Devoir de Mathématiques n°15

Kévin Polisano
MPSI 1

Lundi 25 Mars 2008

Exercice 1 : Puissance de 7

Énoncé :

Déterminer le dernier chiffre, en numération décimale, de :

$$N = 7 \uparrow\uparrow 7 = 7^{7^{7^{7^{7^{7^{7}}}}}}$$

C'est la notation des puissances itérées de Knuth.

Résultats préliminaires :

$(*)$ On remarque une 2-périodicité de $7^{k'}$ modulo 4 :

$$k' \equiv 0[2] \Rightarrow 7^{k'} \equiv 1[4]$$
$$k' \equiv 1[2] \Rightarrow 7^{k'} \equiv 3[4]$$

$(**)$ De même on remarque une 4-périodicité de 7^k modulo 10 :

$$k \equiv 0[4] \Rightarrow 7^k \equiv 1[10]$$
$$k \equiv 1[4] \Rightarrow 7^k \equiv 7[10]$$
$$k \equiv 2[4] \Rightarrow 7^k \equiv 9[10]$$
$$k \equiv 3[4] \Rightarrow 7^k \equiv 3[10]$$

Posons alors $K = 7 \uparrow\uparrow 5$ qui est clairement impair et donc d'après $(*)$: $K \equiv 1[2] \Rightarrow 7^K \equiv 3[4]$

On pose ainsi $K' = 7^K = 7 \uparrow\uparrow 6$, on a $K' \equiv 3[4]$ donc d'après $(**)$: $7 \uparrow\uparrow 7 = 7^{K'} \equiv 3[10]$.

D'où finalement :

$$\boxed{N \equiv 3[10]}$$

Le dernier chiffre de $7 \uparrow\uparrow 7$ est donc 3.

Remarque : On pourrait prolonger indéfiniment la tour de 7, le chiffre des unités resterait 3 à chaque itération.

Exercice 2 : Diviseurs d'un entier

<u>Énoncé</u> :

Soit n un entier naturel non nul, N le nombre de diviseurs de n et P le produit de ces diviseurs. Donner une relation entre n, N et P.

La décomposition en facteurs premiers de n s'écrit :

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

Un diviseur positif de n s'écrit $p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$.

Le produit des diviseurs s'écrit donc $p_1^{\gamma_1} \cdots p_k^{\gamma_k}$. Calculons les γ_i :

On fixe $a \in \{0, 1, ..., \alpha_1\}$ ainsi il y a $(\alpha_2 + 1) \cdots (\alpha_k + 1)$ diviseurs de n pour lesquels $\beta_1 = a$.

En multipliant tous ces diviseurs on a donc :

$$\gamma_1 = (\alpha_2 + 1) \cdots (\alpha_k + 1) \sum_{a=0}^{\alpha_1} a = \frac{1}{2}\alpha_1(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = \alpha_1 \frac{N}{2}$$

Par symétrie des rôles on a plus généralement :

$$\gamma_k = \alpha_k \frac{N}{2}$$

D'où :

$$P = p_1^{\alpha_1 \frac{N}{2}} \cdots p_k^{\alpha_k \frac{N}{2}} = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})^{\frac{N}{2}} = n^{\frac{N}{2}}$$

On obtient la relation simple :

$$\boxed{P^2 = n^N}$$

Exercice 3 : Sous-groupes distingués

<u>Énoncé</u> :

On suppose connu le théorème de Lagrange.Soit $(G, .)$ un groupe fini, H un sous-groupe de G.

Soit p le plus petit diviseur premier de $\text{Card}(G)$. On suppose que $\frac{\text{Card}(G)}{\text{Card}(H)} = p$.

1) Soit $\mathcal{R}$ la relation définie sur G par :

$$x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$$

• $\mathcal{R}$ est réflexive

Soit $x \in G$ on a $x^{-1}.x = e \in H$ car H sous-groupe de G donc $x\mathcal{R}x$.

• $\mathcal{R}$ est symétrique

Soit $(x, y) \in G^2$, si $x\mathcal{R}y$ alors $x^{-1}y \in H$.

