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

**Corrigé du Devoir Surveillé du 03/03/2008**

**Exercice 1** –

**1)** Si un entier $N \geqslant 1$ admet $k$ chiffres en base 2, alors il s'écrit $N = \sum_{i=0}^{k-1} a_i 2^i$ avec $a_i \in \{0,1\}$ pour tout $i$ et $a_{k-1} = 1$. On a donc $2^{k-1} \leqslant N < 2^k$, d'où $k-1 \leqslant \log_2 N < k$. On en déduit que $k = \lfloor \log_2 N \rfloor + 1$.

**2)** Par récurrence sur $k \in \mathbb{N}$, on montre d'abord que $T(2^k) \leqslant 2^k T(1) + k2^k$. Si $N \geqslant 1$ est un entier quelconque, on peut trouver un entier $k \geqslant 1$ tel que $2^{k-1} \leqslant N < 2^k$. Comme $T$ est croissante, on a donc $T(N) \leqslant T(2^k) \leqslant 2^k(k + T(1))$. Comme $k - 1 \leqslant \log_2 N$, on a donc $T(N) \leqslant \frac{2}{\ln 2} N(lnN + (1 + T(1)) \ln 2) = O(N \ln N)$.

**3)** Si $p$ est un nombre premier et $k \geqslant 1$ un entier, alors on peut construire un corps fini de cardinal $p^k$ en prenant $\mathbb{F}_p[X]/(P)$, où $P$ est un polynôme irréductible dans $\mathbb{F}_p[X]$ de degré $k$. Le polynôme $P := X^3 + X^2 + X + 1 \in \mathbb{F}_3[X]$ est de degré 3, sans racine dans le corps $\mathbb{F}_3$, donc il est irréductible dans $\mathbb{F}_3[X]$. Par conséquent, le quotient $\mathbb{F}_3[X]/(X^3 + X^2 + X + 1)$ est un corps fini de cardinal 27. De même, il n'existe qu'un polynôme irréductible de degré 2 dans $\mathbb{F}_2[X]$ c'est $X^2 + X + 1$. Donc, si un polynôme de degré 4 est réductible dans $\mathbb{F}_2[X]$, alors, soit il a une racine dans $\mathbb{F}_2$, soit il est égal à $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. On en déduit que $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$ et que $\mathbb{F}_2[X]/(X^4 + X + 1)$ est un corps fini de cardinal 16.

**Exercice 2** –

**1)** L'application $u : \mathcal{P}_k \to (\mathbb{F}_q)^n$ qui à $P$ associe $(P(x_1), \ldots, P(x_n))$ est $\mathbb{F}_q$-linéaire et $\Gamma$ est l'image de $u$. Comme $P \in \mathcal{P}_k$ ne peut s'annuler en les $n$ valeurs distinctes $x_1, \ldots, x_n$ sans être nul (car $k \leqslant n$), on voit que $u$ est injective. On en déduit que $\Gamma$ est un sous-espace vectoriel de $(\mathbb{F}_q)^n$ de dimension $k$.

**2)**a) On écrit $Q_0$ (resp. $Q_1$) sous la forme $Q_0 = a_0 + \cdots + a_{n-1-t} X^{n-1-t}$ pour certains $a_i$ à trouver dans $\mathbb{F}_q$ (resp. $Q_1 = b_0 + \cdots + b_{n-1-t-(k-1)} X^{n-1-t-(k-1)}$ avec des $b_i \in \mathbb{F}_q$). Les conditions $Q_0(x_i) + r_i Q_1(x_i) = 0$ pour $i \in \{1, \ldots, n\}$ montrent que les coefficients de $Q_0$ et $Q_1$ que l'on cherche doivent vérifier un système linéaire homogène à $n$ équations. Or le nombre d'inconnues est $n - t + n - t - k + 1 = 2n - k + 1 - 2t$. Puisque $t = \lfloor (n-k)/2 \rfloor$, on voit qu'il y a au moins $n+1$ inconnues et le système admet donc au moins une solution non nulle. Il existe donc bien un polynôme non nul $Q \in \mathbb{F}_q[X, Y]$ vérifiant les conditions voulues.

