$ *for any* $k = 1, 2, \ldots, n$. *Then*

$$J = \{(r_{ik}) \in \mathrm{Mat}_n(D) : r_{ik} \in \mathrm{C.R.S.}(g_k), i, k = 1, 2, \ldots, n\}$$

forms a complete residue modulo G.

Proof. Let $A = (a_{ik}) \in \mathrm{Mat}_n(D)$. For each entry a_{ik}, we consider a_{ik} modulo g_k. Since D is a Euclidean domain, there exist $p_{ik} \in D$ and $r_{ik} \in \mathrm{C.R.S.}(g_k)$ such that

$$a_{ik} = p_{ik} g_k + r_{ik}.$$

Thus $A - (p_{ik} g_k) = (r_{ik})$. Since $g_k E_{ik} = E_{ik} G$, $p_{ik} g_k E_{ik} = p_{ik} E_{ik} G$ and hence

$$(p_{ik} g_k) = \sum_{i=1}^{n} \sum_{k=1}^{n} p_{ik} g_k E_{ik} = \sum_{i=1}^{n} \sum_{k=1}^{n} (a_{ik} - r_{ik}) E_{ik}.$$

Now, we see that $G \mid (p_{ik} g_k)$ and hence $G | A - (r_{ik})$. This shows that $A \equiv (r_{ik}) \bmod G$.

Let $(r_{ik}) \equiv (s_{ik}) \bmod G$ be such that $r_{ik}, s_{ik} \in \mathrm{C.R.S.}(g_k)$ for each $i, k = 1, 2, \ldots, n$. Then $G | (r_{ik} - s_{ik})$. Now, there exists $(c_{ik}) \in \mathrm{Mat}_n(D)$ such that $(r_{ik} - s_{ik}) = (c_{ik})G$. Thus $r_{ik} - s_{ik} = c_{ik} g_k$. Since $r_{ik} \equiv s_{ik} \bmod g_k$ and $r_{ik}, s_{ik} \in \mathrm{C.R.S.}(g_k)$, $r_{ik} = s_{ik}$. This shows that $(r_{ik}) = (s_{ik})$. Therefore J forms a C.R.S. mod G. □

We next define the perfect residue system J of a nonsingular matrix A.

Definition 2. The perfect residue system of a nonsingular matrix A over a Euclidean domain D with a Euclidean function ϕ is a complete residue system such that for any non-zero matrix $I \in J$, $0 < \phi(\det I) < \phi(\det A)$. We denote it by $\mathrm{P.R.S.}(A)$.

If $D = \mathsf{Z}$ equipped with an absolute value function then for any $n \in \mathsf{Z}$, $\{0, 1, 2, \ldots, n-1\}$ is a perfect residue system modulo n.

Theorem 3. *Let D be a Euclidean domain with a Euclidean function ϕ. Let $G = \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \in \mathrm{Mat}_2(D)$ with $\det G \neq 0$. Suppose*

$$J = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(D) : a, c \in \mathrm{P.R.S.}(g_1), b, d \in \mathrm{P.R.S.}(g_2) \right\}.$$

Define

$$C = \bigcup_{i=1}^{6} C_i$$

where

$$C_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in J, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 \right\}$$

$$C_2 = \left\{ \begin{pmatrix} a & b \\ c & d+g_2 \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in J, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 0, a \neq 0 \right\}$$

$$C_3 = \left\{ \begin{pmatrix} 0 & b \\ g_1 & d \end{pmatrix} : \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \in J, b \neq 0 \right\}$$

$$C_4 = \left\{ \begin{pmatrix} 0 & g_2 \\ c & d \end{pmatrix} : \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \in J, c \neq 0 \right\}$$

$$C_5 = \left\{ \begin{pmatrix} g_1 & 0 \\ 0 & d \end{pmatrix} : \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \in J, d \neq 0 \right\}$$

$$C_6 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Then C forms a complete residue system modulo G with all nonzero matrix is a nonsingular matrix. In particular, if ϕ is multiplicative and $\phi(\det A) < \phi(\det G)$ for any matrix $A \in J$, then C is a perfect residue system modulo G.

