UPS – Centre d'Orsay
Mathématiques

**Arithmétique – Maîtrise**
Année 2003–2004

# DEVOIR n° 1 (Correction)

## Problème I

**A)** $(a+b)^2 - 2ab = a^2 + b^2 \equiv 0 \pmod p$. Puisque $(p-1)/4$ est entier, on peut écrire

$$(a+b)^{(p-1)/2} = [(a+b)^2]^{(p-1)/4} \equiv (2ab)^{(p-1)/4} \pmod p$$

par ce qui précède. Si $p \mid a$, $p = a^2 + b^2$, alors $p \mid b$ soit $p^2 \mid p$, absurde. Donc $a$ est premier à $p$, ainsi que $b$ par le même argument. Si $p \mid (a+b)$, alors $p \mid 2ab$, soit ($p$ impair) $p \mid ab$, et $p \mid a$ ou $p \mid b$, absurde. Finalement $p \mid (a-b)$ implique $p \mid (a+b)$ d'après (1).

**B)** D'après les propriétés du symbole de Jacobi,

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{(a-1)(p-1)/4} = \left(\frac{p}{a}\right),$$

puisque $a$ est impair et $p \equiv 1 \pmod 4$. Mais

$$\left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1,$$

puisque $\left(\frac{p}{a}\right) \neq 0$, donc $\left(\frac{b}{a}\right) = \pm 1$. De même ($a+b$ impair, $p \equiv 1 \pmod 4$),

$$\begin{aligned}
\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right) &= \left(\frac{2}{a+b}\right)\left(\frac{2p}{a+b}\right) \\
&= (-1)^{((a+b)^2-1)/8}\left(\frac{(a-b)^2}{a+b}\right) = (-1)^{((a+b)^2-1)/8}
\end{aligned}$$

où on utilise le symbole de Jacobi de 2, (1) et $\left(\frac{a+b}{p}\right) \neq 0$.

**C)** Dans $\mathbb{F}_p$, on a $a^2 + b^2 = p = 0$, soit $(b/a)^2 + 1 = 0$.

**D)**

$$\begin{aligned}
(-1)^{((a+b)^2-1)/8} &= \left(\frac{a+b}{p}\right) \qquad \text{d'après (4)} \\
&= (2ab)^{(p-1)/4} \qquad \text{d'après (2)} \\
&= 2^{(p-1)/4}(a^2)^{(p-1)/4} f^{(p-1)/4} = 2^{(p-1)/4} a^{(p-1)/2} f^{(a^2+b^2-1)/4} \\
&= 2^{(p-1)/4} f^{(a^2+b^2-1)/4} \qquad \text{d'après (3)}
\end{aligned}$$

**E)** Donc

$$\begin{aligned}
(-1)^{((a+b)^2-1)/8} &= f^{((a+b)^2-1)/4} \qquad \text{car } f^2 = -1 \\
&= 2^{(p-1)/4} f^{(a^2+b^2-1)/4} \qquad \text{d'après la question précédente}
\end{aligned}$$

En simplifiant, on trouve $f^{ab/2} = 2^{(p-1)/4}$. Donc, $f$ est d'ordre 4 puisque $f^4 = 1$ et $f^2 = -1 \neq 1$. Comme $\mathbb{F}_p^*$ est cyclique, $x^4 = 2$ a une solution dans $\mathbb{F}_p^*$ si et seulement si

$$\begin{aligned} 2^{(p-1)/4} = 1 &\iff f^{ab/2} = 1 \\ &\iff 4 \mid ab/2 \\ &\iff 8 \mid b \quad (a \text{ impair}) \end{aligned}$$

Si $8 \mid b$, alors $b = 8B$ et $p = a^2 + 64B^2$. Réciproquement, si $p = a^2 + 64B^2$, on peut écrire $p = a^2 + b^2$, avec $b = 8B$, donc 8 divise $b$ est 2 est une puissance 4-ième.

**F)** Par cyclicité de $\mathbb{F}_p^*$, un élément est puissance $r$-ème si est seulement si il est puissance $d$-ème, avec $d = (r, p-1)$. Si $p \equiv 3 \pmod 4$, on obtient $d = 2$ pour $r = 2^k$.

## Problème II

**A)** On peut écrire $m = p^v q$, où $(q,p) = 1$, et la courbe $\mathcal{C}_q$ a les mêmes points que $\mathcal{C}_m$ sur tout corps de caractéristique $p$. Elles ont donc mêmes fonctions zêtas.

**B)** Le groupe multiplicatif $\mathbb{F}_{p^s}^*$ étant cyclique d'ordre $p^s - 1$, il contient un élément d'ordre exact $d$ si et seulement si $d \mid p^s - 1$, soit si et seulement si $s$ est un multiple de l'ordre de $p$ dans $(\mathbb{Z}/d\mathbb{Z})^*$ [*$d$ et $p$ sont nécessairement premiers entre eux*]. On note ce dernier $s(d)$.

**C)** Soit $F$ l'automorphisme de Frobenius sur $\mathbb{F}_{p^s}$, on a

$$J(\chi^p, \rho^p) = \sum_x \chi(F(x))\rho(F(1-x)) = \sum_y \chi(y)\rho(1-y) = J(\chi, \rho),$$

avec le changement de variable $y = F(x)$.

