CRYPTOGRAPHIE ALGÉBRIQUE **4M035** **Feuille 8. TP Sagemath**
P. V. Koseleff

Calculs avec Sagemath

Se connecter sur `https://jupyter.math.upmc.fr/`. Commencer par se mettre sur son répertoire. Ouvrir un nouveau fichier `notebook`, choisir `Sagemath 9.4`. A la fin de la session, sauver le fichier. On peut aussi l'exporter au format `.ipynb` ou `.pdf`.

Exercice 8.1. — Ordre des éléments
SAGE sait calculer l'ordre d'un élément dans un groupe multiplicatif (`multiplicative_order()`).

1. Tester avec l'anneau $A = \mathbf{Z}/n\mathbf{Z}$ (en SAGE : `IntergerModRing(n)`) et des entiers quelconques dans A.
2. Calculer l'ordre de 2 dans $(\mathbf{Z}/n\mathbf{Z})^*$, pour n impair entre 3 et 200.
3. Soit $n = p$ un nombre premier. Trouver le plus petit entier $1 < a < p$ d'ordre $p-1$ dans $(\mathbf{Z}/p\mathbf{Z})^*$. On pourra essayer avec des petites valeurs de p.

Exercice 8.2. — Élément primitif
SAGE sait trouver des éléments primitifs de $\mathbf{F}_p$. *voir* `unit_gens()`.

1. Méthode directe :
   (a) Factoriser $p-1 = \prod p_i^{n_i}$. a est primitif si $a^{(p-1)/p_i} \neq 1$ pour tout i.
   (b) Tirer des nombres x au hasard (`random`) dans $[0,\ldots,p-1]$. Tester si $x_i = x^{(p-1)/p_i} \neq 1$. Dans ce cas x_i est d'ordre d_i un multiple $p_i^{n_i}$. En déduire z_i d'ordre $p_i^{n_i}$. A la fin on obtient un élément primitif en calculant $a = z_1 \cdots z_k$.
2. Soit $p = 89637484042681$. Trouver un élément primitif de $\mathbf{F}_p$.
3. Comparer votre algorithme avec la méthode classique du logiciel (`unit_gens()`) en répétant plusieurs fois la méthode et calculant le temps moyen.
4. Recommencer avec $n = p^k$.
5. Soit $n = M_{127} = 2^{127}-1$. Montrer que $(\mathbf{Z}/n\mathbf{Z})^*$ admet un élément d'ordre $n-1$. En déduire que n est premier.

Exercice 8.3. — Nombres premiers
SAGE peut fournir des nombres premiers. Commandes `is_prime, next_prime`

1. Obtenir la liste des nombres premiers entre 100 et 200.
2. Vérifier quel est le nombre de premiers inférieurs à n, pour n entre 2 et 10^5. Le comparer à la valeur théorique.
3. Prendre un premier p de l'ordre de 10^{40}. Vérifier qu'il est premier en trouvant un élément de $(\mathbf{Z}/p\mathbf{Z})^*$ d'ordre $p-1$.

Exercice 8.4. — RSA

1. Choisir deux nombres premiers $p = 37$ et $q = 41$. Et considérer $n = pq$.
   (a) Choisir e un entier premier à $\varphi(n)$. Calculer d tel que $ed \equiv 1 \pmod{\varphi(n)}$. *On pourra utiliser les commandes* `euler_phi`, `xgcd`.
   (b) Vérifier que pour tout $x \in \mathbf{Z}/n\mathbf{Z}$, on a bien $(x^e)^d = x$.
2. Du point du vue de Bob, prendre deux nombres premiers p et q (au hasard entre 10^N et 10^{N+1}). Recommencer tous les calculs précédents. Est-ce que $n = pq$ est facile à factoriser ? Pour quelles valeurs de N ?
3. Du point de vue Bob, comparer le temps de calcul de $z = x^d \pmod n$ et du calcul du couple $(a,b) = (x^d \pmod p, x^d \pmod q)$ suivi de la résolution de la congruence $z \equiv a \pmod p$, $z \equiv b \pmod n$. *On pourra utiliser la commande* `crt`.

