

$$\dots 8 \ 9 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 + 8 \ 9 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 + 8 \ 9 \ 0$$

$$\frac{1}{4} + \frac{1}{4} = \frac{8}{1}$$

$$\frac{1}{8} + \frac{1}{3} = \frac{1}{1}$$

$$\frac{1}{5} + \frac{1}{5} = \frac{1}{0} = \frac{1}{2 \times 5}$$

$$\frac{1}{5} \times \frac{1}{5} = \frac{1}{5}$$

$$\frac{1}{7} + \frac{1}{7} = \frac{1}{4}$$

$$\frac{1}{7} - \frac{1}{2} = \frac{1}{5}$$

$$\frac{1}{4} - \frac{1}{8} = \frac{1}{6}$$

$$\frac{1}{3} = \frac{1}{7}$$

$$\frac{1}{6} \times \frac{1}{5} = \frac{1}{0}$$

$$\frac{1}{9} \times \frac{1}{9} = \frac{1}{1}$$

$$\frac{1}{6} \times \frac{1}{6} = \frac{1}{6}$$

Congruence:

Soit $n \in \mathbb{N}$, $n > 1$. Soient a et $b \in \mathbb{Z}$, on dit que a et b sont congrus modulo n , lorsque $a - b$ est multiple de n .

On note alors $a \equiv b \pmod{n}$

$a \equiv b \pmod{n} \Leftrightarrow a$ et b ont le même reste lors de la division par n

$$\Leftrightarrow \exists k \in \mathbb{Z}, a = b + kn$$

Soit $n \in \mathbb{N}$, $n > 1$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation de congruence modulo n .

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \bar{n-1}\}$ où \bar{a} est l'ensemble des entiers congrus à a modulo n

Exemple :

$$\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\} \text{ avec } \begin{cases} \bar{0} = \{\text{entiers pairs}\} \\ \bar{1} = \{\text{entiers impairs}\} \end{cases}$$

$$\begin{aligned} \bar{0} + \bar{0} &= \bar{0} \\ \bar{0} + \bar{1} &= \bar{1} \\ \bar{1} + \bar{1} &= \bar{0} \\ \bar{0} \times \bar{0} &= \bar{0} \\ \bar{0} \times \bar{1} &= \bar{0} \\ \bar{1} \times \bar{1} &= \bar{1} \end{aligned}$$

Addition et multiplication

Dans $\mathbb{Z}/5\mathbb{Z}$

$$\begin{aligned} \bar{3} + \bar{1} &= \bar{4} \\ \text{mais } \bar{3} &= \bar{8} \text{ et } \bar{1} = \bar{11} \\ \bar{8} + \bar{11} &= \bar{19} = \bar{4} \end{aligned}$$

Theoreme :

- + Dans $\mathbb{Z}/n\mathbb{Z}$
si $\overline{x} = \overline{a}$ et $\overline{y} = \overline{b}$ alors $\overline{x + y} = \overline{a + b}$
- + Dans $\mathbb{Z}/n\mathbb{Z}$, on peut definir une addition par

$$\overline{a} + \overline{b} = \overline{a + b}$$
- + Dans $\mathbb{Z}/n\mathbb{Z}$, on peut definir une multiplication par

$$\overline{a} \times \overline{b} = \overline{a \times b}$$

Exemple :

10 11 0 1 2 3

Dans $\mathbb{Z}/12\mathbb{Z}$

$$\overline{7} + \overline{8} = \overline{3}$$

$$\overline{4} + \overline{8} = \overline{0}$$

$$\overline{4} - \overline{6} = \overline{10}$$

$$\overline{9} - \overline{3} = \overline{6}$$

$$\overline{4} \times \overline{5} = \overline{8}$$

$$\overline{4} \times \overline{4} = \overline{4}$$

$$\overline{5} \times \overline{5} = \overline{1}$$

$$\overline{6} \times \overline{6} = \overline{0}$$

Addition

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$,

$$\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$$

→ l'addition est associative

$\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$

$\bar{0}$ est un élément neutre

$\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}$, $\exists \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ $\bar{a} + \bar{b} = \bar{0}$ ($b = n-a$)

tout élément possède un opposé!

