Magistère E.N.S. d'Ulm – Universités parisiennes (FIMFA) 2006-2007
Cours de Théorie algorithmique des nombres. (Marc Hindry)
Examen du mardi 5 juin 2007

Les deux problèmes sont indépendants des exercices.

Exercice 1.

Soit un nombre premier $p \equiv 1 \bmod 8$, on sait que $p = a^2 + b^2$, où l'on peut supposer a pair et b impair.

1.a) Montrer que

$$(a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} \equiv 2^{\frac{p-1}{4}}(-1)^{\frac{p-1}{8}}\left(\frac{b}{p}\right) \equiv 2^{\frac{p-1}{4}}(-1)^{\frac{p-1}{8}} \bmod p.$$

1.b) En utilisant l'identité $2p = (a+b)^2 + (a-b)^2$, calculer les symboles $\left(\frac{2p}{a+b}\right)$ et $\left(\frac{a+b}{p}\right)$.

1.c) En déduire la formule :

$$2^{\frac{p-1}{4}} \equiv (-1)^{\frac{ab}{4}} \bmod p,$$

et l'énoncé : 2 *est un bicarré si et seulement si* 8 *divise* ab.

Exercice 2.

On considère l'équation

$$y^2 + 82x^4 = 2. \qquad (E)$$

2.a) Vérifier que $\mathrm{ord}(2 \bmod 41) = 20$ et en déduire que 2 est un carré mais pas un bicarré modulo 41.

Soit $(x, y) \in \mathbf{Q}^2$ une solution de l'équation étudiée. Montrer qu'il existe $a, b, c \in \mathbf{Z}$ tels que $(x, y) = (a/c, 2b/c^2)$ avec $\mathrm{pgcd}(a, c) = \mathrm{pgcd}(b, c) = 1$ et donc $2b^2 + 41a^2 = c^4$.

2.b) Si p impair divise b, montrer que p est un carré modulo 41 et en déduire que b est un carré modulo 41.

2.c) Montrer que l'équation (E) n'admet pas de solution rationnelle $(x, y) \in \mathbf{Q}^2$.

Exercice 3.

On pose $F(x, y, z) = ax^3 + by^3 + cz^3$ et

$$N_p := \left|\left\{(x, y, z) \in \mathbf{F}_p^3 \mid F(x, y, z) = 0\right\}\right| \text{ et } \bar{N}_p := \left|\left\{(x, y, z) \in \mathbf{P}^2(\mathbf{F}_p) \mid F(x, y, z) = 0\right\}\right|$$

de sorte que $\bar{N}_p = (N_p - 1)/(p-1)$. On supposera $abc \not\equiv 0 \bmod p$.

3.a) Montrer que pour $p = 3$ ou $p \equiv 2 \bmod 3$ on a $N_p = p^2$.

On suppose désormais $p \equiv 1 \bmod 3$, on introduit $G = \{\chi_0, \chi_1, \chi_2\}$ l'ensemble des caractères de $\mathbf{F}_p^*$ tels que $\chi_0(x) = 1$ et $\chi^3(x) = 1$ 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 $j = 1, 2$. On note $\mathrm{e}(z) := \exp(2\pi i z)$ et on introduit aussi les sommes de Gauss associées :

$$G(\chi, a) := \sum_{x \in \mathbf{F}_p} \chi(x)\, \mathrm{e}(ax/p) \quad \text{et} \quad G(\chi) := G(\chi, 1),$$

et enfin:

$$R(a) := \sum_{x \in \mathbf{F}_p} \mathrm{e}\left(ax^3/p\right).$$

3.b) 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 $|G(\chi)| = \sqrt{p}$.

3.c) Montrer la formule :

$$\sum_{\chi \in G} \chi(x) = \begin{cases} 3 & \text{si } x \in \mathbf{F}_p^{*3} \\ 1 & \text{si } x = 0 \\ 0 & \text{sinon} \end{cases}$$

et en déduire que

$$R(a) = \bar{\chi}_1(a)G(\chi_1) + \bar{\chi}_2(a)G(\chi_2).$$

3.d) En déduire une formule pour N_p en terme des sommes de Gauss :

$$N_p = p^2 + \frac{p-1}{p}\left(\bar{\chi}_1(abc)G(\chi_1)^3 + \bar{\chi}_2(abc)G(\chi_2)^3\right),$$

ainsi que la formule correspondante pour $\bar{N}_p$.

3.e) Conclure que $\left|\bar{N}_p - (p+1)\right| \leq 2\sqrt{p}$ et en particulier que $\bar{N}_p \geq 1$ pour tout p ne divisant pas abc.

Problème A.

On se propose d'étudier quelques propriétés analytiques de la fonction indicatrice d'Euler $\phi(n) = \mathrm{card}(\mathbf{Z}/n\mathbf{Z})^*$. On rappelle que la notation $f(x) \sim g(x)$, quand x tend vers ∞, signifie que $f(x)/g(x)$ tend vers 1, quand x tend vers ∞. On utilisera plus loin la valeur $\sum_{n \geq 1} n^{-2} = \pi^2/6$.

