Cryptographie et arithmétique – Feuille 7

Exercice 1. On cherche à calculer le logarithme discret de 173 en base 2 dans $(\mathbb{Z}/227\mathbb{Z})^*$.

1. Montrer que 2 engendre $(\mathbb{Z}/227\mathbb{Z})^*$, puis factoriser 2^{32}, 2^{40}, 2^{59} et $2^{156} \mod 227$.
2. En déduire la valeur de $\log_2(3)$, $\log_2(5)$, $\log_2(7)$ et $\log_2(11)$.
3. Factoriser $173 \cdot 2^{177} \mod 227$, et en déduire $\log_2(173)$.

Exercice 2. Soit p un nombre premier impair, s un diviseur de $p-1$ et g un générateur du sous-groupe G d'ordre s de $(\mathbb{Z}/p\mathbb{Z})^*$. On suppose que s se factorise de la manière suivante : $s = \prod_{i=1}^{r} p_i^{e_i}$, où les p_i sont des nombres premiers distincts et pour tout $i \in [\![1, r]\!]$, $e_i \geqslant 1$. Soit $h \in G$, on cherche le logarithme discret x de h en base g. L'algorithme de Pohlig-Hellman calcule $x \mod p^{e_i}$ pour chaque i et retrouve ensuite x par le théorème des restes chinois.

1. Pour tout i, déterminer l'ordre de $\tilde{g}_i = g^{s/p_i}$.
2. On détermine maintenant la valeur de $x \mod p_i^{e_i}$ pour chaque i. Pour alléger les notations, on fixe un indice i et on note $q = p_i$ et e le e_i correspondant. On note $x \mod q^e = x_0 + x_1 q + x_2 q^2 + \cdots + x_{e-1} q^{e-1}$ la décomposition en base q. On suppose x_0, x_1, …, x_k déterminés, avec $k < e - 1$. Montrer comment déterminer x_{k+1} par le calcul d'un logarithme discret en base $\tilde{g}_i$.
3. Montrer que la complexité de cet algorithme est en $O\left(\sum_{i=1}^{r} e_i(\ln(s) + \sqrt{p_i})\right)$.
4. Application : 9 est d'ordre 63 dans $(\mathbb{Z}/127\mathbb{Z})^*$; calculer $\log_9(98)$.

Exercice 3. Soit G un groupe multiplicatif et $\alpha \in G$ un élément fixé d'ordre n. Soit β un élément de $\langle\alpha\rangle$ dont on veut calculer le logarithme discret en base α. L'idée de base de l'algorithme ρ de Pollard pour le logarithme discret est de calculer une suite $x_1, x_2, \ldots, x_i, etc.$, d'éléments de G, de sorte qu'une collision $x_i = x_j$ pour $i < j$ permette de calculer $c = \log_\alpha(\beta)$. Plus précisément, chaque élément x de la suite fait partie d'un triplet (x, a, b) vérifiant $x = \alpha^a \beta^b$. Les triplets (x_i, a_i, b_i) définissent une « marche aléatoire ».

1. Montrer que si (x, a, b) vérifie $x = \alpha^a \beta^b$, alors les triplets $(\beta x, a, b+1)$, $(x^2, 2a, 2b)$ et $(\alpha x, a+1, b)$ vérifient la même relation.

   On partitionne G en trois ensembles de même taille S_1, S_2 et S_3, et on définit l'application f :
   $$\begin{cases} \langle\alpha\rangle \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \langle\alpha\rangle \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ (x, a, b) & \mapsto & \begin{cases} (\beta x, a, b+1) & \text{si } x \in S_1, \\ (x^2, 2a, 2b) & \text{si } x \in S_2, \\ (\alpha x, a+1, b) & \text{si } x \in S_3. \end{cases} \end{cases}$$
   On pose $(x_0, a_0, b_0) = (1,0,0)$, et on définit la suite $((x_i, a_i, b_i))_{i \geqslant 0}$ par récurrence en posant $(x_{i+1}, a_{i+1}, b_{i+1}) = f((x_i, a_i, b_i))$ pour tout $i \geqslant 0$.
2. Montrer que pour tout $i \geqslant 0$, on a $x_i = \alpha^{a_i} \beta^{\beta_i}$.
3. Montrer que s'il existe $i < j$ tels que $x_i = x_j$, alors il existe $s < j$ tel que $x_s = x_{2s}$. Démontrer que si $\operatorname{pgcd}(b_{2s} - b_s, n) = 1$, alors $\log_\alpha(\beta) \equiv (a_s - a_{2s})(b_{2s} - b_s)^{-1} \mod n$.
4. Soit $G = (\mathbb{Z}/47\mathbb{Z})^*$. Vérifier que 2 est d'ordre 23. Calculer $\log_2(37)$; on prendra pour S_1 les entiers congrus à 2 mod 3, S_2 les multiples de 3 et S_3 les autres entiers.

Exercice 4. À partir de l'algorithme de factorisation de Dixon, factoriser $n = 2257$. On prend comme base $\mathcal{B} = \{2,3,5,7\}$ et on teste les entiers 133, 26, 1594, 741, 853, 1811...