$\forall a, b \in \mathbb{Z}, n\mathbb{Z}$, $\bar{a} + \bar{b} = \bar{b} + \bar{a}$
l'addition est commutative

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif

Multiplication

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{a} \times (\bar{b} \times \bar{c}) = (\bar{a} \times \bar{b}) \times \bar{c}$

la multiplication est associative

$\forall \bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{a} \times \bar{b} = \bar{b} \times \bar{a}$

la multiplication est commutative

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{a} \times (\bar{b} + \bar{c}) = \bar{a} \times \bar{b} + \bar{a} \times \bar{c}$

la multiplication est distributive

$\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{a} \times \bar{1} = \bar{a}$

$\bar{1}$ est un élément neutre

$(\mathbb{Z}/n\mathbb{Z}, \times)$ est un groupe commutatif

$(\mathbb{Z}/n\mathbb{Z}, \times, +)$ est un anneau commutatif

Exemple

Dans $\mathbb{Z}/10\mathbb{Z}$

3 0 1 2 3

$$\overline{5} + \overline{8} = \overline{3} \quad \overline{4} \times \overline{9} = \overline{6}$$

$$\begin{aligned}\overline{4} + \overline{6} &= \overline{0} & \overline{3} \times \overline{7} &= \overline{2} \\ \overline{2} \times \overline{5} &= \overline{0} & \overline{5} + \overline{5} &= \overline{0} \\ \overline{3} \times \overline{3} &= \overline{1}\end{aligned}$$

$$\begin{aligned}\overline{3}^{100} &= 3^2^{50} = (\overline{-1})^{50} = \overline{1} \\ \hookrightarrow 3^2 [10] &= -1\end{aligned}$$

Définitions:

Tous les éléments de \mathbb{Z}_n/\mathbb{Z} ont un opposé, mais pas forcément un inverse

Soit \bar{a} un élément de \mathbb{Z}_n/\mathbb{Z} . On dit que \bar{a} est **inversible** si et seulement si il existe $\bar{b} \in \mathbb{Z}_n/\mathbb{Z}$ tel que $\bar{a} \times \bar{b} = \bar{1}$

On appelle \bar{b} l'**inverse** de \bar{a} et on le note \bar{a}^{-1}
L'ensemble des éléments inversible de $\mathbb{Z}/n\mathbb{Z}$ est noté
 $(\mathbb{Z}/n\mathbb{Z})^\times$

Soit a un élément de $\mathbb{Z}/n\mathbb{Z}$. On dit que a est un **diviseur zéro** si et seulement si :

$$- a \neq 0$$

$$- \exists b \in \mathbb{Z}/n\mathbb{Z}, b \neq 0 \text{ et } a \times b = 0$$

Résoudre dans $\mathbb{Z}/20\mathbb{Z}$ les équations suivantes :

$$a) \overline{3x} = \overline{9}$$

$$b) \overline{3x} = \overline{4}$$

$$c) \overline{4x} = \overline{3}$$

$$d) \overline{4x} = \overline{8}$$

$$\begin{aligned} a) \quad & \overline{3x} = \overline{9} \\ & \cancel{7} \times \overline{3x} = \cancel{7} \times \overline{9} \quad [20] \\ & \overline{21x} = \overline{63} \quad [20] \\ & x = \overline{3} \quad [20] \end{aligned}$$

$$\begin{aligned} b) \quad & \overline{3x} = \overline{4} \\ & \cancel{7} \times \overline{3x} = \cancel{4} \times \cancel{7} \quad [20] \\ & \overline{21x} = \overline{28} \quad [20] \\ & x = \overline{8} \quad [20] \end{aligned}$$

pour que
 $n \cdot x = b \quad [20]$

$\hookrightarrow x = a \quad [20]$

$$c) \quad \overline{4x} = \overline{3}$$

$$\hookrightarrow \overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{0}, \overline{4}, \overline{8}, \dots$$

