Préparation à l'agrégation interne de mathématiques - Année 2012-2013
Arithmétique dans **Z** - 10 octobre 2012

1 Divisibilité dans Z

Exercice 1. *En utilisant une combinaison linéaire adéquate, démontrer que :*

1. *Deux entiers consécutifs sont premiers entre eux ;*
2. *Deux entiers impairs consécutifs sont premiers entre eux ;*
3. *Les entiers $3n+5$ et $2n+3$ sont premiers entre eux (n entier).*
4. *Si a et b sont deux entiers tels que a^2-b^2 est pair, alors a^2-b^2 est divisible par 4.*

Exercice 2. *L'ensemble $\{n^2-25 : n \in \mathbf{N}\}$ contient-il des nombres premiers ?*

Exercice 3. **Nombres de Mersenne**

1. *Soient p et q deux entiers naturels non nuls. Démontrer (à l'aide d'une somme de termes d'une suite géométrique) que 2^p-1 divise $2^{pq}-1$.*
2. *En déduire une condition nécessaire simple pour que l'entier $M_n = 2^n-1$ soit premier. Contre-exemple au caractère suffisant ?*

Exercice 4. **Calculs modulo 4.**

1. *Dresser la table de multiplication dans $\mathbf{Z}/4\mathbf{Z}$.*
2. *Montrer que, si un entier est la somme de deux carrés, il est congru à 0, 1 ou 2 modulo 4.*

Exercice 5. **Calculs modulo 5 et modulo 10**

1. *Dresser la table de multiplication dans $\mathbf{Z}/5\mathbf{Z}$.*
2. *Résoudre dans $\mathbf{Z}$ l'équation $x^2+1 \equiv 0 \pmod 5$.*
3. (a) *Déterminer selon l'entier naturel n, le reste de 3^n dans la divion euclidienne par 5.*
   (b) *En déduire selon l'entier naturel n, le reste de 3^n dans la divion euclidienne par 10.*
   (c) *Quel est le chiffre des unités (en notation décimale) du nombre 2013^{2012} ?*

2 Décomposition, $PGCD$, $PPCM$, Euclide, Bézout, Gauss

Exercice 6. **Décomposition et diviseurs**

1. *Décomposer 2600 en produit de facteurs premiers. Combien 2600 admet-il de diviseurs positifs ?*
2. *Déterminer les trois plus petits entiers naturels admettant exactement 35 diviseurs positifs.*
3. *Démontrer qu'un entier non nul est un carré parfait si et seulement s'il admet un nombre impair de diviseurs positifs.*

Exercice 7. **Algorithme d'Euclide**

1. *Appliquer l'algorithme d'Euclide aux nombres 1806 et 714.*
2. *En déduire le $PGCD$, le $PPCM$ ainsi que tous les diviseurs communs*

Exercice 8. **Équation diophantienne linéaire**

1. *Appliquer l'algorithme d'Euclide à $a = 90$ et $b = 77$ et déterminer deux entiers u et v tels que $au + bv = 1$.*
2. *Vérifier qu'il n'y a pas unicité du couple $(u; v)$.*
3. *Résoudre dans $\mathbf{Z}^2$ l'équation $90x + 77y = 1$.*
4. *Résoudre dans $\mathbf{Z}^2$ l'équation $90x + 77y = 5$.*

Exercice 9. **Recherche d'inverse**

Justifier que (la classe de) 53 est inversible dans $\mathbf{Z}/100\mathbf{Z}$ puis déterminer son inverse en utilisant l'algorithme d'Euclide.

Exercice 10. **Codage affine**

On considère un alphabet de n lettres qu'on identifie à l'anneau $\mathbf{Z}/n\mathbf{Z}$.
Pour a et b appartenant à $\mathbf{Z}/n\mathbf{Z}$, on définit la fonction $f : \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z} : x \longmapsto ax + b$.

1. *Quelle(s) condition(s) doivent remplir a et b pour que la fonction f soit bijective ?*
2. *Combien existe-t-il de codages affines différents sur l'alphabet classique (si $n = 26$) ?*

3 Primalité, Fermat, Wilson

Exercice 11. **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).*
4. *Généraliser le petit théorème de Fermat lorsque p n'est pas premier (théorème d'Euler).*

Exercice 12. **Le théorème de Wilson**

. . . est le suivant : si p est un nombre premier, alors

$$(p-1)! \equiv -1 \pmod{p}.$$

1. *Démontrer que pour tout entier $1 \leqslant x \leqslant p-1$, il existe un unique entier y dans $[1; p-1]$ tel que $xy \equiv 1 \pmod{p}$. Que représente y pour x dans $\mathbf{Z}/p\mathbf{Z}$?*
2. *Résoudre $x^2 \equiv 1 \pmod{p}$. Que représentent les solutions dans $\mathbf{Z}/p\mathbf{Z}$?*
3. *Démontrer le théorème de Wilson.*

4 Équations de degré 2 dans $\mathbf{Z}/p\mathbf{Z}$

La résolution d'un équation polynomiale du second degré nécessite de savoir calculer l'inverse du coefficient dominant et de déterminer, si elle existe, une « racine carrée » du discriminant. Ce dernier point peut servir de motivation pour l'étude des carrés du corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

On suppose dans toute la suite que p est un nombre premier strictement supérieur à 2.

