Magistère E.N.S. d'Ulm – Universités parisiennes (FIMFA) 2007-2008
Cours de Théorie algorithmique des nombres. (Marc Hindry)

Devoir tenant lieu de partiel (à rendre au plus tard à la rentrée des congés d'avril). Le devoir est copieux, vous pouvez vous contenter des trois petits exercices et du problème A ou B.

Exercice 1. On rappelle la définition des polynômes cyclotomiques $\Phi_n(X) = \prod_{\zeta \in \mu_n^*}(X - \zeta)$ où μ_n^* est l'ensemble des racines n-èmes *primitives* de l'unité. les polynômes cyclotomiques, a priori définis dans $\mathbf{C}[X]$ sont dans $\mathbf{Z}[X]$ (et sont irréductibles, mais on ne se sert pas de ce fait ici) et vérifient $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.
a) Soient $p_1, \ldots, p_r$ un ensemble fini de nombres premiers, en considérant les nombres premiers divisant $\Phi_n(kp_1 \ldots p_r)$ (pour k variable à choisir), montrer qu'il existe une infinité de nombres premiers $p \equiv 1 \bmod n$.
b) En considérant les facteurs premiers p divisant $N = 4p_1 \ldots p_r - 1$ (resp. $N = 6p_1 \ldots p_r - 1$) montrer qu'il existe une infinité de nombres premiers $p \equiv -1 \bmod 4$. (resp. $\bmod 3$).

Exercice 2. (Normes et traces). Soit L/K une extension *séparable*[1] de corps de degré $[L : K] = n$. On peut voir L comme un K-espace vectoriel; si $\alpha \in L$, la multiplication par α est une application K-linéaire de L vers lui-même que l'on note $M(\alpha)$. On définit alors la *norme* et la *trace* de α par :

$$\mathrm{N}_K^L(\alpha) := \det M(\alpha) \qquad \text{et} \qquad \mathrm{Tr}_K^L(\alpha) := \mathrm{Tr}\, M(\alpha).$$

a) Montrer que $\mathrm{N}_K^L(\alpha\beta) = \mathrm{N}_K^L(\alpha)\,\mathrm{N}_K^L(\beta)$ et $\mathrm{Tr}_K^L(\alpha + \beta) = \mathrm{Tr}_K^L(\alpha) + \mathrm{Tr}_K^L(\alpha)$ et que, si $\alpha \in K$ alors $\mathrm{Tr}_K^L(\alpha) = n\alpha$ et $\mathrm{N}_K^L(\alpha) = \alpha^n$.
b) Montrer que les applications $\mathrm{N}_K^L : L^* \to K^*$ et $\mathrm{Tr}_K^L : L \to K$ sont surjectives si K est fini. Le résultat subsiste-t-il dans le cas général?
c) Soit $\alpha \in L$, notons $d = [K(\alpha) : K]$ et $m = [L : K(\alpha)]$. Soit $P(X) = (X - \alpha_1) \ldots (X - \alpha_d)$ le polynôme minimal de α sur K; montrer que

$$\mathrm{Tr}_K^L(\alpha) = m(\alpha_1 + \ldots + \alpha_d) \qquad \text{et} \qquad \mathrm{N}_K^L(\alpha) = (\alpha_1 \ldots \alpha_d)^m$$

d) Montrer que $(x, y) \mapsto \mathrm{Tr}_K^L(xy)$ est une forme K-bilinéaire de $L \times L$ vers K qui est non dégérérée.

Exercice 3. Soit $N = pq$ le produit de deux nombres premiers très grands. On choisit d exposant public RSA et e secret, son inverse modulo $\phi(N)$, i.e. $ed - 1 = k\phi(N)$ et $1 < e < \phi(N)$.
Etablir la relation

$$\frac{d}{N} - \frac{k}{e} = \frac{1}{eN} - \frac{k}{e}\left(\frac{N - \phi(N)}{N}\right)$$

Utiliser un théorème sur les fractions continuées (par exemple p. 48 des notes de cours) pour montrer que si le membre de droite est inférieur en valeur absolue à $1/2e^2$ alors on peut calculer rapidement k/e et casser le code.
Montrer que la condition est vérifiée si $e \leq N^{1/4}$.