Ainsi $y^{-1}x = (x^{-1}y)^{-1} \in H$ car H est un groupe, donc $y\mathcal{R}x$.

• $\mathcal{R}$ est transitive

Soit $(x, y, z) \in G^3$ on a : $x\mathcal{R}y$ et $y\mathcal{R}z$ donc $x^{-1}y \in H$ et $y^{-1}z \in H$.

Puisque H est un groupe : $(x^{-1}y).(y^{-1}z) \in H$ et par associativité $x.z^{-1} \in H$ donc $x\mathcal{R}z$

On a donc montré que $\mathcal{R}$ est une relation d'équivalence.

On note $X = G/\mathcal{R}$ et soit $x \in G$ on note

$$\begin{array}{rcl} \overline{x} & = & \{y \in G, x\mathcal{R}y\} \\ & = & \{y \in G, x^{-1}y \in H\} \\ & = & \{y \in G, x^{-1}y = h, h \in H\} \\ & = & \{xh, h \in H\} \end{array}$$

On définit également l'application suivante :

$$\begin{array}{rccc} \delta : & H & \to & \overline{x} \\ & h & \mapsto & xh \end{array}$$

L'application δ est une translation donc est bijective.

Par conséquent H et $\overline{x}$ sont équipotents et donc $\text{Card}(H) = \text{Card}(\overline{x})$.

De surcroit on a l'union disjointe :

$$G = \bigcup_{\overline{x} \in X} \overline{x}$$

On en déduit :

$$\text{Card}(G) = \sum_{\overline{x} \in X} \text{Card}(\overline{x}) = \sum_{\overline{x} \in X} \text{Card}(H) = \text{Card}(X) \times \text{Card}(H)$$

Finalement :

$$\boxed{\text{Card}(X) = \frac{\text{Card}(G)}{\text{Card}(H)} = p}$$

2) Soit $g \in G$ on définit l'application :

$$\begin{array}{rccc} \varphi_g : & X & \to & X \\ & \overline{x} & \mapsto & \overline{gx} \end{array}$$

a) Soit $\overline{x} \in X$ on a $\forall (a, b) \in G^2$:

$$\varphi_a \circ \varphi_b(\overline{x}) = \varphi_a(\varphi_b(\overline{x})) = \varphi_a(\overline{bx}) = \overline{a(bx)} = \overline{(ab)x} = \varphi_{ab}(\overline{x})$$

b) Pour montrer que φ est un morphisme de groupe de $(G, .)$ dans $(Bij(X), \circ)$ d'après ce qui précède il reste à montrer que φ est une permutation de X (donc une bijection). Puisque l'ensemble de définition et d'arrivée de l'application est le même on a même cardinal et donc il suffit de prouver l'injectivité.

Supposons que :

$$\varphi_g(\overline{x}) = \varphi_g(\overline{y}) \Leftrightarrow \overline{gx} = \overline{gy}$$

On a donc $gy \in \overline{gx}$ soit :

$$(gx)\mathcal{R}(gy) \Leftrightarrow (gx)^{-1}(gy) \in H \Leftrightarrow x^{-1}(g^{-1}g)y \in H \Leftrightarrow x^{-1}y \in H \Leftrightarrow x\mathcal{R}y$$

Et donc $\overline{x} = \overline{y}$ d'où φ injective.

Remarque : Puisque l'on a procédé par équivalence, on a montré au passage que l'application est bien définie.

c) Par transport de structure on a $Im(\varphi)$ qui est un sous-groupe de $(Bij(X), \circ)$ (on montre sans difficulté que cet ensemble muni de la loi de composition est un groupe de cardinal $p!$).

Or d'après le théorème de Lagrange l'ordre de tout sous groupe divise l'ordre du groupe donc :

$$\boxed{\text{Card}(Im\varphi)|p!}$$

d) Soit $g \in Ker\varphi$ alors $\varphi_g = Id_X$ donc $\forall \overline{x} \in X, \varphi_g(\overline{x}) = \overline{x} \Leftrightarrow \overline{gx} = \overline{x}$ d'où :

$$x \in \overline{gx} \Rightarrow (gx)^{-1}x \in H \Rightarrow x^{-1}g^{-1}x \in H$$

Puisque c'est valable pour tout x alors en particulier pour $x = e$ on obtient $g^{-1} \in H \Rightarrow g \in H$ car H est un groupe.