b) Le polynôme $Q(X, P(X)) = Q_0(X) + P(X)Q_1(X) \in \mathbb{F}_q[X]$ a un degré $\leqslant \max(\deg Q_0, \deg P + \deg Q_1) \leqslant n - t - 1$. Par ailleurs, l'hypothèse $(*)$ montre qu'il y a au moins $n - t$ valeurs de $i \in \{1, \ldots, n\}$ telles que $P(x_i) = m_i = r_i$ et, pour ces valeurs, on a $Q(x_i, P(x_i)) = 0$. Le polynôme $Q(X, P(X))$ a donc au moins $n - t$ racines dans $\mathbb{F}_q$ et est de degré $\leqslant n - t - 1$. Par conséquent,

$Q(X, P(X)) = 0$. On en tire $Q_0 = -PQ_1$. Remarquons que $Q_1 \neq 0$, car sinon on aurait $Q(X, Y) = Q_0 = 0$ aussi. De ce fait, $Q_1$ divise $Q_0$ et on a $P = -Q_0/Q_1$.

c) Pour calculer $m$ à partir de $r$, on cherche d'abord un $Q(X, Y) \neq 0$ en résolvant le système linéaire du 2)a). L'hypothèse $(*)$ entraine alors que $Q_1$ divise $Q_0$ et en faisant la division euclidienne on trouve $P = -Q_0/Q_1$. Finalement, $m = (P(x_1), \ldots, P(x_n))$. Pour ce qui est de la complexité, le calcul de Q demande de résoudre un système linéaire à $n$ équations et $O(n)$ inconnues, ce qui par le pivot demande $O(n^3)$ opérations dans $\mathbb{F}_q$ ; le calcul de $P$ par division euclidienne de $Q_0$ par $Q_1$ demande $O(n^2)$ opérations par la méthode usuelle car les deux polynômes ont un degré $\leqslant n$ ; enfin, le calcul de $m$ par évaluation de $P$ en les $n$ points $x_i$ demande $O(kn) = O(n^2)$ opérations. En tout, celà donne un coût en $O(n^3)$.

**3)** Dans notre exemple, on a $t = 1$, $degQ_0 \leqslant 2$ et $degQ_1 \leqslant 1$. La résolution du système linéaire $Q(1, 0) = Q(2, 4) = Q(3, 3) = Q(4, 0) = 0$ donne $Q_0 = a(X^2 - 1)$ et $Q_1 = a(X + 1)$ avec $a \in \mathbb{F}_5$ non nul. On peut donc prendre $Q_0 = X^2 - 1$ et $Q_1 = X + 1$. Si la condition $(*)$ est vraie, alors $P = -X + 1$ et $m = (0, 4, 3, 2)$. Il y a donc bien une erreur dans ce cas.

**Exercice 3** –

**1)** Les polynômes $P_1, \ldots, P_k \in \mathbb{F}_p[X]$ étant irréductibles non associés, ils sont premiers entre eux deux à deux. Le lemme chinois dit que l'application naturelle $f$ de $A := \mathbb{F}_p[X]/(P)$ vers $\mathbb{F}_p[X]/(P_1) \times \cdots \times \mathbb{F}_p[X]/(P_k)$ qui à $Q \mod P$ associe $(Q \mod P_1, \ldots, Q \mod P_k)$ est un isomorphisme de $\mathbb{F}_p$-algèbres. Par ailleurs, pour tout $i \in \{1, \ldots, k\}$, le quotient $\mathbb{F}_p[X]/(P_i)$ est un corps commutatif car $P_i$ est irréductible dans l'anneau principal $\mathbb{F}_p[X]$. Ce corps est fini de cardinal $p^{\deg P_i}$ car, par division euclidienne, tout $Q \in \mathbb{F}_p[X]$ est dans la classe d'un unique $Q_0 \in \mathbb{F}_p[X]$ de degré $< \deg P_i$.

