DS 3 : *Arithmétiques. Groupes cycliques. Suites numériques.*

MPSI-Maths.
Mr Mamouni & El Hassani : *myismail1@menara.ma*

Lundi 10 Décembre 2007.

Durée: 3 heures 30mn.

بِسمِ اللَّهِ الرَّحمَنِ الرَّحِيمِ
وَ قُلِ إِعمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُم وَ رَسوُلُهُ وَ المُؤ مِنُون

صَدَقَ اللَّهُ العَظِيم

Conseils pour la rédaction et la présentation des copies. (4 points)

- **Chaque variable utilisée dans une démonstration doit être définie.**
- **L'énoncé ne doit pas être recopié sur les copies.**
- **Chaque résutat annoncé doit être justifié en citant précisément le théorème du cours avec ses hypothèses exactes utilisé ou en citant le numéro de la question précèdente utilisée.**
- **Les résultats importants doivent être simplifiés et encadrés.**
- **Les calculs doivent être détaillés et expliqués à l'aide de phrases simples.**
- **Laisser une marge à gauche de chaque feuille, en tirant un trait vertical, et un horizontal de la 1ère double feuille pour la note et les remarques du correcteur.**
- **Numéroter les double feuille de la façon suivante : 1/n,2/n,...,n/n où n est le nombre total de double feuille.**
- **Les questions doivent être traités dans l'ordre de l'énoncé.**
- **Tirer deux traits diagonaux pour rayer une partie du raisonnement que vous considérez fausse.**

Problème 1. (Fonction indicatrice d'Euler.)

Pour tout $n \in \mathbb{N}^*$, on pose

$$\varphi(n) = \textbf{card}\{k \in [|1,n|] \textbf{ tel que } k \wedge n = 1\}$$

1) **Montrer que n est premier $\iff \varphi(n) = 1$.**
2) **Montrer que dans $\mathbb{Z}/n\mathbb{Z}$, on a :**
   $\overline{k}$ est inversible $\iff k \wedge n = 1$
3) **En déduire que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps $\iff n$ est premier.**
4) **On notera $U(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$, que vaut card$U(\mathbb{Z}/n\mathbb{Z})$**
5) **Soit $(m,n) \in \mathbb{N}^*$ tel que $n \wedge m = 1$.**
   a) **Montrer que l'application**
   $$\begin{array}{rccc} \theta: & ((\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}), \times) & \longrightarrow & (\mathbb{Z}/nm\mathbb{Z}, \times) \\ & (\overline{x}, \overline{y}) & \longmapsto & \overline{xy} \end{array}$$
   est un isomorphisme.
   b) **Montrer que :**
   $\overline{x}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{y}$ inversible dans $\mathbb{Z}/m\mathbb{Z}$
   $\iff$ $(\overline{x}, \overline{y})$ inversible dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$
   $\iff$ $\overline{xy}$ inversible dans $\mathbb{Z}/nm\mathbb{Z}$
   c) **Conclure que**
   $$\varphi(nm) = \varphi(n)\varphi(m)$$
6) **Montrer que si $(n_i)_{1 \le i \le r}$ sont des entiers naturels premiers entre eux deux à deux, alors**
   $$\varphi\left(\prod_{i=1}^{r} n_i\right) = \prod_{i=1}^{r} \varphi(n_i)$$
7) **Soit p premier, $\alpha \in \mathbb{N}^*$, montrer que**
   $$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$
8) ***Application :***
   a) **Determiner les entiers naturels $n \ge 2$ tel que $\varphi(n)$ divise n.**
   Indication **: Ecrire n sous la forme $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec p_i premier et $\alpha_i \in \mathbb{N}^*$.**
   b) **Soit d un diviseur de n, parmi les fractions $\frac{k}{n}$, tel que $1 \le k \le n$, combien peut-on mettre sous la forme $\frac{a}{d}$, avec $a \wedge d = 1$. En déduire que**
   $$\sum_{d \textbf{ divise } n} \varphi(d) = n$$

Problème 2. (Groupes cycliques)

Dans tout le problème, G est un groupe de cardinal n, d'élément neutre e, cyclique engendré par a. On notera par $\mathcal{D}_n$ l'ensemble des diviseurs de n dans $\mathbb{N}$ et par $\mathcal{H}$ celui des sous groupes de G. on pose $\varphi(n) = \textbf{card}\{k \in [|1,n|] \textbf{ tel que } k \wedge n = 1\}$.

1) **Montrer que $(G, .)$ est abelien.**
2) **Montrer que si q divise p, alors $\langle a^p \rangle \subset \langle a^q \rangle$.**
3) a) **Montrer que $o(a^k) = \frac{n}{n \wedge k}$**
   b) **En déduire que $G =< a^k > \iff k \wedge n = 1$.**
   c) **Combien G a-t-il de générateurs exactement ?**
4) **On pose $\mathbb{U}_n = \{z \in \mathbb{C} \text{ tel que } z^n = 1\}$. Montrer que $\mathbb{U}_n$ est sous-groupe de $(\mathbb{C}^*, \times)$, cyclique. Ses générateurs s'appellent racines $n^{\text{ème}}$ primitives de l'unité.**
   Combien y'en a t-il exactement.
   Donner ceux de $\mathbb{U}_3$ et $\mathbb{U}_4$.
5) **Pour tout $d \in \mathcal{D}_n$, on pose $H_d = \{x \in G \text{ tel que } x^d = e\}$.**
   a) **Montrer que H_d est un sous-groupe de G, puis que**
   $$H_d = \left\langle a^{\frac{n}{d}} \right\rangle$$

b) **Inversement, soit H un sous groupe de $(G,.)$.**

i. **Montrer que $\exists p \in \mathbb{N}$ tel que $H =< a^p >$.**
Indication **: On pourra utiliser l'application :**
$f : \begin{array}{ccc} (\mathbb{Z},+) & \longrightarrow & (G,.) \\ m & \longmapsto & a^m \end{array}$.

ii. **Montrer que $\langle a^p \rangle = \langle a^{p \wedge n} \rangle$.**

6) **En déduire que l'application :** $\Phi : \begin{array}{ccc} \mathcal{D}_n & \longrightarrow & \mathcal{H} \\ d & \longmapsto & H_d \end{array}$ **est bijective.**

7) **Combien y-a-t exactement de sous groupes dans G, si $n = p^\alpha$, où p est un nombre premier.**

Exercice. (Groupe symétrique.)

Soit $(n,p) \in \mathbb{N}^*$ tel que $p \leq n$ et $\sigma = (i_1, \ldots, i_p)$ un p-cycle.

1) **Montrer que :** $\forall\, \alpha \in \mathcal{S}_n, \quad \alpha\sigma\alpha^{-1} = (\alpha(i_1), \ldots, \alpha(i_p))$.

2) **En déduire : (1 3 2)(1 2 3 4)(1 2 3).**

3) **Calculer (1 2 3 4)^k, pour $k = 2, k = 3$.**

Problème 3. (Étude d'une suite récurrente)

.

.