Université Paris 13
L2 Info, cours MathInfo

Partiel du 15 mars 2013

3 heures sans documents. Toute sortie est définitive.

Les 9 exercices sont indépendants.

Exercice 1 (Diviseurs)

1. *Décomposer 2000 en facteur premiers.*
2. *En déduire le nombre de ses diviseurs dans $\mathbb{N}$ puis dans $\mathbb{Z}$.*
3. *Représenter l'ensemble de ses diviseurs dans $\mathbb{N}$, sous la forme d'un diagramme de Hasse pour l'ordre de divisibilité.*

Exercice 2 *Donner l'ensemble des solutions dans $\mathbb{Z}$ des équations suivantes.*

1. $97u + 18v = 1$
2. $1818u + 18v = 1$

Exercice 3

1. *Comparer les polynômes $(X+1)^6$ et X^6+1 dans $\mathbb{Z}/6\mathbb{Z}$.*
2. *Montrer que pour tout entier $n \geq 1$ et tout entier $k, 1 \leq k \leq n$, $k\binom{n}{k} = n\binom{n-1}{k-1}$*
3. *Montrer que si $p \in \mathbb{P}$, alors $\forall k, 1 \leq k \leq p-1$, $\binom{p}{k} \equiv_p 0$*
4. *Montrer que cette propriété est fausse si $p \notin \mathbb{P}$.*
5. *Pour $p \in \mathbb{P}$, Montrer, en utilisant le binôme de Newton, que polynôme $(X+1)^p$ est congru au polynôme X^p+1 modulo p.*
6. *Donner un argument simple pour expliquer pourquoi dans $\mathbb{R}[X]$, $\forall n \in \mathbb{N}, n \geq 2$, même premier, $(X+1)^n \neq X^n+1$.*

Exercice 4 (Etude d'une suite)

On considère la suite (u_n) d'entiers naturels définie par : $u_0 = 1$ et $\forall n \in \mathbb{N}$, $u_{n+1} = 10u_n + 21$

1. *Calculer u_1, u_2 et u_3.*
2. *Démontrer que $\forall n \in \mathbb{N}$, $3u_n = 10^{n+1} - 7$*
3. *En déduire l'écriture en base 10 de u_n, $\forall n \in \mathbb{N}$.*
   On pourra penser à poser $10^{n+1} = (3.3+1)10^n$ pour, en s'appuyant sur 1., en déduire une nouvelle relation entre u_n et u_{n-1}.
4. *En déduire que, $\forall n \in \mathbb{N}$, u_n n'est divisible ni par 2, ni par 3 ni par 5.*

Exercice 5 (reste)

1. *Déterminer, suivant la valeur de l'entier naturel* n*, le reste dans la division euclidienne par 9 de* 33^n
2. *En déduire que* 2013^{2013} *est divisible par* 9

Exercice 6 (résolution d'un système d'équations) *Résoudre le système (*) et donner la plus petite solution positive et la plus grande solution négative.*

$$(*) \begin{cases} (i) & 5x \equiv 15 \quad (85) \\ (ii) & 4x \equiv 16 \quad (11) \end{cases}$$

Exercice 7 (structure) *Dans* $(\mathbb{N}, +, \times)$*, soit* $*$*, l'opération puissance,* $* \left| \begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ (a,b) & \longmapsto & a * b = a^b \end{array} \right.$*, avec la convention* $\forall a \in \mathbb{N}, a * 0 = 1$*,*

1. $*$ *est-elle commutative ?*
2. $*$ *est-elle associative ?*
3. $*$ *est-elle distributive à gauche par rapport à la multiplication ?*
4. $*$ *est-elle distributive à droite par rapport à la multiplication ?*
5. $*$ *est-elle distributive par rapport à la multiplication ?*
6. *possède-t-elle un élément neutre à gauche ?*
7. *possède-t-elle un élément neutre à droite ?*
8. *possède-t-elle un élément neutre ?*
9. *possède-t-elle des éléments réguliers, à droite, à gauche ?*
10. *possède-t-elle des éléments inversibles ?*

Exercice 8 (structure, congruence)

Soit a*,* b *deux entiers relatifs non nuls. On définit dans l'ensemble* $\mathbb{Z}$ *l'opération* $\top$ *par* $x \top y = ax + by$

1. *Montrer que* $\forall n \in \mathbb{N}_*$*, la relation de congruence modulo* n *est compatible avec* $\top$*.*
2. *En déduire que* $\top$ *induit une opération* $\dot{\top}$ *dans* $\mathbb{Z}/n\mathbb{Z}$*.*
3. *Comment faut-il choisir* a, b *pour que dans* $\mathbb{Z}/7\mathbb{Z}$*,* $\dot{\top}$ *soit commutative ?*
4. *Comment faut-il choisir* a, b *pour que dans* $\mathbb{Z}/7\mathbb{Z}$*,* $\dot{\top}$ *soit associative ?*
5. *Comment faut-il choisir* a, b *pour que dans* $\mathbb{Z}/7\mathbb{Z}$*,* $\dot{\top}$ *possède un élément neutre ?*
6. *Comment faut-il choisir* a, b *pour que* $(\mathbb{Z}/7\mathbb{Z}, \dot{\top})$ *soit un monoïde commutatif (ie possède les trois propriétés)*

