Cryptographie et arithmétique – Feuille 5

Primalité

Exercice 1 (théorème de Pocklington). Soient $n \geqslant 2$ et $d \geqslant 2$ deux entiers. On suppose que pour tout facteur premier p de d, il existe un entier a_p tel que : n divise $a_p^d - 1$ et $\text{pgcd}(n, a_p^{d/p} - 1) = 1$.
Considérons q un facteur premier de n.

1. Soit p un facteur premier de d. On note $v_p(d)$ le plus grand entier k tel que p^k divise d. Montrer que $p^{v_p(d)}$ divise l'ordre de a_p dans le groupe $(\mathbb{Z}/q\mathbb{Z})^*$.
2. En déduire que d divise $q - 1$.
3. Prouver que si $d + 1 > \sqrt{n}$, alors n est premier.

Exercice 2 (test de primalité de Lucas-Lehmer). On pose $s_0 = 4$, et on définit par récurrence la suite $(s_i)_{i\geqslant 0}$ en posant $s_{i+1} = s_i^2 - 2$ pour tout $i \geqslant 0$. Soit $n \geqslant 2$ un entier, et supposons que $s_{n-2} \equiv 0 \mod (2^n - 1)$. Le but de cet exercice est de montrer que $2^n - 1$ est premier.
Soit p un diviseur premier de $2^n - 1$. Notons $A = \mathbb{Z}/p\mathbb{Z}[X]/(X^2 - 4X + 1)$ et désignons par α la classe de X dans A. Posons $\beta = 4 - \alpha$.

1. Montrer par récurrence que $s_i = \alpha^{2^i} + \beta^{2^i}$ pour tout $i \geqslant 0$.
2. Déterminer l'ordre de α dans le groupe A^*.
3. Conclure.

Ainsi, on peut tester la primalité d'un nombre de Mersenne $2^n - 1$ en vérifiant s'il divise s_{n-2}. La réciproque est vraie, donc permet de détecter les nombres de Mersenne composés.

Exercice 3 (nombre pseudo-premier). Soit $a \geqslant 2$ un entier. On dit qu'un entier n est pseudo-premier en base a s'il est composé et vérifie $a^{n-1} \equiv 1 \mod n$ (les nombres de Carmichael, abordés en cours, sont donc des nombres pseudo-premiers en base a pour tout entier a premier avec eux).

1. Montrer que 341 est pseudo-premier en base 2.
   Soit p un nombre premier impair qui ne divise pas $a^2 - 1$. On pose $n = \frac{a^{2p}-1}{a^2-1}$.
2. Montrer que n n'est pas un nombre premier.
3. Montrer que $a^{2p} \equiv 1 \mod n$.
4. Calculer $(a^2 - 1)(n - 1)$, puis montrer que p divise $n - 1$.
5. Montrer que 2 divise $n - 1$, et en déduire que n est pseudo-premier en base a, puis qu'il existe une infinité de nombres pseudo-premiers en base a.

Factorisation

Exercice 4 (algorithme ρ de Pollard). Soit n un nombre entier à factoriser, et soit p le plus petit facteur premier (inconnu) de n. L'idée est de construire une suite « aléatoire » $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_i, \ldots$ d'éléments de $\mathbb{Z}/n\mathbb{Z}$, de sorte qu'une collision $x_i \equiv x_j \mod p$ pour $i < j$ permette de trouver un facteur de n, donné par $\text{pgcd}(x_i - x_j, n)$.

1. Montrer le paradoxe des anniversaires * : la probabilité que r nombres modulo p soient tous distincts est $P_r = \left(1 - \frac{1}{p}\right)\left(1 - \frac{2}{p}\right)\cdots\left(1 - \frac{r-1}{p}\right) \leqslant \exp\left(-\frac{r(r-1)}{2p}\right)$. Ainsi, si r est plus grand que $1 + \sqrt{p}$, la probabilité d'avoir une collision est minorée par la constante $1 - \exp\left(-\frac{1}{2}\right) \simeq 0{,}393$.
   On choisit de définir la suite $(\bar{x}_i)_{i\geqslant 1}$ par la donnée de $\bar{x}_1$ et de la formule de récurrence $\bar{x}_{i+1} = \overline{P(x_i)}$, où P est un polynôme à coefficients entiers.
2. Montrer que si $x_i \equiv x_j \mod p$, alors $x_{i+1} \equiv x_{j+1} \mod p$.

∗. Application : la probabilité que dans un groupe de TD de 32 élèves, deux d'entre eux aient la même date d'anniversaire est d'environ 75% ! Cette probabilité dépasse déjà 50% pour 23 élèves.

