Université Paris 13, Institut Galilée
L2 Info, cours Mathématiques pour l'Informatique

Examen Seconde Session 2013, jeudi 27 juin.
3 heures sans documents.

Il y a 4 exercices indépendants. On rappelle que

– l'indice d'Euler $\varphi(n)$ est le nombre de nombres entiers compris entre 1 et n et premiers avec n ; $\varphi(1) = 1$. On rappelle que si $m \wedge n = pgcd(m, n) = 1$, alors $\varphi(mn) = \varphi(m) \times \varphi(n)$

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.

Exercice 1 *Soit a, b deux nombres entiers différents.*

1. *Montrer que si a et b sont des nombres premiers, alors a et b sont premiers entre eux.*
2. *Ecrire la réciproque.*
3. *La réciproque est-elle vraie ?*

Exercice 2

1. *Calculer l'ensemble des diviseurs de 693 dans* $\mathbb{N}$
2. *A chaque diviseur d de* 693 *donner son indice d'Euler $\varphi(d)$.*
3. *Faire le diagramme de Hasse de cet ensemble muni de l'ordre de divisibilité.*
4. $(\mathbb{Z}/693\mathbb{Z}, +, \times)$ *possède-t'il une structure de corps ?*
5. *Soit $\mathcal{I}$ l'ensemble des nombres qui s'écrivent en base 10 uniquement avec des 1 :* $\mathcal{I} = \{1, 11, 111, 1111, \ldots\}$.

(a) *Montrer que* $(\forall x, y \in \mathcal{I}, x < y)$ $(\exists q \in \mathcal{I}, \exists \alpha \in \mathbb{N})$ *tels que* $(x - y = 10^{\alpha} q)$.

(b) *Montrer que la fonction* $f : \begin{array}{ccc} \mathcal{I} & \longrightarrow & \mathbb{Z}/693\mathbb{Z} \\ x & \longmapsto & [x]_{693} \end{array}$ *n'est pas injective.*

(c) *en déduire qu'il existe au moins un élément de* $\mathcal{I}$ *divisible par 693.*

Exercice 3

1. *Les équations suivantes ont-elles des solutions* (u, v) *dans* $\mathbb{Z}$
   (a) $77u + 1001v = 1$
   (b) $9600u + 181v = 1$
2. *trouver un couple solution de (b) et en déduire l'inverse de* $[181]_{9600}$.
3. *Pour utiliser un chiffrement RSA, il est nécessaire d'avoir un triplet (t,p,q) d'entiers relatifs où p et q sont deux entiers premiers distincts ne divisant pas t. Montrer que le triplet (18200, 97, 101) convient.*
4. *Eve dépose la clé (9797,181). Montrer que c'est une clé RSA, c'est-à-dire de la forme* $(p \times q, e)$, *avec e un nombre premier avec* $\varphi(pq) = (p-1)(q-1)$.
5. *Bob veut transmettre une information secrètement par la méthode RSA à Eve. Il utilise donc la fonction* $[x^{181}]_{9797}$. *Donner la fonction utilisée par Eve pour retrouver l'information initiale.*

Exercice 4 (fonction caractéristique d'un ensemble)

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

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

1. *Montrer que* χ *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. *On suppose maintenant que le cardinal de* E *est quelconque, 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* χ_U *et* χ_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* Δ *confère à* $\mathcal{P}(E)$ *une structure de monoïde commutatif.*