

UNIVERSITÉ PIERRE ET MARIE CURIE 2006–2007

LM220 Maths-Info groupes 2 et 5

Interrogation n° 2

Exercice 1.

1. Expliquer pourquoi 11 est inversible dans $\mathbf{Z}/24\mathbf{Z}$ et calculer son inverse.
2. En déduire que l'équation $11x = 3$ admet 9 pour *unique* solution dans $\mathbf{Z}/24\mathbf{Z}$.
3. Résoudre dans \mathbf{Z} le système de congruences suivant.

$$\begin{cases} 11x \equiv 3 \pmod{24} \\ x \equiv 2 \pmod{29} \end{cases}$$

Exercice 2.

1. Donner la liste complète des éléments du groupe $(\mathbf{Z}/14\mathbf{Z})^*$.
2. Montrer que $(\mathbf{Z}/14\mathbf{Z})^*$ est cyclique d'ordre 6.
3. Combien a-t-il de générateurs ?
4. Calculer le reste de la division euclidienne de 297^{365} par 14.

Question de cours. Énoncer le théorème chinois.