COMPLETE RESIDUE SYSTEMS IN THE RING OF MATRICES OF RATIONAL INTEGERS

JAU-SHYONG SHIUE
Department of Mathematical Sciences
National Chengchi University
Taipei, Taiwan
Republic of China

and

CHIE-PING HWANG
Department of Mathematics
National Central University
Chungli, Taiwan
Republic of China

(Received April 1, 1977 and in revised form August 29, 1977)

ABSTRACT. This paper deals with the characterizations of the complete residue system mod. $G$, where $G$ is any $n \times n$ matrix, in the ring of $n \times n$ matrices.

KEY WORDS AND PHRASES. Complete residue system, ring of Gaussian integers, representations for the complete residue system.

AMS(MOS)SUBJECT CLASSIFICATION (1970) CODES. 12F05, 12B35.

1. INTRODUCTION.

Let $\mathbb{Z}$ denote the ring of rational integers and $\mathbb{Z}(i)$ be the ring of
Gaussian integers. Jordan and Potratz [1] have exhibited several represen-
tations for the complete residue system (in short, C.R.S.) mod.\( r \) in the ring
of Gaussian integers. Also it is well known that the ring of Gaussian
integers is isomorphic to the ring of \( 2 \times 2 \) matrices of the form \[
\begin{pmatrix}
a & b \\
-b & a
\end{pmatrix},
\]
a, b in \( \mathbb{Z} \). This raises the question of characterizing the C.R.S. mod. \( G \),
where \( G \) is any \( n \times n \) matrix, in the ring of \( n \times n \) matrices of which we denote by
\( \text{Mat}_n(\mathbb{Z}) \).

2. THE COMPLETE RESIDUE SYSTEM IN \( \text{Mat}_n(\mathbb{Z}) \).

First of all, we define \( A \mid B \) mean there is a matrix \( C \) such that \( B = CA \),
and \( A \equiv B \mod. U \) means that \( U \mid A - B \). Now we can give a definition of the
C.R.S. mod. \( U \) in the ring of \( \text{Mat}_n(\mathbb{Z}) \).

**DEFINITION.** Let \( U \) be in \( \text{Mat}_n(\mathbb{Z}) \) with \( \det U \neq 0 \). Then a subset \( J \) of \( \text{Mat}_n(\mathbb{Z}) \)
is called a C.R.S. mod. \( U \) if and only if for any \( A \) in \( \text{Mat}_n(\mathbb{Z}) \) there exists
uniquely a matrix \( B \) in \( J \) such that \( A \equiv B \mod. U \).

**LEMMA 1.** Let \( G = \text{diag}(g_1, g_2, \ldots, g_n) \) with \( g_i \neq 0 \), \( i = 1, 2, \ldots, n \). Let
\( E_{ij} \) be the matrix units, then
\[
I_{ik} = \{ a \in \mathbb{Z} : G | \sum_{m=1}^{n} \sum_{j=1}^{n} a_{mj} E_{mj} \text{ where } a_{mj} \text{ in } \mathbb{Z}, a_{11} = a_{12} = \ldots = a_{ik-1} = 0, a_{ik} = a \}
\]
is the principal ideals generated by a positive integer \( g_k \), where
\( i, k = 1, 2, \ldots, n \).

**PROOF.** It is clear the \( I_{ik} \) are ideals in \( \mathbb{Z} \). But \( \mathbb{Z} \) is a P.I.D., therefore
\( I_{ik} \) are principal ideals generated by a positive integer \( d_{ik} \). Since
\( g_k E_{ik} = E_{ik} G \), then \( g_k \) is in \( I_{ik} \), i.e., \( d_{ik} \mid g_k \). On the other hand, for \( d_{ik} \) in
\( I_{ik} \) we have \( \sum_{m=1}^{n} \sum_{j=1}^{n} a_{mj} E_{mj} = (t_{ik}) G \) for some \( (t_{ik}) \), where \( a_{mj} \) is in \( \mathbb{Z} \),
\( a_{11} = a_{12} = \ldots = a_{ik-1} = 0, a_{ik} = d_{ik} \). It follows that \( d_{ik} = t_{ik} g_k \), i.e., \( d_{ik} = |g_k| \).
This completes the proof.
LEMMA 2. Let $G = \text{diag}(g_1, g_2, \ldots, g_n)$ with $g_k \neq 0$, $k = 1, 2, \ldots, n$. Then $J = \{(r_{ik}) : 0 \leq r_{ik} < |g_k|, i, k = 1, 2, \ldots, n\}$ forms a complete residue system mod. $G$.

