Déf PLD sur courbe elliptique.

Soit $\mathcal{E}$ une courbe elliptique sur $\mathbb{Z}_p$.
Soit P un élément primitif et $T \in C$.

Trouver $d \in \mathbb{N}$, $1 \leq d \leq \#C$ tq.

$$\underbrace{P + \dots + P}_{d \text{ fois}} \quad dP = T$$

Rq 1) d est la clé privée et T est publique.

2) On adapte l'algo (S and M.) ici :

Entrée C avec $P \in C$ et $d = \sum_{i=0}^{t} d_i 2^i$ binaire.

Sortie $T = dP$.

- $T = P$
- Pour $i =$ ~~1~~ jusqu'à d par -1 faire :
  - $T = T + T$ (mod p)
  - si $d_i = 1$, $T = T + P$ (mod p)
- Retourner (T).

§§ 5.3. Protocole DH d'échange de clé sur CE.

SETUP : 1. Soit p premier et $C : y^2 = x^3 + a.x + b$ (p).

2. Soit $\mathcal{P} = (x_p, y_p)$ primitif.

$(p, a, b, \mathcal{P})$ publique.