UGA Master 1-Algèbre effective 2024

Controle continu du mercredi 20 mars, 9h-11h.
Documents interdits à l'exception d'une feuille manuscrite A4 recto-verso. Calculatrice autorisée.
Téléphones portables, ordinateurs, ... interdits.
Ce sujet est composé de 2 exercices (barême indicatif non contractuel : 13, 7).

Exercice 1

Soient p et q deux nombres premiers impairs et $n = pq$. On recherche les solutions en x de l'équation $x^2 = a \pmod n$ ("racines carrées" de a modulo n) où a est un entier fixé. On rappelle que $x^2 = a \pmod p$ admet 1 solution si $a = 0 \pmod p$, et 0 ou 2 solutions selon la valeur de $a^{\frac{p-1}{2}} \pmod p$.

1. Déterminer en appliquant le théorème des restes chinois le nombre de solutions en fonction de a.
2. Exemple : résoudre $x^2 = a \pmod n$ pour $p = 103$, $q = 127$ et $a = 2024$ puis $a = 2025$. Indication : on pourra calculer le carré de $a^{\frac{p+1}{4}} \pmod p$ avec la calculatrice en indiquant les commandes utilisées.
3. On suppose qu'il y a 4 solutions et que $p = 3 \pmod 4$ et $q = 3 \pmod 4$. Déterminer ces 4 solutions en fonction de $a \pmod p$ et $a \pmod q$.
4. Estimer dans ce cas le cout en fonction de la taille de p et de q.
5. Lorsque $p = 1 \pmod 4$, et $a \neq 0 \pmod p$ admet une racine carrée modulo p, on choisit un nombre entier aléatoire r et on calcule $R = (X + r)^{\frac{p-1}{2}} - 1 \pmod{p, X^2 - a}$ puis le PGCD de R et $X^2 - a$. Si le PGCD est de degré 1, la racine du PGCD est une racine carrée de a modulo p.
   Tester avec $x^2 = 3 \pmod{13}$, $r = 0$ et $r = 1$. On pourra utiliser les fonctions `powmod, gcd, rem` de la calculatrice en indiquant sur la copie les commandes.
6. Déterminer le cout d'un test en fonction de la taille de p.
7. On suppose toujours que a admet deux racines carrées mod p que l'on note $\pm b$. Montrer que le PGCD ci-dessus est de degré 0 ou 2 si et seulement si r est solution de l'équation polynomiale en r

$$(b + r)^{\frac{p-1}{2}} = (-b + r)^{\frac{p-1}{2}} \pmod p$$

   En déduire une majoration du nombre de valeurs de r pour lesquelles le PGCD est de degré 0 ou 2.
8. Déterminer une majoration du nombre moyen de tests que l'on devra effectuer pour obtenir un succès. En déduire le cout moyen d'une recherche de racine carrée modulo p en fonction de la taille de p.
9. En déduire le cout moyen de la résolution de $x^2 = a \pmod n$.

Exercice 2

Pour déterminer le produit de deux polynômes A et B à coefficients entiers, on se propose de faire le produit de ces polynômes dans $\mathbb{Z}/a\mathbb{Z}[X]$ où $a = 2^{(2^n)} + 1$

1. Tester à la calculatrice si a est premier pour $n = 3, 4, 5, 6$.
2. (question de cours) Quelle méthode peut-on utiliser pour déterminer si a est presque surement premier et quel est son cout en fonction de n ?
3. On souhaite utiliser l'algorithme de FFT (Fast Fourier Transform) pour effectuer le produit $AB \in \mathbb{Z}/a\mathbb{Z}[X]$. Pour quelles valeurs des degrés de A et B est-ce possible ? Expliquer comment procéder et déterminer le cout de la multiplication en fonction des degrés de A et B.
4. À quelle condition sur les coefficients de AB pourra-t-on reconstruire le produit de A et B dans $\mathbb{Z}[X]$ à partir du produit dans $\mathbb{Z}/a\mathbb{Z}[X]$?