Université de Paris 6 Master M1 de mathématiques 05-06
M. Bertrand *Théorie des Nombres*

Partiel du 5 Mai 2006

Durée: 3 heures

L'usage du polycopié du cours et des feuilles d'exercices est autorisé.
Les 3 énoncés sont indépendants.

I

Soient p un nombre premier impair, et $f(T) \in \mathbf{F}_p[T]$ un polynôme à coefficients dans $\mathbf{F}_p$. On note $N = N(f)$ le nombre de solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ de l'équation $y^2 = f(x)$, et $\overline{N}$ la classe de N modulo p, vue comme un élément de $\mathbf{F}_p$.

1°/ On suppose ici que $f(T) = aT^2 + bT + c$ est de degré 2.

i) Montrer que l'ensemble $R_1 = \{y^2\,, y \in \mathbf{F}_p\}$ a $\frac{p-1}{2} + 1$ éléments, et que l'ensemble $R_2 = \{f(x)\,, x \in \mathbf{F}_p\}$ a également $\frac{p-1}{2} + 1$ éléments.

ii) En déduire que $N(f) \geq 1$.

2°/ On ne fait plus d'hypothèse sur f.

i) Montrer que $N = \Sigma_{x \in \mathbf{F}_p}((\frac{f(x)}{p}) + 1)$, où $(\frac{-}{p})$ désigne le symbole de Legendre.

ii) En déduire que $\overline{N} = \Sigma_{x \in \mathbf{F}_p} f(x)^{(p-1)/2}$ (égalité dans $\mathbf{F}_p$).

iii) Soit i un entier > 0. Montrer que dans le corps $\mathbf{F}_p$, on a :

$$\Sigma_{x \in \mathbf{F}_p} x^i = -1 \text{ si } p-1 \text{ divise } i\ ; \quad \Sigma_{x \in \mathbf{F}_p} x^i = 0 \text{ si } p-1 \text{ ne divise pas } i.$$

3°/ On suppose ici que f est un polynôme de degré 3, et on note $A \in \mathbf{F}_p$ le coefficient du terme de degré $p-1$ du polynôme $f(T)^{(p-1)/2} = \ldots + AT^{p-1} + \ldots.$

i) Déduire de 2^o/ que $\overline{N} = -A$.

ii) On suppose que $f(T) = T(T-1)(T-\lambda)$, où $\lambda \in \mathbf{F}_p$, et on pose $m = (p-1)/2$. Montrer que $A = (-1)^m \, \Sigma_{j=0,\ldots,m} \begin{pmatrix} m \\ j \end{pmatrix}^2 \lambda^j$, où $\begin{pmatrix} m \\ j \end{pmatrix}$ désigne le coefficient binomial C_m^j.

II

On note G le groupe multiplicatif $\mathbf{F}_{41}^*$. On rappelle qu'il est cyclique, et on se propose de déterminer l'ensemble S de tous les générateurs de G.

1°/ i) Déterminer l'ordre de G, et le nombre d'éléments de S.

ii) Calculer le symbole de Legendre $(\frac{2}{41})$. En déduire que $2 \notin S$.

iii) Calculer $(\frac{3}{41}), (\frac{5}{41}), (\frac{-1}{41})$.

2°/ Soit $\Phi_8 \in \mathbf{F}_{41}[T]$ le polynôme cyclotomique d'ordre 8.

i) Montrer que l'équation $\Phi_8(x) = 0$ admet 4 racines $x_1, ..., x_4$ dans $\mathbf{F}_{41}$.

ii) Déterminer ces racines. (On pourra remarquer que $-1 \equiv 9^2$ mod. 41.)

3°/ Soit $\Phi_5 \in \mathbf{F}_{41}[T]$ le polynôme cyclotomique d'ordre 5.

i) Montrer que l'équation $\Phi_5(y) = 0$ admet 4 racines $y_1, ..., y_4$ dans $\mathbf{F}_{41}$.

ii) Vérifier que $y_1 = -4$ est l'une de ces racines.

4°/ i) Montrer que pour tout $1 \leq i, j, \leq 4$, le produit $x_i y_j$ appartient à S.

ii) Déterminer l'ensemble S.

III

Soient $q = p^n$ une puissance d'un nombre premier p, et $\mathbf{F}_q$ le corps à q éléments. On suppose que n divise $p-1$.

