

F is a field, and $\mathbf{u}, \mathbf{v}, \mathbf{w} \in F$. $\text{MAT}_{3 \times 5}(F)$ is the set of 3×5 -matrices in F , written $\text{MAT}(F)$ if the 3×5 is understood or $\text{MAT}_{3 \times 5}$ if the field is understood, or just MAT if both are understood.

For $A \in \text{MAT}_{3 \times 5}$, let L_A be the *lefthand action* of A ; the linear trn mapping F^5 to F^3 , sending column-vectors to column-vectors.

For p an odd prime, always give answers in *symmetric residues*, e.g working over $\mathbb{Z}_{17}$, answers should be in $[-8..8]$. The phrase “*working over*” a field F means that all vectors, matrices, LinCombs etc., are over that field. If the field is $\mathbb{Z}_p$, then $\equiv$ means $\equiv_p$. E.g: “*Working over $\mathbb{Z}_{19}$, compute the determinant and inverse of $M := \begin{bmatrix} 21 & 15 \\ 10 & 4 \end{bmatrix}$.*”

Soln. Reducing, $M \equiv \begin{bmatrix} 2 & -4 \\ -9 & 4 \end{bmatrix}$, so $D := \text{Det}(M)$ equals

$$2 \cdot 4 - [-4][-9] = 8 - 36 \equiv 8 - 28 \equiv 8 + 2 = 10 \equiv -9.$$

Hence reciprocal $R := \langle 1 \div D \rangle_{19} = 2$. Thus

$$M^{-1} \equiv R \cdot \begin{bmatrix} 4 & 4 \\ 9 & 2 \end{bmatrix} = \begin{bmatrix} 8 & 8 \\ 18 & 4 \end{bmatrix} \equiv \begin{bmatrix} 8 & 8 \\ -1 & 4 \end{bmatrix}.$$

Checking

$$\begin{bmatrix} 2 & -4 \\ -9 & 4 \end{bmatrix} \cdot \begin{bmatrix} 8 & 8 \\ -1 & 4 \end{bmatrix} \stackrel{\text{expect}}{=} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \quad \blacklozenge$$

“*Working over $\mathbb{C}$, compute the determinant of $B := \begin{bmatrix} 2+i & 3 \\ 1 & 1+i \end{bmatrix}$. Compute s , the $(1, 2)$ -entry of B^{-1} .*”

Well, $\delta := \text{Det}(B) = -2 + 3i$. Thus $\frac{1}{\delta} = \bar{\delta}/|\delta|^2 = \bar{\delta}/13$. So $13s$ equals $\bar{\delta} \cdot [-3] = 6 + 9i$. So $s = \frac{6}{13} + \frac{9}{13}i$. $\blacklozenge$

§A Reciprocal tables in $\mathbb{Z}_p$

RECIPROCAL TABLES

$$\text{Modulo } 2: \begin{array}{c|c} x & \langle 1/x \rangle_2 \\ \hline 1 & 1 \end{array}$$

$$\text{Modulo } 3: \begin{array}{c|c} x & \langle 1/x \rangle_3 \\ \hline \pm 1 & \pm 1 \end{array}$$

$$\text{Modulo } 5: \begin{array}{c|c} x & \langle 1/x \rangle_5 \\ \hline \pm 1 & \pm 1 \end{array} \quad \parallel \quad \begin{array}{c|c} x & \langle 1/x \rangle_5 \\ \hline \pm 2 & \mp 2 \end{array}$$

$$\text{Modulo } 7: \begin{array}{c|c} x & \langle 1/x \rangle_7 \\ \hline \pm 1 & \pm 1 \\ \pm 2 & \mp 3 \end{array} \quad \parallel \quad \begin{array}{c|c} x & \langle 1/x \rangle_7 \\ \hline \pm 3 & \mp 2 \end{array}$$

