Université Paris Diderot
Département de Sciences Exactes

MI4– Année 2009/10
L2 Info

Feuille d'exercices n°4 :

Test de primalité, cryptographie (RSA)

TESTS DE PRIMALITÉ

Si $N \geq 2$ est impair et $\text{pgcd}(a, N) = 1$*, 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 1 Calculer le cardinal de H et S pour les valeurs suivantes : $N = 9$, 15, $N = 91$.

Exercice 2

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 (Cf feuille précédente) on a
$$\frac{|H|}{\phi(N)} \leq \frac{1}{2}$$
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 $c \equiv +1 \mod p$ 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 3 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 4 Soit $N = 561 = 3.11.17$ le plus petit nombre de Carmichaël, on se propose de calculer le cardinal de S.

1. Vérifier que $N-1=2^sM$ 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 5 [Exercice numérique : à faire sur un ordinateur] Trouver le plus petit entier N impair composé tel que :

1. N vérifie $F(2,N)$, $F(3,N)$, $F(5,N)$.
2. N vérifie $T(2,N)$, $T(3,N)$, $T(5,N)$.

Exercice 6 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 $3^{\frac{F_n-1}{2}}\equiv -1$, 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 $3^{\frac{F_n-1}{2}}\equiv -1$.

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 7 Soit $N=39$ et $c=29$.

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

Exercice 8 Votre clef publique est $(N,c)=(35,5)$, vous recevez le message $m'=10$, retrouver le message original m.

Exercice 9 Dans une entreprise deux employés paresseux choisissent d'utiliser le même $N=pq$ mais avec tout de même c_1 et c_2 différents (et donc chacun connait 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. Montrer que le concurrent indélicat qui intercepte les deux messages m_1 et m_2 peut retrouver m ainsi :

1. Calculer b_1 l'inverse de $c_1 \mod c_2$ [On suppose donc que c_1 et c_2 sont premiers entre eux, ce qui est raisonnable].
2. Calculer $b_2=\frac{b_1c_1-1}{c_2}$.

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 10 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 11 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 $2100^2 - N = 4410000 - 4397231 = 12769 = 113^2$ On en tire $p = 2213$ et $q = 1987$.]

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

Exercice 12 Vérifier que 2 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^*$. Trouver a tel que $2^a = 3$.

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

Exercice 14 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 engendré par x et y a pour cardinal $\mathrm{ppcm}(r, s)$.
2. Comment peut-on choisir un générateur de la forme $g = x^i y^j$?
3. Soit $G = (\mathbb{Z}/41\mathbb{Z})^*$; calculer l'ordre de 2 (resp. l'ordre de 3) et en déduire un générateur en utilisant la question précédente.
4. Combien de générateurs le groupe $(\mathbb{Z}/41\mathbb{Z})^*$ possède-t-il ?