Université Paris 7 **Deuxième semestre 2003-2004**
DEUG MIAS Info - 1ère année **MT132 - groupe 1B4**

Interrogation écrite n°1

Durée : 1h
Les cours, documents, calculatrices, téléphones ne sont pas autorisés.

Questions de cours.

1) Énoncer le théorème de Gauss et le lemme d'Euclide.
2) Quels sont les éléments inversibles de $\mathbb{Z}$? de $K[X]$ (où $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$) ?
3) Simplifier les deux écritures suivantes : $9\mathbb{Z} \cap 30\mathbb{Z}$; $6\mathbb{Z} + 8\mathbb{Z} + 3\mathbb{Z}$.

Exercice 1. Résoudre les équations suivantes dans $\mathbb{Z}$:

1) $7x \equiv 1 \mod 35$;
2) $5x \equiv 1 \mod 7$;
3) $5x \equiv 2 \mod 7$.

(*indication pour la dernière :* prendre une solution particulière de l'équation 2), et multiplier l'équation 3) par cet entier).

Exercice 2. On définit les polynômes $A(X) = -2X^3 + 3X^2 + 4X - 6$ et $B(X) = -4X^4 + 4X^3 - X^2 + 4X + 3$. Déterminer un pgcd de A et B dans $\mathbb{R}[X]$. Le polynôme $2X - 3$ est-il un pgcd de A et B ?

Exercice 3. On se propose de démontrer qu'un entier naturel p est premier si et seulement si p divise $(p-1)! + 1$ (théorème de Wilson). On note E_p l'ensemble $\{1, 2, \ldots, p-1\}$.

1) Soit p un nombre premier. Démontrer que tout élément de E_p est premier avec p.
2) Soit p un nombre premier supérieur ou égal à 3.
   a) Rappeler pourquoi, pour tout entier a de E_p, il existe un entier $b \in \mathbb{Z}$ tel que $ab \equiv 1 \mod p$.
   b) En déduire que pour tout entier a de E_p il existe un c dans E_p tel que $ac \equiv 1 \mod p$ (on pourra commencer par trouver un c vérifiant $0 \leq c \leq p-1$, puis démontrer que $c \neq 0$).
   c) Démontrer qu'un tel c est unique.
   d) Démontrer que les seules solutions de $x^2 \equiv 1 \mod p$ dans E_p sont $x = 1$ et $x = p - 1$ (penser au lemme d'Euclide).
   e) En utilisant b), c) et d), démontrer que $(p-1)! \equiv 1 \times (p-1) \mod p$. En déduire que p divise $(p-1)! + 1$.
   f) Vérifier que ce résultat reste vrai pour $p = 2$.
3) Réciproquement : supposons que p soit un entier naturel divisant $(p-1)! + 1$. En utilisant l'identité de Bezout, démontrer que p est premier.

Barème approximatif : 5 pts, 4 pts, 3 pts, 8 pts.