Université Paris Diderot

Groupes et arithmétique
L2 Info – *MI4*

Feuille d'exercices n° 4

Test de primalité, cryptographie (RSA).

RÉCIPROCITÉ QUADRATIQUE

Exercice 1. Est-ce que les équations suivantes admettent des solutions dans $\mathbb{Z}$?

a) 1. $x^2 = -1 \mod 31$
   2. $x^2 = -1 \mod 61$
   3. $x^2 = -1 \mod 67$

b) 1. $x^2 = 2 \mod 11$
   2. $x^2 = 2 \mod 59$
   3. $x^2 = 2 \mod 23$

c) on sait que 97, 167, et 839 sont des nombres premiers
   1. $x^2 = 3 \mod 97$
   2. $x^2 = 11 \mod 167$
   3. $x^2 = 13 \mod 839$
   4. $x^2 = 29 \mod 839$
   5. $x^2 = 17 \cdot 19 \mod 839$

d) on sait que $1001 = 7 \cdot 11 \cdot 13$
   1. $x^2 = 24 \mod 35$
   2. $x^2 = 15 \mod 1001$
   3. $x^2 = 5 \mod 28$
   4. $x^2 = 196 \mod 9999$

TESTS DE PRIMALITÉ

Nombres de Carmichaël

Rappel : $N > 1$ est dit un nombre de Carmichaël si $a^{N-1} \equiv 1 \mod N$ pour tout entier a tel que $pgcd(a, n) = 1$. D'après un théorème du cours, un nombre $N > 1$ non premier est de Carmichaël si et seulement si, pour tout diviseur p premier de N, on a $p - 1 | N - 1$ et $p^2 \not| N$.

Exercice 2 (exemples numériques). Vérifier que 1729, 6601 et 278545 sont des nombres de Carmichaël. [Indication : $1729 = 7.13.19$, $6601 = 7.23.41$ et $278\,545 = 5.17.29.113$.]

Exercice 3 (une caractérisation des nombres de Carmichaël). Montrer qu'un entier non premier $N > 1$ est un nombre de Carmichaël si et seulement si $b^N \equiv b \mod N$ pour tout entier $b \in \mathbb{Z}$.

Exercice 4 (nombres de Carmichaël avec 3 diviseurs premiers).

1. Montrer que tout nombre non premier de Carmichaël a au moins 3 diviseurs premiers. *Indication :* par l'absurde, écrire $n = pq$ avec $p < q$, p et q premiers.
2. Montrer que pour r premier fixé, il n'existe qu'un nombre fini de nombres de Carmichaël de la forme $n = rpq$ avec p et q premiers. [indication : on peut supposer que $p > q$ et il y aura deux cas possible $r > q$ et $r < q$, montrer que pour chaque cas il n'y a qu'un nombre fini de (p, q) possible.]
3. Trouver tous les nombres de Carmichaël de la forme précédente pour $r = 3$ et pour $r = 5$.

Note : *il existe une infinité de nombre de Carmichaël ; la démonstration (difficile) date de 1994 et est due à Alford, Granville et Pomerance.*

Test de Rabin-Miller

Si $N \geqslant 2$ est impair et pgcd$(a, N) = 1$, on factorise $N - 1 = 2^s M$ avec M impair et on note ainsi les tests de Fermat et de Rabin-Miller

$$F(a, N) \quad : \quad a^{N-1} \equiv 1 \mod N$$

$$T(a, N) \quad : \quad a^M \equiv 1 \mod N \text{ ou } \exists r \in [0, s-1],\ a^{2^r M} \equiv -1 \mod N.$$

On définit également les deux sous-ensembles correspondants :

$$H := \{a \in (\mathbb{Z}/N\mathbb{Z})^* \mid F(a, N)\} \quad \text{et} \quad S := \{a \in (\mathbb{Z}/N\mathbb{Z})^* \mid T(a, N)\}.$$

Exercice 5. Calculer le cardinal de H et S pour les valeurs suivantes : $N = 9$, 15, $N = 21$.

Exercice 6.

1. Montrer que H est un sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^*$.
2. En déduire que, sauf lorsque N est un nombre de Carmichaël on a
$$\frac{|H|}{\phi(N)} \leqslant \frac{1}{2}$$
3. Montrer que $S \subset H$ (conclusion : le test de Rabin-Miller est meilleur que celui de Fermat).
4. Montrer sur un exemple que S n'est pas toujours un sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^*$. [Indication : on pourra choisir deux premiers p et q congrus à 1 modulo 4 et poser $N = pq$, choisir c de telle façon que $c \equiv +1 \mod p$ et $c \equiv -1 \mod q$, prendre a tel que $a^{2M} \equiv -1 \mod N$ et $b = a^{-1}c$ et montrer $a, b \in S$ mais $ab \notin S$]

Exercice 7. Existe-t-il un nombre N composé impair tel que $H = S$? (on demande seulement des exemples avec égalité et inégalité ; on pourra pousser l'exercice plus loin et montrer qu'il y a égalité $H = S$ si $N = p^m$ mais sinon $S \neq H$).

Exercice 8. Soit $N = 561 = 3.11.17$ le plus petit nombre de Carmichaël, on se propose de calculer le cardinal de S.