Pas de solution

$$4x = 3 + 20n$$

$$4(x - 5n) = 3$$

$$dy - 4x = 8$$

$$4x = 8 + 20n$$

$$x = 2 + 5n$$

L'ensemble de solution est $\{2, 7, 12, 17\}$

Donner les éléments de $(\mathbb{Z}, 5\mathbb{Z})^*$ et $(\mathbb{Z}/6\mathbb{Z})^*$

Dans $\mathbb{Z}, n\mathbb{Z}$, i et $-i$ sont toujours leur propre inverse

Dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{2} \times \overline{3} = \overline{1}$

$$(\mathbb{Z}/5\mathbb{Z})^* = \{1, 2, 3, 4\}$$

Dans $\mathbb{Z}/6\mathbb{Z}$,

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$$\Rightarrow (\mathbb{Z}, 6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}$$

Un diviseur de 0 de $\mathbb{Z}/n\mathbb{Z}$ ne peut pas être inversible

Exemple : $(\mathbb{Z}/30\mathbb{Z})^\times$

$$\left\{ \begin{array}{l} \cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, \cancel{7}, \cancel{8}, \cancel{9}, \cancel{10}, \cancel{11}, \cancel{12}, \cancel{13}, \cancel{14}, \cancel{15}, \cancel{16} \\ \cancel{17}, \cancel{18}, \cancel{19}, \cancel{20}, \cancel{21}, \cancel{22}, \cancel{23}, \cancel{24}, \cancel{25}, \cancel{26}, \cancel{27} \\ \cancel{28}, \cancel{29} \end{array} \right\}$$

$$\cancel{2} \times \cancel{15} = \bar{0}$$

$$\cancel{3} \times \cancel{10} = \bar{0}$$

$$\cancel{8} \times \cancel{5} = \bar{0}$$

$$\cancel{4} \times \cancel{15} = \bar{0}$$

$$\cancel{8} \times \cancel{10} = \bar{0}$$

Nbr pair (Multiple de 2)

Multiple de 3

$$\cancel{7} \times \cancel{13} = \cancel{91} = \bar{1}$$

On en déduit que

$$\bar{a} \times \bar{b} = \bar{1} \Rightarrow (-\bar{a}) \times (-\bar{b}) = \bar{1}$$

Soit \bar{a} un inversible de $\mathbb{Z}/n\mathbb{Z}$. Si \bar{a} est inversible alors $(-\bar{a})$ est inversible et

$$(-\bar{a})^{-1} = -\bar{a}^{-1}$$

Inversible

Soit \bar{a} un élément de $\mathbb{Z}/n\mathbb{Z}$, on a \bar{a} est inversible $\Leftrightarrow a$ est premier avec n

Première: L'argument essentiel est le théorème de Bachet - Bezout:

a est premier avec n

$$\Leftrightarrow \exists s, t \in \mathbb{Z}, as + nt = 1$$

$$\Leftrightarrow \exists s, t \in \mathbb{Z}, as - 1 = nt$$

$$\Leftrightarrow \exists s \in \mathbb{Z}, \bar{as} - \bar{1} = \bar{0} \text{ dans } \mathbb{Z}/n\mathbb{Z}$$

$\Leftrightarrow \bar{a}$ est inversible.

