TP test

Ce TP de 3h compte pour la note de CC du module de Cryptographie. C'est un examen individuel.

À la fin du TP, vous devez envoyer un email à vanessa.vitse@univ-grenoble-alpes.fr *avec votre fichier intitulé* `CC_VOTRENOM.ipynb`. *Chaque cellule de votre fichier SageMath doit commencer par un commentaire comportant le numéro de la question, chaque programme doit être commenté, et dans le cas où il ne fonctionnerait pas, vous devez le signaler explicitement.*

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 la fonction `next_prime(x)` qui renvoie le premier nombre premier strictement supérieur à x.
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 $B = 1000$.

III. Calcul d'indices et factorisation

6. Soient a, b, n trois entiers tels que $a^2 = b^2 \bmod n$ et $a \neq \pm b \bmod n$. Montrer que n n'est pas premier et expliquer comment retrouver un facteur non trivial de n.
   Application : factoriser 20003 sachant que $245^2 = 16 \bmod 20003$.
7. Factoriser 30049 sachant que $177^2 = 1280 = 2^8.5 \bmod 30049$ et que $361^2 = 10125 = 3^4.5^3 \bmod 30049$. Indication : combiner les deux équations pour trouver une congruence de carrés.

Trouver des congruences de carrés est encore aujourd'hui la méthode de factorisation la plus rapide. La version élémentaire de la méthode de calcul d'indices pour factoriser un entier n est la suivante :

— On se fixe une borne de friabilité B et on considère la base de factorisation $\mathcal{F} = \{q_1, \dots, q_{\pi(B)}\} = \{q \in \mathbb{N} \mid q \text{ est premier et } q \leq B\}$.
— On teste pour plusieurs $x \in \mathbb{Z}/n\mathbb{Z}$ si le représentant de x^2 dans $[\![0, n-1]\!]$ est B-friable. Cela permet de produire des relations de la forme

$$x_i^2 = \prod_{j=1}^{\pi(B)} q_j^{a_{ij}} \bmod n.$$

— Une fois que $N = \pi(B) + 1$ relations ont été trouvées, on les combine pour obtenir une congruence de carrés.

8. Soit $A = \begin{pmatrix} \overline{a_{11}} & \dots & \overline{a_{1\pi(B)}} \\ \vdots & & \vdots \\ \overline{a_{N1}} & \dots & \overline{a_{N\pi(B)}} \end{pmatrix} \in \mathcal{M}_{N,\pi(B)}(\mathbb{Z}/2\mathbb{Z})$ (chaque coefficient est réduit modulo 2). Soit $V = (\epsilon_1\ \epsilon_2 \dots \epsilon_N)$ un élément non nul de $\mathcal{M}_{1,N}(\{0,1\})$ tel que $V.A = 0$.
Montrer que $\prod_{\substack{1 \leq i \leq N \\ \epsilon_i = 1}} \prod_{j=1}^{\pi(B)} q_j^{a_{ij}}$ est un carré (dans $\mathbb{N}$), puis en déduire une congruence de carrés modulo n.

Exemple jouet : avec $B = 5$ (et donc $\mathcal{F} = \{2, 3, 5\}$) et $n = 3053$, en démarrant avec $\lceil \sqrt{3053} \rceil = 56$, les relations obtenues sont

$$\begin{array}{rcl} 79^2 & = & 3^3.5 \mod 3053 \\ 97^2 & = & 2.5^3 \mod 3053 \\ 125^2 & = & 2^3.3^2.5 \mod 3053 \\ 127^2 & = & 2^5.3 \mod 3053 \end{array} \quad \text{correspondant à la matrice des relations } M = \begin{pmatrix} 0 & 3 & 1 \\ 1 & 0 & 3 \\ 3 & 2 & 1 \\ 5 & 3 & 0 \end{pmatrix}.$$

On obtient alors modulo 2 la matrice $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, et le vecteur $V = (0\ 1\ 1\ 0)$ vérifie clairement $V.A = (0\ 0\ 0)$ (noter qu'il est possible que SageMath renvoie un autre vecteur dans le noyau à gauche de A). En revenant aux relations, on obtient alors la congruence

$$97^2.125^2 = 2^4.3^2.5^4 \bmod 3053.$$

Maintenant $97.125 = 2966 \bmod 3053$ et $2^2.3.5^2 = 300$, donc finalement $\gcd(2966 - 300, 3053) = 43$ est un facteur non trivial de 3053.

9. Écrire un programme qui factorise un entier donné n en utilisant des variantes des programmes écrits dans la section II.
Afin d'accélerer la recherche de relations, on parcourra les entiers x en démarrant à $x = \lceil \sqrt{N} \rceil$.
La fonction `A=M.change_ring(Zmod(2))` peut être utilisée pour réduire les coefficients de la matrice M modulo 2 ; il est également recommandé d'utiliser la commande `A.kernel()[1]` ou `A.left_kernel()[1]`.

10. (a) Trouver la factorisation de 20099 en prenant $B = 15$.
    (b) Trouver la factorisation de $10^{13} + 73$ en prenant $B = 1000$.