Internat. J. Math. & Math. Sci.
Vol. 1 (1978) 217-225

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×n matrix, in the ring of n×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 Z denote the ring of rational integers and Z(i) be the ring of

Gaussian integers. Jordan and Potratz [1] have exhibited several representations 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 2×2 matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, a, b in 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 $Mat_n(Z)$.

2. THE COMPLETE RESIDUE SYSTEM IN $Mat_n(Z)$.

First of all, we define $A|B$ mean there is a matrix C such that $B = CA$, and $A \equiv B$ mod. U means that $U|A - B$. Now we can give a definition of the C.R.S. mod. U in the ring of $Mat_n(Z)$.

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

LEMMA 1. Let $G = \mathrm{diag}(g_1,g_2,\ldots,g_n)$ with $g_i \neq 0$, $i = 1,2,\ldots,n$. Let E_{ij} be the matrix units, then

$$I_{ik} = \{a\varepsilon Z : G|\sum_{m=i}^{n}\sum_{j=1}^{n} a_{mj}E_{mj} \text{ where } a_{mj} \text{ in } Z, a_{i1}=a_{i2}=\ldots=a_{ik-1}=0,\ a_{ik}=a\}$$

are 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 Z. But Z is a P.I.D., therefore I_{ik} are principal ideals generated by a positive integer d_{ik}. Since $g_kE_{ik} = E_{ik}G$, then g_k is in I_{ik}, i.e., $d_{ik}|g_k$. On the other hand, for d_{ik} in I_{ik} we have $\sum_{m=i}^{n}\sum_{j=1}^{n} a_{mj}E_{mj} = (t_{ik})G$ for some (t_{ik}), where a_{mj} is in Z, $a_{i1}=a_{i2}=\ldots=a_{ik-1}=0$, $a_{ik}=d_{ik}$. 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_{ik}, r_{ik} in Z such that $a_{ik} = p_{ik}\,|g_k| + r_{ik}$, where $0 \leq r_{ik} < |g_k|$. Therefore

$A - (p_{ik} \cdot |g_k|) = (r_{ik})$. But $|g_k| \cdot E_{ik} = |g_k| \cdot g_k^{-1} E_{ik}G$, and therefore $G \mid A - (r_{ik})$. This shows that $A \equiv (r_{ik})$ mod. G.

(2) If $(r_{ik}) \equiv (s_{ik})$ mod. G, where $0 \leq r_{ik}, s_{ik} < |g_k|$, then $G \mid (r_{ik} - s_{ik})$, i.e., $r_{11} - s_{11}$ is in I_{11} (by Lemma 1). This implies that $g_1 \mid (r_{11} - s_{11})$, 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 $g_2 \mid (r_{12} - s_{12})$ 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×n matrix with $\det G \neq 0$, and if U and V are unimodular n×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×n matrix A, there exists a matrix(r_{ik}) with $0 \leq r_{ik} < |g_k|$ such that $AV \equiv (r_{ik})$ mod. UGV., i.e., $A \equiv (r_{ik})V^{-1}$ 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 $(r_{ik}) \equiv (s_{ik})$ mod. UGV. Therefore $(r_{ik}) = (s_{ik})$.

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

COROLLARY 2. If G is a n×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 $Mat_2(Z)$.

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

LEMMA 3. Let $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \varepsilon\ Mat_2(Z)$ with $\det U \neq 0$, then

(1) $I_o = \{a \varepsilon Z : U \mid \begin{pmatrix} a & \alpha \\ \beta & r \end{pmatrix}$ for some $\alpha, \beta, r \varepsilon Z\}$ and

$I_o' = \{a \varepsilon Z : U \mid \begin{pmatrix} 0 & 0 \\ a & \delta \end{pmatrix}$ for some $\delta \varepsilon Z\}$ are nonzero principal ideals of Z generated by a positive integer $d = g.c.d.(u_1, u_2)$. Moreover $I_o = I_o'$.