Proof. It is not difficult to see that

$$|C| = |C_1| + |C_2| + |C_3| + |C_4| + |C_5| + |C_6| = |J|.$$

It suffices to show that for any two distinct elements of C are incongruent modulo G. Suppose R_1, R_2 are two distinct elements of C. Define $J_1, J_2, J_3, J_4, J_5, J_6$ by

$$J_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in J : \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 \right\},$$
$$J_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in J : \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 0, a \neq 0 \right\},$$
$$J_3 = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \in J : b \neq 0 \right\},$$
$$J_4 = \left\{ \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \in J : c \neq 0 \right\},$$
$$J_5 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \in J : d \neq 0 \right\},$$
$$J_6 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in J \right\}.$$

Then J is partitioned into $J_1, J_2, \ldots, J_n$. Next we define a function $f : J \to C$ by

$$f(R) = \begin{cases} R & \text{if } R \in J_1, \\ R + \begin{pmatrix} 0 & 0 \\ 0 & g_2 \end{pmatrix} & \text{if } R \in J_2, \\ R + \begin{pmatrix} 0 & 0 \\ g_1 & 0 \end{pmatrix} & \text{if } R \in J_3, \\ R + \begin{pmatrix} 0 & g_2 \\ 0 & 0 \end{pmatrix} & \text{if } R \in J_4, \\ R + \begin{pmatrix} g_1 & 0 \\ 0 & 0 \end{pmatrix} & \text{if } R \in J_5, \\ R & \text{if } R \in J_6. \end{cases}$$

It is easy to see that f is bijective. Let R_1, R_2 be two distinct elements in C. Then $f^{-1}(R_1) = S_1$ and $f^{-1}(R_2) = S_2$ for some $S_1, S_2 \in J$. Since f is injective, $S_1 \neq S_2$ and hence they are incongruent modulo G. Since $S_1 \equiv f(S_1) \equiv R_1 \bmod G$ and $S_2 \equiv f(S_2) \equiv R_2 \bmod G$, R_1 and R_2 are incongruent modulo G as desired. Therefore, any two distinct elements of C are incongruent modulo G. We conclude that C is a complete residue system modulo G. Next,

if ϕ is multiplicative and $\phi(\det A) < \phi(\det G)$ for any $A \in J$ then it is easy to see that J is a perfect residue system. □

In fact, one can show that with some appropriate Euclidean functions, a nonsingular matrice in $\mathrm{Mat}_2(\mathsf{Z})$ and $\mathrm{Mat}_2(\mathsf{Z}[\omega])$ has a perfect residue system.

Corollary 4. *Any nonsingular diagonal matrices in* $\mathrm{Mat}_2(\mathsf{Z})$ *has a perfect residue system.*

Proof. Let $G = \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \in \mathrm{Mat}_2(D)$ with $\det G \neq 0$ be a diagonal matric in $\mathrm{Mat}_2(\mathsf{Z})$. Since an absolute value function is multiplicative and $\{0, 1, 2, \ldots, |g| - 1\}$ is a perfect residue system modulo g for any nonzero $g \in \mathsf{Z}$, one can show that for any $A \in J$ where J is defined as in Theorem 3, $|\det A| < |\det D|$. □

Corollary 5. *Any nonsingular diagonal matrices in* $\mathrm{Mat}_2(\mathsf{Z}[\omega])$ *where* $\omega = \frac{-1+i\sqrt{3}}{2}$ *has a perfect residue system.*

Proof. Let $G = \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \in \mathrm{Mat}_2(D)$ where $D = \mathsf{Z}[\omega]$ with $\det G \neq 0$. For any $g = a - b\omega$, define $N(a + b\omega) = a^2 - ab + b^2$. The function N is multiplicative and it is a Euclidean function for D. Using G.E. Bergum's result [1], namely, for any nonzero $g \in D$, a set S consisting of points interior to the hexagon $ABCDEF$ whose vertices are given respectively by $\frac{g}{3}(1 - \omega)e^{\frac{\pi k i}{3}}$ where $1 \leq k \leq 6$ and points on the line segments CD, DE and EF except the vertex F is a prefect residue system modulo g, we can show that for any $r \in S$, $N(r) \leq \frac{N(g)}{3}$. Thus it is not hard to see that for any $A \in J$ where J is defined as in Theorem 3, $N(\det A) < N(\det D)$. □

