UPS – Centre d'Orsay
Mathématiques

Arithmétique – Maîtrise
Année 2003–2004

FEUILLE D'EXERCICES n° 2

Exercice 1 –

a) 1475 est-il un carré modulo 2389 ?

b) Soit $n \in \mathbb{N}$ tel que $p = 4n + 3$ et $q = 2n + 1$ soient premiers. Quand 3 est-il racine primitive modulo p ?

Exercice 2 – Déterminer les nombres premiers p tels que 6 soit un carré modulo p.

Exercice 3 – Soit p premier $p \equiv 3 \pmod 4$. Montrer que $2p + 1$ est premier si, et seulement si $2^p \equiv 1 \pmod{2p+1}$. En déduire que les nombres de Mersenne M_{11}, M_{23}, M_{83}, M_{131} (définis par $M_p = 2^p - 1$) ne sont pas premiers.

Exercice 4 – Soit $n \in \mathbb{N}^*$. Montrer que si $p = 2^{2^n} + 1$ est premier (nombre de Fermat), 3 est racine primitive modulo p [*il suffit de montrer que ce n'est pas un carré*].

★ **Exercice 5** – Déterminer le nombre de carrés de $\mathbb{Z}/m\mathbb{Z}$.

Exercice 6 – [*Une preuve de la loi de réciprocité quadratique*] Soient p, ℓ deux nombres premiers impairs distincts ; $\mathbb{F}_q$ une extension finie de $\mathbb{F}_p$ contenant une racine primitive ℓ-ième ω de l'unité. On pose $y = \sum_{x \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{x}{\ell}\right)\omega^x \in \mathbb{F}_q$.

★ **a)** Montrer que $y^2 = (-1)^{(\ell-1)/2}\ell$.

b) Montrer que $y^{p-1} = \left(\frac{p}{\ell}\right)$ et montrer la loi de réciprocité.

c) Soit $\mathbb{F}_q$ une extension finie de $\mathbb{F}_p$ contenant ω une racine primitive 8-ième de l'unité. En considérant $y = \omega + \omega^{-1}$, y^2 et y^p, montrer que

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Exercice 7 – Pour p premier impair, on définit la somme de Salié par la formule suivante

$$K(m,n) = \sum_{x \in \mathbb{F}_p^*} \lambda(x)\psi(mx + nx^{-1}),$$

où λ est le caractère de Legendre et ψ le caractère additif $\psi(x) = \exp(2i\pi x/p)$ modulo p. On note $g(\lambda)$ la somme de Gauss associée au caractère λ.

a) Calculer cette somme lorsque $p|mn$.

b) On se propose de calculer $K(n,n)$ dans le cas $(p,2n)=1$. Pour tout $y \in \mathbb{F}_p$, montrer l'égalité

$$f_p(y) := \sum_{x+x^{-1} \equiv y \pmod p} \lambda(x) = \lambda(y-2) + \lambda(y+2).$$

[*considérer la quantité* $\lambda(y-2)f_p(y)$]

c) En déduire que

$$K(n,n) = 2g(\lambda)\lambda(n)\cos\Big(\frac{4\pi n}{p}\Big),$$

★ **d)** Calculer $K(m,n)$ si $(2mn,p)=1$ [*discuter suivant que* mn *est un carré ou non modulo* p].

Exercice 8 – On considère $a_1,\dots,a_n \in \mathbb{Z}$, $r_1,\dots,r_n \in \mathbb{N}^*$. Lorsque $p \nmid a_1a_2\dots a_n$, on note $N(p)$ le nombre de solutions dans $\mathbb{F}_p^n$ de l'équation

$$a_1x_1^{r_1} + \cdots + a_nx_n^{r_n} = 0 \pmod p.$$

Le but de cet exercice est de démontrer l'inégalité

$$|N(p) - p^{n-1}| \leqslant C(p-1)p^{n/2-1},$$

avec $C = (d_1-1)(d_2-1)\dots(d_n-1)$ et $d_j = (r_j, p-1)$. On note ψ le caractère additif $\psi(x) = \exp(2i\pi x/p)$ modulo p.

