Arithmétique - L3 - MI
Contrôle n^{0}2 - 2009

NOM :

Question 1

Que signifie "n est fortement pseudo-premier en base b " ? En quoi le test de Rabin-Miller est-il probabiliste ?

Question 2

Montrer que l'on a l'équivalence suivante :

$$p \text{ est premier } \iff \forall a \in \{1, 2, \cdots p-1\}, \quad a^{p-1} \equiv 1 \bmod p.$$

Ce test sépare notamment les nombres premiers des nombres de Carmichael. Pourquoi, à votre avis, n'est-il jamais utilisé ?

Question 3

Déterminer les racines du polnôme $X^5 - 6X^4 + 15X^3 - 26X^2 + 36X - 24$ dans $\mathbb{Q}$.

Question 4

Montrer que le polynôme $X^6 + X + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.