

Linear Algebra 1: Tutorial 1

Irena Penev

Adam Morawski

Winter 2026

$\mathbb{Z}_2 :$	<table><tr><td>+</td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	+	0	1	0	0	1	1	1	0	<table><tr><td>·</td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td></tr></table>	·	0	1	0	0	0	1	0	1																																																						
+	0	1																																																																								
0	0	1																																																																								
1	1	0																																																																								
·	0	1																																																																								
0	0	0																																																																								
1	0	1																																																																								

$\mathbb{Z}_3 :$	<table><tr><td>+</td><td>0</td><td>1</td><td>2</td></tr><tr><td>0</td><td>0</td><td>1</td><td>2</td></tr><tr><td>1</td><td>1</td><td>2</td><td>0</td></tr><tr><td>2</td><td>2</td><td>0</td><td>1</td></tr></table>	+	0	1	2	0	0	1	2	1	1	2	0	2	2	0	1	<table><tr><td>·</td><td>0</td><td>1</td><td>2</td></tr><tr><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td><td>2</td></tr><tr><td>2</td><td>0</td><td>2</td><td>1</td></tr></table>	·	0	1	2	0	0	0	0	1	0	1	2	2	0	2	1																																								
+	0	1	2																																																																							
0	0	1	2																																																																							
1	1	2	0																																																																							
2	2	0	1																																																																							
·	0	1	2																																																																							
0	0	0	0																																																																							
1	0	1	2																																																																							
2	0	2	1																																																																							

$\mathbb{Z}_5 :$	<table><tr><td>+</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td></tr><tr><td>0</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td></tr><tr><td>1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>0</td></tr><tr><td>2</td><td>2</td><td>3</td><td>4</td><td>0</td><td>1</td></tr><tr><td>3</td><td>3</td><td>4</td><td>0</td><td>1</td><td>2</td></tr><tr><td>4</td><td>4</td><td>0</td><td>1</td><td>2</td><td>3</td></tr></table>	+	0	1	2	3	4	0	0	1	2	3	4	1	1	2	3	4	0	2	2	3	4	0	1	3	3	4	0	1	2	4	4	0	1	2	3	<table><tr><td>·</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td></tr><tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td></tr><tr><td>2</td><td>0</td><td>2</td><td>4</td><td>1</td><td>3</td></tr><tr><td>3</td><td>0</td><td>3</td><td>1</td><td>4</td><td>2</td></tr><tr><td>4</td><td>0</td><td>4</td><td>3</td><td>2</td><td>1</td></tr></table>	·	0	1	2	3	4	0	0	0	0	0	0	1	0	1	2	3	4	2	0	2	4	1	3	3	0	3	1	4	2	4	0	4	3	2	1
+	0	1	2	3	4																																																																					
0	0	1	2	3	4																																																																					
1	1	2	3	4	0																																																																					
2	2	3	4	0	1																																																																					
3	3	4	0	1	2																																																																					
4	4	0	1	2	3																																																																					
·	0	1	2	3	4																																																																					
0	0	0	0	0	0																																																																					
1	0	1	2	3	4																																																																					
2	0	2	4	1	3																																																																					
3	0	3	1	4	2																																																																					
4	0	4	3	2	1																																																																					

Fermat's Little Theorem. If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is **not** a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.

Fermat's Little Theorem. If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.

$$\left[\begin{array}{cccccccccccc} 0 & \blacksquare & * & * & * & * & * & * & * & * & * \\ 0 & 0 & 0 & \blacksquare & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & \blacksquare & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad \left[\begin{array}{cccccccccccc} 0 & 1 & * & 0 & 0 & * & * & 0 & * & * \\ 0 & 0 & 0 & 1 & 0 & * & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 1 & * & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

REF

RREF

Exercise 1. Compute the following:

(a) $1 + 1 + 1 - 1 + 1$ in $\mathbb{Z}_2$;

(d) $1 + 2 + 1 + 2 + 1 + 2$ in $\mathbb{Z}_3$;

(b) $2 \cdot 2 - 1$ in $\mathbb{Z}_3$;

(e) $2 \cdot 3 + 4 - 3 \cdot 1 + 2 \cdot 2$ in $\mathbb{Z}_5$;

(c) 2^7 in $\mathbb{Z}_3$;

(f) $1 \cdot 2 \cdot 3 \cdot 4$ in $\mathbb{Z}_5$.

