TP BONUS : RACINES CARRÉES DANS $\mathbf{F}_p$

► **PRÉREQUIS** : $\mathbf{F}_p^\times$ *est cyclique.*

Soient p un nombre premier impair, et $a \in \mathbf{F}_p$. On pose $\left(\frac{a}{p}\right) = 0$ si $a = 0$ ou p, $\left(\frac{a}{p}\right) = 1$ si a est un carré non nul de $\mathbf{F}_p$, et $\left(\frac{a}{p}\right) = -1$ sinon. Dans cet exercice on décrit des algorithmes d'extraction de racines carrées dans $\mathbf{F}_p^\times$; autrement dit, on part de $a \in \mathbf{F}_p^\times$ tel que $\left(\frac{a}{p}\right) = 1$, et on cherche à déterminer un $x \in \mathbf{F}_p^\times$ tel que $x^2 = a$.

Symbole de Legendre

1. Montrer que pour tout $a \in \mathbf{F}_p$, on a

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}.$$

En déduire une fonction qui détermine si un élément $a \in \mathbf{F}_p$ est un carré on non. Peut-on généraliser, disons par exemple, aux cas des cubes ?

Cas où p est congru à 3 modulo 4

2. Soit q un nombre entier impair. Soit $a \in \mathbf{Z}/2q\mathbf{Z}$. On suppose que a peut s'écrire $2x$ avec $x \in \mathbf{Z}/2q\mathbf{Z}$. Montrer que s'il existe un tel x, alors on peut en trouver un de la forme $x = na$ où n est un entier ne dépendant que de q.

3. On suppose que $p \equiv 3 \mod 4$. Appliquez ce qui précède avec $q = \frac{p-1}{2}$ pour obtenir un algorithme d'extraction de racines carrées dans $\mathbf{F}_p^\times$. L'implémenter et le tester.

Algorithme de Tonelli-Shanks

Soit p un nombre premier impair. On peut écrire $p = 1 + 2^n q$ où q est un entier impair et $n \geq 1$. On considère l'algorithme suivant pour déterminer des racines carrées dans $\mathbf{F}_p$.

(Initialisation) Soit $a \in \mathbf{F}_p^\times$ tel que $\left(\frac{a}{p}\right) = 1$. On suppose que l'on a trouvé $u \in \mathbf{F}_p^\times$ tel que $\left(\frac{u}{p}\right) = -1$. On pose $z := u^q$, $x := a^{\frac{q+1}{2}}$, $b := a^q$, $k := n$.

(Boucle) Tant que $b \neq 1$, on détermine le plus petit entier m tel que $b^{2^m} = 1$ et on pose $t := z^{2^{k-m-1}}$, $z := t^2$, $b := bz$, $x := xt$, $k = m$.

(Terminaison) Renvoyer x.

4. Quelle est la structure du groupe $G = \mathbf{F}_p^\times$?

5. Pour chaque entier $i \geq 1$, combien y a-t-il d'éléments a de G tels que $a^{2^i} = 1$? Les décrire en fonction d'un élément ρ d'ordre 2^n fixé.

6. Soit $c \in \mathbf{F}_p^\times$ tel que $c^{2^n} = 1$ et $\left(\frac{c}{p}\right) = -1$. Montrer que c peut s'écrire ρ^i avec i impair.

7. Montrer qu'après l'initialisation z est d'ordre 2^n, et que b est d'ordre divisant 2^{n-1}.

8. Montrer que "$x^2 = ab$, z est d'ordre 2^k et b est d'ordre divisant 2^{k-1}" est un invariant de boucle.

9. Montrer que l'algorithme termine et renvoie une racine carrée de a.

10. Écrire une fonction prenant en argument un nombre premier impair p et renvoyant un u tel que $\left(\frac{u}{p}\right) = -1$.

11. Implémenter l'algorithme de Shanks sous la forme d'une fonction prenant en argument a et p et renvoyant x.

12. Que donne l'algorithme de Shanks lorsque $p \equiv 3 \mod 4$?

13. Que dire des complexités des algorithmes mis en jeu dans ce TP ? Et que dire du cas $p = 2$?

Algorithme de Cipolla-Lehmer

On considère l'algorithme suivant pour déterminer des racines carrées dans $\mathbf{F}_p$.

(Initialisation) Soit $a \in \mathbf{F}_p^\times$ *tel que* $\left(\frac{a}{p}\right) = 1$. *On suppose que l'on a trouvé* $u \in \mathbf{F}_p^\times$ *tel que* $\left(\frac{u}{p}\right) = -1$. *On pose* $z := u^q$, $x := a^{\frac{q+1}{2}}$, $b := a^q$, $k := n$.

(Première étape) On trouve par tirage aléatoire un élément $u \in \mathbf{F}_p$ *tel que* $u^2 - a$ *n'est pas un carré.*

(Terminaison) On calcule alors $x = \left(u + \sqrt{u^2 - a}\right)^{\frac{p+1}{2}}$ *dans* $\mathbf{F}_{p^2} = \mathbf{F}_p[X]/(X^2 - u^2 + a)$. *Renvoyer* x.

14. Justifier que l'algorithme produit bien une racine carrée de a dans $\mathbf{F}_p$. Quelle est la probabilité de tirer $u \in \mathbf{F}_p$ tel que $u^2 - a$ ne soit pas un carré ?

15. Implémenter et tester cet algorithme.

Pour aller plus loin

16. Expliquer et implémenter comment trouver une racine carrée dans $\mathbf{Z}/p^\alpha\mathbf{Z}$ avec $\alpha \in \mathbb{N}^*$.

17. Faire de même pour $\mathbf{Z}/pq\mathbf{Z}$ avec p et q deux nombres premiers distincts.

18. Pourquoi est-ce un problème difficile d'extraire une racine carrée dans $\mathbf{Z}/n\mathbf{Z}$ pour un entier n quelconque ?

19. Que se passe-t-il pour le calcul de racines cubiques ?