UPS – Centre d'Orsay **Arithmétique – Maîtrise**
Mathématiques Année 2002–2003

Examen (09/2003). Durée : 4 heures.

Partie A

Soit $K = \mathbb{Q}(i) \subset \mathbb{C}$ ($i^2 = -1$), $\mathcal{O}$ l'anneau des entiers de K.

1)a) Préciser l'anneau des entiers, le discriminant, le groupe des unités et le nombre de classes de K.

b) Pour p *impair*, donner suivant la valeur de p modulo 4 le nombre d'idéaux premiers de $\mathcal{O}$ divisant (p) et le cardinal de leur corps résiduel.

2) On notera π un élément irréductible de $\mathcal{O}$ ne divisant pas 2.

a) Montrer que $N\pi \equiv 1 \pmod 4$.

b) Montrer que les images de $1, i, -i, -1$ dans $k := \mathcal{O}/\pi\mathcal{O}$ sont distinctes et sont donc les quatre racines quartiques (= d'ordre 4) de l'unité dans k.

c) Montrer que pour tout $x \in \mathcal{O}$ non divisible par π, $x^{(N\pi-1)/4}$ est congru modulo π à une unique racine quartique de l'unité dans $\mathcal{O}$.

Si π est irréductible, $\pi \nmid 2$, et si $x \in \mathcal{O}$, $x \notin \pi\mathcal{O}$, on définit le *symbole biquadratique* $(x/\pi)_4 \in \{1, i, -i, -1\}$ par

$$x^{(N\pi-1)/4} \equiv (x/\pi)_4 \pmod \pi.$$

3) Démontrer les propriétés suivantes du symbole $(x/\pi)_4$:

a) $((x+\pi y)/\pi)_4 = (x/\pi)_4 \quad (x, y \in \mathcal{O},\ x \notin \pi\mathcal{O})$

b) $(x/\pi)_4 (y/\pi)_4 = (xy/\pi)_4 \quad (x, y \in \mathcal{O} \setminus \pi\mathcal{O})$

On pourra donc considérer $x \mapsto (x/\pi)_4$ comme un caractère d'ordre 4 de k^*, où $k := \mathcal{O}/\pi\mathcal{O}$.

c) $(x/\pi)_4 = 1$ si et seulement si $z^4 \equiv x \pmod \pi$ a une solution dans $\mathcal{O}$.

d) $(\overline{x}/\overline{\pi})_4 = \overline{(x/\pi)_4}$, où $z \mapsto \overline{z}$ désigne la conjugaison complexe dans $\mathcal{O}$.

4) Si p est le nombre premier divisible par π et $a \in \mathbb{Z}$ est premier à p, montrer que $(a/\pi)_4 = 1$ si $p \equiv -1 \pmod 4$

5) On dit qu'un élément irréductible $\pi \in \mathcal{O}$ est *primaire* si $\pi \equiv 1 \pmod{2+2i}$.

a) Montrer que $\pi = a + ib$ est primaire si et seulement si $a \equiv 1, b \equiv 0 \pmod 4$ ou $a \equiv 3, b \equiv 2 \pmod 4$.

b) Montrer que tout idéal premier $\mathfrak{p} \nmid 2$ de $\mathcal{O}$ admet un générateur primaire. [*Soit* p *le nombre premier tel que* $\mathfrak{p} \mid p$ *; distinguer les cas* $p \equiv 1$ *et* $p \equiv 3 \pmod 4$.]

c) Montrer que ce générateur primaire est unique.

Partie B

Dans cette partie on fixe un nombre premier $p \equiv 1 \pmod 4$. Soit $\mathfrak{p} \mid p$ un idéal premier de $\mathcal{O}$ et π le générateur primaire de $\mathfrak{p}$ (cf. A.5). On identifie $k = \mathcal{O}/\pi\mathcal{O}$ à $\mathbb{F}_p$. Notons χ le caractère de $\mathbb{F}_p^*$ défini en A.3 : $\chi(x) := (x/\pi)_4$, $x \in \mathbb{F}_p^*$.

1) Montrer que χ est d'ordre exact 4.

2) Montrer que $J(\chi, \chi)$ est de la forme $u\pi$ ou $v\overline{\pi}$, u et v étant des unités de $\mathcal{O}$.

