Université Bordeaux 1
Mathématiques

MAT823 – Calcul Formel
Année 2007–2008

Deuxième session, 15 juin 2007

Durée 3 heures. Documents interdits, calculettes autorisées.

Exercice 1 – 17 est-il un carré modulo 77 ?

Exercice 2 – On choisit l'ordre lexicographique sur les monômes de $\mathbb{C}[x, y, z]$, avec $x > y > z$.
a) Calculer un reste de la division de $x^2 + xy + yz$ par $(x + y + z, y^2 + yz + z^2, z^3)$.
b) Parmi les éléments suivants lesquels sont des restes possibles d'une division de $f \in \mathbb{C}[x, y, z]$ par les trois polynômes ci-dessus : $2yz + 3$, $yz^2 + yz + z^2 + 1$, xyz ?

Exercice 3 – On dit que l'entier $N > 1$ vérifie la condition (C) de Carmichael si

$$\text{(C)} \qquad a^N \equiv a \pmod N \quad \text{pour tout } a \in \mathbb{Z}.$$

1) On suppose que N vérifie (C) et que p est un diviseur premier de N.
a) Montrer par l'absurde que $p^2 \nmid N$.
b) Montrer que $p - 1 \mid N - 1$.

2) Réciproquement, montrer que tout N vérifiant les deux conditions du 1) pour tout diviseur premier p de N vérifie (C).

3) Montrer par l'absurde que, si N vérifie (C), il n'est pas de la forme $N = pq$, où p et q sont premiers. [*On peut supposer $p < q$; montrer que $p \equiv 1 \pmod{q-1}$.*]

4) On suppose que N vérifie (C), et qu'il est impair. On écrit $N - 1 = 2^e q$, q impair, et on applique avec succès le test de non-primalité de Rabin-Miller à N : on dispose donc de $a \in \mathbb{Z}/N\mathbb{Z}$ qui est témoin de non-primalité.
a) Montrer que $a^{N-1} = 1$ ou bien $\mathrm{pgcd}(a, N) > 1$.
b) Montrer qu'on peut facilement en déduire un facteur non trivial de N. [*Dans le cas intéressant, combien de racines carrées de* 1 *connaît-on ?*]

Problème

Soit $N = pq$ produit de deux nombres premiers impairs distincts ; on pose $T := \log N$. On pourra supposer qu'addition et multiplication dans $\mathbb{Z}/N\mathbb{Z}$ utilisent $\widetilde{O}(T)$ opérations élémentaires, ainsi que le calcul du symbole de Jacobi $\left(\frac{a}{N}\right)$ quand $|a| < N$.

1) Soit $a \in (\mathbb{Z}/N\mathbb{Z})^*$. Montrer que a est un carré si et seulement si $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$.

2) Dans cette question, on veut décider si $a \in (\mathbb{Z}/N\mathbb{Z})^*$ est un carré.
a) Montrer que si $\left(\frac{a}{N}\right) = -1$, alors a n'est pas un carré.
b) Montrer que si $\left(\frac{a}{N}\right) = 1$, on ne peut rien dire.
c) Montrer que, connaissant a, p et q, on peut répondre à la question en temps $\widetilde{O}(T)$.
d) Écrire une fonction Maple complète qui prend en argument a, p, q comme ci-dessus et répond `true` ou `false`.

3) Dans cette question, on suppose connus p et q.

a) Donner un algorithme probabiliste pour trouver un d qui ne soit pas un carré dans $\mathbb{Z}/N\mathbb{Z}$, *mais* satisfaisant $\left(\frac{d}{N}\right) = 1$.

b) Calculer l'espérance du nombre d'essais avant d'obenir d.

4) Le procédé cryptographique RSA fonctionne de la façon suivante : Alice choisit $N = pq$, ainsi que d, e dans $]2, N[$ tels que $de \equiv 1 \pmod{\varphi(N)}$ et publie d et N (clé publique). Tout un chacun peut alors chiffrer un message $M \in \mathbb{Z}/N\mathbb{Z}$ à destination d'Alice en calculant $C = M^d$; munie de sa clé privée e, Alice déchiffre C en calculant $C^e = M$.

a) Montrer que C et M sont de taille $O(T)$ puis que chiffrage et déchiffrage utilisent $\widetilde{O}(T^2)$ opérations élémentaires.

b) On suppose N et $\varphi(N) = (p-1)(q-1)$ connus. Écrire un programme Maple en déduisant p et q, sans utiliser de commande de factorisation.

5) Détailler et commenter le protocole cryptographique suivant :

> Alice choisit $N = pq$ et d comme au **3)** : (d, N) est sa clé publique, et (p, q) sa clé secrète. Pour chiffrer un message, constitué d'une suite finie $(\varepsilon_n) \in \{0,1\}^k$ de 0 et de 1, on construit une suite $(x_n) \in (\mathbb{Z}/N\mathbb{Z})^k$ de la façon suivante : pour $u_n \in (\mathbb{Z}/N\mathbb{Z})^*$ choisi uniformément au hasard, il pose
> $$x_n := u_n^2 d^{\varepsilon_n}$$
> et expédie le message chiffré (x_n). Alice, munie de sa clé secrète, peut facilement décider si x_n est un carré modulo N ou non, et ainsi déterminer ε_n pour tout n.

6) Modifier le protocole précédent pour permettre à Alice de donner une « preuve probabiliste » qu'elle connaît la factorisation de $N = pq$, sans dévoiler aucune information sur ladite factorisation. Plus précisément, décrire une épreuve en k étapes qu'Alice n'aurait qu'une chance sur 2^k de réussir si elle répondait au hasard.