We next show that one can construct a perfect residue system of any nonsingular 2×2 matrices. We first modified H.L. Keng's result[2] to show that for any $A \in Mat_2(D)$, there exist two unimodular matrices U and V such that UAV is a diagonal matrix where unimodular matrix is a matrix whose determinant is a unit in D.

Lemma 6. *Let D be a Euclidean domain with a Euclidean function ϕ. Any 2×2 matrix is equivalent to a matrix of the form*

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_1 a_2 \end{pmatrix}$$

where $a_1, a_2 \in D$.

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(D)$. This lemma is trivial if M is a zero matrix. We may assume that $a \neq 0$. We first prove that M must be equivalent to a matrix of the form $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ where $a_1 \mid \gcd(b_1, c_1, d_1)$. We do the induction on $\phi(a)$. If a is a unit then

$$\begin{pmatrix} 1 & 0 \\ -cu^{-1} & 1 \end{pmatrix} \begin{pmatrix} u & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -bu^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u & 0 \\ 0 & d - bcu^{-1} \end{pmatrix}.$$

We may assume that a is not a unit. If $a \mid \gcd(b, c, d)$, then there exist b_1, c_1, d_1 such that $b = ab_1$, $c = ac_1$ and $d = ad_1$ and we have

$$\begin{pmatrix} 1 & 0 \\ -c_1 & 1 \end{pmatrix} \begin{pmatrix} a & ab_1 \\ ac_1 & ad_1 \end{pmatrix} \begin{pmatrix} 1 & -b_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a(d_1 - b_1c_1) \end{pmatrix}.$$

If $a \nmid b$, then there exist $q, r \in D$ such that $b = a(-q) + r$ where $\phi(r) < \phi(a)$. Thus $aq + b = r$ and hence $\phi(aq + b) = \phi(r) < \phi(a)$. Then we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} aq + b & * \\ * & * \end{pmatrix}$$

where $\phi(aq + b) < \phi(a)$. If $a \mid b$ but $a \nmid c$, then we choose q' such that $\phi(aq' + c) < \phi(a)$ and we have

$$\begin{pmatrix} q' & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} aq' + c & * \\ * & * \end{pmatrix}.$$

If $a \mid \gcd(b, c)$ and $a \nmid d$, then we may assume that $c = c'a$ for some $c' \in D$. So that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c' & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & (1 - c')b + d \\ * & * \end{pmatrix}$$

and $a \nmid (1 - c')b + d$ which reduces back to the case $a \nmid b$. The argument induction is now complete. This lemma is proved. □

The next corollary follows similarly as in [3]. We will use it to provide a complete residue system for any nonsingular matrix.

Theorem 7. *Let D be a Euclidean Domain and G be an element of $\mathrm{Mat}_n(D)$ with $\det G \neq 0$. If U and V are unimodular matrices in D such that*

$$UGV = \begin{pmatrix} g_1 & 0 & \cdots & 0 \\ 0 & g_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_n \end{pmatrix}$$

then

$$J = \left\{(r_{ik})V^{-1} \in \mathrm{Mat}_n(D) | r_{ik} \in \mathrm{C.R.S.}(g_k), i, k = 1, 2, \ldots, n\right\}$$

forms a complete residue system modulo G.