3) Soit λ le caractère de Legendre de $\mathbb{F}_p^*$: $\lambda = \chi^2$. Montrer que $g(\chi)^4 = pJ(\chi,\chi)^2$ puis que

$$J(\chi,\chi) = \chi(-1)J(\chi,\lambda).$$

4) Montrer que $\chi((p+1)/2)^2 = \chi(-1)$ [*utiliser* $(1+i)^2 = 2i$]. En déduire que

$$J(\chi,\chi) \equiv -\chi(-1) \pmod{2+2i},$$

puis que $-\chi(-1)J(\chi,\chi)$ est un élément irréductible primaire.

5) a) Soit $a \in \mathbb{N}$. Calculer $\sum_1^{p-1} x^a \pmod p$ suivant la valeur de a modulo $(p-1)$.

b) Montrer que

$$J(\chi,\chi) \equiv \sum_{x=1}^{p-1} x^{(p-1)/4}(1-x)^{(p-1)/4} \pmod \pi.$$

En déduire que $\pi = -\chi(-1)J(\chi,\chi)$.

c) Montrer que $g(\chi)^4 = \pi^3\overline{\pi}$.

Partie C

La loi de réciprocité biquadratique est le résultat suivant :

Théorème 1. *Soit $p \neq r$ des nombres premiers impairs, π, ρ des éléments irréductibles primaires de $\mathcal{O}$ divisant respectivement p et r. Alors*

$$\text{(R)} \qquad (\pi/\rho)_4 = (\rho/\pi)_4 \times (-1)^{((N\pi-1)/4)((N\rho-1)/4)}.$$

1) Montrer que (R) est vrai si $p \equiv r \equiv -1 \pmod 4$.

2) On suppose $p \equiv 1$, $r \equiv -1 \pmod 4$. Soit π un irréductible primaire divisant p et χ_π, χ_r les caractères quartiques de $\mathbb{F}_p$, $\mathbb{F}_{r^2}$ associés à π et r.

a) Soit $L := \mathbb{Q}(i,\zeta)$, où ζ est une racine primitive p-ème de l'unité. Démontrer les congruences suivantes dans $\mathcal{O}_L$:

$$\begin{aligned} g(\chi_\pi)^r &\equiv \sum_{x\in\mathbb{F}_p} \chi_\pi^3(x)\zeta^{rx} \pmod r \\ &\equiv \chi_\pi(r)g(\overline{\chi_\pi}) \pmod r. \end{aligned}$$

En déduire que

$$(\pi^3\overline{\pi})^{(r+1)/4} \equiv \chi_\pi(r)g(\chi_\pi)g(\overline{\chi_\pi}) \pmod r.$$

b) Montrer que le groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$ opère non trivialement sur le corps résiduel $k = \mathcal{O}/r\mathcal{O}$. En déduire que $\overline{\pi} \equiv \pi^r \pmod r$.

★ c) Montrer enfin que $\pi^{(r+1)(r+3)/4} \equiv \chi_\pi(-r)\pi^{r+1} \pmod r$.

3) Conclure que $\chi_r(\pi) \equiv \chi_\pi(-r) \pmod r$, puis que $\chi_r(\pi) = \chi_\pi(-r)$. Montrer que (R) est vrai sous les hypothèses de la question 2.

N.B. : Il resterait à traiter le cas $p \equiv r \equiv 1 \pmod 4$. La démonstration est analogue mais plus compliquée.

Exercice

L'équivalent $\psi(x) \sim x$ est une des formes du théorème des nombres premiers. On l'a déduit de la non-annulation de la fonction ζ de Riemann sur la droite $\Re(s) = 1$. [*Si les* a_n *sont définis par* $(-\zeta'/\zeta)(s) = \sum_{n\geqslant 1} a_n n^{-s}$, *on rappelle que* $\psi(x) := \sum_{n\leqslant x} a_n$.] On montre ici l'implication réciproque : en supposant que $\psi(x) \sim x$, on veut déduire que $\zeta(s)$ ne s'annule pas si $\Re(s) = 1$.

1) Montrer que si $s_0 = 1 + i\tau$ est un zéro d'ordre $m \geqslant 1$ de ζ, on a

$$\lim_{\sigma\to 1+} (\sigma - 1)\frac{\zeta'(\sigma + i\tau)}{\zeta(\sigma + i\tau)} = m.$$

2) Montrer que, pour $\Re(s) > 1$, on a

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{s}{s-1} + s\int_1^{+\infty} (\psi(t) - t)t^{-s-1}dt.$$

★ **3)** En déduire que

$$\lim_{\sigma\to 1+} (\sigma - 1)\frac{\zeta'(\sigma + i\tau)}{\zeta(\sigma + i\tau)} = 0$$

et conclure.