Université Bordeaux 1 — **MHT911 – Algorithmique**
Mathématiques — Année 2012–2013

Partiel, 14 novembre 2008 (10:15 – 12:15)
Durée 2 heures. Notes de cours et programmes GP autorisés.

La clarté des programmes et la pertinence des commentaires est un élément important d'appréciation.

- Pour répondre aux questions, créer *un* fichier par exercice, intitulés `login1.gp`, puis `login2.gp`, etc. Par exemple, `kbelabas1.gp`.
- Pour rendre votre copie, taper `~kbelabas/copie` dans un terminal, depuis le répertoire où se trouvent vos fichiers. (Vous pouvez rendre plusieurs fois votre copie : seule la dernière fait foi, les précédentes sont détruites.)

Autour de la Transformation de Fourier rapide (FFT).

Soit $n > 1$ un entier, et K un corps commutatif contenant une racine primitive n-ième de l'unité ω, c'est-à-dire que ω est d'ordre exactement n dans $(K^*, \times)$. On pose par définition $\omega^0 = 1$. En particulier, si $K = \mathbb{F}_q$ est un corps fini, un tel ω existe si et seulement si $n \mid (q-1)$.

Exercice 1 – [Exemples]

1) Trouver un tel ω pour $q =$ `nextprime(10^60)` et $n = q - 1$.

2) Trouver un tel ω d'ordre 2^{16} dans un corps fini quadratique $\mathbb{F}_{p^2}$, tel que $\omega \notin \mathbb{F}_p$.

3) On fixe $n = 2^{32}$; trouver p premier satisfaisant $n \mid p-1$ et un ω d'ordre n dans $\mathbb{F}_p^*$.

Exercice 2 – [Transformée de Fourier]
On note $(a_i \colon 0 \leqslant i < n)$ pour $(a_0, \dots, a_{n-1})$. Soit $(a_i \colon 0 \leqslant i < n) \in K^n$, que l'on considère comme donnant les coefficients du polynôme $f = \sum_{i=0}^{n-1} a_i X^i$ de $K[X]$. La Transformée de Fourier de (a_i) relativement à ω est le vecteur

$$\mathcal{F}((a_i), \omega) = \mathcal{F}(f, \omega) = (b_j \colon 0 \leqslant j < n) \in K^n, \quad \text{où} \quad b_j = f(\omega^j).$$

Si $k \in \mathbb{Z}$, on a $\sum_{i=0}^{n-1} \omega^{ik} = 0$ si $n \nmid k$ et la somme vaut n sinon. On en déduit que

$$\mathcal{F}((b_j \colon 0 \leqslant j < n), \omega^{-1}) = (n a_i \colon 0 \leqslant i < n),$$

ce qui donne une formule simple pour la transformée inverse $\mathcal{F}^{-1}(\cdot, \omega) = \frac{1}{n}\mathcal{F}(\cdot, \omega^{-1})$.

1) Programmer un algorithme naïf pour calculer la transformée de Fourier de (a_i) en $O(n^2)$ opérations dans K (additions et multiplications).

2) Même question pour la transformée inverse.

Exercice 3 – [FFT]
On suppose dorénavant que $n = 2^k$, pour un entier $k \geqslant 1$. Pour $f \in K[X]$ de degré au plus n, ou définit f_{pair} et f_{impair} par

$$f = \sum_{i=0}^{n-1} a_i X^i = f_{\text{pair}}(X^2) + X f_{\text{impair}}(X^2).$$

Soient

$$(u_i \colon 0 \leqslant i < n/2) = \mathcal{F}(f_{\text{pair}}, \omega^2),$$
$$(v_i \colon 0 \leqslant i < n/2) = \mathcal{F}(f_{\text{impair}}, \omega^2).$$

Par abus de language, u_j et v_j sont prolongés par périodicité modulo $n/2$. On a alors $f(\omega^j) = u_j + \omega^j v_j$ pour tout $j \geqslant 0$.

1) Programmer un algorithme de calcul récursif de $\mathcal{F}(f, \omega)$, s'inspirant de ces formules.

2) En supposant que l'ensemble de ω^i, $i < n$ sont précalculées, l'algorithme utilise $O(n \log n)$ opérations dans K. Pour plusieurs corps K bien choisis, déterminer des seuils expérimentaux à partir desquels on bat l'algorithme naïf.

Exercice 4 – [Application : multiplication dans $\mathbb{Z}[X]$]
Soient $f, g \in \mathbb{Z}[X]$ deux polynômes non constants de degrés inférieurs à $n = 2^k$, et de norme infinie inférieure à B.

1) Écrire une fonction trouvant un nombre premier $p > 2(n+1)B^2$, tel que $\mathbb{F}_p$ contienne une racine primitive $2n$-ième de l'unité ω.

2) Préciser et implanter l'algorithme suivant du calcul de $f \times g$:

- Calculer $(u_i) = \mathcal{F}(f, \omega)$ et $(v_i) = \mathcal{F}(g, \omega)$.
- $f \times g$ est un relèvement à $\mathbb{Z}[X]$ convenable de

$$\frac{1}{2n} \mathcal{F}\big((u_i v_i \colon 0 \leqslant i < 2n), \omega^{-1}\big).$$

On pourra en particulier remarquer que les coefficients de $f \times g$ sont de valeur absolue inférieure à $(n+1)B^2$, et que $2n$ est nécessairement inversible modulo p.

3) Proposer et évaluer une implantation utilisant l'algorithme ci-dessus modulo plusieurs *petits* premiers p et reconstruisant le résultat par lemme chinois.

4) Proposer et évaluer une implantation utilisant des calculs approchés dans $\mathbb{C}$ (dans lequel existent des ω de tout ordre) au lieu de calculs exacts dans $\mathbb{F}_p$.

Exercice 5 – [Application : multiplication dans $\mathbb{Z}$]
On fixe $k > 0$, $n = 2^k$ et $B = 2^{16}$. On veut multiplier deux entiers positifs F, G strictement inférieus à $2^{16 \times 2^k} = B^n$. On écrit

$$F = f(B), \quad G = g(B)$$

les décompositions en base B de ces deux entiers, où f, g sont deux polynômes de $\mathbb{Z}[X]$ de degré $< n$ de norme infinie $< B$. On calcule $FG = (f \times g)(B)$.