PROOF. (1) For any $A = (a_{ik})$ in $\text{Mat}_n(Z)$, there exist $p_{1k}, r_{ik}$ in $Z$ such that $a_{ik} = p_{1k} |g_k| + r_{ik}$, where $0 \leq r_{ik} < |g_k|$. Therefore

$$A - (p_{1k} |g_k|) = (r_{ik}).$$

But $|g_k| \cdot \mathbb{1}_{ik} = |g_k| \cdot \mathbb{1}_{ik} G$, and therefore $G | A - (r_{1k})$. This shows that $A \equiv (r_{1k}) \mod. G$.

(2) If $(r_{ik}) \equiv (s_{ik}) \mod. G$, where $0 \leq r_{ik}, s_{ik} < |g_k|$, then $G | (r_{ik} - s_{ik})$, i.e., $r_{11} - s_{11}$ is in $I_{11}$ (by Lemma 1). This implies that $g_1 | (r_{11} - s_{11})$, and so $r_{11} = s_{11}$, for $0 \leq |r_{11} - s_{11}| < |g_1|$. It follows that $r_{12} - s_{12}$ is in $I_{12}$. Therefore $g_2 | (r_{12} - s_{12})$ and $r_{12} = s_{12}$, for $0 \leq |r_{12} - s_{12}| < |g_2|$. Continuing in this way, we must have $r_{ik} = s_{ik}$, for all $i, k = 1, 2, \ldots, n$.

THEOREM 1. If $G$ is a $n \times n$ matrix with $\det G \neq 0$, and if $U$ and $V$ are unimodular $n \times n$ matrices such that $UGV = \text{diag}(g_1, g_2, \ldots, g_n)$, then $J = \{(r_{ik}) V^{-1} : 0 \leq r_{ik} < |g_k|, i, k = 1, 2, \ldots, n\}$ forms a complete residue system mod. $G$.

PROOF. (1) By Lemma 2, for any $n \times n$ matrix $A$, there exists a matrix $(r_{ik})$ with $0 \leq r_{ik} < |g_k|$ such that $AV \equiv (r_{1k}) \mod. UGV$, i.e., $A \equiv (r_{1k}) V^{-1} \mod. G$.

(2) Let $(r_{ik}) V^{-1} \equiv (s_{ik}) V^{-1} \mod. G$, where $0 \leq r_{ik}, s_{ik} < |g_k|$. It follows that $(r_{1k}) \equiv (s_{1k}) \mod. UGV$. Therefore $(r_{1k}) = (s_{1k})$.

COROLLARY 1. If $J$ forms a C.R.S. mod. $G$, and $U$ and $V$ are unimodular $n \times n$ matrices, then $\{URV : R \in J\}$ forms a C.R.S. mod. $GV$.

COROLLARY 2. If $G$ is a $n \times n$ matrix with $\det G \neq 0$, then the cardinality of the C.R.S. mod. $G$ is $|\det G|^n$. 
3. THE COMPLETE RESIDUE SYSTEM IN $\text{Mat}_2(\mathbb{Z})$.

By restricting the order of the matrix we may relax the condition on the diagonable matrix.

**Lemma 3.** Let $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \in \text{Mat}_2(\mathbb{Z})$ with $\det U \neq 0$, then

1. $I_o = \{a \in \mathbb{Z} : U \begin{pmatrix} a & \alpha \\ \beta & r \end{pmatrix}$ for some $\alpha, \beta, r \in \mathbb{Z}\}$ and

   $I'_o = \{a \in \mathbb{Z} : U \begin{pmatrix} 0 & 0 \\ a & \delta \end{pmatrix}$ for some $\delta \in \mathbb{Z}\}$ are nonzero principal ideals of $\mathbb{Z}$ generated by a positive integer $d = \text{g.c.d.}(u_{11}, u_{12})$. Moreover $I_o = I'_o$.

2. $I_1 = \{a \in \mathbb{Z} : U \begin{pmatrix} 0 & a \\ \beta & r \end{pmatrix}$ for some $\beta, r \in \mathbb{Z}\}$ and

   $I'_1 = \{a \in \mathbb{Z} : U \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}\}$ are nonzero principal ideals of $\mathbb{Z}$ generated by a positive integer $\frac{|\det U|}{d}$. Moreover, $I_1 = I'_1$.

