Préparation à l'agrégation interne de mathématiques - Année 2013-2014
Arithmétique dans **Z** - 11 septembre 2013

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, *modulo* 5 *et modulo* 10.

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.
3. *Dresser la table de multiplication dans* $\mathbf{Z}/5\mathbf{Z}$.
4. *Résoudre dans* $\mathbf{Z}$ *l'équation* $x^2+1 \equiv 0 \pmod 5$.
5. (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^{2014} *?*

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

Exercice 5. *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 6. *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 positifs de* 1806 *et* 714.

Exercice 7. *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 $90x + 77y = 1$ puis l'équation $90x + 77y = 5$.*

Exercice 8. *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.

3 Application à l'étude des nombres de Fermat

Exercice 9. *Nombres premiers de la forme $a^m + 1$ et nombres de Fermat*

1. *On établit d'abord des conditions nécessaires sur les entiers naturels $a \geqslant 2$ et $m \geqslant 2$ pour que $a^m + 1$ soit premier. On suppose donc ici $a^m + 1$ premier.*
   (a) *Justifier que a est pair.*
   (b) *En utilisant la somme $\displaystyle\sum_{k=0}^{m-1}(-a)^k$, justifier que l'entier m est pair.*
   (c) *Justifier que l'entier m ne possède aucun diviseur premier impair.*
2. *Les nombres de Fermat correspondent aux choix $a = 2$ et $m = 2^n$. On note ainsi $F_n = 2^{2^n} + 1$ où n est un entier naturel.*
   Calculer les entiers F_1, F_2, F_3, F_4 et F_5 et vérifier que F_1, F_2 et F_3 sont premiers.
3. *Justifier que 2 est inversible dans l'anneau $\mathbf{Z}/F_n\mathbf{Z}$ et déterminer son ordre dans le groupe $(\mathbf{Z}/F_n\mathbf{Z})^\times$.*

Exercice 10. *Les nombres de Fermat sont premiers entre eux deux à deux*

1. *Vérifier l'égalité*
$$F_{n+1} + F_n(2 - F_n) = 2$$
   et en déduire que F_n et F_{n+1} sont premiers entre eux.
2. *Vérifier l'égalité*
$$F_{n+1} - 2 = \prod_{k=0}^{n} F_k$$
   et en déduire que deux nombres de Fermat distincts sont premiers entre eux.

Exercice 11. *Diviseurs premiers d'un nombre de Fermat*

1. *On montre que tout diviseur premier éventuel p du nombre de Fermat F_n est de la forme $p = k \times 2^{n+1} + 1$ avec k entier naturel.*
   (a) *En adaptant la dernière question de l'exercice 9, justifier que l'ordre de 2 dans le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est 2^{n+1}.*
   (b) *Justifier que $p - 1$ est un multiple de 2^{n+1} et conclure.*
2. *Application à l'étude de F_4 et F_5.*
   (a) *Dresser une « liste réduite de diviseurs premiers éventuels » de F_4 et vérifier que F_4 est premier.*
   (b) *Vérifier que F_5 n'est pas premier.*