(1) Si vous n'avez jamais vu la définition de "séparable", contentez-vous de démontrer l'énoncé dans les deux cas suivants : K est un corps de caractéristique zéro, K est un corps fini.

Problème A.
On écrit les vecteurs de $\mathbf{R}^n$ en colonne et on note $e_1, \ldots, e_n$ les vecteurs de la base canonique. On note $\mathrm{GL}_n(A)$ le groupe des matrices carrés de taille n à coefficients dans l'anneau A et telles que $\det(A) \in A^*$ (ce qui équivaut à dire que A^{-1} existe et est à coefficients dans A). Si A est un sous-anneau de $\mathbf{R}$, on note $\mathcal{S}_n(A)$ l'ensemble des matrices symétriques définies positives à coefficients dans A. Si $Q[x] = {}^t xQx$ est une forme quadratique à coefficients entiers, on dira qu'elle représente un entier m si il existe $x \in \mathbf{Z}^n$ tel que $Q[x] = m$. On se propose d'étudier quelques propriétés des formes à coefficients entiers et de démontrer le théorème des trois carrés:

$\ll$ *La forme* $x_1^2 + x_2^2 + x_3^2$ *représente un entier positif* m *si et seulement si* m *n'est pas de la forme* $4^a(8n+7)$. $\gg$

a) On dit que Q est équivalente à Q' si il existe $U \in \mathrm{GL}_n(\mathbf{Z})$ telles que $Q' = Q[U] := {}^tUQU$. Montrer que deux formes équivalentes représentent les mêmes entiers.
b) Soit $x \in \mathbf{Z}^n$ tel que $\mathrm{pgcd}(x_1, \ldots, x_n) = 1$, montrer qu'il existe une matrice $U \in \mathrm{GL}_n(\mathbf{Z})$ dont la première colonne est x.
c) Soit Q une matrice dans $\mathcal{S}_n(\mathbf{R})$, posons

$$m(Q) := \min_{x \in \mathbf{Z}^n \setminus \{0\}} Q[x].$$

Soit $x \in \mathbf{Z}^n \setminus \{0\}$ réalisant $m(Q)$, montrer qu'on peut construire $U \in \mathrm{GL}_n(\mathbf{Z})$ telle que la matrice $Q' = Q[U]$ vérifie

$$Q'[e_1] = m(Q') = m(Q).$$

d) Soit Q une matrice dans $\mathcal{S}_n(\mathbf{R})$, telle que $Q'[e_1] = m(Q')$. Montrer qu'on peut construire $U \in \mathrm{GL}_n(\mathbf{Z})$ de la forme $U = \begin{pmatrix} 1 & {}^tb \\ 0 & \\ \vdots & V \\ 0 & \end{pmatrix}$ (avec $b \in \mathbf{Z}^{n-1}$ et V matrice carrée de taille $n-1$) telle que la matrice $Q'' = Q'[U]$ vérifie

$$Q''[e_1] = m(Q'') = m(Q') \quad \text{et} \quad Q''[e_2] = \min_{\substack{x \in \mathbf{Z}^n \\ \mathrm{pgcd}(x_2, \ldots, x_n) = 1}} Q''[x].$$

e) On dit qu'une matrice $Q \in \mathcal{S}_n(\mathbf{R})$ est *réduite* si elle vérifie la propriété:

$$\forall k \in [1, n], \qquad Q[e_k] = \min_{\substack{x \in \mathbf{Z}^n \\ \mathrm{pgcd}(x_k, \ldots, x_n) = 1}} Q[x].$$

