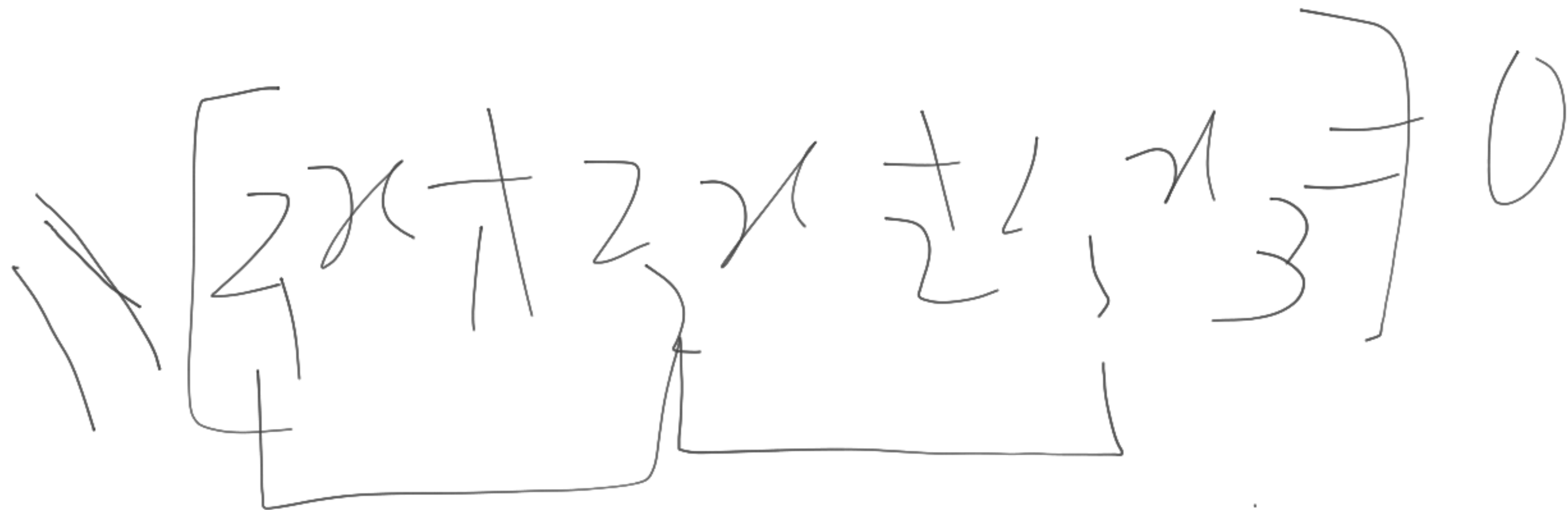


LWE

SIS



$[A]$

✓

$$Z_1 x_1 + Z_2 x_2$$

$$+ Z_3 x_3 = 0$$

\_\_\_\_\_

→

Group

$\mathbb{Z}_p$

五

五

二

五

、