On a montré que :

$$\boxed{Ker(\varphi) \in H}$$

3) Considérons la relation $\mathcal{R}'$ définie sur G par

$$x\mathcal{R}'y \Leftrightarrow x^{-1}y \in Ker(\varphi) \Leftrightarrow y = xKer(\varphi) \text{ avec } xKer(\varphi) = \{xk, k \in Ker(\varphi)\}$$

On a alors $\overline{x} = xKer(\varphi)$ et $G/\mathcal{R}' = \{xKer(\varphi), x \in G\}$.

Pour tout $x \in G$ l'application translation $x \mapsto xy$ est une bijection de $Ker(\varphi)$ dans $Ker(\varphi)$.

Donc $Card(xKer(\varphi)) = Card(Ker(\varphi))$. Par ailleurs $G/\mathcal{R}'$ est une partition de G donc :

$$Card(G) = \sum_{a \in G/\mathcal{R}'} Card(a) = \sum_{a \in G/\mathcal{R}'} Card(Ker(\varphi)) = Card(G/\mathcal{R}').Card(Ker(\varphi))$$

Par morphisme de φ on a :

$$\varphi(x) = \varphi(y) \Leftrightarrow \varphi(x^{-1}y) = Id_X \Leftrightarrow x^{-1}y \in Ker(\varphi) \Leftrightarrow x\mathcal{R}'y$$

D'après le théorème de la décomposition canonique d'une application, appliqué à φ on a une bijection entre $G/\mathcal{R}'$ et $Im(\varphi)$ donc $Card(G/\mathcal{R}') = Card(Im(\varphi))$.

D'où finalement :

$$\boxed{Card(G) = Card(Im\varphi).Card(Ker\varphi)}$$

4) $Card(Im\varphi)$ divise $p!$ donc $Card(Im\varphi) = \prod_i a_i$ avec $1 \leq a_i \leq p$.

Puisque $Card(G) = Card(Ker\varphi).Card(Im\varphi)$ les a_i divisent $Card(G)$.

Or p étant le plus petit diviseur premier de $Card(G)$ on a à fortiori un i_0 tel que $a_{i_0} = p$

et les autres égaux à 1 sinon un des a_i diviserait $Card(G)$ en étant plus petit que p, absurde.

D'où $Card(Im\varphi) = p$ puis comme $Card(G) = p.Card(H)$ on en déduit $Card(H) = Card(Ker\varphi)$.

Par ailleurs $Ker\varphi \subset H$ donc $H = Ker\varphi$ qui est un sous-groupe distingué comme tout noyau de morphisme.

Donc on a bien :

$$\boxed{\forall x \in G, x^{-1}Hx = H}$$

Exercice 4 : Analogie entre espace vectoriel et groupe

Énoncé :

Soit $(G, .)$ un groupe abélien.

On suppose qu'il existe un entier naturel non nul n tel que $x^n = e$ pour tout x de G.

1) On suppose que $n = ab$ avec $a \wedge b = 1$. On pose $G_a = \{x^a, x \in G\}$.

G_a est non vide car G est non vide (c'est un groupe).

Soit $(x_1, x_2) \in G_a^2$ il existe $(y_1, y_2) \in G^2$ tel que $x_1 = y_1^a$ et $x_2 = y_2^a$.

Et ainsi $x_1.x_2 = y_1^a.y_2^a = (y_1.y_2)^a$ par commutativité.

Or puisque $(G, .)$ est un groupe $y_1.y_2 \in G$ et par suite :

$$\boxed{x_1.x_2 \in G_a}$$

De plus soit $x \in G_a$ il existe $y \in G$ tel que $x = y^a$.

Par la structure de groupe y est inversible d'inverse y^{-1}.

Posons $x^{-1} = (y^{-1})^a \in G_a$ et alors :

$$\boxed{x.x^{-1} = y^a.(y^{-1})^a = (y.y^{-1})^a = e^a = e}$$

Donc x est inversible dans G_a.

Il vient que $(G_a, .)$ est un sous-groupe de $(G, .)$.