En itérant le procédé des questions précédentes, montrer que toute matrice de $\mathcal{S}_n(\mathbf{R})$ est équivalente à une matrice réduite.
f) Soit $Q \in \mathcal{S}_n(\mathbf{R})$ une matrice réduite de coefficients $q_{i,j}$. Montrer que $0 < q_{1,1} \leq q_{2,2} \leq \ldots \leq q_{n,n}$ et que $2|q_{i,j}| \leq q_{i,i}$.

g) Soit $Q \in \mathcal{S}_n(\mathbf{R})$, montrer qu'il existe $D = \mathrm{diag}(d_1, \ldots, d_n)$ et T matrice triangulaire supérieure telles que $Q = D[T]$; en déduire l'inégalité d'Hadamard

$$\det(Q) \leq q_{1,1} q_{2,2} \ldots q_{n,n}.$$

h) Soit $Q \in \mathcal{S}_n(\mathbf{R})$ une matrice réduite, montrer l'existence d'une constante C_n telles que

$$\det(Q) \leq q_{1,1} q_{2,2} \ldots q_{n,n} \leq C_n \det(Q).$$

(dans la suite on pourra prendre comme valeur admissible $C_2 = 4/3$ et $C_3 = 2$). [Indication : si $q_{n,n} \ll q_{1,1}$ on peut conclure facilement; sinon il existe $k \leq n-1$ tel que $q_{n,n} \ll q_{k+1,k+1}$ mais $q_{k,k} \ll q_{k+1,k+1}$; on écrit alors une décomposition $Q = \begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix} \begin{bmatrix} I & U \\ 0 & I \end{bmatrix}$, où Q_1 est la matrice $k \times k$ extraite de Q et on en tirera une inégalité du type $q_{k+1,k+1} \leq \frac{k^2}{4} q_{k,k} + m(Q_2)$ et on conclura en appliquant le théorème de Hermite à Q_2 et une hypothèse de récurrence à Q_1.]
i) On note $\mathcal{H}_n(D)$ l'ensemble des classes d'équivalence de matrices de $\mathcal{S}_n(\mathbf{Z})$ dont le déterminant vaut D. Montrer que $h_n(D) := \mathrm{card}\, \mathcal{H}_n(D)$ est fini.
j) Montrer que $h_2(1) = h_3(1) = 1$. [On pourra montrer qu'une matrice 2×2 ou 3×3 réduite et de déterminant 1 est l'identité].
k) Montrer qu'une forme $Q = ((q_{i,j}))_{1 \leq i,j \leq n}$ est définie positive si et seulement si

$$\forall k \in [1, n], \quad \det((q_{i,j}))_{1 \leq i,j \leq k}) > 0$$

l) Soit $m \in \mathbf{N}$, on suppose qu'on connaît un entier $d \geq 1$ vérifiant la propriété suivante: l'entier $-d$ est un carré modulo $r := md - 1$, i.e. il existe k, ℓ entiers tels que $-d = k^2 - \ell r$. Montrer que m est somme de trois carrés. [On pourra introduire la forme quadratique associée à

$$A = \begin{pmatrix} \ell & k & 1 \\ k & r & 0 \\ 1 & 0 & m \end{pmatrix}$$

et utiliser la question j).]
m) On admet le *théorème de la progression arithmétique* de Dirichlet (voir cours ou l'exercice 1 pour quelques cas) : si $\mathrm{pgcd}(a, b) = 1$ il existe un nombre premier $p \equiv a \bmod b$. Pour démontrer le théorème des trois carrés, on propose la démarche suivante:
- Si $m = 2(2m' + 1)$ est $\equiv 2 \bmod 4$, trouver p de la forme $(4u + 1)m - 1$, poser $d = 4u + 1$, vérifier que $\left(\frac{-d}{p}\right) = +1$ et conclure que m est somme de trois carrés en utilisant l).
- Si $m \equiv 1$ ou $5 \bmod 8$, poser $c = 3$, trouver p de la forme $4mu + (cm - 1)/2$, poser $d = 8u + c$ (donc $2p = md - 1$), vérifier $\left(\frac{-d}{p}\right) = +1$ et conclure que m est somme de trois carrés en utilisant l).
- Modifier l'alinéa précédent si $m \equiv 3 \bmod 8$ pour aboutir à la même conclusion.
- Conclure la preuve du cas général.

