Université Pierre et Marie Curie 2006–2007

LM220 Maths-Info groupes 2 et 5

Interrogation écrite n° 3

**Exercice 1.**

1. Calculer $76^{29}$ modulo 7 et $76^{29}$ modulo 13.
2. Dans un cryptosystème utilisant la méthode RSA avec la clé publique $(n, e) = (91, 5)$, on souhaite envoyer le message $M_1 = 9$. Déterminer le message codé $C_1$ à envoyer.
3. Déterminer la clé secrète de ce cryptosystème et décoder le message $C_2 = 76$.

**Exercice 2.** On considère les deux polynômes suivants de $\mathbf{Q}[X]$ :

$$P(X) = X^4 + X^3 + 2X^2 - X + 3 \quad \text{et} \quad Q(X) = X^3 + 1.$$

1. Calculer le pgcd de $P$ et $Q$.
2. En déduire la factorisation de $P$ en produit de facteurs irréductibles dans $\mathbf{Q}[X]$.

**Question de cours.**
Démontrer le théorème suivant.

**Théorème.** Soient $K$ un corps et $I$ un idéal non nul de $K[X]$. Il existe un unique polynôme unitaire $P \in K[X]$ tel que l'on ait $I = (P)$.