**2)** Notons que, puisque l'on est en caractéristique $p$, l'application $\Phi$ est bien $\mathbb{F}_p$-linéaire. Comme l'application $f$ du lemme chinois est un isomorphisme de $\mathbb{F}_p$-algèbres, le noyau de $\Phi$ s'identifie par $f$ à l'ensemble des éléments de l'anneau-produit $\prod_{i=1}^{k} \mathbb{F}_{p^{\deg P_i}}$ qui sont fixes par l'élévation à la puissance $p$. Or, dans le corps fini $\mathbb{F}_{p^{\deg P_i}}$, les racines de $X^p - X$ sont exactement les éléments de $\mathbb{F}_p$. L'application $f$ induit donc un isomorphisme de $\mathbb{F}_p$-espaces vectoriels entre $\mathrm{Ker}(\Phi)$ et $(\mathbb{F}_p)^k$. Par le théorème du rang, on a alors $k = \dim_{\mathbb{F}_p} A - \mathrm{rg}(\Phi) = n - \mathrm{rg}(\Phi)$.

**3)**a) Dans $\mathbb{F}_p[X][Y]$, on a $Y^p - Y = \prod_{a \in \mathbb{F}_p}(Y - a)$. En sustituant $Q \in \mathbb{F}_p[X]$ dans $Y$, on trouve $Q^p - Q = \prod_{a \in \mathbb{F}_p}(Q - a)$.

b) Les $a \mod P$ pour $a \in \mathbb{F}_p$ sont toujours dans $Ker(\Phi)$. Si $k > 1$, alors on peut trouver dans le noyau de $\Phi$ une classe $Q \mod P$ avec $Q$ non congru à une constante modulo $P$. Comme $Q \in \mathrm{Ker}(\Phi)$, on a $Q^p - Q \equiv 0 \mod P$, donc $P$ divise $Q^p - Q = \prod_{a \in \mathbb{F}_p}(Q - a)$ dans $\mathbb{F}_p[X]$ par le a). Si pour tout $a \in \mathbb{F}_p$, le polynôme $P$ était premier avec $Q - a$, alors $P$ serait premier avec $Q^p - Q$. Comme $P$ divise $Q^p - Q$ et est non constant, c'est impossible. Donc il existe $a \in \mathbb{F}_p$ tel

que $\mathrm{pgcd}(P, Q-a) \neq 1$. Si ce pgcd était $P$ (à un inversible près), alors on aurait $Q \equiv a \mod P$. Or, par hypothèse sur le choix de $Q$, c'est faux. Pour ce $a$, on voit donc que $\mathrm{pgcd}(P, Q-a)$ est un facteur non trivial de $P$.

**4)** Pour calculer $k$ on détermine d'abord la matrice $M$ de $\Phi$ dans une base simple de $A$, par exemple $\mathcal{B} := (1, x, \ldots, x^{n-1})$, où $x$ est la classe de $X$ dans $A$. Le calcul de $x^p \mod P$ par exponentiation rapide modulo $P$ nécessite $O(\log p)$ operations dans $A$ ; la complexité d'une opération dans $A$ est $\widetilde{O}(n \log p)$ ; soit $\widetilde{O}(n \log^2 p)$ au total. Les $(x^i)^p = (x^{i-1})^p \times x^p$ pour $i > 1$ s'obtiennent en $n-1$ multiplication dans $A$ successives, soit un coût $\widetilde{O}(n^2 \log p)$. Bien sûr $(x^0)^p = 1$. En tout, nous en sommes à $O(n \log p(n + \log p))$ pour construire $M$.

Le calcul du rang de $M \in M_n(\mathbb{F}_p)$ par le pivot demande $O(n^3)$ opérations dans $\mathbb{F}_p$, d'où une complexité $\widetilde{O}(n^3 \log p)$ pour calculer $k$, et en fait pour calculer une forme échelonnée de $M$. Il faut ensuite trouver $Q$ si $k > 1$.

On obtient une base de $\mathrm{Ker}(\Phi)$ en résolvant un système de Cramer triangulaire de taille $\mathrm{rg}(M) \leqslant n$ : celà nécessite $O(n^2)$ opérations dans $\mathbb{F}_p$. On prend $Q$ parmi cette base de $\mathrm{Ker}(\Phi)$. Ensuite, on calcule un à un les $\mathrm{pgcd}(P, Q-a)$, $a \in \mathbb{F}_p$ jusqu'à en trouver un de degré $\in ]0, n[$. La complexité binaire de cette étape est au plus $p\widetilde{O}(n \log p) = \widetilde{O}(pn)$.

Finalement, le calcul total d'un facteur non trivial lorsque $k > 1$ a pour complexité $\widetilde{O}(pn + n^3 \log p)$.