Problème B.
On notera dans cet exercice $\mathrm{e}(x) := \exp(2\pi i x)$ et on remarquera que, si $x \in \mathbf{F}_p$ l'expression $\mathrm{e}(x/p)$ a un sens. Soit q une puissance de p on définit un caractère additif par la formule

$$\psi(x) = \mathrm{e}\left(\frac{\mathrm{Tr}_{\mathbf{F}_p}^{\mathbf{F}_q} x}{p}\right).$$

Si χ est un caractère non trivial de $\mathbf{F}_q^*$ (c'est-à-dire un homomorphisme non constant de $\mathbf{F}_q^*$ vers $\mathbf{C}^*$ que l'on étend par $\chi(0) = 0$ à tout $\mathbf{F}_q$). Si χ_0 est le caractère trivial $\chi_0(x) = 1$ pour tout $x \in \mathbf{F}_q^*$, on le prolonge par $\chi_0(0) = 1$. On définit également les *sommes de Gauss* pour $a \in \mathbf{F}_q^*$ par :

$$G(\chi, \psi, a) := \sum_{x \in \mathbf{F}_q} \chi(x)\psi(ax) \qquad \text{et} \qquad G(\chi, \psi) := G(\chi, \psi, 1).$$

B.1 (Quelques propriétés des sommes de Gauss sur $\mathbf{F}_q$.)
a) Montrer que $\sum_{a \in \mathbf{F}_q} \psi(ab) = 0$ sauf si $b = 0$ (et alors la somme vaut q).
b) Montrer les formules $G(\chi_0, \psi, a) = 0$, $G(\chi, \psi, a) = \bar{\chi}(a)G(\chi, \psi)$ et $|G(\chi, \psi)| = \sqrt{q}$ (si $\chi \neq \chi_0$).
c) Pour $f(X) = X^n - a_1 X^{n-1} + \ldots + (-1)^n a_n \in \mathbf{F}_q[X]$ on pose $\lambda(f) = \psi(a_1)\chi(a_n)$. Montrer que λ est multiplicatif, i.e. que $\lambda(fg) = \lambda(f)\lambda(g)$.
d) Montrer que si N, Tr sont les norme et trace de $\mathbf{F}_{q^m}$ vers $\mathbf{F}_q$ alors

$$G(\chi \circ \mathrm{N}, \psi \circ \mathrm{Tr}) = \sum_{f, \deg(f) \mid m} \deg(f)\lambda(f)^{m/\deg(f)}$$

où f parcourt les polynômes unitaires irréductibles dans $\mathbf{F}_q[X]$ de degré divisant m.
e) Montrer l'identité

$$1 + G(\chi, \psi)T = \sum_f \lambda(f)T^{\deg(f)} = \prod_g \left(1 - \lambda(g)T^{\deg(g)}\right)^{-1}$$

(où la somme porte sur les polynômes f unitaires de $\mathbf{F}_q[X]$ et le produit porte sur les polynômes g unitaires irréductibles de $\mathbf{F}_q[X]$).
f) En prenant la dérivée logarithmique, déduire la relation de Davenport-Hasse:

$$-G(\chi \circ \mathrm{N}, \psi \circ Tr) = \left(-G(\chi, \psi)\right)^m.$$

B.II. (Nombre de solutions d'une paire d'équations quadratiques)
Soit p impair et $Q_1(x) = a_1 x_1^2 + \ldots + a_n x_n^2$ et $Q_2(x) = b_1 x_1^2 + \ldots + b_n x_n^2$ deux formes quadratiques à coefficients dans $\mathbf{F}_p$. On suppose que n est <u>*impair*</u> et que la condition suivante est réalisée :

