

**FEUILLE D'EXERCICES n° 12**  
Logarithme discret

Soit  $G$  un groupe cyclique et soit  $g$  un générateur de  $G$ . Soit  $a \in G$ . Le problème est de trouver un entier  $k$  tel que

$$a = g^k.$$

On va s'intéresser au cas où  $G = (\mathbb{Z}/p\mathbb{Z})^*$ , où  $p$  désigne un nombre premier.

La commande existe dans **sage** : c'est **log**, appliqué à un élément de  $G$ .

À titre d'exercice, on va quand même programmer un algorithme pour ce problème, de complexité algébrique  $O(\sqrt{p} \log p)$  (la complexité de l'algorithme naïf est en  $O(p)$ ) : c'est l'objet de l'exercice 2. L'exercice 1 consiste à retrouver certaines commandes sage en rapport avec le problème.

**Exercice 1** – [COMMANDES SAGE]

Cet exercice consiste à trouver une commande sage pour chacune des questions.

1) Définir  $A = \mathbb{Z}/2017\mathbb{Z}$ . Soit  $G$  son groupe multiplicatif. Comment trouver un générateur de  $G$  par une commande sage ? Soit  $g$  un tel générateur. En utilisant **log**, trouver  $k$  tel que  $456 = g^k$ .

2) Comment trouver l'ordre de 76 dans  $G$  ?

3) Soit  $l$  une liste d'éléments de  $G$ . Comment décider si un élément  $q$  est ou non dans  $l$  ? Si oui, comment déterminer l'indice correspondant ?

**Exercice 2** – [ALGORITHME : PAS DE BÉBÉ, PAS DE GÉANT]

Soit  $G$  un groupe cyclique de générateur  $g$ , et soit  $a$  un élément de  $G$ . On décrit un algorithme pour trouver  $k$  tel que

$$ag^k = 1.$$

Soit  $N$  l'ordre de  $G$ . Soit  $b = \lceil \sqrt{N-1} \rceil$ . Alors  $b^2 \geq k$ . Soit  $l = [a, ag, \dots, ag^{b-1}]$ . On trie la liste  $l$  : cela va permettre une recherche dans  $l$  en  $O(\log b)$ . On calcule ensuite  $c = g^{-b}$ . Pour  $q \in \{0, 1, \dots, b\}$ , on calcule  $c^q$  et on cherche si cet élément se trouve dans la liste  $l$ . Si c'est le cas, on a trouvé  $r \in [[0, b-1]]$  tel que  $c^q = ag^r$ , c'est-à-dire tel que  $ag^{bq+r} = 1$ .

Programmer cet algorithme dans le cas où  $G = (\mathbb{Z}/p\mathbb{Z})^*$ .