(2) $I_1 = \{a \varepsilon Z : U \mid \begin{pmatrix} 0 & a \\ \beta & r \end{pmatrix}$ for some $\beta, r \varepsilon Z\}$ and

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

PROOF. (1) $a \varepsilon I_o$ implies $U \mid \begin{pmatrix} a & \alpha \\ \beta & r \end{pmatrix}$ for some $\alpha, \beta, r \varepsilon Z$, and then $U \mid \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & \alpha \\ \beta & r \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a & \alpha \end{pmatrix}$, i.e., $a \varepsilon I_o'$. This shows that $I_o \subseteq I_o'$. On the other hand, $b \varepsilon I_o'$ implies $U \mid \begin{pmatrix} 0 & 0 \\ b & \delta \end{pmatrix}$ for some $\delta \varepsilon Z$ and then $U \mid \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ b & \delta \end{pmatrix} = \begin{pmatrix} b & \delta \\ 0 & 0 \end{pmatrix}$, i.e., $b \varepsilon I_o$. Therefore $I_o = I_o'$. It is clear that I_o is an ideal of Z. Now $\det U \varepsilon I_o$, for $U \mid \begin{pmatrix} \det U & 0 \\ 0 & \det U \end{pmatrix}$.
Thus I_o is a nonzero ideal of Z. But Z is a P.I.D., therefore I_o is an ideal generated by a positive integer d. Since $U|U$ implies $U \mid \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} U = \begin{pmatrix} U_{21} & U_{22} \\ 0 & 0 \end{pmatrix}$, we have $U_{11}, U_{12} \varepsilon I_o$, and then $d|U_{11}$, $d|U_{21}$. By $d \varepsilon I_o$, we have $U \mid \begin{pmatrix} 0 & 0 \\ d & \delta \end{pmatrix}$, i.e., $\begin{pmatrix} 0 & 0 \\ d & \delta \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} U$ for some $\begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \varepsilon\ Mat_2(Z)$.
Therefore $d = t_{21}U_{11} + t_{22}U_{21}$. If $x|U_{11}$ and $x|U_{21}$, then $x|d$. Thus $d = g.c.d.(U_{11}, U_{21})$.

(2) $a \in I_1$ implies $U \mid \begin{pmatrix} 0 & a \\ \beta & r \end{pmatrix}$ for some β, $r \in Z$ and then $U \mid \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & a \\ \beta & r \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$, 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 $U \mid \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, i.e., $b \in I_1$. It is also clear that I_1 is an ideal of Z. Now $\frac{\det U}{d} \in I_1$ for all U such that $\begin{pmatrix} 0 & 0 \\ 0 & \frac{\det U}{d} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \frac{-u_{21}}{d} & \frac{u_{12}}{d} \end{pmatrix} U$, and then I_1 is a nonzero ideal of Z. But Z is a P.I.D., and then I_1 is an ideal generated by a positive integer g. Now $\frac{\det U}{d} \in I_1$ implies $\frac{\det U}{d} \in I_1$, i.e., $g \mid \frac{|\det U|}{d}$. By $g \in I_1$, we have $U \mid \begin{pmatrix} 0 & 0 \\ 0 & g \end{pmatrix}$, i.e., $\det U \mid \begin{pmatrix} 0 & 0 \\ 0 & g \end{pmatrix}\begin{pmatrix} u_{22} & -u_{12} \\ -u_{21} & u_{11} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -gu_{21} & gu_{11} \end{pmatrix}$, and then $\det U \mid gU_{21}$, $\det U \mid gU_{11}$.

