Préparation à l'agrégation interne de mathématiques - Année 2013-2014
Arithmétique et polynômes (suite) - 2 octobre 2013

Exercice 1. *(L'anneau $\mathbf{Z}$ est « intégralement clos ».)*

On considère un polynôme P unitaire et à coefficients entiers : $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ avec $a_{d-1}, \cdots, a_0$ dans $\mathbf{Z}$.
Démontrer que toute racine de P qui n'est pas entière n'est pas rationnelle.
(Supposer que $\frac{p}{q}$ est une racine rationnelle écrite sous forme irréductible et utiliser le théorème de Gauss.)

Exercice 2. *(Trois démonstrations du petit théorème de Fermat.)*

Le «petit théorème» de Fermat est le suivant : si p est un nombre premier, alors tout entier a non divisible par p vérifie la congruence

$$a^{p-1} \equiv 1 \pmod{p}.$$

1. *Une démonstration directe.*
   Pour tout entier k, $1 \leqslant k \leqslant p-1$, notons r_k le reste de la division euclidienne de ka par p.
   (a) *Justifier que les restes r_k sont non nuls et distincts deux à deux. En déduire l'égalité ensembliste*
   $$\{r_1, \cdots, r_{p-1}\} = \{1, \cdots, p-1\}$$
   (b) *Démontrer le théorème en considérant le produit $\prod_{k=1}^{p-1} ka$ modulo p.*
2. *Une démonstration par récurrence.*
   (a) *Montrer, à l'aide du théorème de Gauss, que p divise le coefficient binomial $\binom{p}{k} = \frac{p!}{(p-k)!k!}$ pour tout entier $1 \leqslant k \leqslant p-1$.*
   (b) *En déduire, pour tout entier a, la congruence*
   $$(1+a)^p \equiv 1 + a^p \pmod{p}.$$
   (c) *Démontrer par récurrence que, pour tout entier a :*
   $$a^p \equiv a \pmod{p}.$$
   (d) *En déduire le théorème.*
3. *Démontrer le petit théorème de Fermat en utilisant le théorème de Lagrange (sur l'ordre d'un sous-groupe d'un groupe fini).*

Exercice 3. *(Deux applications amusantes.) Soit p un nombre premier différent de 2 et 5.*

1. *Démontrer que p divise un entier de la forme $\underbrace{999\cdots99}_{n}$ et décrire les entiers n vérifiant cette propriété.*
2. *Justifier que le développement décimal du nombre rationnel $\frac{1}{p}$ est périodique et préciser la période.*

Exercice 4. *(Factorisation et théorème de Wilson.) Soit p un nombre premier.*

1. *Factoriser le polynôme $X^{p-1} - 1$ dans $\mathbf{Z}/p\mathbf{Z}[X]$.*
2. *En déduire le théorème de Wilson : $(p-1)! \equiv -1 \pmod{p}$.*

Exercice 5. *(Caractérisation des carrés modulo p.)*

Soit p un nombre premier strictement supérieur à 2. On désigne par $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

1. *Vérifier que l'application $x \longmapsto x^2$ définit un morphisme du groupe multiplicatif $\mathbf{F}_p^*$ dans lui-même. Déterminer son noyau puis le nombre d'éléments de $\mathbf{F}_p^*$ qui sont des carrés.*
2. *Soit y un élément de $\mathbf{F}_p^*$. Démontrer l'équivalence suivante*
$$\left[\exists\ x \in \mathbf{F}_p : y = x^2\right] \Longleftrightarrow y^{\frac{p-1}{2}} = 1.$$
3. *Application 1. Justifier que -1 est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv 1 \pmod 4$. Vérifier que, dans ce cas, l'entier $\frac{p-1}{2}!$ est une racine carrée de -1 (utiliser le théorème de Wilson).*
4. *Application 2 : Justifier que le polynôme $3X^2 + 5X + 1$ est irréductible sur $\mathbf{F}_{11}$.*
5. *Application 3 : Décomposer le polynôme $2X^3+5X^2-8X+1$ en produit de facteurs irréductibles dans $\mathbf{F}_{29}[X]$.*

Exercice 6. *(Le groupe multiplicatif de l'anneau $\mathbf{Z}/n\mathbf{Z}$ et la fonction indicatrice d'Euler.)*

On note φ la fonction indicatrice d'Euler : si $n \geqslant 2$ est un entier naturel, $\varphi(n)$ est le nombre d'entiers k vérifiant $1 \leqslant k \leqslant n$ et premiers avec n.

1. *Justifier que $\varphi(n)$ est l'ordre du groupe $(\mathbf{Z}/n\mathbf{Z})^\times$.*
2. *Généraliser le petit théorème de Fermat lorsque p n'est pas premier (théorème d'Euler).*
3. *Soient $m \geqslant 2$ et $n \geqslant 2$ deux entiers premiers entre eux.*
Définir un isomorphisme entre les groupes multiplicatifs $(\mathbf{Z}/mn\mathbf{Z})^\times$ et $(\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times$ puis en déduire l'égalité $\varphi(mn) = \varphi(m)\varphi(n)$.
4. *Déterminer $\varphi\left(p^\alpha\right)$ lorsque p est premier et α est un entier naturel non nul.*
5. *En déduire que si la décomposition de l'entier n en produits de facteurs premiers est $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors $\varphi(n) = n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$.*

Exercice 7. *(Algèbre linéaire et dénombrement.)*

On désigne par p un nombre premier et par $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$. Soit n un entier naturel non nul.

1. *On fixe ici $p = 5$ et $n = 2$. « Dessiner » toutes les droites vectorielles de l'espace vectoriel $\mathbf{F}_5^2$.*
2. *Déterminer le cardinal du groupe linéaire $\mathrm{GL}(n, \mathbf{F}_p)$ (ensemble des matrices inversibles).*
3. *Déterminer le nombre de matrices non inversibles dans $\mathcal{M}(n, \mathbf{F}_p)$.*
4. *Déterminer le cardinal du groupe spécial linéaire $\mathrm{SL}(n, \mathbf{F}_p)$ (ensemble des matrices de déterminant 1).*

Exercice 8. *(PGCD et racines de l'unité.) Soient a et b deux entiers naturels non nuls.*

Déterminer le PGCD des polynômes $X^a - 1$ et $X^b - 1$ (en tant qu'éléments de $\mathbf{C}[X]$).

Exercice 9. *(Utilisation des racines, exemples de factorisation sur $\mathbf{R}$ et $\mathbf{C}$.)*

1. *Sachant que $P = X^4 - 2X^3 - 11X^2 + 12X + 36$ a deux racines multiples, factoriser P sur $\mathbf{R}$.*
2. *Sachant que $P = X^4+2X^3+7X^2+8X+12$ a une racine imaginaire pure, factoriser P sur $\mathbf{C}$.*
3. *Factoriser $P = X^6 + 1$ sur $\mathbf{C}$ puis sur $\mathbf{R}$.*
4. *Démontrer que, pour tout entier $n \geqslant 1$, le polynôme X^2-3X+2 divise dans $\mathbf{R}[X]$ le polynôme $P_n = (X-2)^{2n} + (X-1)^n - 1$.*
5. *Déterminer l'ensemble $\left\{P \in \mathbf{C}[X] : P(X^2) = P(X)P(X+1)\right\}$.*