Université Pierre et Marie Curie 2006–2007

LM220 Maths-Info groupe 1

Interrogation écrite n° 3

Exercice 1.

1. Soit $n = (a_k \dots a_1 a_0)_{10}$ un entier écrit en base 10. Montrer que n est divisible par 11 si et seulement si $a_0 - a_1 + a_2 + \cdots + (-1)^k a_k$ est également divisible par 11.
2. Dans un cryptosystème utilisant la méthode RSA avec la clé publique $(n, e) = (319, 187)$, on souhaite envoyer le message $M_1 = 12$. Déterminer le message codé C_1 à envoyer.
3. Déterminer la clé secrète de ce cryptosystème et décoder le message $C_2 = 18$.

Exercice 2. On considère les deux polynômes suivants

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

1. Écrire une relation de Bezout entre P et Q dans $\mathbf{Q}[X]$. En déduire le pgcd de P et Q dans $\mathbf{Q}[X]$.
2. Quel est le pgcd de P et Q dans $(\mathbf{Z}/2\mathbf{Z})[X]$?

Question de cours.
Démontrer la proposition suivante.

Propositon. Soient p et q deux nombres premiers distincts. Posons $n = pq$. Soit t un entier naturel congru à 1 modulo $\varphi(n)$. Alors, on a

$$a^t \equiv a \pmod{n} \quad \text{quel que soit } a \in \mathbf{Z}.$$