Exercice 13. **Caractérisation des carrés dans $\mathbf{F}_p$ si $p > 2$**

On note $\mathcal{C}_p$ l'ensemble des éléments de $\mathbf{F}_p$ qui sont des carrés et $\mathcal{C}_p^*$ l'ensemble des éléments non nuls de $\mathcal{C}_p$:

$$\mathcal{C}_p = \left\{x^2 : x \in \mathbf{F}_p\right\} \quad \text{et} \quad \mathcal{C}_p^* = \left\{x^2 : x \in \mathbf{F}_p, x \neq 0\right\} = \mathcal{C}_p \cap \mathbf{F}_p^*$$

Le but de l'exercice est de démontrer la caractérisation suivante. Pour tout x dans $\mathbf{F}_p$:

$$x \in \mathcal{C}_p^* \Longleftrightarrow x^{\frac{p-1}{2}} = 1. \tag{1}$$

1. *Justifier l'implication $\Rightarrow$ et majorer le cardinal de l'ensemble $\mathcal{C}_p^*$.*
   Indication : utiliser Fermat et un polynôme.
2. *Justifier que l'ensemble $\mathcal{C}_p^*$ contient exactement $\frac{p-1}{2}$ éléments.*
   Indication : utiliser l'application $\mathbf{F}_p \longrightarrow \mathcal{C}_p : x \longmapsto x^2$.
3. *Conclure.*

Exercice 14. **Le cas de -1 : recherche d'une racine carrée**

1. *En utilisant le résultat de l'exercice précédent, justifier que -1 est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv 1 \pmod{4}$.*
2. *On suppose ici que $p \equiv 1 \pmod{4}$.*
   En utilisant le théorème de Wilson, justifier que l'entier $x = \left(\frac{p-1}{2}\right)!$ vérifie $x^2 \equiv -1 \pmod{p}$.

Exercice 15. **Résolution manuelle d'une équation de degré 2**

On considère le polynôme $P = 3X^2 + 4X - 1$ (les coefficients appartiennent à $\mathbf{Z}$ ou $\mathbf{Z}/p\mathbf{Z}$) dont on cherche les racines dans le corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

1. *On suppose ici $p = 17$. Déterminer les racines de P.*
2. *On suppose ici $p = 19$. Déterminer les racines de P.*

Préparation à l'agrégation interne de mathématiques - Année 2012-2013
Arithmétique dans Z - Annexe - Résumé de résultats

Je renvoie aux livres [Mon06] et [WAC+02] pour plus de détails et de démonstrations.

1 Divisibilité dans Z, congruences

Proposition 1.1.

1. *Un sous-ensemble non-vide de* $\mathbf{N}$ *possède un plus petit élément.*
2. *Un sous-ensemble non-vide et minoré de* $\mathbf{Z}$ *possède un plus petit élément.*
3. *Quels que soient l'entier naturel* b *non nul et l'entier naturel* a*, il existe un entier naturel* n *tel que* $a < nb$*. (*$\mathbf{N}$ *est* archimédien*).*

Une liste de définitions/vocabulaires :

1. Un entier b divise un entier a (on note $b|a$) s'il existe un nombre entier k tel que $a = b \times k$.
2. L'ensemble $\mathcal{D}_a$ des diviseurs positifs d'un entier a est non vide (et fini si a est non nul).
3. L'entier a est *premier* si $\mathcal{D}_a$ contient exactement deux éléments (qui sont alors 1 et $|a|$).
4. L'ensemble des multiples de a est $a\mathbf{Z}$.
5. La notion de diviseur commun, de multiple commun à deux (ou plus) nombres est naturelle.
6. Deux entiers a et b (ou plus...) sont *premiers entre eux* si $\mathcal{D}_a \cap \mathcal{D}_b = \{1\}$.

Propriété 1.1. *Si* c *divise* a *et* b*, alors* c *divise toutes les combinaisons linéaires* $\alpha a + \beta b$ *avec* α *et* β *entiers relatifs.*

Propriété 1.2 (Sur l'existence des nombres premiers).