Proof. Let $A \in \mathrm{Mat}_n(D)$. By Lemma 1, there exists $(r_{ik}) \in \mathrm{Mat}_n(D)$ where $r_{ik} \in \mathrm{C.R.S.}(g_k)$ such that

$$AV \equiv (r_{ik}) \bmod UGV.$$

So that there exists $W \in Mat_n(D)$ such that $AV - (r_{ik}) = WUGV$. We can see that $A - (r_{ik})V^{-1} = WUG$ and hence $A \equiv (r_{ik})V^{-1} \bmod G$. We next show that any two congruent elements in J are exactly the same element. Let $(r_{ik})V^{-1} \equiv (s_{ik})V^{-1} \bmod G$ where $r_{ik}, s_{ik} \in \mathrm{C.R.S.}(g_k)$. Then there exists $W \in \mathrm{Mat}_n(D)$ such that

$$(r_{ik})V^{-1} - (s_{ik})V^{-1} = WG.$$

We can see that $(r_{ik}) - (s_{ik}) = WU^{-1}UGV$, and hence $(r_{ik}) \equiv (s_{ik}) \bmod UGV$. This implies that $g_k \mid r_{ik} - s_{ik}$. Since $r_{ik}, s_{ik} \in \mathrm{C.R.S.}(g_k), r_{ik} = s_{ik}$ for any i, k. Thus $(r_{ik})V^{-1} = (s_{ik})V^{-1}$. Therefore J forms a C.R.S.(G). □

Theorem 8. *Let D be a Euclidean domain with a Euclidean function ϕ. Let $G \in \mathrm{Mat}_2(D)$ be a non singular matrix. Let U and V be unimodular matrices such that*

$$UGV = \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \quad \textit{for some} \quad g_1, g_2.$$

Suppose

$$J = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(D) : a, c \in \mathrm{P.R.S.}(g_1), b, d \in \mathrm{P.R.S.}(g_2) \right\}$$

and define C as in Theorem 3. Then CV^{-1} forms a complete residue system modulo G with all nonzero matrix is a nonsingular matrix. In particular, if ϕ is multiplicative and $\phi(\det A) < \phi(\det G)$ for any matrix $A \in J$, then CV^{-1} is a perfect residue system modulo G.

Proof. By Theorem 3, we get that C is a complete residue system modulo GV. Next, we can conclude that CV^{-1} is a complete residue system modulo $GVV^{-1} = G$, by Theorem 7. □

The next corollary follows immediately from Lemma 1.

Corollary 9. *Let G be a nonsingular matrix in* $\mathrm{Mat}_n(D)$ *and there are unimodular matrices U and V such that*

$$UGV = \begin{pmatrix} g_1 & 0 & \cdots & 0 \\ 0 & g_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_n, \end{pmatrix}$$

then the cardinality of C.R.S. mod G is

$$\prod_{k=1}^{n} |\ \mathrm{C.R.S.}(g_k)\ |^n$$

where g_k defined in the theorem.

3. Applications

In this section, we provide a method of finding a greatest common divisor of 2×2 matrices A and B. The matrix G is a greatest common divisor of A and B if G divides A and B and for any common divisor H of A and B is also a divisor of G.

We first demonstrate how we can use a perfect residue system to find a greatest common divisor of A and B. Suppose that for any nonsingular matrix $M \in \mathrm{Mat}_n(D)$, a perfect residue system modulo M exists. Then we can successively apply the division algorithm as follows:

$$\begin{aligned} A = Q_1B \quad &\text{or} \quad A = Q_1B + R_1 \quad && 0 < \phi(\det R_1) < \phi(\det B), \\ B = Q_2R_1 \quad &\text{or} \quad B = Q_2R_1 + R_2 \quad && 0 < \phi(\det R_2) < \phi(\det R_1), \\ R_2 = Q_3R_1 \quad &\text{or} \quad R_2 = Q_3R_1 + R_4 \quad && 0 < \phi(\det R_4) < \phi(\det R_3), \\ &\vdots \end{aligned}$$

We can assume that eventually we have $R_n = Q_{n+1}R_{n-1}$. Therefore

$$\mathrm{g.c.d.}(A, B) = R_{n-1}.$$

Example 10. Let $A = \begin{pmatrix} 0 & 3 \\ 3 & 9 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 4 \\ -1 & 2 \end{pmatrix}$. We next apply a division algorithm successively over $\mathrm{Mat}_2(\mathbf{Z})$ as follows: Let

$$U_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, V_1 = \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix}.$$