1°/ i) Calculer l'ordre du groupe $\mu_n(\mathbf{F}_p)$ des racines n-ièmes de l'unité dans $\mathbf{F}_p$.

ii) Soit ζ un élément de $\mu_n(\mathbf{F}_p)$. Montrer que $\zeta^{\frac{p^n-1}{p-1}} = 1$. En déduire que si α est un générateur du groupe cyclique $\mathbf{F}_q^*$, et si $\zeta = \alpha^k$, alors, $p-1$ divise k.

iii) Montrer que pour tout élément ζ de $\mu_n(\mathbf{F}_p)$, il existe un élément x de $\mathbf{F}_q^*$ tel que $x^{p-1} = \zeta$.

2°/ On considère le sous-groupe $G_n = \{x \in \mathbf{F}_q^*, x^n \in \mathbf{F}_p^*\}$ de $\mathbf{F}_q^*$, et on note ϕ l'endomorphisme de G_n défini par $\phi(x) = x^{p-1}$.

i) Déterminer le noyau de ϕ.

ii) Montrer que l'image de ϕ coïncide avec $\mu_n(\mathbf{F}_p)$.

iii) Calculer l'ordre de G_n.

3°/ Montrer que pour tout élément a de $\mathbf{F}_p$, il existe un élément x de $\mathbf{F}_q$ tel que $x^n = a$.

Corrigé

I $1^o/$ i) Toute valeur atteinte du polynôme T^2 l'est en deux points $\{y, -y\}$, qui sont distincts si $y \neq 0$ (NB: $p \neq 2$). Il prend donc $1 + (card\mathbf{F}_p - 1)/2$ valeurs distinctes. Toute valeur atteinte du polynôme $f(T)$ l'est en deux points $\{x_1, x_2 = -\frac{b}{a} - x_1\}$, qui sont distincts si $x_1 \neq -\frac{b}{2a}$ (NB: $p \neq 2$). Il prend donc $1 + (card\mathbf{F}_p - 1)/2$ valeurs distinctes.

ii) Comme $card(R_1) + card(R_2) > card\mathbf{F}_p$, R_1 et R_2 admettent au moins un point commun, et ce point fournit une solution de $y^2 = f(x)$.

$2^o/$ i) Tout point $x \in \mathbf{F}_p$ tel que $f(x)$ est un carré non nul (resp. nul, resp. n'est pas un carré) fournit deux (resp. une, resp. aucune) solutions de l'équation $y^2 = f(x)$, c'est-à-dire dans chaque cas $(\frac{f(x)}{p}) + 1$ solutions. Leur somme sur tous les x vaut donc N.

ii) La deuxième égalité résulte alors des relations $p = 0$ et $(\frac{a}{p}) = a^{(p-1)/2}$ dans $\mathbf{F}_p$.

iii) Dans le premier cas, $\Sigma_x\, x^i = p - 1 = -1$ (NB: $i \neq 0$). Dans le deuxième cas, on choisit un generateur ξ de $\mathbf{F}_p^*$; alors $\xi^i \neq 1, \xi^{i(p-1)} = 1$ et la somme s'ecrit $\Sigma_{k=0,\ldots,p-2}\xi^{ik} = (\xi^{i(p-1)} - 1)/(\xi^i - 1) = 0$.

$3^o/$ i) Comme $deg(f) = 3$, le seul monôme $A_i T^i$ de degré i non nul et divisible par $p-1$ apparaissant dans le développement de $f(T)^{(p-1)/2}$ est celui de degré $p-1$. D'après $2^o/$, on a donc $\overline{N} = A_0\Sigma_x x^0 + A\,\Sigma_x\, x^{p-1} = pA_0 - A = -A$.

ii) Pour un tel f, A est le coefficient du terme de degré m de $(T-1)^m(T-\lambda)^m$, c'est-à-dire $\Sigma_{j=0,\ldots,m} C_m^{m-j}(-1)^{m-j} C_m^j (-\lambda)^j = (-1)^m \Sigma_j (C_m^j)^2 \lambda^j$.

II $1^o/$ i) G a $\phi(41) = 40$ éléments. S est l'ensemble des générateurs d'un groupe cyclique isomorphe à $\mathbf{Z}/40\mathbf{Z}$, donc a $\phi(40) = \phi(8)\phi(5) = 16$ éléments.

ii) $(\frac{2}{41}) = 2^{42.40/8} = 1$; donc 2, carré d'un élément de G, est d'ordre au plus 20.

iii) $(\frac{3}{41}) = (-1)^{1.20}(\frac{41}{3}) = (\frac{2}{3}) = -1$. $(\frac{5}{41}) = (-1)^{2.20}(\frac{41}{5}) = 1$. $(\frac{-1}{41}) = (-1)^{20} = 1$.