**D)** Le nombre de triplets $(X, Y, Z)$ dans $\mathbb{F}_{p^s}^3$ satisfaisant l'équation vaut

$$\sum_{a+b=c} \sum_\chi \chi(a) \sum_\chi \chi(b) \sum_\chi \chi(c)$$

où $\chi$ parcourt les caractères d'exposant $m$ de $\mathbb{F}_{p^s}^*$ dans les trois sommes. Soit, en utilisant les propriétés des sommes de Jacobi triples

$$p^{2s} + (p^s - 1) \sum_{\chi,\rho} J(\chi, \rho)$$

où $\chi, \rho \neq \varepsilon$ sont d'exposant $m$, $\chi\rho \neq \varepsilon$. En supprimant le point $(0,0,0)$ et en quotientant par $\mathbb{F}_{p^s}^*$, on obtient

$$\mathcal{C}_m(\mathbb{F}_{p^s}) = p^s + 1 + \sum_{\chi,\rho} J(\chi, \rho)$$

On obtient l'égalite requise en regroupant les paires de caractères suivant la valeur de $d(\chi, \rho)$.

**E)** Si $d(\chi,\rho) = d$, ces caractères sont induits par des caractères de $\mathbb{F}^*_{p^{s(d)}}$, $\chi = \chi' \circ N_{\mathbb{F}_{p^s}/\mathbb{F}_{p^{s(d)}}}$ et l'analogue pour $\rho$. D'après Hasse-Davenport

$$J(\chi,\rho) = -\big(-J(\chi',\rho')\big)^{s/s(d)},$$

où $J(\chi',\rho')$ désigne la somme de Jacobi sur $\mathbb{F}_{p^{s(d)}}$. En regroupant les paires de caractères suivant la valeur de $d$ et en inversant les sommations sur $s$ et $d$, on obtient

$$Z(T) = \exp \sum_{s\geqslant 1} \#\mathcal{C}(\mathbb{F}_{p^s})\frac{T^s}{s} = \frac{1}{(1-T)(1-p^T)}\exp(-S),$$

où

$$S = \sum_{d|m}\sum_{\chi',\rho'}\sum_{k\geqslant 1}\big(-J(\chi',\rho')\big)^k \frac{T^{ks(d)}}{ks(d)}$$

où $\chi',\rho' \neq \varepsilon$ parcourent les caractères de $\mathbb{F}^*_{p^{s(d)}}$, tels que $\chi'\rho' \neq \varepsilon$ et $d(\chi',\rho') = d$. On a posé $k = s/s(d)$.

On note $F$ le Frobenius de $\mathbb{F}_{p^{s(d)}}$. Il agit sur les paires de caractères comme ci-dessus, via $F \cdot (\chi',\rho') = (\chi' \circ F, \rho' \circ F)$. Comme $(\chi',\rho')$ est d'ordre $d$ dans $X(\mathbb{F}^*_{p^{s(d)}})^2$, chaque orbite est de cardinal $s(d)$, l'ordre de $F$. Comme la somme de Jacobi $J(\chi',\rho')$ est constante sur une orbite, on peut sommer sur les classes d'équivalence modulo l'action de $F$ et non plus sur $(\chi',\rho')$, ce qui simplifie le dénominateur $s(d)$, soit

$$S = \sum_{d|m}\sum_{(\chi',\rho')/\sim}\sum_{k\geqslant 1}\big(-J(\chi',\rho')\big)^k \frac{T^{ks(d)}}{k}$$

et

$$Z(T) = \frac{1}{(1-T)(1-pT)}\prod_{d|m}\prod_{(\chi',\rho')/\sim}\big(1 + J(\chi',\rho')T^{s(d)}\big).$$

Soit $f(X,Y,Z) = X^m + Y^m + Z^m$. Comme $\operatorname{grad} f = m(X^{m-1}, Y^{m-1}, Z^{m-1})$ ne s'annule qu'en $(0,0,0)$, la courbe $\mathcal{C}_m$ est lisse. Soit $g = (m-1)(m-2)/2$. La fonction zêta est bien une fraction rationnelle de la forme $P_{2g}(T)/(1-T)(1-pT)$ où $P_{2g}$ est de degré $2g = (m-1)(m-2)$. En effet le degré du numérateur est

$$\begin{aligned}\sum_{d|m} s(d)\#\left\{(\chi',\rho')/\sim \colon d(\chi',\rho') = d\right\} &= \sum_{d|m}\#\left\{(\chi',\rho')\colon d(\chi',\rho') = d\right\}\\ &= \sum_{d|m}\#\left\{(\chi,\rho)\colon d(\chi,\rho) = d\right\},\end{aligned}$$

où $\chi,\rho$ sont des caractères d'exposant $m$ d'une extension $K/\mathbb{F}_p$ contenant les racines $m$-èmes de l'unité, par exemple $K = \mathbb{F}_p^{s_m}$. On a utilisé la bijection entre caractères d'exposants $d$ de $K^*$ et de $\mathbb{F}^*_{p^{s(d)}}$. La dernière somme vaut

$$\#\left\{(\chi,\rho)\colon d(\chi,\rho) \mid m\right\} = \#\left\{(\chi,\rho)\colon \operatorname{ord}(\chi)\mid m, \operatorname{ord}(\rho)\mid m\right\},$$

Soit $m-1$ possibilité pour $\chi \neq \varepsilon$, et $m-2$ pour $\rho \neq \varepsilon, \chi$.