Exercice 8.5. — Dans un cryptosystème utilisant la méthode RSA, déterminer la clé secrète $(\varphi(n),d)$ et le message envoyé $M \in (\mathbf{Z}/n\mathbf{Z})^*$ pour les les clés publiques (n,e) et les cryptogrammes $C = M^e$ suivants :

i) $n = 35, e = 5, C = 10$ *ii)* $n = 265, e = 139, C = 10$ *iii)* $n = 667, e = 493, C = 10$
iv) $n = 1763, e = 611, C = 2$ *v)* $n = 3599, e = 31, C = 60$

Exercice 8.6. — Méthode de Héron pour le calcul de la racine carrée
Soit à calculer une approximation de $\sqrt{n}$, où $n \in \mathbf{N}$.

1. On utilise la méthode de Héron. $x_0 = \frac{1}{2}(n+1)$, $x_{k+1} = \frac{1}{2}\left(x_k + \frac{n}{x_k}\right)$.
   (a) Montrer que $(x_k)_k$ est décroissante et converge vers $\sqrt{n}$.
   (b) Montrer que $\frac{x_{k+1}-\sqrt{a}}{\sqrt{a}} \leq \frac{1}{2}\left(\frac{x_k-\sqrt{a}}{\sqrt{a}}\right)^2$ et finalement, $x_k \leq \sqrt{a} + \frac{1}{2}\left(\frac{\sqrt{a}-1}{2\sqrt{a}}\right)^{2^k}$.
   (c) Ecrire une boucle SAGEMATH permettant de calculer rapidement $E(\sqrt{n})$. Tester la rapidité de convergence et comparer avec la borne théorique. *Attention aux erreurs d'arrondi.*
2. On considère une variante qui calcule $\lfloor\sqrt{n}\rfloor$. Pour cela, on part de $y_0 > \sqrt{n}$, par exemple $y_0 = \lfloor\frac{1}{2}(n+1)\rfloor$, puis $y_{k+1} = \lfloor\frac{1}{2}\left(y_k + \frac{n}{y_k}\right)\rfloor$
   (a) Montrer que si $x \in \mathbf{N}$, alors $\lfloor\frac{1}{2}\left(x + \frac{n}{x}\right)\rfloor = \lfloor\frac{1}{2}\left(x + \lfloor\frac{n}{x}\rfloor\right)\rfloor$.
   (b) Montrer que la suite y_k est strictement décroissante puis, si $y_r \leq \sqrt{n}$, on a $y_{r+1} \geq y_r$. Montrer alors que $y_r = \lfloor\sqrt{n}\rfloor$.
   (c) Implanter cette méthode et tester avec $n = (10^{10} + 10^5 + 1)^2 + m$, m petit.

Exercice 8.7. — Recherche d'une racine carrée de -1
Soit p un nombre premier. -1 est un carré dans $(\mathbf{Z}/p\mathbf{Z})^*$ si et seulement si $p \equiv 1 \pmod 4$. On rappelle le théorème de Wilson : $(p-1)! \equiv -1 \pmod p$. Dans toute la suite, on suppose $p \equiv 1 \pmod 4$.

1. Montrer que $\left(\frac{p-1}{2}!\right)$ est une racine carrée de -1.
2. On écrit $p - 1 = 2^s m$ où m est impair et $s \geq 2$.
   (a) Soit $a \in \mathbf{Z}/p\mathbf{Z}$ et $b = a^m$. Montrer que l'ordre de b est 2^k où $k \leq s$.
   (b) En déduire que $b^{2^{k-1}} = -1$ et en déduire une racine carrée de -1 lorsque $k \geq 2$.
   (c) En déduire que méthode (probabiliste) pour trouver une racine de -1.
   (d) Comparer avec la méthode précédente.

Exercice 8.8. — Recherche de racines carrées dans $\mathbf{F}_p$
Soit $a \in \mathbf{F}_p^*$. On suppose que a est un carré (en calculant $a^{(p-1)/2} \pmod p$).

1. Montrer que si $p \equiv 3 \pmod 4$, alors $b = a^{(p+1)/4}$ est une racine de a.
2. (a) Montrer qu'il y a exactement $(p-1)/2$ valeurs de t telles que $P = X^2 - tX + a$ soit irréductible dans $\mathbf{Z}/p\mathbf{Z}$.
   (b) Montrer que si α est une racine de $X^2 - tX + a$ irréductible, alors $b = \alpha^{(p+1)/2} \in \mathbf{Z}/p\mathbf{Z}$ vérifie $b^2 = a$.
   (c) Tester cette méthode pour p un grand nombre premier et a pris au hasard. *On prendra t au hasard et on vérifiera que P est irréductible. Comment ?*