Exercice 9 (Etude des triplets de pythagore) *Le but du problème est la recherche des triplet pytagoriciens, c'est-à-dire des triplets d'entiers naturels* (a, b, c) *satisfaisant* $a^2 + b^2 = c^2$*.*

1. *Montrer que (3,4,5) est un triplet pytagoricien.*

2. *préliminaires. Soit* $a, b, c \in \mathbb{N}$
   (a) *Montrer que*
   $$\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \\ b \wedge c = 1 \end{cases} \Longrightarrow a \wedge b \wedge c = 1$$
   (b) *Montrer qu'en général*
   $$a \wedge b \wedge c = 1 \not\Longrightarrow \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \\ b \wedge c = 1 \end{cases}$$
   (c) *Montrer que*
   $$\begin{cases} a^2 + b^2 = c^2 \\ a \wedge b \wedge c = 1 \end{cases} \Longrightarrow \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \\ b \wedge c = 1 \end{cases}$$
3. *Etude des solutions évidentes.*
   Etudier les cas où l'un au moins des trois entiers est nul.
4. *On suppose maintenant que* $a, b, c \neq 0$
   (a) *Montrer que l'on peut se ramener à* $a \wedge b \wedge c = 1$
   (b) *Montrer que* $\forall n \in \mathbb{N}, n^2 \equiv_4 0$ *ou* $n^2 \equiv_4 1$.
   (c) *En déduire que* a *ou* b *est pair.*
   (d) *On supposera à partir de maintenant que* $a = 2r$ *et* $a \wedge b \wedge c = 1$
      i. *En déduire la parité de* b *et* c.
      ii. *Montrer que* $r^2 = (\frac{c-b}{2})(\frac{c+b}{2})$
      iii. *Montrer que* $\frac{c-b}{2}$ *et* $\frac{c+b}{2}$ *sont deux nombres entiers et qu'ils sont premiers entre eux.*
      iv. *En déduire que* $\frac{c-b}{2}$ *et* $\frac{c+b}{2}$ *sont deux carrés* α^2 *et* β^2.
      v. *Exprimer* a, b, c *en fonction de* α *et* β.
5. *en déduire une condition nécessaire sur un triplet quelconque (non nécessairement premiers entre eux)* (a, b, c) *pour que l'équation* $a^2 = b^2 + c^2$ *ait une solution.*

Notes de cours :

Dans $\mathbb{Z}$,

• Voici la liste des premiers nombres premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101,

• Théorème fondamental de l'arithmétique : tout nombre entier strictement supérieur à 1 est factorisable de manière unique à une permutation près en un produit de puissance non nulle d'un nombre fini de nombre premiers.

• On note $a \wedge b$ le pgcd de a et b, $a \vee b$ le ppcm de a et b

• Théorème de Gauss : Si $c|ab$ et $c \wedge a = 1$ alors $c|b$.

• Si $a|c$ et$b|c$ et $a \wedge b = 1$ alors $ab|c$.

• Si $d|a$ et$d|b$ alors $d|\lambda a + \mu b$, $\forall \lambda, \mu \in \mathbb{Z}$.

• $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$; $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$

• Théorème de Bezout : $a \wedge b = 1$ si et seulement si $\exists u, v \in \mathbb{Z}, au + bv = 1$

• Les éléments réguliers (et inversibles) de $\mathbb{Z}/n\mathbb{Z}$ sont les $\dot{a}$ tels que $a \wedge n = 1$

• Dans un ensemble E, deux polynômes P et Q sont égaux si et seulement si $P(a) = Q(a), \forall a \in E$

• Une opération $\top$ dans un ensemble E, est
– commutative si $a \top b = b \top a$, $\forall a, b \in E$
– associative si $(a \top b) \top c = a \top (b \top c)$, $\forall a, b, c \in E$
– e est élément neutre à gauche si $e \top a = a$, $\forall a \in E$
– e est élément neutre à droite si $a \top e = a$, $\forall a \in E$
– e est élément neutre s'il est élément neutre à gauche et à droite.
– c est régulier à gauche si $c \top a = c \top b \Longrightarrow a = b$, $\forall a, b \in E$
– c est régulier à droite si $a \top c = b \top c \Longrightarrow a = b$, $\forall a, b \in E$
– c est régulier s'il est régulier à gauche et à droite.
– S'il existe un élément neutre e, c est inversible si $\exists b \in E, b \top c = c \top b = e$
– $\top$ est distributive à gauche pour la loi $\perp$ si $a \top (b \perp c) = (a \top b) \perp (a \top c)$, $\forall a, b, c \in E$
– $\top$ est distributive à droite pour la loi $\perp$ si $(b \perp c) \top c = (b \top a) \perp (c \top a)$, $\forall a, b, c \in E$
– compatible avec une relation d'équivalence $\equiv$ si $x \equiv x'$ et $y \equiv y' \Longrightarrow x \top y \equiv x' \top y'$, $\forall x, y, x', y' \in E$. Dans ce cas, induit une opération $\dot{\top}$ dans $E/\equiv$ définie par $[x]_\equiv \dot{\top} [y]_\equiv = [x \top y]_\equiv$.