Exercise 2. By consulting the appropriate addition and multiplication tables, solve the following equations:

- | | | |
|--------------------------------------|--------------------------------------|--|
| (a) $x + 1 = 0$ in $\mathbb{Z}_2$; | (e) $2x + 1 = 0$ in $\mathbb{Z}_5$; | (i) $x^2 + 1 = 0$ in $\mathbb{Z}_2$; |
| (b) $x + 1 = 0$ in $\mathbb{Z}_3$; | (f) $2x + 2 = 1$ in $\mathbb{Z}_3$; | (j) $x^2 + 1 = 0$ in $\mathbb{Z}_3$; |
| (c) $x + 1 = 0$ in $\mathbb{Z}_5$; | (g) $2x + 2 = 1$ in $\mathbb{Z}_5$; | (k) $x^2 + 1 = 0$ in $\mathbb{Z}_5$; |
| (d) $2x + 1 = 0$ in $\mathbb{Z}_3$; | (h) $3x + 2 = 0$ in $\mathbb{Z}_5$; | (l) $2x^3 + 2 = 0$ in $\mathbb{Z}_5$. |

Exercise 3. Find the **additive inverses** of all the numbers in $\mathbb{Z}_7$. Find the **multiplicative inverses** of all the **non-zero** numbers in $\mathbb{Z}_7$.

Exercise 4. Compute the following (and give a formal proof by **mathematical induction** that your proof is correct):

- (a) the last digit of 2027^{2026} ; (b) the last two digits of 2026^{2027} .

Exercise 5. For a positive integer n , we define $\varphi(n)$ to be the number of integers $k \in \{1, \dots, n\}$ such that k is relatively prime to n . For instance, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, and $\varphi(4) = 2$. By imitating the proof of Fermat's Little Theorem, prove the following.

Euler's theorem. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Then, explain how Euler's theorem implies Fermat's Little Theorem.

Exercise 6. For each of the matrices below, state the size of the matrix (i.e. determine the n and m such that the matrix is $n \times m$), and determine which of the following holds:

- (i) the matrix is in reduced row echelon form (RREF),
(ii) the matrix is in row echelon form (REF), but **not** in reduced row echelon form (RREF),
(iii) the matrix is **not** in row echelon form (REF).

(a) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	(c) $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 & 3 \\ 0 & 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix}$	(e) $\begin{bmatrix} 7 & 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
(b) $\begin{bmatrix} 1 & 8 & 0 & 7 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	(d) $\begin{bmatrix} 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 4 & 4 \\ 0 & 0 & 3 & 3 & 3 \\ 0 & 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	(f) $\begin{bmatrix} 0 & 1 & 0 & 6 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

Exercise 7. Perform the specified elementary row operation on the specified matrix.

- (a) matrix: $\begin{bmatrix} 1 & 2 & 2 & 1 \\ 2 & 1 & 1 & 2 \end{bmatrix}$ (entries in $\mathbb{Z}_3$); elementary row operation: $R_2 \rightarrow 2R_2$;
- (b) matrix: $\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$ (entries in $\mathbb{Z}_2$); elementary row operation: $R_2 \rightarrow R_2 + R_1$;
- (c) matrix: $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 2 & 2 \\ 3 & 3 & 3 \end{bmatrix}$ (entries in $\mathbb{R}$); elementary row operation: $R_1 \leftrightarrow R_3$.