UPS – Centre d'Orsay
Mathématiques

Arithmétique – Maîtrise
Année 2003–2004

DEVOIR n° 1 (pour la semaine du 28/03)

Problème I

Théorème 1 (Eisenstein)**.** *Un nombre premier* $p \equiv 1 \pmod 4$ *est de la forme* $A^2 + 64B^2$, $A, B \in \mathbb{Z}$ *si et seulement si* 2 *est une puissance* 4*-ième dans* $\mathbb{F}_p$.

Soit donc $p \equiv 1 \pmod 4$ un nombre premier. On rappelle qu'alors $p = a^2 + b^2$, $a, b \in \mathbb{Z}$. On choisit $a, b > 0$, a impair, et donc b pair. Noter que

$$2p = (a + b)^2 + (a - b)^2 \tag{1}$$

A) Montrer que $(a + b)^2 \equiv 2ab \pmod p$, puis

$$(a + b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \pmod p, \tag{2}$$

et enfin que a, b, $a + b$ et $a - b$ sont étrangers à p.

B) Montrer que

$$\left(\frac{a}{p}\right) = 1, \tag{3}$$

puis à l'aide de (1) que

$$\left(\frac{a+b}{p}\right) = (-1)^{((a+b)^2-1)/8}. \tag{4}$$

C) On considère maintenant a, b comme des éléments de $\mathbb{F}_p^*$. Soit $f = b/a$. Montrer que $f^2 = -1$.

D) En utilisant (4), (2) et (3), montrer que

$$(-1)^{((a+b)^2-1)/8} = 2^{(p-1)/4} f^{(a^2+b^2-1)/4}$$

dans $\mathbb{F}_p$.

E) Montrer enfin que $2^{(p-1)/4} = f^{ab/2}$. Quel est l'ordre de f dans $\mathbb{F}_p^*$? En déduire le Théorème d'Eisenstein.

F) Montrer que si $p \equiv 3 \pmod 4$, alors tout carré est une puissance 4-ième.

Problème II

Soit $m \geqslant 1$ un entier et $p \nmid m$ un nombre premier. On veut étudier la fonction zêta sur $\mathbb{F}_p$ de la courbe projective plane

$$\mathcal{C}_m : X^m + Y^m = Z^m.$$

L'entier $s \geqslant 1$ sera utilisé pour paramétrer les extensions $\mathbb{F}_{p^s}$ de $\mathbb{F}_p$, χ, ρ désignent deux caractères de $(\mathbb{F}_{p^s})^*$, étendus à $\mathbb{F}_{p^s}$ de la façon habituelle. On note

$$J(\chi, \rho) = \sum_{x \in \mathbb{F}_{p^s}} \chi(x)\rho(1-x)$$

la somme de Jacobi.

A) Montrer que la restriction $p \nmid m$ n'est pas une perte de généralité.

B) Caractériser en fonction de l'ordre de p dans $(\mathbb{Z}/d\mathbb{Z})^*$ les corps $\mathbb{F}_{p^s}$ contenant une racine primitive d-ème de l'unité.

C) Montrer que $J(\chi^p, \rho^p) = J(\chi, \rho)$ pour tous caractères χ, ρ de $(\mathbb{F}_{p^s})^*$.

D) Si χ, ρ sont deux caractères, on note $d(\chi, \rho)$ le ppcm de leurs ordres exacts. Montrer que

$$\#\mathcal{C}_m(\mathbb{F}_{p^s}) = p^s + 1 + \sum_{\substack{d \mid m \\ \mu_d \subset \mathbb{F}_{p^s}}} \sum_{\chi, \rho} J(\chi, \rho),$$

où χ, ρ parcourent les caractères de $\mathbb{F}_{p^s}$ tels que $d(\chi, \rho) = d$, $\chi \neq \varepsilon$, $\rho \neq \varepsilon$, et $\chi\rho \neq \varepsilon$.

E) En déduire que $\mathcal{C}_m$ vérifie les hypothèses et les conclusions du théorème de Weil. Expliciter le degré du numérateur de la fonction zêta.