**Proof.** (1) $a \in I_o$ implies $U \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & \alpha \\ \beta & r \end{pmatrix}$, i.e., $a \in I'_o$. This shows that $I_o \subseteq I'_o$.

On the other hand, $b \in I'_o$ implies $U \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ b & \delta \end{pmatrix}$, i.e., $b \in I_o$. Therefore $I_o = I'_o$. It is clear that $I_o$ is an ideal of $\mathbb{Z}$. Now $\det U \in I_o$, for $U \begin{pmatrix} \det U & 0 \\ 0 & \det U \end{pmatrix}$.

Thus $I_o$ is a nonzero ideal of $\mathbb{Z}$. But $\mathbb{Z}$ is a P.I.D., therefore $I_o$ is an ideal generated by a positive integer $d$. Since $U \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} U = \begin{pmatrix} u_{21} & u_{22} \\ 0 & 0 \end{pmatrix}$, we have $u_{11}, u_{12} \in I_o$, and then $d | u_{11}$, $d | u_{21}$. By $d \in I_o$, we have

$U \begin{pmatrix} 0 & 0 \\ d & \delta \end{pmatrix}$, i.e., $U \begin{pmatrix} 0 & 0 \\ d & \delta \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} U$ for some $\begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \in \text{Mat}_2(\mathbb{Z})$.

Therefore $d = t_{21} u_{11} + t_{22} u_{21}$. If $x | u_{11}$ and $x | u_{21}$, then $x | d$. Thus $d = \text{g.c.d.}(u_{11}, u_{21})$. 


(2) \( a \in I_1 \) implies \( U \mid \begin{pmatrix} 0 & a \\ \beta & r \end{pmatrix} \) for some \( \beta, r \in \mathbb{Z} \) and then
\[ U \mid \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & a \\ \beta & r \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \] i.e., \( a \in I'_1 \). Thus \( I_1 \subseteq I'_1 \). Conversely, if \( b \in I'_1 \), then \( U \mid \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} \) and so \( U \mid \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \) i.e., \( b \in I'_1 \). It is also clear that \( I_1 \) is an ideal of \( \mathbb{Z} \). Now \( \frac{\text{det} U}{d} \in I_1 \) for all \( U \) such that \( \begin{pmatrix} 0 & 0 \\ 0 & \text{det} U/d \end{pmatrix} = \begin{pmatrix} -u_{21} & u_{12} \\ -u_{21} & u_{11} \end{pmatrix} U, \) and then \( I_1 \) is a nonzero ideal of \( \mathbb{Z} \). But \( \mathbb{Z} \) is a P.I.D., and then \( I_1 \) is an ideal generated by a positive integer \( g \). Now \( \frac{\text{det} U}{d} \in I_1 \) implies \( \frac{\text{det} U}{d} \in I_1 \), i.e., \( g \mid \frac{\text{det} U}{d} \). By \( g \in I_1 \), we have
\[ U \mid \begin{pmatrix} 0 & 0 \\ 0 & g \end{pmatrix}, \] i.e., \( \text{det} U \mid \begin{pmatrix} u_{11} & -u_{12} \\ -u_{21} & u_{11} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -gu_{21} & gu_{11} \end{pmatrix}, \) and then
\[ \text{det} U \mid gu_{21}, \quad \text{det} U \mid gu_{11}. \]

By the proof of (1), we have \( d = t_{21} u_{11} + t_{22} u_{21} \), and then
\[ gd = t_{21} (gu_{11}) + t_{22} (gu_{21}) \text{ or } \frac{\text{det} U}{d} \mid g. \] Therefore \( g = \frac{\text{det} U}{d} \). This completes the proof of (2).

**Theorem 2.** Let \( U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}) \) with \( \text{det} U \neq 0 \), let
\[ d = \text{g.c.d.}(u_{11}, u_{21}). \] Then \( J = \{ R = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}) : 0 \leq r_{11}, \] \( r_{21} < d, 0 \leq r_{12}, r_{22} < \frac{\text{det} U}{d} \} \) is a complete residue system (mod. \( U \)) in \( \text{Mat}_2(\mathbb{Z}) \).