Exercice 5. On présente le crible quadratique, qui est un raffinement de l'algorithme de Dixon. On commence par choisir une *base de facteurs* $\mathcal{B} = \{-1, p_1, \dots, p_k\}$, où p_i est un nombre premier pour tout $i \in [\![1, k]\!]$. Ensuite, pour chaque entier relatif j, on calcule $x_j = [\sqrt{n}] + j$ et $y_j = x_j^2 - n$ jusqu'à avoir $k+2$ entiers dont tous les facteurs premiers sont dans $\mathcal{B}$ (on dit alors que y_j est *lisse* sur $\mathcal{B}$). Pour chaque y_j lisse, on a

$$y_j = \pm \prod_{i=1}^{k} p_i^{a_{i,j}}, \text{ et on pose } v_{0,j} = \begin{cases} 0 & \text{si } y_j > 0, \\ 1 & \text{si } y_j < 0, \end{cases} \quad \text{puis } v_{i,j} \equiv a_{i,j} \mod 2 \text{ pour } i \geqslant 1.$$

1. On cherche un ensemble S d'entiers j tels que y_j est lisse et tels que pour tout $i \in [\![1, k]\!]$, on ait $\sum_{j \in S} v_{i,j} \equiv 0 \mod 2$. Expliquer comment obtenir un facteur non trivial de n à partir de $x = \prod_{j \in S} x_j$ et $y^2 = \prod_{j \in S} y_j$, si $x \not\equiv \pm y \mod n$.
2. Montrer que s'il n'existe pas d'entier s tel que $n \equiv s^2 \mod p$ pour un certain nombre premier p, alors on doit exclure p de $\mathcal{B}$ pour que la méthode fonctionne.
3. On pose $n = 30167$, et on choisit $\mathcal{B} = \{-1, 2, 7, 11, 17, 29, 31, 37, 41, 43, 53, 67\}$. Déduire une factorisation de n du tableau obtenu :

j	0	-1	-5	5	-6	7	11
x_j	173	172	168	178	167	180	184
y_j	$-2 \cdot 7 \cdot 17$	$-11 \cdot 53$	$-29 \cdot 67$	$37 \cdot 41$	$-2 \cdot 17 \cdot 67$	$7 \cdot 11 \cdot 29$	$7 \cdot 17 \cdot 31$

j	14	-15	-17	18	-23	28
x_j	187	158	156	191	150	201
y_j	$2 \cdot 7^4$	$-11 \cdot 43$	$-7^3 \cdot 17$	$2 \cdot 7 \cdot 11 \cdot 41$	$-11 \cdot 17 \cdot 41$	$2 \cdot 7 \cdot 17 \cdot 43$

Exercice 6. Soient $p \geqslant 3$ un nombre premier et $N \geqslant 2$. On veut montrer que $(\mathbb{Z}/p^N\mathbb{Z})^*$ est cyclique et en exhiber un générateur, à partir d'un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.

1. Montrer que pour tout élément $\bar{x}$ de $(\mathbb{Z}/p^N\mathbb{Z})^*$, il existe un unique couple $(u \mod p, v \mod p^n)$ dans $(\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}/p^N\mathbb{Z}$ tel que $x \equiv u(1+pv) \mod p^N$.
2. Soit $n \geqslant 2$ un entier. On rappelle (feuille 3, exercice 4) que $v_p(n!) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor$. En déduire que pour tout x divisible par p, $v_p\left(\frac{x^n}{n!}\right) \geqslant \frac{n}{2} > 0$.

   Ceci permet de définir l'application suivante, par analogie avec l'exponentielle réelle :

$$\forall \bar{x} \in p\mathbb{Z}/p^N\mathbb{Z}, \quad \exp_p(\bar{x}) \equiv 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \equiv \sum_{n=0}^{\infty} \frac{x^n}{n!} \mod p^N,$$

   où, pour calculer une fraction $\frac{a}{b} \mod p$ où $v_p(a) \geqslant v_p(b)$, on écrit $a = p^{v_p(a)}a'$, $b = p^{v_p(b)}b'$, et alors $\frac{a}{b} \equiv p^{v_p(a)-v_p(b)}a'b'^{-1} \mod p^N$.
3. Montrer que la somme a un sens, et est finie. On peut écrire $\exp_p(\bar{x}) \equiv \sum_{n=0}^{N_0} \frac{x^n}{n!} \mod p^N$.
4. Montrer soigneusement que pour tous k, l entiers et tous $\bar{x}, \bar{y} \in p\mathbb{Z}/p^N\mathbb{Z}$, on a $\frac{x^k y^l}{k!l!} \equiv \binom{k+l}{k} \frac{x^k y^l}{(k+l)!} \mod p^N$. En déduire que $\exp_p(\bar{x}) \exp_p(\bar{y}) = \exp_p(\bar{x} + \bar{y})$, et que $\exp_p$ est un isomorphisme de groupes entre $p\mathbb{Z}/p^N\mathbb{Z}$ et $1 + p\mathbb{Z}/p^N\mathbb{Z}$.
5. En déduire que si $u \mod p$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$, alors $u \exp_p(p)$ engendre $(\mathbb{Z}/p^N\mathbb{Z})^*$.
6. Application : calculer $\exp_3(3) \mod 81$, et en déduire un générateur de $(\mathbb{Z}/81\mathbb{Z})^*$.