A.1) Rappeler brièvement pourquoi $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ et vérifier que pour tout $n \geq 2$ on a $\phi(n) \leq n - 1$.

A.2) On définit $P(x) := \prod_{p \leq x} \left(1 - \frac{1}{p}\right)$; en comparant $\log P(x)$ avec $\sum_{p \leq x} p^{-1}$, montrer qu'il existe une constante $C_0 > 0$ telle que :

$$P(x) \sim \frac{C_0}{\log x}.$$

A.3) Soit l'entier $N := \prod_{p \leq x} p$. En utilisant le théorème des nombres premiers et la question précédente, montrer que :

$$\phi(N) \sim \frac{C_0 N}{\log \log N}.$$

A.4) Notons $p_1 < p_2 < p_3 < \ldots$ la suite croissante des nombres premiers. Donner un équivalent de p_r. Pour $n \geq 2$, on note $\omega(n)$ le nombre de nombres premiers qui divisent n. Montrer qu'il existe une constante $c > 0$ telle que :

$$\omega(n) \leq \frac{c \log n}{\log \log n}.$$

A.5) Soit maintenant $n \geq 2$, montrer que

$$\prod_{k=1}^{\omega(n)} \left(1 - \frac{1}{p_k}\right) \leq \frac{\phi(n)}{n}$$

et en déduire

$$\liminf_{n \to \infty} \frac{\phi(n) \log \log n}{n} = C_0.$$

A.6) On définit la fonction de Moebius $\mu(n)$ par

$$\mu(n) := \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 \ldots p_k \\ 0 & \text{sinon} \end{cases}$$

Montrer que :

$$\sum_{d \,|\, n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$$

et en déduire que, pour $\Re(s) > 1$ on a $\zeta(s)^{-1} = \sum_{n=1}^{\infty} \mu(n) n^{-s}$ et que, si $f(n) = \sum_{d \,|\, n} g(d)$ alors $g(n) = \sum_{d \,|\, n} \mu(d) f(n/d)$. En déduire la formule :

$$\phi(n) = \sum_{d \,|\, n} \mu(d) \frac{n}{d}.$$

A.7) Montrer que, "en moyenne", $\phi(n)$ vaut $3n/\pi^2$ au sens suivant :

$$\frac{1}{X}\sum_{n\leq X}\phi(n) \sim \frac{3}{\pi^2}X.$$

A.8) Montrer la formule suivante, pour $\Re(s) > 2$:

$$\sum_{n=1}^{\infty}\phi(n)n^{-s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

Problème B.

On se propose de déterminer les entiers naturels s'écrivant sous la forme x^2+3y^2 ou sous la forme x^2-xy+y^2.

B.1) On note $j := \frac{-1+i\sqrt{3}}{2}$. On considère les anneaux $A_0 = \mathbf{Z}[i\sqrt{3}]$ et $A = \mathbf{Z}[j]$. Rappeler brièvement lesquels sont principaux ou factoriels et quels sont leurs groupes des unités A_0^* et A^*.

B.2) Soit $N : \mathbf{Q}(i\sqrt{3}) \to \mathbf{Q}$ la norme, vérifier que $N(a+bi\sqrt{3}) = a^2+3b^2$, $N(x+yj) = x^2-xy+y^2$ et montrer qu'un entier n est la norme d'un élément de A_0 si et seulement si c'est la norme d'un élément de A [Indication : on pourra montrer que, si α est dans A sans être dans A_0, alors $j\alpha$ ou $j^2\alpha$ est dans A_0].

B.3) Soit p premier différent de 2 et 3, montrer que, si p est la norme d'un élément de A_0 (ou A) alors -3 est un carré modulo p et en déduire $p \equiv 1 \bmod 3$.

B.4) Soit p premier différent de 2. Montrer que si $p \equiv 2 \bmod 3$ et $n = mp$ est une norme d'un élément de A_0 (ou A), alors $m = n'p$ et n' est encore une norme.

B.5) Montrer que 2 est un élément irréductible de A et en déduire que si $n = 2m$ est une norme d'un élément de A_0 (ou A), alors $m = 2n'$ et n' est encore une norme.

B.6) Supposons maintenant que $p \equiv 1 \bmod 3$; montrer que -3 est un carré modulo p et en déduire que p n'est pas irréductible dans A et par conséquent que c'est une norme.

B.7) En utilisant les questions précédentes montrer l'énoncé suivant :

Théorème. *Un entier $n \geq 1$ s'écrit sous la forme x^2+3y^2 ou sous la forme x^2-xy+y^2 avec $x, y \in \mathbf{Z}$ si et seulement si, pour chaque premier $p \equiv 2 \bmod 3$, on a $\mathrm{ord}_p(n)$ pair.*