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

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

PROOF. (1) From $d \in I_0$, $\frac{|\det U|}{d} \in I_1$, we have

$$U \,\Big|\, \begin{pmatrix} d & \alpha \\ \beta & r \end{pmatrix},\ U \,\Big|\, \begin{pmatrix} 0 & 0 \\ d & \eta \end{pmatrix},\ U \,\Big|\, \begin{pmatrix} 0 & \frac{|\det U|}{d} \\ \varepsilon & \delta \end{pmatrix},\ U \,\Big|\, \begin{pmatrix} 0 & 0 \\ 0 & \frac{|\det U|}{d} \end{pmatrix}, \text{ i.e.,}$$

there exists $T_i \in Mat_2(Z)$, $i = 1,2,3,4$ such that

$$\begin{pmatrix} d & \alpha \\ \beta & r \end{pmatrix} = T_1U, \quad \begin{pmatrix} 0 & \frac{|detU|}{d} \\ \varepsilon & \delta \end{pmatrix} = T_2U, \quad \begin{pmatrix} 0 & 0 \\ d & \eta \end{pmatrix} = T_3U, \quad \begin{pmatrix} 0 & 0 \\ 0 & \frac{|detU|}{d} \end{pmatrix} = T_4U.$$

For any matrix $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in Mat_2(Z)$, there exists p_{11}, $r_{11} \in Z$ such that $a_{11} = p_{11}d + r_{11}$ where $0 \le r_{11} < d$. Thus $A - p_{11}T_1U = \begin{pmatrix} r_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, for some $b_{12}, b_{21}, b_{22} \in Z$. Moreover, $b_{12} = P_{12}\frac{|detU|}{d} + r_{12}$ for some p_{12}, $r_{12} \in Z$, $0 \le r_{12} < \frac{|detU|}{d}$. Then $A - p_{11}T_1U - p_{12}T_2U = \begin{pmatrix} r_{11} & r_{12} \\ c_{21} & c_{22} \end{pmatrix}$ for some $c_{21}, c_{22} \in Z$. Again $c_{21} = p_{21} - d + r_{21}$ for some $p_{21}, r_{21} \in Z$, $0 \le r_{21} < d$. Then $A - p_{11}T_1U - p_{12}T_2U - p_{21}T_3U = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}$ for some $d_{22} \in Z$. Finally $d_{22} = p_{22}\frac{|detU|}{d} + r_{22}$ for some $p_{22}, r_{22} \in Z$, $0 \le r_{22} < \frac{|detU|}{d}$, implies $A - p_{11}T_1U - p_{12}T_2U - p_{21}T_3U - p_{22}T_4U = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}$ or

$$U \,\Big|\, A - \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}, \text{ where } 0 \le r_{11}, r_{21} < d,\ 0 \le r_{22}, r_{12} < \frac{|detU|}{d}.$$

This proves that for any matrix $A \in Mat_2(Z)$ there exists $R \in J_2$ such that $A \equiv R(\text{mod. } U)$.

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

This implies

$$U \,\Big|\, \begin{pmatrix} r_{11}-s_{11} & r_{12}-s_{12} \\ r_{21}-s_{21} & r_{22}-s_{22} \end{pmatrix}, \text{ i.e., } r_{11} - s_{11} \in I_o, \text{ or } d \mid r_{11} - s_{11}.$$

Now $0 \leq |r_{11} - s_{11}| < d$, $r_{11} = s_{11}$. It follows that $U \,\Big|\, \begin{pmatrix} 0 & r_{12}-s_{12} \\ r_{21}-s_{21} & r_{22}-s_{22} \end{pmatrix}$, i.e., $r_{12} - s_{12} \in I_1$, or $\frac{|\det U|}{d} \,\Big|\, (r_{12} - s_{12})$. But $0 \leq |r_{12}-s_{12}| < \frac{|\det U|}{d}$, so that $r_{12} = s_{12}$.

