PROJET H : LE PROBLÈME DU LOGARITHME DISCRET

1. Le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique.

Soit G un groupe abélien fini, noté multiplicativement.

1. Soit g et h deux éléments de G d'ordres respectifs a et b, avec $\operatorname{pgcd}(a,b)=1$.
   (i) Si $(gh)^m = 1$, démontrer que b divise am.
   (ii) En déduire que gh est d'ordre ab.
2. On pose $n = |G|$ et on suppose en outre que le groupe G vérifie la propriété suivante :
   (P) *pour tout diviseur d de n, l'équation $x^d = 1$ a au plus d solutions dans G.*
   Considérons un diviseur premier q de n et écrivons $n = q^\alpha m$, avec $q \nmid m$.
   (i) Démontrer qu'il existe $g \in G$ tel que $g^{q^{\alpha-1}m} \neq 1$.
   Indication : on pourra raisonner par l'absurde.
   (ii) En déduire que G contient un élément d'ordre q^α.
3. Déduire de ce qui précède que tout groupe abélien fini vérifiant la condition (P) est cyclique.
4. Soit p un nombre premier. Démontrer que le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ vérifie la condition (P), et donc est cyclique.

2. Recherche d'un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$

Soit p un nombre premier.

1. Soit $a \in \mathbf{Z}$ un entier distinct de p. Démontrer que (la classe de) a engendre le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ si et seulement si
$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$$
   pour tout nombre premier q divisant $p-1$.
2. Écrire une fonction `Générateur(p)` renvoyant le plus petit entier $a \in \{1,\dots,p-1\}$ dont la classe modulo p engendre le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$.
3. Lorsque p parcourt tous les nombres premiers inférieurs à 10^6, quel est le plus grand entier renvoyé par la fonction `Générateur(p)` ? Pour quelle valeur de p l'obtient-on ?

3. Le logarithme discret

Soit p un nombre premier et soit $a \in \{1,\dots,p-1\}$ un générateur du groupe $(\mathbf{Z}/p\mathbf{Z})^\times$. Étant donné $b \in \{1,\dots,p-1\}$, on souhaite résoudre l'équation
$$a^x = b$$
d'inconnue $x \in \{0,\dots,p-2\}$.

1. Écrire une fonction `Logarithme(p,a,b)` qui renvoie l'unique entier $x \in \{0,\dots,p-2\}$ tel que $a^x = b$.

2. Pour $k \in \{3,4,5,6,7,8\}$, sélectionner un nombre premier $10^k \leqslant p < 10^{k+1}$ et choisir un entier $b \in \{1,\ldots,p-1\}$ au hasard [1].
   (i) Déterminer le temps de calcul nécessaire pour résoudre l'équation $a^x = b$ avec l'algorithme précédent, où $a =$ `Générateur(p)`.
   (ii) Représenter graphiquement le temps de calcul en fonction de k.

4. Application en cryptographie

On peut utiliser ce qui précède pour réaliser un système cryptographique à clef publique.

— Alice sélectionne un nombre premier p et un générateur a de $(\mathbf{Z}/p\mathbf{Z})^\times$; elle choisit également au hasard un entier $x \in \{0,\ldots,p-1\}$.

— Alice rend public le triplet (p,a,y), où b est l'unique élément de $\{1,\ldots,p-1\}$ tel que $b \equiv a^x \pmod{p}$).

— Bob veut envoyer un message à Alice, qu'il commence par transformer en un (ou plusieurs éléments) M de $\{1,\ldots,p-1\}$. Il choisit également au hasard $z \in \{0,\ldots,p-1\}$.

— Bob calcule les entiers $c,d \in \{1,\ldots,p-1\}$ tels que $c \equiv a^z \pmod{p}$ et $d \equiv M \cdot b^z \pmod{p}$, qu'il envoie à Alice.

— Ayant reçu (c,d), Alice calcule c^x modulo p puis $d \cdot (c^x)^{-1}$ modulo p.

1. Vérifier qu'Alice a bien retrouvé le message M.
2. Si l'on ne connaît pas x, comment peut-on faire pour retrouver M à partir du couple (c,d) envoyé par Bob ?
3. Implémenter ce protocole en Python, en utilisant un nombre premier suffisamment grand pour que le temps de calcul de la fonction `Logarithme(p,a,b)` soit excessivement long.

1. Utiliser la fonction `random.randint(m,n)` du module *random* pour obtenir un nombre entier choisi au hasard dans l'ensemble {m,m+1,...,n}.