Licence de Mathématiques.
Université d'Artois.
12/1/07.
Durée 3h

Examen
ARITHMÉTIQUE

Les calculatrices et les documents sont interdits.

La rédaction sera prise en compte dans la notation.

Dans tout le sujet, sauf mention explicite contraire, la notation $\dot{x}$ désigne la classe de x dans l'ensemble quotient considéré. S'il y a ambiguïté (plusieurs ensembles quotients) alors les notations seront précisées.

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

1)a) Soit E un ensemble. Quelle est la définition de "E est dénombrable"?
b) Est-ce que $\mathbb{Z}$ est dénombrable? Le justifier.

2) Soient $n \in \mathbb{N}$ avec $n \geq 1$, et $x \in \mathbb{Z}$.
a) A quelle condition nécessaire et suffisante a-t-on: "il existe $u \in \mathbb{Z}$ tel que $\dot{u}.\dot{x} = 1$ dans $\mathbb{Z}/n\mathbb{Z}$"?
b) Le démontrer.

Exercice 1. (4 points=1,5+1,5+1)

On cherche à trouver tous les $x \in \mathbb{Z}$ tels que

$$x \equiv 1\ [3] \qquad \text{et} \qquad x \equiv 2\ [5] \qquad \text{et} \qquad x \equiv 3\ [7]$$

1) Montrer que si $x_0 \in \mathbb{Z}$ est une solution particulière alors l'ensemble des solutions est $x_0 + 105\mathbb{Z} = \{x_0 + 105k |\, k \in \mathbb{Z}\}$.

2) a) Trouver $b_1 \in \mathbb{Z}$ tel que la classe de $35.b_1$ soit $\dot{1}$ dans $\mathbb{Z}/3\mathbb{Z}$?
b) Trouver $b_2 \in \mathbb{Z}$ tel que la classe de $21.b_2$ soit $\dot{1}$ dans $\mathbb{Z}/5\mathbb{Z}$?
c) Trouver $b_3 \in \mathbb{Z}$ tel que la classe de $15.b_3$ soit $\dot{1}$ dans $\mathbb{Z}/7\mathbb{Z}$?

3) Conclure en considérant $a = 35b_1 + 42b_2 + 45b_3$.

Exercice 2. (5,5 points=0,5+1+1+0,5+1,5+1)

Soit $n \in \mathbb{N}$ avec $n \geq 1$. On note σ_n le nombre de bijections de $\{1, \dots, n\}$ sur lui-même. On dit que $\sigma \in \sigma_n$ est un dérangement si pour tout $i \in \{1, \dots, n\}$, on a $\sigma(i) \neq i$. On note D_n l'ensemble des dérangements. On cherche à déterminer le cardinal de D_n.

1) Que vaut le cardinal de σ_n?

Pour $i \in \{1, \dots, n\}$, on note $A_i = \{\sigma \in \sigma_n | \, \sigma(i) = i\}$.

2) Que vaut le cardinal de A_i?

3) Pour tout k-uplet d'indices $1 \leq i_1 < \dots < i_k \leq n$, déterminer le cardinal de $A_{i_1} \cap \ldots \cap A_{i_k}$?

4) Comparer D_n et $\bigcup\limits_{1 \leq i \leq n} A_i$.

5) En déduire que $\mathrm{card}(D_n) = n! - \sum\limits_{k=1}^{n} (-1)^{k-1} \binom{n}{k} [(n-k)!]$.

6) Simplifier cette expression afin de déterminer $\lim\limits_{n \to +\infty} \dfrac{\mathrm{card}(D_n)}{\mathrm{card}(\sigma_n)}$.

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

On suppose qu'il y a un nombre fini de nombres premiers congrus à 1 modulo 4: $q_1 < \dots < q_n$. On pose alors $A = q_1 \ldots q_n$ et $B = A^2 + 1$.

1) On suppose qu'il existe un nombre premier $p > 2$ qui divise B.

a) Justifier que $p \equiv 3$ [4]. Indication: montrer que p n'est pas congru à 1 modulo 4.
On peut donc écrire $p = 3 + 4m$ où $m \in \mathbb{N}$.

b) Justifier que:

i) p divise $A^4 - 1$.

ii) p divise $A^{4m+2} - 1$.

c) Montrer que le reste de la division euclidienne de $A^{4m+2} - 1$ par $A^4 - 1$ est $A^2 - 1$. Indication: $A^{4m+2} - 1 = A^{4m+2} - A^2 + A^2 - 1$.

d) En déduire que p divise $A^2 - 1$ puis que p divise 2.

e) En déduire quel est le seul diviseur premier de B.

2) Montrer que B est congru à 2 modulo 4.

3) Conclure.