UGA Master 1-Algèbre effective 2025

Controle continu du jeudi 13 mars, 14h30-16h.
Documents interdits à l'exception d'une feuille manuscrite A4 recto-verso.
Calculatrice ou smartphone **en mode avion** *autorisé.*
Autres appareils électroniques interdits.
Ce sujet est composé de 2 exercices (barême indicatif non contractuel : 10, 10).

Exercice 1

Soient p et q deux nombres premiers impairs, $n = pq$ et c un entier, on souhaite calculer efficacement $a^c \pmod n$. On propose une méthode de calcul alternative à l'exponentiation rapide lorsqu'on connait p et q :

— On calcule $a^c \pmod p$ et $a^c \pmod q$ par l'algorithme d'exponentiation rapide.

— On reconstruit $a^c \pmod n$ par le théorème des restes chinois.

Dans les analyses de coût (en nombre d'opérations binaires), on supposera que le nombre de bits à 1 de l'écriture des exposants (par exemple c ci-dessus) est proche de la moitié de la taille de l'écriture en base 2 de l'exposant.

1. Question de cours : rappeler le coût (en équivalent du nombre de multiplications dans $\mathbb{Z}/n\mathbb{Z}$ puis en équivalent du nombre d'opérations binaires) du calcul de $a^c \pmod n$ pour $a \in [0, n[$ un entier en fonction de c et n, sans connaitre p et q.
2. Illustrer la méthode alternative dans le cas où $p = 7, q = 11, a = 3, c = 60$
3. Déterminer le coût du calcul par la méthode alternative en fonction de c, p et q. Comparer au coût de la question 1 lorsque p et q sont proches de $\sqrt{n}$.
4. On suppose que c est de l'ordre de grandeur de n. On peut alors utiliser le petit théorème de Fermat pour calculer $a^c \pmod p$ et $a^c \pmod q$. Illustrer sur l'exemple.
5. Déterminer le coût par cette méthode en fonction de p et de q, puis de n en supposant que p et q sont proches de $\sqrt{n}$.
6. Discuter l'intérêt de ces méthodes pour crypter et décrypter un message par la méthode RSA.

Exercice 2

Dans cet exercice, on se propose de chercher des racines carrées dans $\mathbb{Z}/p\mathbb{Z}$ avec $p > 2$ premier fixé.
Partout dans la suite, x est un élément non nul de $\mathbb{Z}/p\mathbb{Z}$, représenté explicitement comme un entier $m \in \{1, \cdots, p-1\}$

1. Question de cours : rappeler pourquoi x est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $m^{(p-1)/2} = 1 \mod p$. Donner le coût de cette vérification (avec exponentiation rapide) en nombre de multiplications modulo p puis en nombre d'opérations binaires (en fonction de p).

   Supposons maintenant jusqu'à la fin qu'on a vérifié que x est bien un carré dans $\mathbb{Z}/p\mathbb{Z}$. On cherche à trouver y tel que $y^2 = x$, c'est-à-dire explicitement un entier $m \in \{1, \cdots, p-1\}$ tel que $m^2 = n \mod p$.
2. Si $p \equiv 3 \mod 4$, montrer que $y = x^{(p+1)/4} \mod p$ convient. Conclure sur le coût de calcul de m dans ce cas.
3. On suppose désormais que $p \equiv 1 \mod 4$.
4. Montrer que $\mathbb{F}_p[X]/(X^2 - x) \cong \mathbb{F}_p^2$ comme anneau, et en déduire que pour tout $z \in \mathbb{F}_p$,
$$X^2 - x \quad \text{divise} \quad (X-z)^p - (X-z).$$
5. Montrer que pour au moins $(p-1)/2$ valeurs de z,
$$1 \neq \gcd(X^2 - x, (X-z)^{(p-1)/2} - 1) \neq X^2 - x$$
6. Pour une telle valeur de z, en déduire un moyen de trouver une racine carrée de x dans $\mathbb{F}_p$ et donner son coût de calcul.