Travaux Pratiques
Séance n° 3

I. Entiers friables

1. Écrire une fonction `list_primes(B)` qui renvoie la liste de tous les nombres premiers inférieurs ou égaux à B. On utilisera le crible d'Ératosthène fr.wikipedia.org/wiki/Crible_d'Ératosthène.
2. Écrire une fonction `factor_smooth(n,L)` qui prend en entrées un entier positif ou nul n et une liste L de nombres premiers, et qui teste si tous les facteurs premiers de n sont dans L. Si tel est le cas, la fonction doit renvoyer `True` ainsi que la liste des exposants dans la factorisation de n ; autrement la fonction renvoie `False` (et une liste qui n'a possiblement pas de sens).

   Exemple :

```
>> L=list_primes(20)
>> L
[2,3,5,7,11,13,17,19]
>> factor_smooth(1238328)
(True,[3,5,0,2,0,1,0,0])
>> 2^3*3^5*7^2*13
1238328
>> factor_smooth(46,L)
(False,[1,0,0,0,0,0,0,0])
```

Soit $B \in \mathbb{N}^*$; un entier n est dit *B-friable* si tous ses facteurs premiers sont plus petits que B. Les deux fonctions précédentes peuvent être utilisées pour déterminer si un nombre est B-friable, et déterminer dans ce cas sa factorisation.

II. Une méthode de calcul d'indices pour les logarithmes discrets dans $\mathbb{Z}/p\mathbb{Z}$

Soit p un grand nombre premier, g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$, et $h = g^x$ un élément aléatoire de $(\mathbb{Z}/p\mathbb{Z})^*$. L'idée de la méthode de calcul d'indices est d'obtenir des logarithmes discrets en collectant suffisant de relations entre des puissances de g et de h et les éléments d'une base de factorisation.

Plus précisément, on se donne un paramètre B et on pose

$$\mathcal{F} = \{q \in \mathbb{N} \mid q \text{ est premier et } q \leq B\} = \{q_1, \ldots, q_{\pi(B)}\}$$

où $\pi(B)$ est le nombre d'entiers premiers inférieurs ou égaux à B.
Pendant la première étape, on teste pour plusieurs entiers $y_i \in \mathbb{N}$ si g^{y_i} (ou plutôt son représentant dans $[\![0, p-1]\!]$) est B-friable. Si c'est le cas, cela donne une relation de la forme

$$g^{y_i} = \prod_{j=1}^{\pi(B)} q_j^{a_{ij}} \mod p.$$

Après avoir trouvé N relations, en passant aux logarithmes on obtient le système (défini sur $\mathbb{Z}/(p-1)\mathbb{Z}$)

$$\begin{cases} y_1 = \sum_{j=1}^{\pi(B)} a_{1j} \log_g(q_j) \mod p-1 \\ \vdots \\ y_N = \sum_{j=1}^{\pi(B)} a_{Nj} \log_g(q_j) \mod p-1 \end{cases}$$

ou sous forme matricielle :

$$\begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1\pi(B)} \\ \vdots & & \vdots \\ a_{N1} & \dots & a_{N\pi(B)} \end{pmatrix} \begin{pmatrix} \log_g(q_1) \\ \vdots \\ \log_g(q_{\pi(B)}) \end{pmatrix}$$

Si N est suffisamment grand (au moins égal à $\pi(B)$), alors ce système a une unique solution modulo $p-1$, ce qui donne le logarithme individuel de chacun des éléments de la base de factorisation $\mathcal{F}$.

Il est alors facile de retrouver le logarithme discret du challenge h si h est B-friable. Si ce n'est pas le cas, on calcule gh, $g^2h, \dots$ jusqu'à ce qu'un élément friable soit trouvé. On déduit alors de $g^k h = \prod_j q_j^{n_j}$ que $\log_g(h) = \sum_j n_j \log_g(q_j) - k$.

3. Écrire une fonction `matrix_rel` qui prend en entrées p, un générateur g de $(\mathbb{Z}/p\mathbb{Z})^*$ et un entier B, et qui renvoie la matrice $A = (a_{ij})_{ij}$ ainsi que le vecteur ou la liste $Y = (y_i)_i$ (afin d'être sûr que le système n'aura bien qu'une seule solution, on prendra une matrice A ayant un nombre de lignes légèrement supérieur au nombre de colonne, par exemple $N = \pi(B) + 5$).
   Dans Sagemath, la commande `matrix(Zmod(p-1),N1,N2)` crée une matrice nulle de taille $N1 \times N2$ à coefficients dans $\mathbb{Z}/(p-1)\mathbb{Z}$; on peut accéder/affecter une ligne d'une matrice en utilisant directement `M[i]`.
4. Implémenter enfin le calcul d'indices complet esquissé précédemment pour calculer des logarithmes discrets dans $\mathbb{Z}/p\mathbb{Z}$.
   Étant donnés une matrice M et un vecteur V à coefficients dans $\mathbb{Z}/(p-1)\mathbb{Z}$, on peut appeler la commande `M.solve_right(V)` pour obtenir une solution de l'équation $MX = V$; si L est une liste, la commande `vector(L)` permet de la transformer en vecteur.
5. (a) Calculer le logarithme discret de $h = 2$ en base $g = 201$ dans $\mathbb{Z}/p\mathbb{Z}$ où $p = 10007$, en prenant $B = 10$, puis celui de $h = 202$.
   (b) Calculer le logarithme discret de 2027 en base $g = 2017$ dans $\mathbb{Z}/p\mathbb{Z}$ où $p = 10^{13} + 391$, en prenant $B = 1000$.