On définit de même $G_b = \{x^b, x \in G\}$, montrons que $\forall x \in G, \exists!(u,v) \in G_a \times G_b, x = uv$.

Puisque $a \wedge b = 1$ d'après Bézout $\exists(u_1, v_1) \in \mathbb{Z}^2, au_1 + bv_1 = 1$ et ainsi :

$$x = x^1 = x^{au_1+bv_1} = \underbrace{(x^{u_1})^a}_{u}.\underbrace{(x^{v_1})^b}_{v}$$

On pose alors $x_1 = x^{u_1} \in G$ et $y_1 = x^{v_1} \in G$ par stabilité de la loi ., ce qui prouve l'existence.

On suppose qu'il existe également $(x_2, y_2) \in G^2$ tel que $x = x_2^a.y_2^b$.

On peut écrire $x_1^a.y_1^b = x_2^a.y_2^b$ que l'on élève à la puissance a :

$$x_1^{a^2}.y_1^n = x_2^{a^2}.y_2^n$$

Or comme $\forall x \in G, x^n = e$ on a :

$$x_1^{a^2} = x_2^{a^2} \Leftrightarrow (x_1.x_2^{-1})^{a^2} = e$$

Notons d l'ordre de l'élément $x_1.x_2^{-1}$ alors deux choses l'une :

$$d|ab \text{ et } d|a^2$$

En reprenant l'identité de Bézout on a :

$$au_1 + bv_1 = 1 \Rightarrow a^2u_1 + abv_1 = a$$

Puisque $d|ab$ et $d|a^2$ alors $d|a$ donc il existe $d_1 \in \mathbb{Z}$ tel que $a = dd_1$.

Et on a par définition de d :

$$(x_1.x_2^{-1})^d = e \Rightarrow (x_1.x_2^{-1})^{dd_1} = e^{d_1} \Rightarrow (x_1.x_2^{-1})^a = e$$

On en déduit :

$$\boxed{x_1^a = x_2^a}$$

Par symétrie des rôles on détermine de même :

$$\boxed{y_1^b = y_2^b}$$

Ce qui prouve l'unicité.

2) Soit $k \in \mathbb{N}^*$ tel que $k \wedge n = 1$. Montrons que l'application $f : x \mapsto x^k$ est un automorphisme de G.

Soit $(x, y) \in G^2$ on a par commutativité :

$$\boxed{f(x.y) = (x.y)^k = x^k.y^k = f(x).f(y)}$$

Donc f est un endomorphisme de G.

Par ailleurs f est clairement surjective, montrons qu'elle est injective :

$$f(x) = f(y) \Leftrightarrow x^k = y^k \Leftrightarrow (x.y^{-1})^k = e = (x.y^{-1})^n$$

D'après le théorème de Lagrange soit $k|n$ soit $n|k$, ces deux cas étant exclus puisque $k \wedge n = 1$.

Donc il vient :

$$\boxed{x.y^{-1} = e \Leftrightarrow x = y}$$

f est injective et par suite bijective de G dans G.

Ces deux points montrent que l'application f est un automorphisme de G.

Exercice 5 : Résoudre des congruences linéaires

Énoncé :

1) Résoudre les équations d'inconnue x dans $\mathbb{Z}$:

$$\begin{array}{ll} a) & 10.x \equiv 15[15] \\ b) & 10.x \equiv 14[18] \end{array}$$

2) Plus généralement si a et b sont des entiers relatifs et m un entier naturel non nul, comment résoudre l'équation d'inconnue x :

$$a.x \equiv b[m]$$

1)a. L'équation $10.x \equiv 14[15]$ n'admet pas de solutions car $10.x$ et 15 sont divisibles par 5 mais pas 14.

b. On cherche des entiers x tels qu'il existe $k \in \mathbb{Z}$ vérifiant $10x = 14 + 15k \Leftrightarrow 5x - 9k = 7$.

Les entiers 5 et 9 sont premiers entre eux, et par l'algorithme d'Euclide on a : $2 \times 5 - 9 = 1$.