$2^o/$ i) Comme 8 divise 40, G admet un unique sous-groupe cyclique d'ordre 8, et ses $\phi(8) = 4$ générateurs $x_1, ..., x_4 \in \mathbf{F}_{41}^*$ sont par définition les racines de Φ_8.

ii) $\Phi_8(T) = \frac{T^8-1}{T^4-1} = T^4 + 1$. Ses racines sont les solutions de $(x^2)^2 = -1 = 9^2$, soit $x^2 = 9$ et $x_1 = 3, x_2 = -3$, ou $x^2 = -9 = (9.3)^2$ et $x_3 = -14, x_4 = 14$.

$2^o/$ i) Comme 5 divise 40, G admet un unique sous-groupe cyclique d'ordre 5, et ses $\phi(5) = 4$ générateurs $y_1, ..., y_4 \in \mathbf{F}_{41}^*$ sont les racines de Φ_5.

ii) $(-4)^2 = 16, 16^2 = 10$ et $-4.10 = 1$, donc $y_1 = -4$ est d'ordre 5 dans G. Les autres racines sont donc $y_2 = 16, y_3 = y_1^3 = 18, y_4 = 10$.

$3^o/$ i) L'ordre de chaque $z = x_i y_j$ divise 40. Comme $z^8 = y_j^8 = y_j^3 \neq 1$ et $z^{20} = x_i^4 \neq 1$, z est d'ordre 40, donc est un des générateurs de G.

ii) Ces z sont distincts, car un élément d'ordre divisant 8 ne peut être égal à un élément d'ordre divisant 5 que s'il vaut 1. Il y a donc $4 \times 4 = 16 = cardS$ tels produits, et

$S = \{x_i y_j ; 1 \leq i, j, \leq 4\}$.
[NB : 2 et 5 (et 4) n'appartiennent pas à S, d'après le $1^o/$; 3 non plus, car d'ordre 8 par le $2^o/$. Le "plus petit" élément de S est en fait $x_4 y_3 = 14 \times 18 = 252 = 6$.]

III $1^o/$ i) Comme n divise $p-1$, le groupe cyclique $\mathbf{F}_p^*$ admet un unique sous-groupe d'ordre n, dont les éléments forment par définition le groupe $\mu_n(\mathbf{F}_p)$.

ii) Comme $\zeta \in \mathbf{F}_p$, $\zeta^p = \zeta$, donc $\zeta^{\frac{p^n-1}{p-1}} = \zeta^{1+p+\ldots+p^{n-1}} = \zeta^{1+1+\ldots+1} = \zeta^n = 1$. Ainsi, $\alpha^{k\frac{p^n-1}{p-1}} = 1$, et l'ordre p^n-1 de α divise $k\frac{p^n-1}{p-1}$, donc $p-1$ divise k.

iii) Si $\zeta = \alpha^k$, $x = \alpha^{\frac{k}{p-1}} \in \mathbf{F}_q^*$ vérifie $x^{p-1} = \zeta$.

$2^o/$ i) Si $x \in Ker\phi$, $x^p = x$ donc $x \in \mathbf{F}_p$. Si $x \in \mathbf{F}_p^*$, $\phi(x) = 1$ et la condition $x^n \in \mathbf{F}_p^*$ est automatiquement réalisée. Donc $Ker\phi = \mathbf{F}_p^*$.

ii) Pour tout $y = \phi(x), x \in G_n$, on a : $y^n = x^{(p-1)n} = (x^n)^{p-1} = 1$ car $x^n \in \mathbf{F}_p^*$, donc $Im\phi \subset \mu_n(\mathbf{F}_p)$. Inversément, on vient de voir que pour tout $\zeta \in \mu_n(\mathbf{F}_p)$, il existe $x \in \mathbf{F}_q^*$ tel que $\phi(x) = \zeta$; ce x vérifie $(x^n)^{p-1} = \zeta^n = 1$, donc $x^n \in \mathbf{F}_p^*$, et $x \in G_n$. Ainsi, $Im\phi = \mu_n(\mathbf{F}_p)$.

iii) $|G_n|/|Ker\phi| = |Im\phi|$, donc $|G_n| = (p-1)n$.

$3^o/$ C'est clair pour $a = 0$. Considérons maintenant l'homomorphisme ψ de G_n dans $\mathbf{F}_p^*$ défini par $\psi(x) = x^n$. Son noyau est $\mu_n(\mathbf{F}_p)$, donc son image a $|G_n|/|Ker\psi| = (p-1)n/n = card\mathbf{F}_p^*$ éléments, et ψ est surjective. Ainsi, tout élément a de $\mathbf{F}_p^*$ est racine n-ième d'un élément x de $G_n \subset \mathbf{F}_q^*$.