Examen, 05 mai 2006

Durée 3 heures. Documents interdits, calculettes autorisées.

Exercice 1 – Soit $N = 143$ et $\mathcal{B} = \{2, 3, 5\}$. On remarque que dans $\mathbb{Z}/N\mathbb{Z}$, on a $17^2 = 3$, $19^2 = 3 \times 5^2$ et $21^2 = 2^2 \times 3$. En *déduire* une identité $x^2 = y^2$ exhibant un facteur non trivial de N.

Exercice 2 – Trouver les solutions dans $\mathbb{Z}^2$ du système d'équations

$$\begin{cases} 3x + 2y & \equiv & 1 \pmod{9}, \\ 2x + 5y & \equiv & 0 \pmod{12}. \end{cases}$$

Exercice 3 – Soit $N > 1$ un entier.

1) Soit $p \mid N - 1$ un nombre premier et $e := v_p(N - 1)$. On suppose qu'il existe $a \in \mathbb{Z}$ vérifiant

- $a^{N-1} \equiv 1 \pmod{N}$,
- $\text{pgcd}\left(a^{(N-1)/p} - 1, N\right) = 1$.

Montrer que tout diviseur d de N vérifie $d \equiv 1 \pmod{p^e}$. [*On peut supposer d premier ; introduire l'ordre de a dans* $(\mathbb{Z}/d\mathbb{Z})^*$.]

2) On suppose que $N - 1 = FU$, où $F \geqslant \sqrt{N}$ est un facteur dont tous les diviseurs premiers sont connus, et que pour chaque $p \mid F$, on connaît $a(p)$ vérifiant les propriétés du 1). Soit $d > 1$ un diviseur de N.

a) Montrer que $d \equiv 1 \pmod{F}$.

b) En déduire que $d > \sqrt{N}$, puis que N est premier.

3) On suppose N premier, et on fixe $p \mid N - 1$. Tirant a uniformément au hasard dans $[1, N]$, quelle est la probabilité de trouver un $a(p)$ convenable ?

Problème (Multi-évaluation)

Dans les estimations de complexité, on utilisera la notation $\widetilde{O}$ pour ne pas avoir à tenir compte des facteurs logarithmiques ou des constantes. On rappelle qu'une opération ($+, \times$, division euclidienne ou pgcd) sur deux polynômes de degré $\leqslant n$ dans $K[X]$ utilise $\widetilde{O}(n)$ opérations élémentaires dans K. Une opération sur deux entiers de valeur absolue $\leqslant 2^n$ utilise $\widetilde{O}(n)$ opérations élémentaires sur des chiffres. Dans les deux cas, on dira « en temps $\widetilde{O}(n)$ » au lieu de « en utilisant $\widetilde{O}(n)$ opérations élémentaires ». On note $a \bmod b$ le reste de la division euclidienne de a par b.

1) Soit $P \in K[X]$ non constant, et $\mathcal{L} = [x_0, \ldots, x_{n-1}] \in K^n$ une liste d'éléments de K.

a) Écrire une procédure Maple qui teste si $P(x_i) \neq 0$ pour tout $0 \leqslant i < n$.

b) Majorer la complexité de cette procédure, en fonction de $\deg P$ et n.

2) Soit $N > 0$ un entier et $\mathcal{L} = [x_0, \ldots, x_{n-1}] \in \mathbb{Z}^n$ une liste de n entiers > 1.

a) Écrire une procédure MAPLE qui teste si N n'est divisible par aucun $x \in \mathcal{L}$.

b) Expliquer pourquoi on peut supposer que les éléments de $\mathcal{L}$ sont inférieurs à N. Majorer la complexité de cette procédure, en fonction de $\log N$ et n.

3) Expliquer en quoi les deux questions précédentes résolvent essentiellement le même problème.

4) On se concentre désormais sur le cas $N \in \mathbb{Z}$, $\mathcal{L} \in \mathbb{Z}^n$, plus facile à décrire, et on s'intéresse plus généralement à l'ensemble des $N \bmod \mathcal{L}[i]$. On suppose dans toute la suite que $\#\mathcal{L} = n = 2^k$ est une puissance de 2.

a) Montrer que l'on peut toujours se ramener à $n = 2^k$.

b) Pour $0 \leqslant i \leqslant k$ et $0 \leqslant j < 2^{k-i}$, on pose

$$M_{i,j} = \prod_{0 \leqslant \ell < 2^i} \mathcal{L}[j2^i + \ell].$$

Si $k = 3$, dessiner l'arbre binaire naturel dont les noeuds sont les $M_{i,j}$ et tel que chaque noeud contienne le produit de ses deux fils.

c) Montrer que l'ensemble des $M_{i,j}$ se calculent en temps $\widetilde{O}(\log \mathcal{L})$, où la taille totale $\log \mathcal{L}$ de la liste $\mathcal{L}$ est définie par $\log \mathcal{L} := \sum_{i \leqslant n} \log \mathcal{L}[i]$.

d) Écrire une procédure MAPLE calculant tous les $M_{i,j}$.

5) On suppose que les $M_{i,j}$ sont précalculés, stockés sur un arbre organisé de telle sorte que l'on puisse détacher le sous-arbre gauche ou droit de la racine, respectivement associés à la première ou deuxième moitié de $\mathcal{L}$, en temps négligeable. On ne s'intéressera pas à l'implantation de l'arbre[1]. On considère l'algorithme suivant

---

Entrées: $N \in \mathbb{Z}_{>0}$, un arbre des $M_{i,j}$ associé à une liste $\mathcal{L} \in \mathbb{Z}^n$. On suppose que $\log N < \log \mathcal{L}$ et $n = 2^k$.

Sorties: La liste des $N \bmod \mathcal{L}[i]$, $0 \leqslant i < n$.

Si $n = 1$, retourner N.

Soit $r_0 \leftarrow N \bmod M_{k-1,0}$. Calculer récursivement les $r_0 \bmod \mathcal{L}[i]$, $0 \leqslant i < n/2$.

Soit $r_1 \leftarrow N \bmod M_{k-1,1}$. Calculer récursivement les $r_1 \bmod \mathcal{L}[i]$, $n/2 \leqslant i < n$.

Renvoyer la concaténation des résultats.

---

a) Détailler le passage « Calculer récursivement… ». Avec quelles entrées rappelle-t-on la fonction ?

b) Montrer que l'algorithme est correct et calcule les $N \bmod \mathcal{L}[i]$ en temps $\widetilde{O}(\log \mathcal{L})$.

6) On rappelle que le crible d'Ératosthène calcule $\mathcal{L} := \{p \leqslant x \colon p \text{ premier}\}$ en temps $\widetilde{O}(x)$, et que $\log \mathcal{L} = \sum_{p \leqslant x} \log p \sim x$ quand $x \to \infty$.

a) Montrer que l'on peut trouver tous les facteurs premiers de N inférieurs à $\log N$ en temps $\widetilde{O}(\log N)$.

b) Comparer avec la méthode naïve de division successive par les éléments de $\mathcal{L}$. Utilisant la méthode récursive, à quel coût détecte-t-on *tous* les facteurs premiers de N (dans le cas le pire) ?

[1]La représentation standard de la structure de tas par un tableau unidimensionnel convient.