1. Vérifier que $N - 1 = 2^s M$ avec $s = 4$ et $M = 35$.
2. Combien de solution possède l'équation $a^{2M} \equiv -1 \mod 3$?
3. En déduire que $S = \left\{a \in (\mathbb{Z}/N\mathbb{Z})^* \mid a^M = \pm 1\right\}$.
4. Calculer $|S|$.

Exercice 9. On propose une méthode "rapide" (du point de vue algorithmique) pour vérifier si un nombre de Fermat $F_n := 2^{2^n} + 1$ est premier.

1. Montrer que, si F_n est premier, alors $3^{\frac{F_n - 1}{2}} \equiv \pm 1 \mod F_n$.
2. Montrer que F_n est premier si et seulement si il existe dans $(\mathbb{Z}/F_n\mathbb{Z})^*$ un élément d'ordre $F_n - 1$.
3. Supposons $3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$, montrer que F_n est premier [Indication : calculer l'ordre de 3 mod F_n].

Note : la réciproque est vraie, i.e. si F_n est premier, alors $3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$, on peut prouver cela en utilisant la loi de réciprocité quadratique.

SYSTÈME RSA

On suppose que $N = pq$ est le produit de deux premiers distincts, que c est le paramètre pour coder, i.e. on transforme un message m en $m' = m^c \mod N$ avant de l'envoyer. On note d l'inverse de $c \mod \phi(N)$, de sorte que le décodage s'effectue en calculant $m = m'^d \mod N$. Dans le système RSA les paramètres (N, c) sont publics, le paramètre d est secret.

Exercice 10. Soit $N = 39$ et $c = 29$.

1. Calculer d.
2. Coder le message $m = 2$ et vérifiez le résultat en le décodant.

Exercice 11. Votre clef publique est $(N, c) = (35, 5)$, vous recevez le message $m' = 10$, retrouver le message original m.

Exercice 12. Dans une entreprise deux employés paresseux choisissent d'utiliser le même $N = pq$ mais avec tout de même c_1 et c_2 différents mais supposés premiers entre eux (et donc chacun connait sa clef secrète d_1 ou d_2). Le patron imprudent envoie un message m sous les deux formes cryptées $m_1 = m^{c_1}$ au premier employé, $m_2 = m^{c_2}$ au deuxième employé. En suivant les étapes, montrer que le concurrent indélicat qui intercepte les deux messages m_1 et m_2 peut retrouver m ainsi :

étape 1 Calculer b_1 l'inverse de $c_1 \mod c_2$.

étape 2 Calculer $b_2 = \frac{b_1 c_1 - 1}{c_2}$.

étape 3 Calculer $m_1^{b_1} m_2^{-b_2} \mod N$. [Justifier que ce dernier est égal à $m \mod N$ et que chacun des calculs peut être effectué rapidement.]

Exercice 13. Trois amis choisissent des clefs avec cette fois-ci le même exposant $c = 3$ et des entiers N_1, N_2, N_3 différents ; une amie commune leur envoie le message m sous la forme $m_1 = m^3 \mod N_1$ (au premier), $m_2 = m^3 \mod N_2$ (au second) et $m_3 = m^3 \mod N_3$ (au troisième). Un espion intercepte les trois messages.

1. Montrer que l'espion peut calculer $m^3 \mod N_1 N_2 N_3$.
2. Supposons que $m \in [1, N_i]$ pour $i = 1, 2, 3$, montrer que l'espion peut calculer m^3.
3. Conclure que l'espion peut déchiffrer le message.

Exercice 14. Soit $N = pq$ impair avec $p > q$

1. Vérifier que $N = t^2 - s^2 = (t + s)(t - s)$ avec $t = \frac{p+q}{2}$ et $s = \frac{p-q}{2}$.
2. On suppose maintenant que p est très proche de q (ou encore que s est petit), montrer que t est supérieur à $\sqrt{N}$ et très proche de $\sqrt{N}$.
3. Utiliser ces remarques pour factoriser $N = 4397231$.

[La racine carrée de N vaut 2096,... On essaie pour $t = 2097$, 2098, etc si $t^2 - N$ est un carré ; la stratégie est gagnante pour 2100.]

PROTOCOLE EL GAMAL, GÉNÉRATEURS DE $(\mathbb{Z}/p\mathbb{Z})^*$

Exercice 15. Vérifier que 2 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^*$. Trouver a tel que $2^a = 3$ dans $(\mathbb{Z}/11\mathbb{Z})^*$.

Exercice 16. Vérifier que -2 est un générateur de $(\mathbb{Z}/23\mathbb{Z})^*$. Trouver a tel que $(-2)^a = 13$.

Exercice 17. Soit G un groupe cyclique, soit x un élément d'ordre r et y un élément d'ordre s.

1. Montrer que le sous-groupe H engendré par x et y est un groupe cyclique.

2. Soit $t = ppcm(r, s)$ et soient a, b deux nombres entiers tels que $t = ar$ et $t = bs$. Montrer que $pgcd(a, b) = 1$.
3. En écrivant $1 = ua + vb$ avec $u, v \in \mathbb{Z}$, on pose $z = x^u y^v$ et on admet le fait que z est d'ordre t dans G et que z est un générateur de H. Calculer un générateur de $G = (\mathbb{Z}/41\mathbb{Z})^*$ en suivant les étapes :
   - Calculer l'ordre de 2.
   - Calculer l'ordre de 3.
   - Donner un générateur de G.
4. Combien de générateurs le groupe $(\mathbb{Z}/41\mathbb{Z})^*$ possède-t-il ?