**Proof.** (1) From \( d \in I_o, \frac{\text{det} U}{d} \in I_1 \), we have
\[ U \mid \begin{pmatrix} d & a \\ \beta & r \end{pmatrix}, \quad U \mid \begin{pmatrix} 0 & 0 \\ d & \eta \end{pmatrix}, \quad U \mid \begin{pmatrix} 0 & \frac{\text{det} U}{d} \\ \varepsilon & \delta \end{pmatrix}, \quad U \mid \begin{pmatrix} 0 & 0 \\ 0 & \frac{\text{det} U}{d} \end{pmatrix}, \] i.e.,
there exists $T_i \in \text{Mat}_2(\mathbb{Z})$, $i = 1, 2, 3, 4$ such that
\[
\begin{pmatrix}
d & a \\
b & r
\end{pmatrix} = T_1 U, 
\begin{pmatrix}
d & 0 \\
|\text{det}U| & d
\end{pmatrix} = T_2 U, 
\begin{pmatrix}
o & 0 \\
o & d
\end{pmatrix} = T_3 U, 
\begin{pmatrix}
0 & 0 \\
|\text{det}U| & 0
\end{pmatrix} = T_4 U.
\]

For any matrix $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \text{Mat}_2(\mathbb{Z})$, there exists $p_{11}, r_{11} \in \mathbb{Z}$ such that $a_{11} = p_{11}d + r_{11}$ where $0 \leq r_{11} < d$. Thus $A - p_{11}T_1 U = \begin{pmatrix} r_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, for some $b_{12, b_{21}, b_{22}} \in \mathbb{Z}$. Moreover, $b_{12} = p_{12} \frac{|\text{det}U|}{d} + r_{12}$ for some $p_{12}, r_{12} \in \mathbb{Z}, 0 \leq r_{12} < \frac{|\text{det}U|}{d}$. Then $A - p_{11}T_1 U - p_{12}T_2 U = \begin{pmatrix} r_{11} & r_{12} \\ c_{21} & c_{22} \end{pmatrix}$ for some $c_{21, c_{22}} \in \mathbb{Z}$. Again $c_{21} = p_{21} - d + r_{21}$ for some $p_{21}, r_{21} \in \mathbb{Z}$, $0 \leq r_{21} < d$. Then $A - p_{11}T_1 U - p_{12}T_2 U - p_{21}T_3 U = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}$ for some $d_{22} \in \mathbb{Z}$. Finally $d_{22} = p_{22} \frac{|\text{det}U|}{d} + r_{22}$ for some $p_{22}, r_{22} \in \mathbb{Z}, 0 \leq r_{22} < \frac{|\text{det}U|}{d}$, implies $A - p_{11}T_1 U - p_{12}T_2 U - p_{21}T_3 U - p_{22}T_4 U = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}$ or
\[
A - \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}, \text{ where } 0 \leq r_{11}, r_{21} < d, 0 \leq r_{22}, r_{12} < \frac{|\text{det}U|}{d}.
\]
This proves that for any matrix $A \in \text{Mat}_2(\mathbb{Z})$ there exists $R \in \mathcal{J}_2$ such that $A \equiv R(\text{mod. } U)$.

(2) Assume that $\begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} \equiv \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \pmod{U}$ where $0 \leq r_{11}, r_{21}, s_{11}, s_{21} < d, 0 \leq r_{12}, r_{22}, s_{12}, s_{22} < \frac{|\text{det}U|}{d}$. 

This implies
\[ U \left( \begin{array}{cc} r_{11}-s_{11} & r_{12}-s_{12} \\ r_{21}-s_{21} & r_{22}-s_{22} \end{array} \right), \text{i.e., } r_{11}-s_{11} \in \mathbb{I}, \text{ or } d \mid r_{11}-s_{11}. \]

Now \( 0 < |r_{11}-s_{11}| < d, \) \( r_{11} = s_{11}. \) It follows that \( U \left( \begin{array}{cc} 0 & r_{12}-s_{12} \\ r_{21}-s_{21} & r_{22}-s_{22} \end{array} \right), \)
\[ \text{i.e., } r_{12}-s_{12} \in \mathbb{I}, \] or \( d \mid (r_{12}-s_{12}). \) But \( 0 < |r_{12}-s_{12}| < \frac{|\det U|}{d}, \)
so that \( r_{12} = s_{12}. \)

