**Université Paris 13**
L2 Info, cours MathInfo

---

# Examen du 21 mai 2013
# 3 heures sans documents.

---

Il y a 5 exercices. Les exercices 2 et 3 ne sont pas indépendants.

**Exercice 1 (Diviseurs et indicatrice d'Euler)**

1. *Décomposer 792 en facteurs premiers.*
2. *En déduire le nombre de ses diviseurs dans* $\mathbb{N}$ *puis dans* $\mathbb{Z}$*.*
3. *Représenter l'ensemble de ses diviseurs, ainsi que leur indicatrice d'Euler dans* $\mathbb{N}$*, sous la forme d'un diagramme de Hasse pour l'ordre de divisibilité.*
4. *Quel est le nombre de sous-groupes de* $\mathbb{Z}/792\mathbb{Z}$ *?*

**Exercice 2** *Les équations suivantes ont-elles des solutions entières ? Justifier mathématiquement vos réponses.*

1. $181181u + 181v = 1$
2. $9600u + 181v = 1$

*Calculer l'inverse de* $[181]_{9600}$*. L'exprimer sous la forme* $[r]_{9600}$*, avec* $1 \leq r \leq 9599$*.*

**Exercice 3 (code RSA)** *La résolution de l'exercice 2 aide à la résolution numérique de cet exercice.*

1. *Soit* $n \in \mathbb{N}, n \geq 2$*, donner pour chaque type de fonctions de* $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$*, les conditions sur* $a$ *et/ou* $b$*,* $a, b \in \mathbb{N}$ *pour que* $f$ *soit bijective.*
   (a) *les translations :* $f(x) = x + b$
   (b) *les fonctions affines :* $f(x) = ax + b$
   (c) *les fonctions puissances :* $f(x) = x^a$

2. *Pour utiliser un chiffrement RSA, on utilise les fonctions puissances. Il faut choisir et garder secret deux nombres premiers $p$ et $q$, et déposer dans l'annuaire public RSA une clé de la forme $(p \times q, e)$, satisfaisant $e \wedge (p-1)(q-1) = 1$.*
   (a) *Expliquer pourquoi $e$ doit être un nombre premier avec $(p-1)(q-1)$.*
   (b) *Alice dépose (9797,181). Montrer que c'est une clé RSA et donner sa fonction de décodage.*
3. *Bob veut transmettre une information secrètement par la méthode RSA. Quelle fonction utilise-t-il ? Donner la fonction utilisée par Alice pour retrouver l'information initiale.*
4. *L'information que Bob doit transmettre est représentée par le nombre 9796. Que transmet-il à Alice ?*

**Exercice 4** *Soit $A$ l'alphabet $\{a, b\}$. Soit $(A^*, ., \varepsilon)$ le monoïde non commutatif des séquences finies (ou mots) sur $A$, muni du produit de concaténation. Soit $\phi : A^* \to \mathbb{N}^2$ tel que $\phi(f) = (|f|_a, |f|_b)$, où $|f|_x$ désigne le nombre d'occurrences de la lettre $x$ dans le mot $f$. Par exemple $\phi(abbaa) = (3, 2)$.*

1. *Montrer que $\phi$ est un morphisme de monoïdes de $(A^*, ., \varepsilon)$ sur $(\mathbb{N}^2, +, (0, 0))$*
2. *Montrer que $Ker\phi = \{\varepsilon\}$.*
3. *Montrer que $\phi$ est surjectif mais non injectif.*
4. *Ce résultat permet-il de conclure à la dénombrabilité de $A^*$ ?*
5. *Calculer $\forall n, p \in \mathbb{N}$, $\#\phi^{-1}[(n, p)]$.*
6. *En déduire que $A*$ est un ensemble dénombrable.*
7. *On considère maintenant l'ensemble $A^\omega$ des séquences infinies sur $A$, montrer que $A^\omega$ n'est pas dénombrable.*

**Exercice 5 (fonction caractéristique d'un ensemble)**

*Soit $E$ un ensemble quelconque, et $\mathcal{P}(E)$ l'ensemble des parties de $E$ noté aussi $2^E$.*

$$\chi \left| \begin{array}{ccc} \mathcal{P}(E) & \longrightarrow & \{0,1\}^E \\ U & \longmapsto & \chi_U \end{array} \right. \qquad \left| \begin{array}{ccc} E & \longrightarrow & \{0,1\} \\ x & \longmapsto & \begin{cases} \chi_U(x) = 1 & si\ x \in U \\ \chi_U(x) = 0 & si\ x \notin U \end{cases} \end{array} \right.$$

1. *Montrer que $\chi$ est une bijection.*
2. *Montrer que* $i \left| \begin{array}{ccc} E & \longrightarrow & 2^E \\ x & \longmapsto & \{x\} \end{array} \right.$ *est une injection non surjective*
3. *Supposons $\#E = n$,*
   (a) *Montrer que $2^E$ est fini et calculer son cardinal.*
   (b) *En déduire que $2^n > n$*
4. *Montrer que quelque soit la fonction $f$ de $E$ dans $2^E$, l'ensemble $\{x \in E, x \notin f(x)\}$ n'a pas d'antécédent.*
5. *En déduire que l'ensemble des surjections de $E$ dans $2^E$ est l'ensemble vide.*
6. *En déduire que quelque soit l'ensemble $E$ non vide $\#E < \#2^E$.*
7. *En déduire que si $2^E$ est soit fini soit non dénombrable.*

8. *Montrer que $\chi_{U \cap V} = \chi_U \cdot \chi_V$,*
9. *Montrer que $\chi_{U-V} = sup(0, \chi_U - \chi_V)$,*
10. *Montrer que $\chi_{U \cup V} = \chi_U + \chi_V - \chi_U \cdot \chi_V$.*
11. *On rappelle que $U \Delta V = (U \cup V) - (V \cap U)$.*
    *En déduire une expression de $\chi_{U \Delta V}$ en fonction de $\chi_U$ et $\chi_V$.*

    *$A$, $B$ et $C$ étant trois sous-ensembles quelconques de $E$,*
12. *Montrer que $\chi_{A \Delta B} = \chi_{B \Delta A}$.*
13. *Montrer que $\chi_{(A \Delta B) \Delta C} = \chi_{A \Delta (B \Delta C)}$.*
14. *En déduire que $\Delta$ confère à $\mathcal{P}(E)$ une structure de monoïde commutatif.*