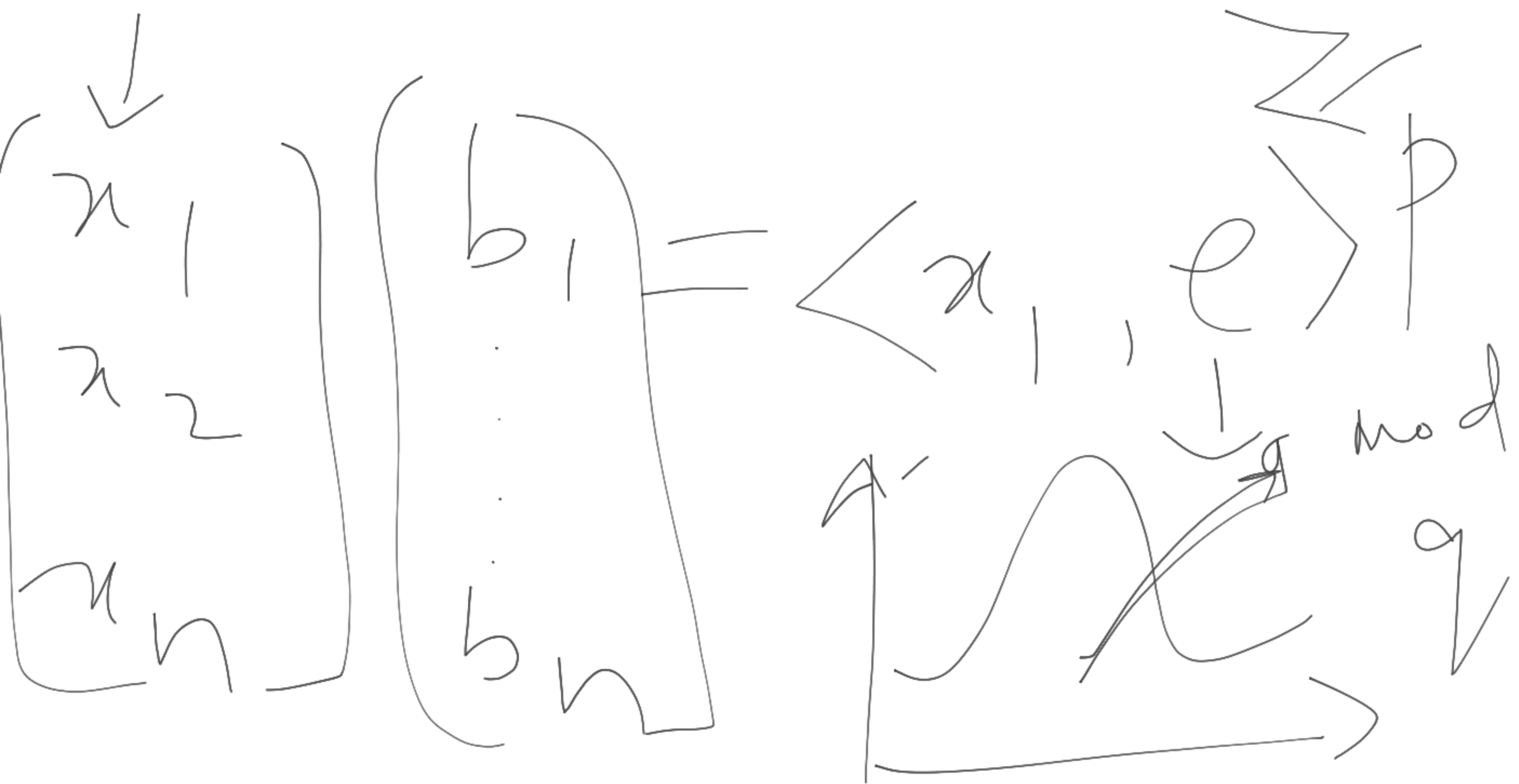
↓

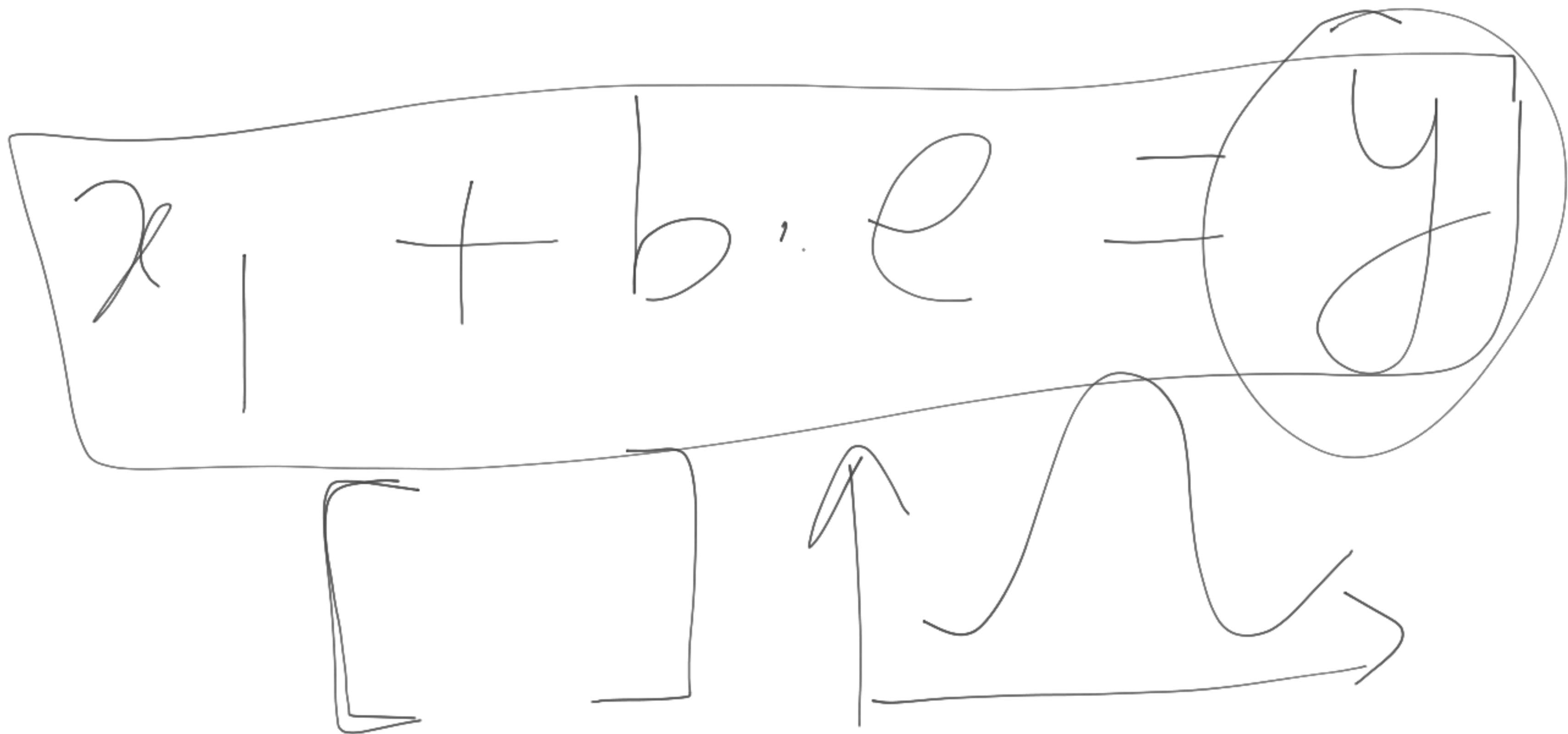
bam

LWE

$x_1, x_2, \dots, x_n$

$b = \langle x_1, e \rangle$





$$a_1 + b \cdot c \rightarrow [P] \rightarrow \left[ \begin{array}{c} \text{Z} \\ p \end{array} \right]$$

2 Case

---

$$1. \quad [x] + [b]e = [y]$$

---





2.