$\mathbb{Z}/p\mathbb{Z}$

p : un nombre premier

Soit $p \in \mathbb{N}$, un nombre premier

Tout $a \in \{1, 2, \dots, p-1\}$, a est premier avec p ;
donc \bar{a} est inversible dans $\mathbb{Z}/p\mathbb{Z}$

$$(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$$

$\mathbb{Z}/p\mathbb{Z}$ est un corps

Corps: Anneau dont tous les éléments non nuls, son inversible s'appelle un Corps (Ex: $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}$)

Un polynôme de $\mathbb{Z}/p\mathbb{Z}[x]$ de degré d admet au plus d racine

de polynôme $x^3 - x$ de $\mathbb{Z}/6\mathbb{Z}[x]$ admet 6 racines

Exemple :

Dans $\mathbb{Z}/180\mathbb{Z}$, les éléments suivants sont-ils inversibles

o ~~68~~ \checkmark

o ~~11~~ \checkmark

o ~~49~~ \checkmark

o ~~100~~ \checkmark

o ~~55~~ \checkmark

o ~~149~~ \checkmark

o ~~87~~ \checkmark

o ~~91~~ \checkmark

Calculons l'inverse de 37 dans $\mathbb{Z}/63\mathbb{Z}$

$$63 = 1 \times 37 + 26$$

$$37 = 1 \times 26 + 11$$

$$26 = 2 \times 11 + 4 \quad a \text{ est premier avec } n$$

$$11 = 2 \times 4 + 3$$

$$\Leftrightarrow \exists s, t \in \mathbb{Z}, as + nt = 1$$

$$4 = 1 \times 3 + 1$$

$$\Leftrightarrow \exists s, t \in \mathbb{Z}, as - 1 = nt$$

$$3 = 3 \times 1 + 0$$

$$\Leftrightarrow \exists s \in \mathbb{Z}, \bar{as} - \bar{1} = \bar{0} \text{ dans } \mathbb{Z}/n\mathbb{Z}$$

$$\Leftrightarrow a \text{ est inversible.}$$

On résout $37u + 63v = 1$

$$1 = 4 - 1 \times 3$$

$$1 = 4 - 1 \times (11 - 2 \times 4)$$

$$1 = 4 - 1 \times 11 + 2 \times 4$$

$$1 = -1 \times 11 + 3 \times 4$$

$$1 = -1 \times 11 + 3(26 - 2 \times 11)$$

$$1 = -1 \times 11 + 3 \times 26 - 6 \times 11$$

$$1 = 3 \times 26 - 7 \times 11$$

$$1 = 3 \times 26 - 7 \times (37 - 1 \times 26)$$

$$1 = 3 \times 26 - 7 \times 37 + 7 \times 26$$

$$1 = -7 \times 3f + 10 \times 26$$

$$1 = -7 \times 3f + 10(63 - 1 \times 3f)$$

$$1 = -7 \times 3f + 10 \times 63 - 10 \times 3f$$

$$1 = 10 \times 63 - 17 \times 3f$$

On trouve donc $10 \times 63 - 17 \times 3f = 1$

On constate que 10×63 dans $\mathbb{Z}/63\mathbb{Z}$ est $\overline{1}$

On en déduit que dans $\mathbb{Z}/63\mathbb{Z}$, on a

$$\overline{-17} \times \overline{3f} = \overline{1}$$

L'inverse de $\overline{3f}$ est $-\overline{17} = 46$

$$\overline{-17}[63] = \overline{46}$$

exemple :

Dans $\mathbb{Z}/180\mathbb{Z}$, calculer l'inverse suivant :

$$a) \overline{11} \quad b) \overline{173} \quad c) \overline{31} \quad d) \overline{49}$$