We have $U_1BV_1 = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$ and by applying a method in Theorem 7 we have

$$AV_1 = \begin{pmatrix} 0 & 3 \\ 3 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix} + \begin{pmatrix} 0 & 3 \\ 0 & 3 \end{pmatrix}.$$

By Theorem 3, $f \begin{pmatrix} 0 & 3 \\ 3 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 1 & 3 \end{pmatrix}$. Thus

$$AV_1 - \begin{pmatrix} 0 & 3 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}.$$

This implies that

$$A = \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix} B + \begin{pmatrix} 0 & 3 \\ 1 & 7 \end{pmatrix}.$$

By successively applying the same method as above, we have

$$B = \begin{pmatrix} -1 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 0 & 3 \\ 1 & 7 \end{pmatrix}.$$

Therefore a greatest common divisor of A and B is $\begin{pmatrix} 0 & 3 \\ 1 & 7 \end{pmatrix}$.

Example 11. Let

$$A = \begin{pmatrix} -3+5\omega & 4+\omega \\ 3 & -9-6\omega \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 2 & 4+6\omega \\ 2+6\omega & 6 \end{pmatrix}$$

where $\omega = \dfrac{-1+\sqrt{-3}}{2}$. We next apply a division algorithm successively over $\mathrm{Mat}_2(\mathbf{Z}[\omega])$ as follows: Let

$$U_1 = \begin{pmatrix} 1 & 0 \\ -1-3\omega & 1 \end{pmatrix}, V_1 = \begin{pmatrix} 1 & -2-3\omega \\ 0 & 1 \end{pmatrix}.$$

We have $U_1BV_1 = \begin{pmatrix} 2 & 0 \\ 0 & 20 \end{pmatrix}$ and by applying a method in Theorem 7

$$\begin{aligned} AV_1 &= \begin{pmatrix} -3+5\omega & 25+15\omega \\ 3 & -15-15\omega \end{pmatrix} \\ &= \begin{pmatrix} -1+3\omega & 1+\omega \\ 2 & -1-\omega \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 20 \end{pmatrix} + \begin{pmatrix} -1-\omega & 5-5\omega \\ -1 & 5+5\omega \end{pmatrix}. \end{aligned}$$

This implies that

$$A = \begin{pmatrix} 3+2\omega & 1+\omega \\ 2 & -1-\omega \end{pmatrix} B + \begin{pmatrix} -1-\omega & 6-7\omega \\ -1 & 3+2\omega \end{pmatrix}.$$

We apply the same method to B and $R_1 = \begin{pmatrix} -1-\omega & 6-7\omega \\ -1 & 3+2\omega \end{pmatrix}$. and successively apply the same method in Theorem 7 we have,

$$B = \begin{pmatrix} \omega & -1 \\ -1-\omega & -1-5\omega \end{pmatrix} R_1 + \begin{pmatrix} 0 & -5\omega \\ 1 & 12+13\omega \end{pmatrix}.$$

Again we apply the same method to R_1 and $R_2 = \begin{pmatrix} 0 & -5\omega \\ 1 & 12+13\omega \end{pmatrix}$. We obtain that

$$R_1 = \begin{pmatrix} R_2\omega & -1-\omega \\ 3\omega & -1 \end{pmatrix}.$$

Therefore a greatest common divisor of A and B is $\begin{pmatrix} 0 & -5\omega \\ 1 & 12+13\omega \end{pmatrix}$.

References

[1] Gerald E. Bergum, Complete residue systems in the quadratic domain $\mathsf{Z}(e^{2\pi i/3})$, *International Journal of Mathematics and Mathematical Sciences*, **1**, 1(1978), 75-85, **doi:** 10.1155/S0161171278000101.

[2] Hua Loo Keng, *Introduction to Number Theory*, Springer-Verlag, USA (1982).

[3] Jau-Shyong Shiue, Chie-Ping Hwang, Complete residue systems in the ring of matrices of rational integers, *International Journal of Mathematics and Mathematical Sciences*, **1**, No. 1 (1978), 217-225, **doi:** 10.1155/S0161171278000253.