Université Bordeaux 1 — **MHT812/MHT839 – Calcul Formel**
Mathématiques — Année 2012–2013

**Examen, 21 avril 2008, 8h30 – 11h30**
**Durée 3 heures. Documents interdits, calculettes autorisées.**

Les exercices sont essentiellement indépendants (à part II.2 et III.5). Soit $N > 1$, on rappelle que :

- Si $a, b$ sont deux entiers de valeur absolue $\leqslant N$, la complexité binaire des opérations suivantes est $\widetilde{O}(\log N)$ : $a \pm b$, $a \times b$, division euclidienne de $a$ par $b$, calcul de $\mathrm{pgcd}(a, b)$.
- le calcul de $x^N$ dans un groupe $G$ nécessite $O(\log N)$ multiplications.

**Exercice I** – Soit $N = pq$, produit de deux nombres premiers impairs distincts et soit $P \in \mathbb{Z}/N\mathbb{Z}$ un « message ». Le protocole cryptographique RSA repose sur le principe suivant :

- un expéditeur connaissant les paramètres *publics* $N$ et $c \in (\mathbb{Z}/\varphi(N)\mathbb{Z})^*$ peut calculer et transmettre un message chiffré $Q = P^c \in \mathbb{Z}/N\mathbb{Z}$, sous la forme de son représentant dans $[0, N-1]$.
- si le récepteur connaît la factorisation de $N$, il peut déchiffrer $Q$, en calculant successivement $\varphi(N) = (p-1)(q-1)$, un inverse $d$ de $c$ dans $(\mathbb{Z}/\varphi(N)\mathbb{Z})^*$ et $Q^d = P^{cd} = P$ dans $\mathbb{Z}/N\mathbb{Z}$.

[*On ne demande pas de justifier ou détailler les assertions ci-dessus.*] Connaître la factorisation de $N$ permet manifestement de déchiffrer. On veut réciproquement montrer que la connaissance d'un $d$ tel que $cd \equiv 1 \pmod{\varphi(N)}$ permet de factoriser $N$ facilement.

**1)** Soit $\ell$ un nombre premier et $t > 0$ un entier.

a) Montrer que l'équation $a^t \equiv 1 \pmod{\ell}$ a exactement $\mathrm{pgcd}(t, \ell - 1)$ solutions $a \in \mathbb{Z}/\ell\mathbb{Z}$.

b) En déduire que le nombre de $a \in \mathbb{Z}/N\mathbb{Z}$, qui sont solutions de $a^t \equiv 1 \pmod{N}$ est $\mathrm{pgcd}(t, p-1)\,\mathrm{pgcd}(t, q-1)$.

**2)** On suppose dorénavant que $t$ est *impair*.

a) Montrer qu'au plus $1/4$ des $(p-1)(q-1)$ éléments de $(\mathbb{Z}/N\mathbb{Z})^*$ vérifient $a^t = 1$.

b) Plus généralement, montrer que pour tout $b \in (\mathbb{Z}/N\mathbb{Z})^*$ fixé, au plus $1/4$ des éléments de $(\mathbb{Z}/N\mathbb{Z})^*$ vérifient $a^t = b$.

**3)** On suppose donc $c, d, N$ connus comme dans l'introduction et on écrit $cd - 1 = 2^e t$, avec $t$ impair.

a) Montrer que pour tout $a \in (\mathbb{Z}/N\mathbb{Z})^*$ on a $a^{t2^e} = 1$, puis que pour au moins la moitié d'entre eux il existe $0 < i \leqslant e$ tel que $x := a^{t2^{i-1}} \neq \pm 1$ et $x^2 = a^{t2^i} = 1$.

b) Comment déduire la factorisation de $N$ de l'équation $(x-1)(x+1) \equiv 0 \pmod{N}$ ?

**4)** Écrire un algorithme *probabiliste* complet de factorisation de $N$, sous l'hypothèse que l'on connaît une clé de décodage RSA $d$ et les paramètres publics $c, N$.

**5)** Peut-on en déduire qu'il est essentiellement aussi difficile de factoriser un entier $N$ et de casser un système RSA reposant sur $N$ ?

**Exercice II** – Soit $(G, \times)$ un groupe. On suppose connue la factorisation de $n := |G| = \prod p_i^{e_i}$, où les $p_i$ sont premiers et 2 à 2 distincts.

**1)** a) Quelles sont les valeurs possibles pour l'ordre d'un élément $x$ de $G$ ?

b) On pose $q_1 := n/p_1^{e_1}$, puis $x_1 := x^{q_1}$. Quelles sont les valeurs possibles pour l'ordre de $x_1$ ? Comment le déterminer efficacement ?

c) Si $q$ est un entier non nul et $p$ un nombre premier, on note $v_p(q)$ le plus grand entier $k$ tel que $p^k \mid q$. Montrer que $v_{p_1}(\text{ordre}(x_1)) = v_{p_1}(\text{ordre}(x))$.

**2)** En déduire un algorithme pour calculer l'ordre de $x$ par le biais de sa factorisation. Estimer la complexité algébrique de votre algorithme (en nombre de multiplications dans $G$).

**Exercice III** – Soit $a/b \in \mathbb{Q}$ une fraction irréductible avec $\text{pgcd}(b, 10) = 1$ et $b \neq 0$. On définit une suite $r_i$ d'entiers modulo $b$ par divisions euclidiennes successives :

$$\begin{aligned} a &= q_0 b + r_0 \\ 10 r_0 &= q_1 b + r_1 \\ &\cdots \\ 10 r_{i-1} &= q_i b + r_i \end{aligned}$$

**1)** a) Trouver une formule simple pour $r_i$ (dans $\mathbb{Z}/b\mathbb{Z}$).

b) À quelle condition a-t-on $r_i = r_j$ ?

**2)** Montrer qu'il existe $i_0$ et $k > 0$ tel que $r_{i_0} = r_{i_0+k}$

**3)** Montrer que le développement décimal de $a/b$ est ultimement périodique, et que la période est égale à l'ordre de 10 dans $(\mathbb{Z}/b\mathbb{Z})^*$.

**4)** Écrire une fonction Maple calculant la période du développement décimal d'une fraction de dénominateur premier à 10, utilisant un Euclide modifié comme ci-dessus.

**5)** Estimer sa complexité binaire en supposant que $0 < a < b < N$ et $\text{pgcd}(a, b) = 1$. Comparer avec ce que donnerait la méthode de l'exercice II. [*On ne suppose pas la factorisation de b connue.*]