Université Pierre et Marie Curie 2006–2007

LM220 Maths-Info groupe 1

Interrogation n° 2

**Exercice 1.**

1. Expliquer pourquoi 12 est inversible dans $\mathbf{Z}/25\mathbf{Z}$ et calculer son inverse.
2. En déduire que l'équation $12x = 7$ admet 11 pour *unique* solution dans $\mathbf{Z}/25\mathbf{Z}$.
3. Résoudre dans $\mathbf{Z}$ le système de congruences suivant.

$$\begin{cases} 12x \equiv 7 \mod 25 \\ x \equiv 2 \mod 21 \end{cases}$$

**Exercice 2.**

1. Donner la liste complète des éléments du groupe $(\mathbf{Z}/20\mathbf{Z})^*$.
2. Montrer que $(\mathbf{Z}/20\mathbf{Z})^*$ n'est pas cyclique. [*On pourra au choix utiliser le théorème chinois, ou calculer l'ordre de chaque élément.*]
3. Calculer le reste de la division euclidienne de $383^{127}$ par 20.

**Question de cours.**

1. Définir la fonction $\varphi$ d'Euler, et donner une formule explicite pour calculer $\varphi(n)$.
2. Énoncer le théorème d'Euler.