Magistère E.N.S. d'Ulm – Universités parisiennes (FIMFA) 2005-2006
Cours de Théorie algorithmique des nombres. (Marc Hindry)
Examen du jeudi 1er juin 2006

Les trois exercices et le problème sont indépendants.

Exercice 1.

1.a) Montrer que l'anneau $\mathbf{Z}[i\sqrt{2}]$ est euclidien et que $\mathbf{Z}[i\sqrt{2}]^* = \{\pm 1\}$.

1.b) Soit $(x, y) \in \mathbf{Z}^2$ tels que $y^2 = x^3 - 2$. Montrer que x et y sont impairs et en déduire que $y + i\sqrt{2}$ est un cube dans $\mathbf{Z}[i\sqrt{2}]$.

1.c) Conclure que la courbe elliptique $y^2 = x^3 - 2$ ne possède que deux points entiers $(x, y) = (3, \pm 5)$.

Exercice 2. Soit μ_n^* l'ensemble des racines n-ème primitives de l'unité et $\zeta \in \mu_n^*$. On sait que son polynôme minimal est le n-ème polynôme cyclotomique $\Phi_n(X) = \prod_{\xi \in \mu_n^*}(X - \xi) \in \mathbf{Z}[X]$ et que l'anneau des entiers algébriques de $K := \mathbf{Q}(\zeta)$ est $\mathcal{O}_K = \mathbf{Z}[\zeta]$.

2.a) Soit p premier ne divisant pas n et soit $\bar{\Phi}_n \in \mathbf{F}_p[X]$ la réduction modulo p de Φ_n; soit β un racine n-ème primitive dans $\bar{\mathbf{F}}_p$. Montrer qu'un facteur irréductible de $\bar{\Phi}_n$ s'écrit $Q = \prod_{j \in J}(X - \beta^j)$ avec J sous-ensemble de $(\mathbf{Z}/n\mathbf{Z})^*$ stable par multiplication par p.

2.b) Soit r l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$, en déduire que la décomposition en facteurs irréductibles de $\bar{\Phi}_n$ dans $\mathbf{F}_p[X]$ s'écrit :

$$\bar{\Phi}_n = P_1 \dots P_g, \qquad \text{avec } g = \phi(n)/r \text{ et } \deg(P_i) = r.$$

2.c) Soit p ne divisant pas n, montrer que

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbf{F}_p[X]/P_1\mathbf{F}_p[X] \times \dots \times \mathbf{F}_p[X]/P_g\mathbf{F}_p[X]$$

et que, par conséquent, la décomposition en idéaux premiers de p dans $\mathcal{O}_K$ s'écrit

$$p\mathcal{O}_K = \wp_1 \dots \wp_g, \qquad \text{avec } \mathrm{N}(\wp_i) = p^r.$$

Exercice 3. On définit la fonction arithmétique suivante :

$$\gamma(n) := \max_{m_1 + \dots + m_r = n} \mathrm{ppcm}\,(m_1, \dots, m_r)$$

où les m_i sont entiers ≥ 1. [Note : l'intérêt de la fonction $\gamma(n)$ est qu'elle représente l'ordre maximal d'un élément du groupe des permutations sur n lettres]. On se propose de montrer que

$$\lim_{n \to \infty} \frac{\log \gamma(n)}{\sqrt{n \log n}} = 1$$

3.a) Montrer qu'on peut écrire

$$\gamma(n) := \max_{p_1^{\alpha_1} + \dots + p_s^{\alpha_s} \leq n} (p_1^{\alpha_1} \cdots p_s^{\alpha_s})$$

où les p_i sont des premiers distincts.

3.b) En utilisant l'inégalité de la moyenne arithmétique et géométrique :

$$\sqrt[m]{y_1 \cdots y_m} \leq \frac{y_1 + \cdots + y_m}{m}$$

montrer que si $p_1^{\alpha_1} + \ldots + p_r^{\alpha_r} \leq n$ alors $p_1^{\alpha_1} \ldots p_r^{\alpha_r} \leq (n/r)^r$.

3.c) Montrer que la somme des r premiers nombres premiers est équivalente à $\frac{r^2}{2} \log r$ en utilisant le théorème des nombres premiers. En déduire que, dans la question précédente, on a $n \geq \frac{r^2}{2} \log r(1 + o(1))$ et donc $r \leq 2\sqrt{n/\log n}(1 + o(1))$.

3.d) En observant que la fonction $f(x) = (n/x)^x$ est croissante sur l'intervalle $[1, n/e]$, conclure des questions précédentes que

$$\log \gamma(n) \leq \sqrt{n \log n}(1 + o(1)).$$

3.e) Pour n donné (grand), on choisit $r = r(n)$ le plus grand entier tel que $p_1 + \ldots + p_r \leq n$ (où p_i désigne maintenant la suite des nombres premiers rangés en ordre croissant). Montrer que r est équivalent à $2\sqrt{n/\log n}$. Montrer que $\log \gamma(n) \geq \theta(p_r)$ et conclure en utilisant de nouveau le théorème des nombres premiers.

Problème.

On se propose d'étudier les solutions de l'équation

$$2y^2 = x^4 - 17, \qquad (*)$$

sur les corps $\mathbf{Q}$, $\mathbf{F}_p$ *et l'anneau* $\mathbf{Z}/N\mathbf{Z}$.

Première partie : solutions rationnelles.

A.1) Montrer qu'une solution $(x, y) \in \mathbf{Q}^2$ de $(*)$ peut s'écrire $(x, y) = \left(\frac{a}{b}, \frac{c}{b^2}\right)$ où $a, b, c \in \mathbf{Z}$ et $\text{pgcd}(a, b) = \text{pgcd}(c, b) = 1$.

