Licence 3 – MHT633 Université Bordeaux 1
2010/2011

Feuille 4 : carrés et factorisation

Exercice 1. L'idée de Fermat

Soit $n \in \mathbb{N}$ et $x, y, \in \mathbb{Z}$ tels que $x^2 \equiv y^2 \pmod{n}$ et $x \neq \pm y \pmod{n}$. Montrer que $d = \text{pgcd}(x - y, n)$ est un diviseur non trivial de n.

Exercice 2. Les carrés de $\mathbb{Z}/p\mathbb{Z}$

Soit p un nombre premier impair et

$$\begin{array}{rcl} \phi : (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \longmapsto & x^2 \end{array}$$

1. Montrer qu'il y a $(p-1)/2$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.
2. Soit $y \in (\mathbb{Z}/p\mathbb{Z})^\times$, montrer que y a soit 2 racines carrés soit aucune.
3. Montrer que dans $(\mathbb{Z}/p\mathbb{Z})^\times$ on a l'équivalence :

$$y \text{ est un carré } \iff y^{(p-1)/2} = 1$$

4. On suppose que $p \equiv 3 \pmod{4}$. Soit y un carré de $(\mathbb{Z}/p\mathbb{Z})^\times$, monter que les racines carrés de y sont $y^{\frac{p+1}{4}}$ et $-y^{\frac{p+1}{4}}$.

Exercice 3. Les carrés de $\mathbb{Z}/n\mathbb{Z}$

Soit $n = pq$ où p et q sont des nombres premiers impairs distincts congrus à 3 modulo 4.

1. Caractériser les carrés de $(\mathbb{Z}/n\mathbb{Z})^\times$.
2. Ecrire un algorithme qui prend pour entrées n, p, q et $y \in \{0, 1, \ldots, n-1\}$ tel que $n = pq$ et qui détermine si $y \in \{0, 1, \ldots, n-1\}$ représente un carré modulo n. Quelle est sa complexité ?
3. Si $y \in (\mathbb{Z}/n\mathbb{Z})^\times$, montrer que l'équation $x^2 = y$ admet soit quatre solutions soit aucune.
4. Ecrire un algorithme qui prend pour entrées n, p, q et $y \in \{0, 1, \ldots, n-1\}$ tel que $n = pq$ et y est un carré modulo n et qui renvoie ces 4 racines carrés. Quelle est sa complexité ?
5. Supposons que l'on dispose d'un algorithme qui calcule toutes les racines carrés d'un carré de $\mathbb{Z}/n\mathbb{Z}$ sans connaitre p et q. En déduire un algorithme qui factorise n.

Exercice 4. Le système de Goldwaser-Micali

Soit $n = pq$ où p et q sont des nombres premiers impairs distincts congrus à 3 modulo 4. On fixe $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui n'est pas un carré modulo n, ni modulo p, ni modulo q. Le système de Goldwasser-Micali chiffre un élément $m \in \{0, 1\}$ avec la clé publique (n, α) par $\alpha^m x^2$ où x est un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ choisit au hasard.

1. Quelle est la clé privée ?
2. Montrer que le chiffré de m est un carré modulo p si et seulement si $m = 0$.
3. En déduire la fonction de déchiffrement.
4. Si on veut envoyer un message de l bits, quelle est la taille du message chiffré.
5. Expliquer comment construire un élément α convenable.
6. Ecrire un algorithme aléatoire qui renvoie un α convenable. Quelle est sa probabilité de réussite ?

Exercice 5. Algorithme de Dixon

Trouvez un diviseur non trivial de $N = 1829$ avec l'algorithme de Dixon et la base de facteurs $\mathcal{B} = \{2, 5, 7\}$. On pourra utiliser les entiers $43, 49, 52, 53, \ldots$.

Exercice 6. L'algorithme ρ de Pollard pour la factorisation

Soit n un nombre entier dont on veut calculer un facteur non trivial. Soit p le plus petit facteur premier (inconnu) de n. L'idée est de construire une suite « aléatoire » $x_1, x_2, \ldots, x_i, \ldots$ d'éléments de $\mathbb{Z}/n\mathbb{Z}$, de sorte qu'une collision $x_i = x_j \mod p$ pour $i < j$ permette de trouver un facteur de n donné par $\text{pgcd}(x_i - x_j, n)$.

On admettra le résultat suivant, connu sous le nom de *paradoxe des anniversaires* : en tirant au hasard des éléments d'un ensemble de cardinal N, on obtient une collision avec probabilité supérieure à $1/2$ au bout d'environ $\sqrt{N}$ tirages.

1. Estimez le nombre de termes de la suite et le nombre de pgcd à calculer avant de trouver un facteur de n.
2. On choisit de définir la suite x_i par la donnée de x_1 et la formule de récurrence $x_{i+1} = P(x_i)$, où $P \in \mathbb{Z}[X]$.
   (a) Montrez que $x_i = x_j \mod p \Longrightarrow x_{i+1} = x_{j+1} \mod p$.
   (b) En déduire que, si $x_i = x_j \mod p$ avec $i < j$ alors $x_u = x_{2u} \mod p$ pour un indice u tel que $u < j$.
   (c) Comment calculer $(x_{i+1}, x_{2(i+1)})$ à partir de (x_i, x_{2i}) ?
   (d) On *suppose* que la suite (x_i) obtenue a le même comportement qu'une suite de tirages indépendants dans $\mathbb{Z}/n\mathbb{Z}$, et donc qu'on peut appliquer le paradoxe des anniversaires. En déduire un algorithme qui nécessite environ $\sqrt{p}$ calculs de pgcd de nombres entiers naturels $\leq n$ pour factoriser n.
3. Factorisez $n = 7171$ avec $x_1 = 39$ et $P(x) = x^2 + 1$.