$$a) 180 = 16 \times 11 + 4$$

$$11 = 2 \times 4 + 3$$

$$4 = 1 \times 3 + 1$$

$$3 = 3 \times 1 + 0$$

$$1 = 4 - 1 \times 3$$

$$1 = 4 - 1 \times (11 - 2 \times 4)$$

$$1 = 4 - 1 \times 11 + 2 \times 4$$

$$1 = -1 \times 11 + 3 \times 4$$

$$1 = -1 \times 11 + 3(180 - 16 \times 11)$$

$$1 = -1 \times 11 + 3 \times 180 - 48 \times 11$$

$$1 = 3 \times 180 - 49 \times 11$$

$$-49 \times 11 = \overline{1}$$

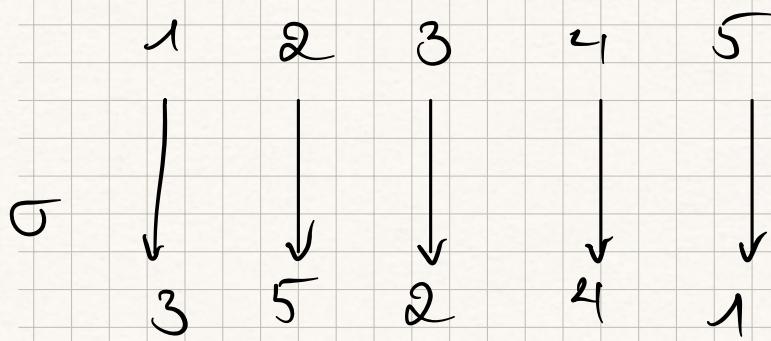
$$\overline{-49} [180] = \overline{131}$$

$$\Rightarrow \text{pour la d , } \overline{49}^{-1} = -11 = \overline{169}$$

179 inverse est -1

$\overline{91}$ dans $\mathbb{Z}/180\mathbb{Z}$

Permutation



$$\sigma(1) = 3 \quad \sigma(2) = 5 \quad \sigma(3) = 2 \quad \sigma(4) = 4$$

$$\sigma(5) = 1$$

Pour $n \in \mathbb{N}^*$, une permutation de degré n est une bijection de $\{1, \dots, n\}$ dans $\{1, \dots, n\}$.

L'ensemble des permutations de degré n est appelé groupe symétrique et noté S_n .

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$$

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & ? \\ ? & 6 & 5 & 1 & 2 & 3 & 4 \end{pmatrix} \in S_7$$

Combien d'éléments dans S_4 ?

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Nombre de façons d'arranger ces nombres
① On choisit à où mettre le

$$4 \times 3 \times 2 \times 1 \\ = 4! = 24$$

1 : On a 4 possibilités de mettre

② pour le 2¹: 3 possibilités

③ pour le 3²: 2 possibilités

④ pour le 4³: 1 possibilité

Ca donne $S_n = n!$

Produit de 2 permutations

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} \in S_5$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \in S_5$$

$$\sigma_1 \sigma_2 = \sigma_1 \circ \sigma_2, (\sigma_1 \sigma_2)(i) = \sigma_1(\sigma_2(i))$$

$$\sigma_1 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$

$$\sigma_2 \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$$

Exercise

$$id = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \in S_5$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \in S_5$$

Que valent $\sigma \cdot id$ et $id \cdot \sigma$?

$$\sigma \cdot id = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \quad \textcolor{red}{\sigma \cdot id = id \cdot \sigma}$$

$$id \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \quad \textcolor{red}{= \sigma}$$

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix} \in S_5$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \in S_5$$

$$\tau \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\mu\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\tau\mu = \mu\sigma$$

$$\tau = \mu^{-1} \quad \mu = \sigma^{-1}$$

S_n est un groupe non-commutatif

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 2 & 1 \end{pmatrix} \in S_6$$

Calculer σ^2 et σ^{-1}

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

Transpositions

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} = (1, 4) = (4, 1)$$

Une transposition est une permutation qui échange uniquement deux nombres

La transposition qui échange les nombres i et j est notée (i, j)

Dans S_4 calculer :

a $(1, 2)(3, 4)$

b $(3, 4)(1, 2)$

c $(1, 2)(2, 3)$

d $(2, 3)(1, 2)$

$$a \times (1, 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$(3, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$(1,2)(3,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

$$a_7 = (3,4)(1,2) b_7$$

$$b_7(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad (2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$(1,2)(2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$(2,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$