Université Paul-Cézanne Licence MI, S4 2006/2007

Algèbre et arithmétique – Examen

3 heures, calculatrice et documents interdits.

Question de cours 1 (3 points). Donner la définition d'un idéal et montrer que $\mathbb{Z}$ est un anneau principal.

Question de cours 2 (3 points). Démontrer que les transpositions engendrent S_n.

Exercice 1. Si $a \in \mathbb{Z}$, on notera $\overline{a}$ la classe de a modulo 29.

1) Rappeler le théorème de Wilson.

2) Rappeler pourquoi tout élément non nul de $\left(\mathbb{Z}/29\mathbb{Z}\right)$ est inversible.

3) Déterminer l'inverse de $\overline{2}$ dans le groupe multiplicatif $\left(\mathbb{Z}/29\mathbb{Z}\right)^*$.

4) En utilisant les questions 1), 2) et 3), déterminer le reste de la division euclidienne de 26! par 29.

Exercice 2. Soit p un nombre premier et a un entier positif.

1. Combien y a-t'il de multiples de p parmi $0, 1, \ldots, p^a - 1$.

2. Montrer que l'ordre du groupe multiplicatif $(\mathbb{Z}/p^a\mathbb{Z})^\times$ est $p^{a-1}(p-1)$.

3. Donner tous les éléments de $(\mathbb{Z}/8\mathbb{Z})^\times$ et montrer qu'ils sont tous d'ordre 2.

4. $(\mathbb{Z}/8\mathbb{Z})^\times$ est-il un groupe cyclique ?

5. Montrer que $(\mathbb{Z}/9\mathbb{Z})^\times$ est un groupe cyclique d'ordre 6 et préciser un isomorphisme de groupes entre $(\mathbb{Z}/6\mathbb{Z}, +, \tilde{0})$ et $((\mathbb{Z}/9\mathbb{Z})^\times, \times, \overline{1})$.

Exercice 3. Soit n un entier, S_n le groupe symétrique de degré n et G un sous-groupe de S_n. On appelle P l'ensemble des permutations paires de G et I l'ensemble des permutations impaires de G.

1. Montrer que P est un sous-groupe de G.

2. On suppose dans cette question que $I \neq \emptyset$ et on choisit une permutation impaire α dans I.

a. Montrer que pour toute permutation $\sigma \in P$, les permutations $\alpha \circ \sigma$ et $\sigma \circ \alpha$ sont dans I.

b. Montrer que l'application $\varphi : \begin{array}{ccc} P & \to & I \\ \sigma & \mapsto & \varphi(\sigma) = \sigma \circ \alpha \end{array}$ est injective.

c. Montrer que φ est bijective.

d. Déduire des questions précédentes que G contient autant de permutations paires que de permutations impaires.

e. Exprimer l'ordre de P en fonction de l'ordre de G.

3. On prend $n = 4$, $G = \{id, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$ et $\alpha = (12)$.

a. Déterminer P.

b. Déterminer complètement l'application φ.

c. Déterminer I.

d. Montrer que I n'est pas un sous-groupe de G.

Exercice 4.

Un triplet d'entiers naturels strictement positifs (x, y, z) est appelé **triplet pythagoricien** si c'est une solution de l'équation diophantienne

$$x^2 + y^2 = z^2 \quad (*).$$

On se propose dans cet exercice de donner tous les triplets (x, y, z) pythagoriciens.

On suppose d'abord que $\text{pgcd}(x, y, z) = 1$ (c.-à-d. x, y et z n'ont aucun facteur > 1 en commun).

Un tel triplet est dit **primitif**.

1. Donner un exemple de triplet pythagoricien primitif qui ne contient pas 0.

2. Démontrer que $x \wedge y = y \wedge z = z \wedge x = 1$ (c.-à-d. que x, y et z sont premiers entre eux deux à deux). En déduire que x et y ne sont pas tous les deux pairs.

3. En résolvant l'équation $(*)$ dans $\mathbb{Z}/4\mathbb{Z}$, démontrer que les entiers x et y sont de parités différentes.

On suppose dorénavant que x est impair et y est pair. On en déduit aussitôt que z est impair.

On considère l'entier y' tel que $y = 2y'$.

4. Démontrer que $z + x$ et $z - x$ sont pairs.

On considère donc les entiers naturels m et n tels que $z + x = 2m$ et $z - x = 2n$.

5. Exprimer x et z en fonction de p et q. En déduire que, puisque x et z sont premiers entre-eux, p et q sont premiers entre-eux.

6. Démontrer que $mn = {y'}^2$.

7. Déduire des deux questions précédentes, en utilisant les décompositions en facteurs premiers, que m et n sont des carrés.

On considère donc les nombres entiers naturels u et b tels que $m = u^2$ et $n = b^2$.

8. En exprimant x en fonction de u et b, démontrer que u et b sont de parités différentes.

On suppose donc que u est pair et b est impair.

On considère l'entier naturel a tel que $u = 2a$.

9. En déduire le théorème suivant, déjà connu d'EUCLIDE :

Si (x, y, z) est un triplet pythagoricien primitif tel que y est pair, alors il existe des entiers naturels a et b premiers entre-eux, b impair tels que

$$\left\{ \begin{array}{ccl} x & = & |4a^2 - b^2| \\ y & = & 4ab \\ z & = & 4a^2 + b^2 \end{array} \right.$$

On notera en particulier que y non seulement est pair, mais, de plus, un multiple de 4.

10. Déterminer les 16 triplets pythagoriciens primitifs pour lesquelles $z \leq 100$.

11. La réciproque du théorème ci-dessus est-elle vraie ?

12. Soit (x, y, z) un triplet pythagoricien quelconque. Montrer qu'il existe un entier naturel k et un triplet pythagoricien primitif (x', y', z') tels que $x = kx'$, $y = ky'$ et $z = kz'$.