Cherchons alors tous les couples vérifiant :

$$5u + 9v = 1 \Leftrightarrow 5u + 9v = 5 \times 2 + 9 \times (-1) \Leftrightarrow 5(u - 2) = 9(-1 - v)$$

Ainsi $5|9(-1-v)$ et $5 \wedge 9 = 1$ donc $5|(-1-v)$ donc $\exists k' \in \mathbb{Z}$ tel que $v = -1-5k'$.

De même $9|5(u-2)$ et $5 \wedge 9 = 1$ donc $9|(u-2)$ donc $u = 2+9k'$.

On a donc :

$$(2+9k') \times 5 - (1+5k') \times 9 = 1$$

Multiplions cette dernière égalité par 7 :

$$(14+63k') \times 5 - (7+35k') \times 9 = 7$$

Puis encore par 2 :

$$(14+63k') \times 10 - (7+35k') \times 18 = 14$$

On a $63 = 3 \times 18 + 9$ donc modulo 18 :

• $k' = 0$ et alors $x = 14$ convient.
• $k' = 1$ et $x = 14+9 = 23 = 5$ convient.
• $k' = 2$ et $x = 14+18 = 14$ déjà pris.

On en déduit que les seules solutions sont :

$$\boxed{\begin{array}{l} x \equiv 5[18] \\ x \equiv 14[18] \end{array}}$$

2) Montrons que l'équation $ax \equiv b[m]$ admet des solutions si et seulement si $pgcd(a,m)|b$.

• Notons $d = pgcd(a,m)$ ainsi $a = da'$ et $m = dm'$;

$$ax \equiv b[m] \Leftrightarrow \exists k \in \mathbb{Z}, ax - mk = b \Leftrightarrow d(a'x - m'k) = b$$

Donc la condition $d|b$ est nécessaire.

• Supposons alors $d|b$, d'après l'algorithme d'Euclide étendu il existe $(u,v) \in \mathbb{Z}^2$ tel que :

$$au + mv = d$$

Puisque $d|b$ il existe $\alpha \in \mathbb{Z}$ tel que $b = d\alpha$ d'où :

$$(\alpha u)a + (\alpha v)m = b$$

Et donc $x_0 = \alpha u = \frac{bu}{d}$ est solution.

Donc la condition $d|b$ est suffisante.

L'ensemble des solutions est $\{x_0 + k\frac{n}{d}, k \in \mathbb{Z}\}$.

Exercice 6 : Liberté d'une famille

Énoncé :

Soit n un entier naturel non nul ; pour tout $k \in [0, n]$, $f_k : \mathbb{R} \to \mathbb{R}$ est définie par :

$$f_k(x) = \cos^k(x). \sin^{n-k}(x)$$

Étudions la liberté de la famille $(f_k)_{0 \leq k \leq n}$.

Soit $(\lambda_0, ...\lambda_n)$ des scalaires tels que :

$$\lambda_0 \sin^n(x) + \lambda_1 \cos(x) \sin^{n-1}(x) + \cdots + \lambda_{n-1} \cos^{n-1}(x) \sin(x) + \lambda_n \cos^n(x) = 0$$

Évaluons cette expression en $x = 0$, les sinus s'annulent et il reste :

$$\lambda_n \cos^n(0) = 0 \Rightarrow \lambda_n = 0$$

Évaluons désormais en $x = \frac{\pi}{2}$, les cosinus s'annulent et il reste :

$$\lambda_0 \sin^n(\frac{\pi}{2}) = 0 \Rightarrow \lambda_0 = 0$$

On a donc à ce stade :

$$\lambda_1 \cos(x) \sin^{n-1}(x) + \cdots + \lambda_{n-1} \cos^{n-1}(x) \sin(x) = 0$$

On factorise par $\sin(x)$ et on évalue de nouveau en $x = 0$ on en tire $\lambda_{n-1} = 0$.

De même en factorisant par $\cos(x)$ et en évaluant en $x = \frac{\pi}{2}$ il vient $\lambda_2 = 0$.

De proche en proche tous les coefficients s'annulent par cette méthode :

$$\boxed{\forall k \in [0, n], \lambda_k = 0}$$

On en conclut que la famille $(f_k)_{0 \leq k \leq n}$ est libre.