1. *Tout nombre entier naturel* $n \geqslant 2$ *admet pour diviseur un nombre premier.*
2. *Tout nombre entier naturel* $n \geqslant 2$ *non premier admet un diviseur premier* p *vérifiant* $p^2 \leqslant n$*.*
3. *L'ensemble des nombres premiers est infini.*

Théorème 1 (Division euclidienne). *Soient* a *et* b *deux entiers avec* $b \neq 0$*.*
Il existe un unique couple $(q; r)$ *(quotient ; reste) d'entiers vérifiant :*

$$a = bq + r \ \textbf{\textit{et}}\ 0 \leqslant r < |b|.$$

Définition 1.1. *Deux entiers relatifs* a *et* b *sont dits* congrus modulo l'entier n *si* n *divise* $b - a$*. On note* $a \equiv b \pmod{n}$*.*

Remarque 1.1. *Il est équivalent de dire que* a *et* b *ont même reste dans la division euclidienne par* n *(si* $n \neq 0$*).*

Propriété 1.3. *La congruence est compatible avec les opérations usuelles (*$+$ *;* $-$ *;* $\times$ *; exponentiation).*

La congruence modulo n est une relation d'équivalence sur $\mathbf{Z}$ constituée de n classes (si $n > 0$). L'ensemble quotient est (l'anneau) $\mathbf{Z}/n\mathbf{Z} = \left\{\overline{0}; \overline{1}; \ldots; \overline{n-1}\right\}$.

2 Décomposition, $PGCD$, $PPCM$, Euclide, Bézout, Gauss

Théorème 2 (**Décomposition en produit de facteurs premiers**). *Tout entier naturel $n \geqslant 2$ peut s'écrire de façon unique comme un produit :*

$$n = \prod_{i=1}^{i=m} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

où $p_1, p_2, \dots, p_m$ sont des nombres premiers vérifiant $2 \leqslant p_1 < p_2 < \dots < p_m$
et $\alpha_1, \alpha_2, \dots, \alpha_m$ sont des nombres entiers naturels non nuls.

Les deux définitions suivantes ne sont pas les plus habituelles mais ont l'avantage de ne pas nécessiter d'hypothèses de non-nullité sur a et b.

Propriété et définition 2.1 (**Plus Grand Commun Diviseur**). *Soient a et b deux entiers relatifs. Il existe un unique entier naturel $\delta = PGCD(a;b) = PGCD(b;a)$ vérifiant :*

- *δ est un diviseur commun à a et b ;*
- *tout autre diviseur commun à a et b divise δ.*

Si a et b sont non nuls, le nombre $PGCD(a;b)$ est le dernier reste non nul obtenu en appliquant l'algorithme d'Euclide aux entiers a et b.

Propriété et définition 2.2 (**Plus Petit Commun Multiple**). *Soient a et b deux entiers relatifs. Il existe un unique entier naturel $\mu = PPCM(a;b) = PPCM(b;a)$ vérifiant :*

- *μ est un multiple commun à a et b ;*
- *tout autre multiple commun à a et b est un multiple de μ.*

Remarque 2.1. *Le nombre $\mu = PPCM(a;b)$ vérifie $a\mathbf{Z} \cap b\mathbf{Z} = \mu\mathbf{Z}$.*

Théorème 3 (**Bézout**). *Soient a et b deux entiers relatifs.*

1. *il existe des entiers relatifs u et v tels que $au + bv = PGCD(a;b)$.*
2. *(Corollaire) Les entiers a et b sont premiers entre eux si et seulement s'il existe des entiers relatifs u et v tels que $au + bv = 1$.*

Propriété 2.1. *Soient a, b, c, d et k des entiers relatifs.*

1. *Si $a|c$ et $b|d$, alors $PGCD(a;b)|PGCD(c;d)$ et $PPCM(a;b)|PPCM(c;d)$.*
2. *$PGCD(ka;kb) = |k| \times PGCD(a;b)$ et $PPCM(ka;kb) = |k| \times PPCM(a;b)$*
3. *$PGCD(a;b) \times PPCM(a;b) = |ab|$*

Théorème 4 (**Gauss**). *Soient a, b et c trois entiers relatifs.*

1. $\left.\begin{array}{r} a \mid bc \\ PGCD(a;c) = 1 \end{array}\right\} \Longleftrightarrow a \mid b$
2. *Plus généralement : si $PGCD(a;c) = 1$ alors $PGCD(a;bc) = PGCD(a;b)$.*
3. *(Corollaire) Un nombre premier p divise ab si et seulement si p divise a ou p divise b.*

Références

[Mon06] Jean-Marie Monier. Algèbre MPSI, Cours, méthodes et exercices corrigés, 4eédition. J'intègre. Dunod, Paris, 2006.

[WAC+02] André Warusfel, Paul Attali, Michel Collet, Christian Gautier, and Serge Nicolas. Arithmétique. Mathématiques, Cours et exercices TS. Vuibert, Paris, 2002.