A.2) Soit a, b, c comme à la question précédente. Soit p premier impair, montrer que si p divise c, alors p est un carré modulo 17; en déduire que c est un carré modulo 17.

A.3) Vérifier que 2 est un carré mais n'est pas un bicarré (puissance quatrième) modulo 17 et conclure que $(*)$ n'admet aucune solution rationnelle.

Deuxième partie : existence de solutions modulo N.

B.1) Montrer qu'une équation polynomiale $F(x_1, \ldots, x_n) = 0$ à coefficients entiers possède une solution modulo N pour tout N si et seulement si elle possède une solution modulo p^m pour tout premier p et exposant $m \geq 1$.

B.2) Soit $z_0 \in \mathbf{Z}^n$ tel que $F(z_0) \equiv 0 \bmod p$ mais $\nabla F(z_0) \not\equiv 0 \bmod p$; montrer que, pour tout $m \geq 1$ il existe $z_m \in \mathbf{Z}^n$ tel que $z_m \equiv z_0 \bmod p$ et $F(z_m) \equiv 0 \bmod p^m$. [On note ici $\nabla F(z) := \left(\frac{\partial F}{\partial x_1}(z), \ldots, \frac{\partial F}{\partial x_n}(z)\right)$]. Généraliser cet énoncé en partant de $z_0 \in \mathbf{Z}^n$ vérifiant pour un

certain $\delta \geq 0$ les relations $F(z_0) \equiv 0 \bmod p^{2\delta+1}$ et $\nabla F(z_0) \equiv 0 \bmod p^{\delta}$ mais $\nabla F(z_0) \not\equiv 0 \bmod p^{\delta+1}$.

B.3) Soit $p \neq 2, 17$, Montrer que si $(*)$ admet une solution modulo p, elle en admet aussi modulo p^m pour tout $m \geq 1$.

B.4) Montrer que $(*)$ admet une solution modulo 2^m ou 17^m, pour tout $m \geq 1$.[On pourra observer et utiliser que $2.5^2 \equiv 2^4 \bmod 17$ et $3^4 - 17 \equiv 0 \bmod 2^6$]

Troisième partie : on se propose de calculer, pour chaque premier $p \neq 2, 17$, le nombre $N_p := \mathrm{card}\{(x, y,) \in (\mathbf{F}_p)^2 \mid 2y^2 = x^4 - 17\}$.

C.1) Calculer les nombres $L_p := \mathrm{card}\{(x, y, z) \mid 2y^2 = x^2 - 17z^2\}$ et en déduire le calcul de $M_p := \mathrm{card}\{(x, y, z) \mid 2y^2 = x^2 - 17\}$.

C.2) Lorsque $p \equiv 3 \bmod 4$ montrer que $N_p = M_p$ et en déduire :

$$N_p = \begin{cases} p+1 & \text{si } p \equiv 3 \bmod 8 \\ p-1 & \text{si } p \equiv 7 \bmod 8 \end{cases}$$

C.3) On note $\mathrm{e}(z) := \exp(2\pi i z)$ et on pose:

$$\tau(a) := \sum_{x \in \mathbf{F}_p} \mathrm{e}\left(ax^2/p\right), \quad \text{et} \quad \rho(a) := \sum_{x \in \mathbf{F}_p} \mathrm{e}\left(ax^4/p\right)$$

Montrer que

$$N_p = p + p^{-1} \sum_{a=1}^{p-1} \mathrm{e}(17a/p)\tau(2a)\rho(-a).$$

On suppose désormais $p \equiv 1 \bmod 4$, on introduit $G = \{\chi_0, \chi_1, \chi_2, \chi_3\}$ l'ensemble des caractères de $\mathbf{F}_p^*$ tels que $\chi_0(x) = 1$ et $\chi^4(x) = 1$ pour $x \in \mathbf{F}_p^*$. On les prolonge à $\mathbf{F}_p$ par la convention $\chi_0(0) = 1$ et $\chi_j(0) = 0$ pour $j = 1, 2, 3$. On supposera que χ_1 est le caractère de Dirichlet $\chi_1(x) := \left(\frac{x}{p}\right)$. On introduit aussi les sommes de Gauss associées :

$$G(\chi, a) := \sum_{x \in \mathbf{F}_p} \chi(x)\,\mathrm{e}(ax/p) \quad \text{et} \quad G(\chi) := G(\chi, a).$$

C.4) Rappeler brièvement pourquoi $G(\chi_0, a) = 0$, $G(\chi, a) = \bar{\chi}(a)G(\chi)$ et enfin, si $\chi \neq \chi_0$, on a $|G(\chi)| = \sqrt{p}$.

C.5) Montrer la formule :

$$\sum_{\chi \in G} \chi(x) = \begin{cases} 4 & \text{si } x \in \mathbf{F}_p^{*4} \\ 1 & \text{si } x = 0 \\ 0 & \text{sinon} \end{cases}$$

et en déduire que

$$\rho(a) = \bar{\chi}_1(a)G(\chi_1) + \bar{\chi}_2(a)G(\chi_2) + \bar{\chi}_3(a)G(\chi_3)$$

C.6) En déduire une formule pour N_p en terme des sommes de Gauss de la forme(où $|\epsilon_i| = 1$) :

$$N_p = p - \epsilon_0 + \frac{\tau(1)}{p}\left(\epsilon_1 G(\chi_2)^2 + \epsilon_2 G(\chi_3)^2\right)$$

.

C.7) Conclure que $N_p \geq 1$ pour tout $p \neq 2, 17$.