$$\text{Modulo } 11: \begin{array}{c|c} x & \langle 1/x \rangle_{11} \\ \hline \pm 1 & \pm 1 \\ \pm 2 & \mp 5 \\ \pm 3 & \pm 4 \end{array} \quad \parallel \quad \begin{array}{c|c} x & \langle 1/x \rangle_{11} \\ \hline \pm 4 & \pm 3 \\ \pm 5 & \mp 2 \end{array}$$

$$\text{Modulo } 13: \begin{array}{c|c} x & \langle 1/x \rangle_{13} \\ \hline \pm 1 & \pm 1 \\ \pm 2 & \mp 6 \\ \pm 3 & \pm 4 \end{array} \quad \parallel \quad \begin{array}{c|c} x & \langle 1/x \rangle_{13} \\ \hline \pm 4 & \mp 3 \\ \pm 5 & \mp 5 \\ \pm 6 & \mp 2 \end{array}$$

$$\text{Modulo } 17: \begin{array}{c|c} x & \langle 1/x \rangle_{17} \\ \hline \pm 1 & \pm 1 \\ \pm 2 & \mp 8 \\ \pm 3 & \pm 6 \\ \pm 4 & \mp 4 \end{array} \quad \parallel \quad \begin{array}{c|c} x & \langle 1/x \rangle_{17} \\ \hline \pm 5 & \pm 7 \\ \pm 6 & \pm 3 \\ \pm 7 & \pm 5 \\ \pm 8 & \mp 2 \end{array}$$

$$\text{Modulo } 19: \begin{array}{c|c} x & \langle 1/x \rangle_{19} \\ \hline \pm 1 & \pm 1 \\ \pm 2 & \mp 9 \\ \pm 3 & \mp 6 \\ \pm 4 & \pm 5 \\ \pm 5 & \pm 4 \end{array} \quad \parallel \quad \begin{array}{c|c} x & \langle 1/x \rangle_{19} \\ \hline \pm 6 & \mp 3 \\ \pm 7 & \mp 8 \\ \pm 8 & \mp 7 \\ \pm 9 & \mp 2 \end{array}$$

$$\text{Modulo } 23: \begin{array}{c|c} x & \langle 1/x \rangle_{23} \\ \hline \pm 1 & \pm 1 \\ \pm 2 & \mp 11 \\ \pm 3 & \pm 8 \\ \pm 4 & \pm 6 \\ \pm 5 & \mp 9 \\ \pm 6 & \pm 4 \end{array} \quad \parallel \quad \begin{array}{c|c} x & \langle 1/x \rangle_{23} \\ \hline \pm 7 & \pm 10 \\ \pm 8 & \pm 3 \\ \pm 9 & \mp 5 \\ \pm 10 & \pm 7 \\ \pm 11 & \mp 2 \end{array}$$

MULTIPLICATION

7	2	3
2	-3	
3	-1	2

11	2	3	4	5
2	4			
3	-5	-2		
4	-3	1	5	
5	-1	4	-2	3

13	2	3	4	5	6
2	4				
3	6	-4			
4	-5	-1	3		
5	-3	2	-6	-1	
6	-1	5	-2	4	-3

17	2	3	4	5	6	7	8
2	4						
3	6	-8					
4	8	-5	-1				
5	-7	-2	3	8			
6	-5	1	7	-4	2		
7	-3	4	-6	1	8	-2	
8	-1	7	-2	6	-3	5	-4

19	2	3	4	5	6	7	8	9
2	4							
3	6	9						
4	8	-7	-3					
5	-9	-4	1	6				
6	-7	-1	5	-8	-2			
7	-5	2	9	-3	4	-8		
8	-3	5	-6	2	-9	-1	7	
9	-1	8	-2	7	-3	6	-4	5

23	2	3	4	5	6	7	8	9	10	11
2	4									
3	6	9								
4	8	-11	-7							
5	10	-8	-3	2						
6	-11	-5	1	7	-10					
7	-9	-2	5	-11	-4	3				
8	-7	1	9	-6	2	10	-5			
9	-5	4	-10	-1	8	-6	3	-11		
10	-3	7	-6	4	-9	1	11	-2	8	
11	-1	10	-2	9	-3	8	-4	7	-5	6