Université Paris Diderot
M1 Arithmétique
2010-2011

Feuille d'exercices II

Exercice 1 Soient $a_1, \dots, a_n$ des entiers. Le but de cet exercice est de montrer qu'il existe deux indices k et l dans $\{0, \dots, n\}$, $k < l$, tels que $a_{k+1} + \cdots + a_l$ soit divisible par n.

1) Pour tout $i \in \{0, \dots, n\}$, soit
$$b_i = \sum_{1 \leqslant j \leqslant i} a_j.$$
Montrer qu'il existe deux nombres b_k et b_l $(k < l)$ dont les images dans $\mathbb{Z}/n\mathbb{Z}$ coïncident.
2) Conclure.

Exercice 2 On désigne par $\mathbb{P}(n)$ l'énoncé suivant : pour toute famille $(a_i)_{i=1}^{2n-1}$ de $2n-1$ entiers $(n \geqslant 1)$, il existe un sous-ensemble I de cardinale n de $\{1, \dots, 2n-1\}$ tel que $\sum_{i \in I} a_i$ soit divisible par n.

1) Soient n et m deux entiers $\geqslant 1$. On suppose vérifée la condition $\mathbb{P}(n)$. Soit $(a_i)_{i=1}^{2mn-1}$ une famille de $2mn-1$ entiers. Montrer qu'il exsite $2m-1$ sous-ensembles deux-à-deux disjoints $I_1, \dots, I_{2m-1}$ de $\{1, \dots, 2mn-1\}$ tels que, pour tout $i \in \{1, \dots, 2m-1\}$, la somme $\sum_{j \in I_i} a_j$ soit divisible par n.
2) En déduire que, pour tous entiers $n, m \geqslant 1$, on a
$$\mathbb{P}(n) \text{ et } \mathbb{P}(m) \Longrightarrow P(nm).$$

Dans la suite, on fixe un nombre premier p.

3) Soit $(a_i)_{i=1}^{2p-1}$ une famille de $2p-1$ entiers. Montrer que le système d'équations (dont $X_1, \dots, X_{2p-1}$ sont des indéterminées)
$$\begin{cases} a_1 X_1^{p-1} + \cdots + a_{2p-1} X_{2p-1}^{p-1} = 0, \\ X_1^{p-1} + \cdots + X_{2p-1}^{p-1} = 0 \end{cases}$$
admet une solution $(x_1, \dots, x_{2p-1})$ qui n'est pas identiquement nulle dans $\mathbb{F}_p^{2p-1}$.
4) Soit I l'ensemble des indices $i \in \{1, \dots, 2p-1\}$ tels que $x_i \neq 0$. Montrer que $\mathrm{card}(I)$ est divisible par p. En déduire que $\mathrm{card}(I) = p$.
5) Montrer que $\sum_{i \in I} a_i$ est divisible par p.
6) En déduire que l'énoncé $\mathbb{P}(n)$ est vrai pour tout entier $n \geqslant 1$.

Exercice 3 On appelle *anneau local* tout anneau commutatif qui admet un et un seul idéal maximal.

1) Soient A un anneau et $\mathfrak{m}$ un idéal de A, $\mathfrak{m} \neq A$. On suppose que tout élément dans $A \setminus \mathfrak{m}$ est inversible. Montrer que A est un anneau local.
2) Soient A un anneau local et $\mathfrak{m}$ l'idéal maximal de A. Montrer que tout élément de $A \setminus \mathfrak{m}$ est inversible.

3) Soient A un anneau et $\mathfrak{m}$ un idéal maximal de A. On suppose que tout élément $x \in \mathfrak{m}$ est nilpotent (i.e., il existe un entier $n \geqslant 1$ tel que $x^n = 0$). Montrer que A est un anneau local.
4) Soit p un nombre premier et $\alpha \geqslant 1$ un entier. Montrer que l'anneau $\mathbb{Z}/p^\alpha\mathbb{Z}$ est local.
5) Déterminer l'idéal maximal de $\mathbb{Z}/p^\alpha\mathbb{Z}$ puis le cardinale de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Exercice 4 Soient p un nombre premier impair et $\alpha \geqslant 1$ un entier.
1) Soit ξ la classe de congruence de $1+p$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. Montrer que ξ est un élément de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
2) Montrer que l'ordre de ξ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est $p^{\alpha-1}$. On peut raisonner par récurrence sur α.
3) Montrer que l'application de projection $\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induit un morphisme de groupes $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ qui est surjectif.
4) En déduire qu'il existe un élément x d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
5) Calculer l'ordre de $x\xi$ puis montrer que le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

Exercice 5 Soit $\alpha \geqslant 3$ un entier.
1) Montrer que le groupe $(\mathbb{Z}/4\mathbb{Z})^\times$ est cyclique.
2) Soit ξ la classe de 5 dans $\mathbb{Z}/2^\alpha\mathbb{Z}$. Montrer que ξ est un élément d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.
3) Montrer que $2^{\alpha-1}+1 \not\equiv -1 \pmod{2^\alpha}$. En déduire que la classe de -1 n'est pas dans le sous-groupe de $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ engendré par ξ.
4) En déduire que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Ce groupe est-il cyclique ?

Exercice 6 Soit K un corps commutatif. On appelle valuation discrète sur K tout morphisme de groupes $v : K^\times \to (\mathbb{Z}, +)$ tel que $v(x+y) \geqslant \min(v(x), v(y))$. Si v est une valuation discrète sur K, on étend v en une application de K vers $\mathbb{Z} \cup \{+\infty\}$ de sorte que $v(0) = +\infty$. On convient que $\mathbb{Z} \cup \{+\infty\}$ est muni d'une relation d'ordre qui prolonge la relation d'ordre usuelle et telle que $n \leqslant +\infty$ pour tout $n \in \mathbb{Z}$. Dans la suite, soit K un corps muni d'une valuation discrète v.
1) Montrer que $\mathcal{O}_{K,v} := \{x \in K \mid v(x) \geqslant 0\}$ est un sous-anneau de K.
2) Montrer que l'anneau $\mathcal{O}_{K,v}$ est local dont l'idéal maximal est $\mathfrak{m}_{K,v} := \{x \in K \mid v(x) > 0\}$.
3) Montrer que l'idéal $\mathfrak{m}_{K,v}$ est principal.
4) Soit ϖ un élément qui engendre $\mathfrak{m}_{K,v}$. Montrer que tout idéal non-nul de $\mathcal{O}_{K,v}$ est engendré par une puissance de ϖ. En déduire que $\mathcal{O}_{K,v}$ est un anneau principal.
5) Soit p un nombre premier. Pour tout entier non-nul n, soit $v_p(n)$ l'exposant de p dans la décomposition euclidienne de n. Montrer que la fonction v_p s'étend de façon unique en une valuation discrète sur $\mathbb{Q}$ (appelée la valuation p-adique).
6) Soit p un nombre premier. Établir la relation

$$v_p(n!) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor \qquad (n \geqslant 1)$$

7) En déduire

$$\frac{n}{p} - 1 < v_p(n!) \leqslant \frac{n}{p} + \frac{n}{p(p-1)}.$$