It follows that

$$U \,\Big|\, \begin{pmatrix} 0 & 0 \\ r_{21}-s_{21} & r_{22}-s_{22} \end{pmatrix}, \text{ i.e., } r_{21} - s_{21} \in I_o \text{ or } d \mid (r_{21} - s_{21}).$$

Also $0 \leq |r_{21}-s_{21}| < d$, so that $r_{21} = s_{21}$. This implies that $U \,\Big|\, \begin{pmatrix} 0 & 0 \\ 0 & r_{22}-s_{22} \end{pmatrix}$, i.e., $r_{22} - s_{22} \in I_1$ or $\frac{|\det U|}{d} \,\Big|\, (r_{22} - s_{22})$. Finally $0 \leq |r_{22}-s_{22}| < \frac{|\det U|}{d}$, so that $r_{22} = s_{22}$, i.e., $\begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$. This proves that any two elements in J_2 are incongruent.

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

REMARK. If we consider the ring of 3×3 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 $u = \left(u_{ij}\right) \in \mathrm{Mat}_3(Z)$ with $\det U \neq 0$. Then

(1) $I_o = \{a \in Z : U \begin{pmatrix} a & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix}$ for some $\alpha_{ij} \in Z\}$,

$$I_o' = \{a \in Z : U \left| \begin{pmatrix} 0 & 0 & 0 \\ a & \alpha_{21} & \alpha_{22} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \right. \text{ for some } \alpha_{ij} \in Z\}.$$

$$I_o'' = \{a \in Z : U \left| \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ a & \alpha_{32} & \alpha_{33} \end{pmatrix} \right. \text{ for some } \alpha_{32}, \alpha_{33} \in Z\}$$

are nonzero principal ideals of Z generated by the positive integer $g_o = \text{g.c.d.}(u_{11}, u_{21}, u_{31})$. Moreover, $I_o = I_o' = I_o''$.

(2) $$I_2 = \{a \in Z : U \begin{pmatrix} 0 & 0 & a \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \text{ for some } \alpha_{ij} \in Z\},$$

$$I_2' = \{a \in Z : U \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \text{ for some } \alpha_{ij} \in Z\},$$

$$I_2'' = \{a \in Z : U \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & a \end{pmatrix}\}$$

are nonzero principal ideals of Z generated by the positive integer $g_2 = \frac{|\det U|}{g'}$, where $g' = \text{g.c.d.}(\text{cof}u_{13}, \text{cof}u_{23}, \text{cof}u_{33})$, and $\text{cof}u_{ij}$ is the cofactor of the element u_{ij}. Moreover, $I_2 = I_2' = I_2''$.

(3) $$I_1 = \{a \in Z : U \left| \begin{pmatrix} 0 & a_1 & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \right. \text{ for some } \alpha_{ij} \in Z\}$$

$$I_1' = \{a \in Z : U \left| \begin{pmatrix} 0 & 0 & 0 \\ 0 & a & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \right. \text{ for some } \alpha_{ij} \in Z\}$$

$$I_1'' = \{a \in Z : U \left| \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \alpha_{33} \end{pmatrix} \right. \text{ for some } \alpha_{33} \in Z\}$$

are nonzero principal ideals of Z generated by the positive integer $g_1 = \frac{g'}{g_o}$.
Moreover, $I_1 = I_1' = I_1''$.

THEOREM 3. Let $U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{pmatrix} \varepsilon \ \mathrm{Mat}_3(Z)$ with $\det U \neq 0$, let $g_o = \text{g.c.d.}(u_{11}, u_{21}, u_{31})$, $g' = \text{g.c.d.}(\mathrm{cof}u_{13}, \mathrm{cof}u_{23}, \mathrm{cof}u_{33})$. Then $J_3 = \{R = [r_{ij}] \ \varepsilon \ \mathrm{Mat}_3(Z) : 0 \leq r_{ij} < g_{j-1} \quad i,j = 1,2,3\}$ is a complete residue system (mod. U) where $g_1 = \frac{g'}{g_o}$, $g_2 = \frac{|\det U|}{g'}$.

REFERENCE

1. Jordan, J. H. and C. J. Potratz. Complete Residue Systems in the Gaussian Integers, Math. Mag. 38 (1965) 1-12.