$$\text{Pour } 1 \leq i < j \leq n, \text{ on a} \quad a_i b_j - a_j b_i \neq 0 \qquad (*)$$

et on se propose de calculer $N := \mathrm{card}\{x \in \mathbf{F}_p^n \mid Q_1(x) = Q_2(x) = 0\}$.
a) Montrer que $\sum_{a,b\in\mathbf{F}_p} \sum_{x\in\mathbf{F}_p^n} \mathrm{e}\left(\frac{aQ_1(x)+bQ_2(x)}{p}\right) = p^2 N$ et en déduire la formule :

$$N = p^{n-2} + p^{-2} \sum_{(a,b)\neq(0,0)} \sum_{x\in\mathbf{F}_p^n} \mathrm{e}\left(\frac{aQ_1(x)+bQ_2(x)}{p}\right)$$

où la somme est sur les couples non nuls $(a, b) \in \mathbf{F}_p^2$.
b) Soit $\tau := \sum_{x\in\mathbf{F}_p} \mathrm{e}(x^2/p)$, et soit $Q(x) = c_1x_1^2 + \ldots + c_nx_n^2$. Rappeler la formule donnant $\sum_{x\in\mathbf{F}_p^n} \mathrm{e}(Q(x)/p)$ en fonction des c_i et de τ lorsque $c_1 \ldots c_n \neq 0$. En déduire que si $c_1 \ldots c_{n-1} \neq 0$ mais $c_n = 0$ alors

$$\sum_{x\in\mathbf{F}_p^n} \mathrm{e}(Q(x)/p) = \left(\frac{c_1 \ldots c_{n-1}}{p}\right) \tau^{n-1} p,$$

formule dans laquelle $\left(\frac{\cdot}{p}\right)$ désigne le symbole de Legendre. Rappeler aussi la valeur de τ^2.
c) On note pour abréger $T(a, b) := \sum_{x\in\mathbf{F}_p^n} \mathrm{e}\left(\frac{aQ_1(x)+bQ_2(x)}{p}\right)$. Montrer que, si (a, b) n'est pas proportionnel à un des $(b_i, -a_i)$, alors $\sum_{\lambda\in\mathbf{F}_p^*} T(\lambda a, \lambda b) = 0$. Calculer cette dernière somme lorsque $(a, b) = (b_i, -a_i)$.
d) On pose

$$D_i = \prod_{1\leq j\leq n, j\neq i} (b_ia_j - a_ib_j) \qquad \text{et} \qquad \epsilon_i = \left(\frac{D_i}{p}\right).$$

Déduire de ce qui précède la formule :

$$N = p^{n-2} + (p-1)\left(\frac{-1}{p}\right)^{(n-1)/2} \left(\sum_{i=1}^{n} \epsilon_i\right) p^{(n-3)/2}.$$

e) Enoncer et démontrer une formule analogue pour le nombre de solutions N_m des mêmes équations dans $(\mathbf{F}_{p^m})^n$.
f) On pose $\bar{N}_m = (N_m - 1)/(p^m - 1)$ (il s'agit du nombre de solutions *projectives*). Montrer que la série formelle

$$Z(T) := \exp\left(\sum_{m=1}^{\infty} \bar{N}_m \frac{T^m}{m}\right)$$

est le développement au voisinage de $T = 0$ d'une fraction rationnelle que l'on précisera. Vérifier l'équation fonctionnelle de $Z(T)$ qui est une relation simple entre $Z(1/q^{n-3}T)$ et $Z(T)$ de la forme

$$Z(1/q^{n-3}T) = \pm q^a T^b Z(T),$$

avec des constantes a, b et un signe $\pm$ que l'on déterminera.