a) Soit $F(X_1,\dots,X_n) \in \mathbb{F}_p[X_1,\dots,X_n]$. Montrer que

$$\#\big\{\mathbf{x} \in \mathbb{F}_p^n,\ F(x_1,\dots,x_n) = 0\big\} = \frac{1}{p}\sum_{x,x_1,\dots,x_n \in \mathbb{F}_p} \psi\big(xF(x_1,\dots,x_n)\big).$$

b) Soit $a \in \mathbb{F}_p$, $d \geqslant 1$, montrer que

$$\sum_{\chi^d = \varepsilon} \chi(a) = \#\left\{x \in \mathbb{F}_p, x^d = a\right\},$$

où χ parcourt les caractères de Dirichlet modulo p d'exposant d et ε est le caractère principal (tel que $\varepsilon(x) = 1$ pour tout $x \in \mathbb{F}_p$).

c) Montrer que pour tout $a \in \mathbb{Z}$ et $r \geqslant 1$, $p \nmid a$ on a :

$$\sum_{y \in \mathbb{F}_p} \psi(ay^r) = \sum_{\chi \neq \varepsilon, \chi^d = \varepsilon} g_a(\chi)$$

avec $d = (r, p-1)$ et $g_a(\chi) = \sum_x \chi(x)\psi(ax)$ la somme de Gauss.

d) Conclure. Ce résultat est-il évident lorsque $C = 0$?

e) Montrer que pour tout entier $n \geqslant 2$ l'équation $x^4 - 17y^4 - 2z^2 = 0 \pmod n$ admet une solution non triviale ($(x,y,z,n) = 1$).

Exercice 9 – On veut montrer que l'équation $x^4 - 17y^4 = 2z^2$ n'admet pas de solution non triviale dans $\mathbb{Z}$:

a) Se ramener au cas $(x, y, z) = 1$.

b) En utilisant la multiplicativité (dans $\mathbb{Q}(\sqrt{17})$) de la fonction $N(x + \sqrt{17}y) := x^2 - 17y^2$ et l'égalité $N(5 + \sqrt{17}) = 2 \times 2^2$, montrer que

$$(5x^2 + 17y^2 - 4z)(5x^2 + 17y^2 + 4z) = 17(x^2 + 5y^2)^2$$

c) Montrer que les deux facteurs de gauche n'ont pas de facteur impair commun. En déduire qu'ils sont de la forme $(17u^2, v^2)$ ou $(34u^2, 2v^2)$. Conclure en examinant ces deux cas modulo 17.

Exercice 10 – Soit p un nombre premier impair, χ un caractère non trivial de $\mathbb{F}_p^*$ et λ le caractère de Legendre modulo p. Montrer que

$$J(\chi, \lambda) := \sum_{\substack{a+b=1 \\ (a,b)\in\mathbb{F}_p^2}} \chi(a)\lambda(b) = \sum_{t\in\mathbb{F}_p} \chi(1 - t^2).$$

a) Montrer que, lorsque $k \in \mathbb{F}_p^*$, on a $\sum_{t\in\mathbb{F}_p} \chi(t(k - t)) = \chi(k^2/2^2)J(\chi, \lambda)$.

b) Montrer que, lorsque χ^2 est non trivial, on a $g(\chi)^2 = \overline{\chi(4)}J(\chi, \lambda)g(\chi^2)$.

On suppose dorénavant que χ est d'ordre exact 3.

c) Montrer que $g(\chi)^3 = p\chi(2)J(\chi, \lambda)$.

d) Soit $D \in \mathbb{Z} - \{0\}$. Montrer que le nombre de solutions de $y^2 = x^3 + D$ dans $\mathbb{F}_p$ est $p + \pi + \overline{\pi}$ où $\pi = (\chi\lambda)(D)J(\chi, \lambda)$.

★ **e)** Lorsque $\chi(2) = 1$, montrer que le nombre de solutions de $y^2 = x^3 + 1$ est $p + A$ où $4p = A^2 + 27B^2$ avec $A \equiv 1 \pmod 3$ [*écrire $J(\chi, \lambda)$ dans $\mathbb{Z}[j]$. On pourra montrer que $\mathbb{Z}[\zeta_{3p}] \cap \mathbb{Q} = \mathbb{Z}$, où ζ_{3p} est une racine $3p$-ème de l'unité*].