10. Calculi →

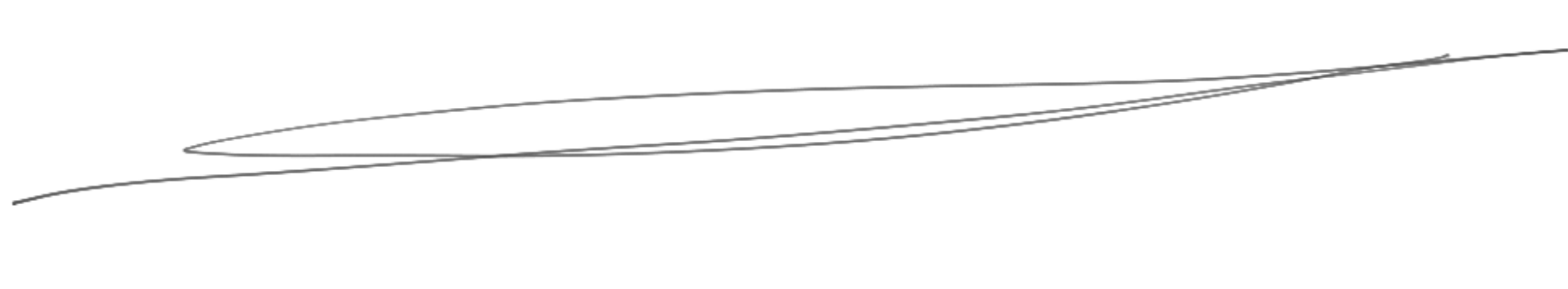
2. Natural only

↓  
[x and only]  
1/n

10th  
100 / 2



$$(x) + (h) e^{-1} > [P]$$

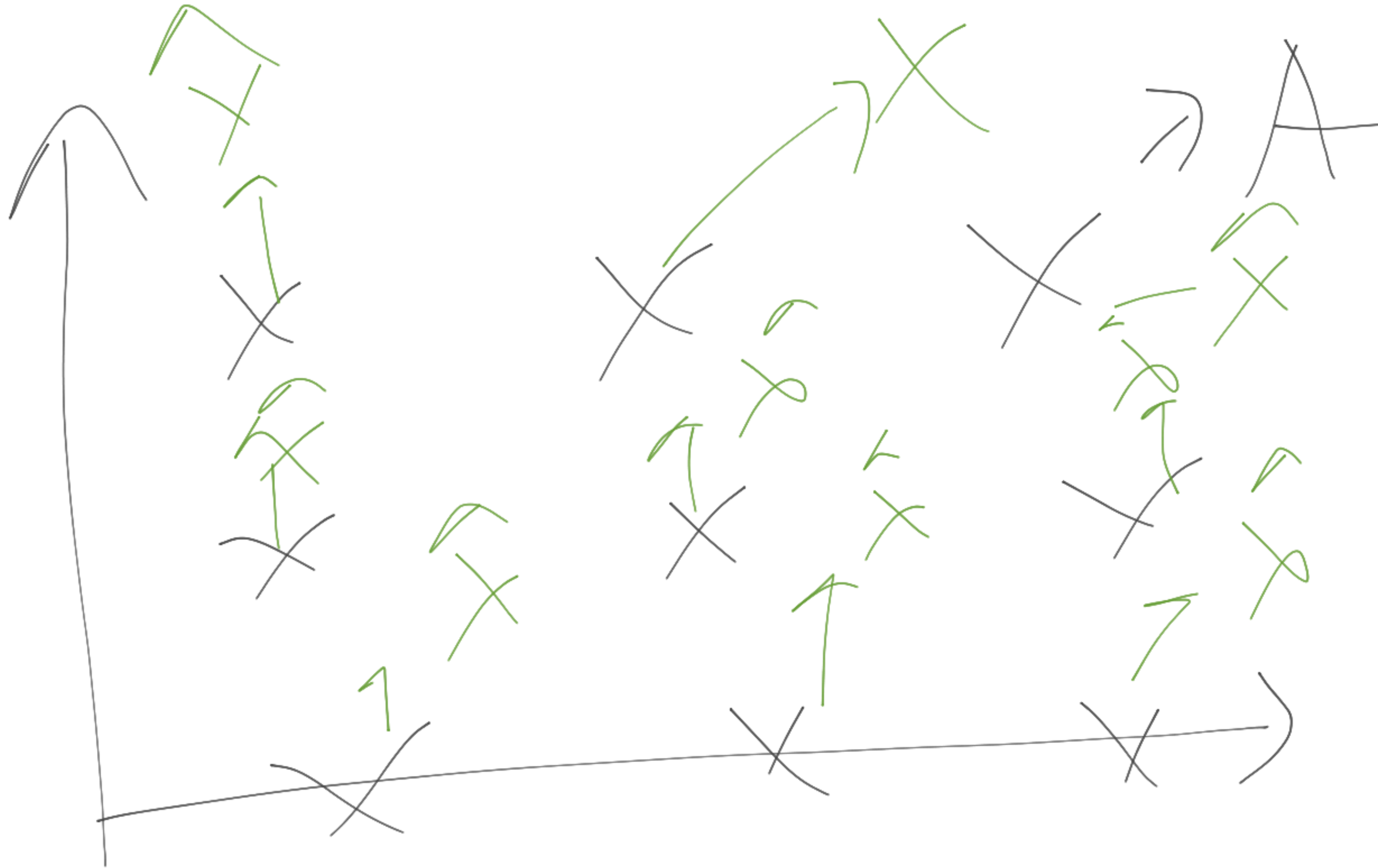


$$\begin{array}{c}
 P \left[ M + b \right] \circ \left[ \sim P \right] \\
 \Downarrow \quad \Downarrow
 \end{array}$$

$$(x) + \overset{\sim}{b} \approx b \cdot [p]$$

---

↓





~~A~~ =  $\begin{bmatrix} \text{A} \end{bmatrix} \rightarrow$  public

$\begin{bmatrix} A \end{bmatrix} + (b) \text{e.s.}$