It follows that
\[ U \left( \begin{array}{cc} 0 & 0 \\ r_{21}-s_{21} & r_{22}-s_{22} \end{array} \right), \text{i.e., } r_{21}-s_{21} \in \mathbb{I}, \text{ or } d \mid (r_{21}-s_{21}). \]

Also \( 0 < |r_{21}-s_{21}| < d, \) so that \( r_{21} = s_{21}. \) This implies that \( U \left( \begin{array}{cc} 0 & 0 \\ 0 & r_{22}-s_{22} \end{array} \right), \)
\[ \text{i.e., } r_{22}-s_{22} \in \mathbb{I}, \] or \( d \mid (r_{22}-s_{22}). \) Finally \( 0 < |r_{22}-s_{22}| < \frac{|\det U|}{d}, \)
so that \( r_{22} = s_{22}, \) i.e., \( \left( \begin{array}{cc} r_{11} & r_{12} \\ r_{21} & r_{22} \end{array} \right) = \left( \begin{array}{cc} s_{11} & s_{12} \\ s_{21} & s_{22} \end{array} \right). \) This proves that any
two elements in \( J_2 \) are incongruent.

**COROLLARY 3.** Let \( U \in \text{Mat}_2(\mathbb{Z}) \) with \( \det U \neq 0. \) Then the cardinality of the
complete residue system \( (\text{mod. } U) \) is \( |\det U|^2. \)

**REMARK.** If we consider the ring of \( 3 \times 3 \) matrices, the corresponding
results will read as follows, the proofs will be as in Lemma 3 and Theorem 2,
with possible minor changes.

**LEMMA 4.** Let \( U = \left( u_{ij} \right) \in \text{Mat}_3(\mathbb{Z}) \) with \( \det U \neq 0. \) Then

(1) \( \mathbb{I}_o = \{ a \in \mathbb{Z} : U \left( \begin{array}{ccc} a & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array} \right) \text{ for some } a_{ij} \in \mathbb{Z} \}, \)
are nonzero principal ideals of \( Z \) generated by the positive integer
\[ g_0 = g.c.d.(u_{11}, u_{21}, u_{31}) \]. Moreover, \( I_0 = I'_0 = I''_0 \).

(2) \[ I_2 = \{ a \in Z : U \begin{pmatrix} a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \text{ for some } a_{ij} \in Z \}, \]
\[ I'_2 = \{ a \in Z : U \begin{pmatrix} 0 & 0 & a \\ 0 & 0 & a \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \text{ for some } a_{ij} \in Z \}, \]
\[ I''_2 = \{ a \in Z : U \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & a \end{pmatrix} \} \]
are nonzero principal ideals of \( Z \) generated by the positive integer
\[ g_2 = \frac{|\det U|}{g'}, \text{ where } g' = g.c.d.(cofu_{13}, cofu_{23}, cofu_{33}), \text{ and} \]
cofu_{ij} is the cofactor of the element \( u_{ij} \). Moreover, \( I_2 = I'_2 = I''_2 \).

(3) \[ I_1 = \{ a \in Z : U \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \text{ for some } a_{ij} \in Z \}, \]
\[ I'_1 = \{ a \in Z : U \begin{pmatrix} 0 & 0 & 0 \\ 0 & a & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \text{ for some } a_{ij} \in Z \}, \]
\[ I''_1 = \{ a \in Z : U \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & a_{33} \end{pmatrix} \} \]
are nonzero principal ideals of \( \mathbb{Z} \) generated by the positive integer \( g_1 = \frac{R}{g_0} \). Moreover, \( I_1 = I'_1 = I''_1 \).

**THEOREM 3.** Let \( U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{pmatrix} \in \text{Mat}_3(\mathbb{Z}) \) with \( \det U \neq 0 \), let 

\[
g_0 = \text{g.c.d.}(u_{11}, u_{21}, u_{31}), \quad g' = \text{g.c.d.}(\text{cofu}_{13}, \text{cofu}_{23}, \text{cofu}_{33}).
\]

Then 

\[
J_3 = \{ R = [r_{ij}] \in \text{Mat}_3(\mathbb{Z}) : 0 \leq r_{ij} < g_{j-1} \quad i,j = 1,2,3 \}
\]

is a complete residue system (mod. \( U \)) where \( g_1 = \frac{R'}{g_0}, \quad g_2 = \frac{|\det U|}{g} \).

**REFERENCE**