UPS – Centre d'Orsay **Arithmétique – Maîtrise**
Mathématiques Année 2003–2004

Partiel 08/04/2004, *durée 3h*

Exercice – Soit $N > 1$ un entier impair, dont on désire tester la primalité. On note $\left(\frac{\cdot}{N}\right)$ le symbole de Jacobi. Si N est premier alors, pour tout $1 < b < N$, on a

$$\left(\frac{b}{N}\right) \equiv b^{(N-1)/2} \pmod{N} \qquad (*)$$

On va montrer une réciproque faible, utilisable pour un test probabiliste. Soit donc $N > 1$ un entier *composé* impair.

1) On veut d'abord montrer qu'il existe *un* contre-exemple à $(*)$ dans $(\mathbb{Z}/N\mathbb{Z})^*$. Soit p un diviseur premier de N :

a) Si $p^2 \mid N$, montrer que $b = 1 + (N/p)$ convient.

b) Si $p^2 \nmid N$, et a n'est pas un carré modulo p, montrer que $b \equiv a \pmod{p}$, $b \equiv 1 \pmod{N/p}$ convient.

★ **2)** En déduire qu'au moins la moitié des $b \in (\mathbb{Z}/N\mathbb{Z})^*$ ne vérifient pas $(*)$.

Problème I

Dans tout ce problème, p désigne un nombre premier congru à 1 modulo 4 et on note λ le caractère de Legendre de $\mathbb{F}_p^*$, étendu à $\mathbb{F}_p$ de la façon habituelle. On rappelle que, d'après Fermat, $p = A^2 + B^2$ où $A, B \in \mathbb{Z}$, A impair et B pair. On cherche une expression explicite de A et B.

1) Soit $D \in \mathbb{F}_p^*$. Écrire le nombre de points sur $\mathbb{F}_p$ de la conique affine d'équation $y^2 = x^2 + D$, en fonction de

$$g(D) := \sum_{x \in \mathbb{F}_p} \lambda(x^2 + D)$$

2) Quel est le nombre de points de la courbe projective associée ? Le nombre de points à l'infini ? En déduire que $g(D) = -1$ pour tout $D \in \mathbb{F}_p^*$.

3) Si $a \in \mathbb{F}_p$, soit

$$\varphi(a) := \sum_{x \in \mathbb{F}_p} \lambda(x)\lambda(x^2 - a) \qquad (*)$$

Si $a = y^2 b$ avec $y, b \in \mathbb{F}_p^*$, montrer que

$$\varphi(a) = \lambda(y)\varphi(b)$$

En déduire que

$$S := \sum_{a \in \mathbb{F}_p} \varphi(a)^2 = \frac{p-1}{2}\left(\varphi^2(1) + \varphi^2(n)\right),$$

où $n \notin (\mathbb{F}_p)^2$ est un non-carré arbitraire.

4) En développant le carré de l'expression $(*)$, montrer d'abord que

$$S = \sum_{x,y,a\in\mathbb{F}_p} \lambda(xy)\lambda(a^2 - a(x^2+y^2) + x^2y^2),$$

puis par changement de variable

$$S = \sum_{x,y} \lambda(xy) \sum_b \lambda(b^2 + D(x,y)), \quad \text{où} \quad D(x,y) = -\left(\frac{x^2-y^2}{2}\right)^2 \in \mathbb{F}_p.$$

5) En utilisant 2), en déduire que $S = 2p(p-1)$. Montrer par ailleurs que $\varphi(a)$ est toujours pair et en déduire que

$$p = \left(\frac{\varphi(1)}{2}\right)^2 + \left(\frac{\varphi(n)}{2}\right)^2$$

est l'expression de Fermat.

6) Considérez la courbe d'équation affine $E_{\text{aff}} : y^2 = x(x^2-1)$. Écrire l'équation de la courbe projective E associée. Montrer que

$$|\#E(\mathbb{F}_p) - (p+1)| < 2\sqrt{p}$$

Ceci est-il conforme au théorème de Weil ?

7) Trouver deux automorphismes linéaires d'ordre 2 de $(\mathbb{F}_p)^2$ préservant $E_{\text{aff}}(\mathbb{F}_p)$, sans point fixe hors de la droite $y = 0$ [*introduire une racine carrée i de -1*]. En déduire que $\#E_{\text{aff}}(\mathbb{F}_p) \equiv 3 \pmod 4$, puis que $A = \varphi(1)/2$.

Problème II

Soit ζ une racine primitive 23-ème de l'unité, de polynôme minimal Φ et $K = \mathbb{Q}(\zeta)$. On veut montrer que $\mathcal{O}_K$ n'est pas principal.

1) À l'aide d'une somme de Gauss convenable, montrer que $\sqrt{-23} \in K$.

2) Soit $k = \mathbb{Q}(\sqrt{-23})$.

a) Expliciter $\mathcal{O}_K$ et $\mathcal{O}_k$.

b) Montrer que $2\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$, où $\mathfrak{p}, \mathfrak{p}'$ sont deux idéaux premiers distincts de $\mathcal{O}_k$ de norme 2, que l'on explicitera [*utiliser Kummer*].

c) Montrer que $\mathfrak{p}$ n'est pas principal.

d) Montrer que $\mathfrak{p}^3$ est principal et en déduire que $\mathfrak{p}^{11}$ ne l'est pas.

3)a) Quel est l'ordre de 2 dans $(\mathbb{Z}/23\mathbb{Z})^*$?

★ b) Montrer que $\overline{\Phi} = \Phi \mod 2$ a toutes ses racines dans $\mathbb{F}_{2^{11}}$, et aucune dans $\mathbb{F}_2$. En déduire la forme de la décomposition de Φ modulo 2.

c) En déduire que $2\mathcal{O}_K = \mathfrak{P}\mathfrak{P}'$, où $\mathfrak{P}\mathfrak{P}'$ sont deux idéaux premiers distincts de $\mathcal{O}_K$, de norme 2^{11} (ne pas les expliciter) [*utiliser Kummer*].

4) Pour tout idéal fractionnaire $\mathfrak{A}$ de k, on note

$$\mathfrak{A}\mathcal{O}_K = \left\{ \sum_{i\in I} a_i z_i, a_i \in \mathfrak{A}, z_i \in \mathcal{O}_K, I \text{ fini} \right\}$$

a) Montrer que $\mathfrak{A}\mathcal{O}_K$ est un idéal fractionnaire de K.

b) On *admet* que $i : \mathfrak{A} \mapsto \mathfrak{A}\mathcal{O}_K$ est un morphisme de groupes [*vérifications explicites*]. Si $\mathfrak{A}\mathcal{O}_K = \mathcal{O}_K$, montrer que $\mathfrak{A} \subset \mathcal{O}_k$. En déduire que i est injective.

c) On peut supposer $\mathfrak{p} \subset \mathfrak{P}$. Déduire de (2.b) et (3.c) que $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}$.

5) Supposons que $\mathfrak{P}$ est principal, engendré par $b \in \mathcal{O}_K$.

a) Montrer que $\mathfrak{p}\mathcal{O}_K = (\sigma b)\mathcal{O}_K$ pour tout $\sigma \in \mathrm{Gal}(K/k)$.

b) Soit $a = N_{K/k}b$. Montrer que $a \in \mathcal{O}_k$, puis que $\mathfrak{p}^{11} = a\mathcal{O}_k$.

c) En déduire que $\mathcal{O}_K$ n'est pas principal.