Université Bordeaux 1 **MHT812 – Master**
Mathématiques Année 2007–2008

Devoir Surveillé, 5 mars 2008

Durée 1h30. Documents interdits.

On rappelle que si a et b sont deux entiers de longueurs $\leqslant l$ (c'est-à-dire vérifiant $|a|, |b| < 2^l$), la complexité binaire des opérations suivantes est en $\tilde{O}(l)$: $a \pm b$, $a \times b$, division euclidienne de a par b, algorithme d'Euclide (étendu ou non) appliqué à a et b.

Exercice 1 – [Inversion modulaire via Fermat]
Soient p un nombre premier et a un entier vérifiant $0 < a < p$.

1) Montrer comment calculer l'inverse de a modulo p en se servant du petit théorème de Fermat. On rappelle que ce dernier s'énonce : $a^{p-1} \equiv 1 \mod p$.

2) Rédiger l'algorithme correspondant. On fera bien sûr appel à l'exponentiation binaire.

3) Estimer, en fonction de p, la complexité algébrique (nombre d'opérations dans $\mathbb{Z}$) et la complexité binaire de cet algorithme.

4) Rappeler comment se servir de l'algorithme d'Euclide étendu pour résoudre le même problème d'inversion.

5) Comparer les complexités binaires des deux procédés d'inversion.

Exercice 2 – [Newton linéaire]
Soient $\varphi \in \mathbb{Z}[X]$ et p un nombre premier. Soient également s et $g \in \mathbb{Z}$ vérifiant

(i) $\varphi(g) \equiv 0 \mod p^k$, pour un entier $k \geqslant 1$ donné
(ii) $s\varphi'(g) \equiv 1 \mod p$.

On définit h par $h \equiv g - s\varphi(g) \mod p^{k+1}$.

1) Montrer que $\varphi(h) \equiv 0 \mod p^{k+1}$, $h \equiv g \mod p^k$ et $s\varphi'(h) \equiv 1 \mod p$.

2) En déduire un algorithme qui, à partir de s et $g \in \mathbb{Z}$ vérifiant

(a) $\varphi(g) \equiv 0 \mod p$
(b) $s\varphi'(g) \equiv 1 \mod p$,

permet de trouver $h \in \mathbb{Z}$ vérifiant

(1) $\varphi(h) \equiv 0 \mod p^l$
(2) $h \equiv g \mod p$,

où $l \geqslant 1$ est un entier donné.

3) Soient P un polynôme de $\mathbb{Z}[X]$ de degré m et $a \in \mathbb{Z}$. Estimer la complexité algébrique (nombre d'opérations dans $\mathbb{Z}$) de l'évaluation de P en a en fonction de m.

4) Soit n le degré de φ. Estimer la complexité algébrique (nombre d'opérations dans $\mathbb{Z}$) de l'algorithme décrit en **2)** en fonction de l et n.

Exercice 3 – [Lemme chinois]
On cherche $f \in \mathbb{F}_5[X]$ vérifiant

$$(S)\ \left\{\begin{array}{rcll} f & \equiv & 1 & \mod x+1 \\ xf & \equiv & x+1 & \mod x^2+1 \\ (x^2-1)f & \equiv & x+1 & \mod x^3+1. \end{array}\right.$$

1) Transformer (S) en un système équivalent ne comportant que des congruences de la forme $f \equiv \nu \mod \mu$ avec $\nu, \mu \in \mathbb{F}_5[X]$.

2) Montrer que les μ précédemment obtenus sont premiers entre eux deux à deux.

3) Montrer que (S) admet une unique solution g de degré < 5 et décrire l'ensemble de toutes les solutions f de (S).

4) Calculer g.