3. En déduire que, si $x_i \equiv x_j \mod p$ avec $i < j$ alors $x_u \equiv x_{2u} \mod p$ pour un indice u tel que $u < j$.
4. Comment calculer $(\bar{x}_{i+1}, \bar{x}_{2(i+1)})$ à partir de $(\bar{x}_i, \bar{x}_{2i})$?
5. On suppose que la suite $(\bar{x}_i)_{i\geqslant 1}$ 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 inférieurs à n pour factoriser n.
6. Décrire une faiblesse de cet algorithme.
7. Factoriser $n = 7171$ avec $x_1 = 39$ et $P(X) = X^2 + 1$.

Exercice 5 (algorithme $p-1$ de Pollard). Soient $n \geqslant 2$ et $a \geqslant 2$ deux entiers premiers entre eux, et soit $b \geqslant 2$ un entier. Supposons qu'il existe un facteur premier p de n tel pour tout facteur premier q de $p-1$, on a $q^{v_q(p-1)} \leqslant b$. Notons M le ppcm de $1, 2, \ldots, b$. On calcule a^M modulo n, puis $d = \text{pgcd}(n, a^M - 1)$.

1. Montrer que d est un diviseur de n différent de 1. Cet algorithme trouve donc un facteur non trivial de n si $a^M \not\equiv 1 \bmod n$.
2. Tester l'algorithme avec $n = 221$ et $a = 2$ (en faisant varier b).

Exercice 6. Soient p et q des nombres premiers impairs distincts et $n = pq$.

1. Soit $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. On note (α_p, α_q) son image dans $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$. Montrer que l'ordre de α égale le ppcm des ordres de α_p et de α_q.
2. Soit $d = \text{pgcd}(p-1, q-1)$. Montrer qu'il existe un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre $\frac{\varphi(n)}{d}$.
   Dans la suite on suppose de plus que $p > 3$, $q > 3$ et $\text{pgcd}(p-1, q-1) = 2$.
3. Montrer que $2n < 3\varphi(n)$.
4. Soit α un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre $\frac{\varphi(n)}{2}$ et $0 \leqslant a < \frac{\varphi(n)}{2}$ le logarithme de α^n en base α. Montrer que $n - a = \varphi(n)$.
5. Écrire un algorithme polynomial en la taille de n qui prend pour entrées n et a et qui renvoie les facteurs p et q de n.

Exercice 7. Supposons que n soit un entier produit de deux nombres premiers impairs distincts p et q. On note e, premier avec $\varphi(n)$, l'exposant public d'un système RSA de module n. Connaissant p et q, l'exposant privé d se calcule en temps polynomial. Le but de l'exercice est de montrer que si un attaquant connaît d, alors il peut factoriser n en temps polynomial.

1. Montrer comment, à partir de e, d et n, on peut construire un multiple B de $\varphi(n)$.
2. On note $m = \text{ppcm}(p-1, q-1)$. Montrer que pour tout $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $\bar{a}^m = \bar{1}$. Montrer que $\bar{a}^{\frac{m}{2}}$ peut prendre quatre valeurs et que deux de ces valeurs permettent de factoriser n.
3. On pose $H = \{\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*; a^{\frac{m}{2}} \equiv \pm 1 \mod n\}$. Montrer que H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$.
4. Montrer qu'il existe $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $\bar{b}$ soit d'ordre $p-1$ modulo p et d'ordre $\frac{q-1}{2}$ modulo q.
5. On pose $p - 1 = 2^{v_p} p'$ et $q - 1 = 2^{v_q} q'$ avec p', q' impairs et on suppose, sans perte de généralité, que $v_p \geqslant v_q$. Exprimer $\frac{m}{2}$ en fonction de v_p et du ppcm de p' et q'. En déduire que $\bar{b}$ n'appartient pas à H. Si on prend $\bar{x}$ au hasard dans $(\mathbb{Z}/n\mathbb{Z})^*$, montrer que la probabilité que $\bar{x}$ n'appartienne pas à H est supérieure ou égale à $\frac{1}{2}$.
6. Montrer que m divise B et en déduire qu'il existe un entier naturel k tel que pour tout $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $x^{\frac{m}{2}} \equiv x^{B/2^{k+1}} \mod n$.
7. En déduire un algorithme probabiliste polynomial qui factorise n étant donnés n, e et d, et donner sa probabilité de succès.
8. L'appliquer à $n = 77$, $e = 7$ et $d = 43$.