Licence de Mathématiques.
Université d'Artois. 05/03/2012.
Durée 3h

EXAMEN - session **2**
ARITHMÉTIQUE

Les calculatrices et les documents sont interdits.
La rédaction sera prise en compte dans la notation.

Cours. (5 points=1+1+3)

1) Quelle est la définition d'un ensemble dénombrable ?

2) Donner la définition du pgcd de n entiers relatifs, $a_1, \ldots, a_n$, non tous nuls.

3) Expliquer le principe du codage RSA.

Exercice 1 : (4 points=1+(1,5+0,5)+1)

Soit $n \geq 1$ un entier naturel.

1) Compléter cet énoncé (théorème de Wilson): n est premier si et seulement si n divise $\cdots$

On souhaite prouver ce théorème.

2) On suppose que n est premier. On notera $\overline{a}$ la classe dans $\mathbb{Z}/n\mathbb{Z}$ d'un entier a.

(i) Que vaut $\overline{(n-1)!}$? (on justifiera la réponse)

(ii) Conclure.

3) Prouver la réciproque.

Exercice 2 :(4 points=1+1,5+0,5+1+0,5)

Soient a et b deux entiers naturels non nuls avec $a > b \geq 1$.

On définit la suite $\left(F_n\right)_{n\in\mathbb{N}}$ par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour tout $n \in \mathbb{N}$. Soit ρ la racine positive de $X^2 - X - 1$.

1) Montrer que pour tout $n \geq 1$, on a $F_n \geq \rho^{n-2}$.

2) Rappeler comment fonctionne l'algorithme d'Euclide appliqué à $a = r_0$ et $b = r_1$, en n étapes, dont la dernière étape s'écrit $r_{n-1} = q_n r_n$.

Que vaut alors r_n ? (en fonction de a et b)

3) Justifier que $r_{n-1} \geq 2$.

4) Montrer que pour tout entier $k \in \{1, \ldots, n\}$, on a $\quad r_{n-k} \geq F_{k+2}$.

5) En déduire que $n \leq \dfrac{\ln(b)}{\ln(\rho)} + 1$.

Exercice 3 : (7,5 points=(1+0,5+2+0,5+1)+(1,5+1)

On note $\mathcal{A} = \{A, B, .., Z\}$ l'alphabet et $\mathcal{E} = \{0, 1, .., 25\}$ l'ensemble des 26 premiers entiers naturels. On note enfin f la bijection naturelle de $\mathcal{A}$ sur $\mathcal{E}$ donnée par la place de chaque lettre dans l'alphabet (en commennçant par 0), c'est-à-dire :

$$f(A) = 0,\ f(B) = 1,\ ..,\ f(Z) = 25$$

1) Pour chaque entier x de $\mathcal{E}$, on note $g(x)$ le reste de la division euclidienne de $15x$ par 26.

a) Montrer que g est une bijection de $\mathcal{E}$ sur $\mathcal{E}$.

Ceci montre que cette méthode de codage est sans ambiguïté.

On code un mot quelconque par la méthode suivante : chaque lettre de $\mathcal{A}$ est envoyée sur son numéro via f, on applique ensuite g puis f^{-1}.

b) Comment se code le mot ART ?

c) On veut déterminer les points fixes par le codage $f^{-1} \circ g \circ f$.

(i) Soit $x \in \mathcal{E}$ tel que $15x \equiv x$ [26]. Montrer que nécessairement 13 divise x.

(ii) Conclure.

d) Quel est le mot dont le codage est NUN ?

e) On veut généraliser cette méthode en remplaçant $15x$ par $ax + b$ avec a et b des entiers naturels (a différent de 0). Quelle(s) hypothèse(s) doit-on faire pour que l'on puisse utiliser la même méthode ?

2) Pour tout couple d'entiers (x, y) de $\mathcal{E} \times \mathcal{E}$, on note $h(x, y)$ et $k(x, y)$ les uniques entiers de $\mathcal{E}$ tels que :

$$h(x, y) \equiv 3x + 4y \pmod{26} \quad \text{et} \quad k(x, y) \equiv 9x + 5y \pmod{26}$$

a) Montrer que l'application $h \times k$ est une bijection de $\mathcal{E} \times \mathcal{E}$ sur $\mathcal{E} \times \mathcal{E}$.

Ceci montre que le codage est sans ambiguïté et que tout mot d'un nombre pair de lettres est le codage d'un et d'un seul mot.

b) On convient de coder chaque mot contenant un nombre pair de lettres de la manière suivante : En partant de gauche à droite, on remplace chaque couple de lettres successives (α, β) (ayant pour numéros x et y) par le couple de lettres (δ, γ) dont les numéros s et t sont donnés par :

$$s = h(x, y) \quad \text{et} \quad t = k(x, y)$$

Comment se code le mot ANNE ? Le codage d'une lettre dépend-il de la place de cette lettre dans le mot?