UNIVERSITÉ DE RENNES 1
UFR Mathématiques

Licence STS 2006-2007

NOMBRES ENTIERS ET RATIONNELS. CONGRUENCES. PERMUTATIONS. (A02)

Examen du 13 juin 2007. Session 2

10 h 30 - 12 h 30

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits. Justifiez toutes vos réponses.

L'énoncé comporte cinq exercices indépendants.

EXERCICE 1 (Question de cours)

Soient $f : X \to Y$ et g : $Y \to Z$ deux applications.

1. Montrer que si f et g sont injectives, alors gof est injective.
2. Montrer que si gof est surjective alors g est surjective.

EXERCICE 2

Montrer de deux manières différentes que pour tout entier $n \geq 0$,

$$\sum_{k=0}^{n} C_n^k \times 2^k = 3^n$$

1. par récurrence ;
2. de manière directe.

EXERCICE 3

Comme chaque année, à la fin de la saison, le club du Varetz AC organise un tournoi de football pour les enfants de la région. Les dirigeants du club tentent de créer des équipes au mieux. Ils constatent que s'ils regroupent les enfants par équipes de *onze*, il reste *neuf* enfants sans équipe. S'ils constituent des équipes de *sept*, il reste *six* enfants et avec des groupes de *six*, il reste *un* enfant sans équipe.
Sachant que selon les organisateurs, une centaine d'enfants s'étaient inscrit, quel est le nombre exact de participants ?

Suite au verso, TSVP

EXERCICE 4

1. Décomposer 25 en base 2. En déduire 5^{25} mod 133.
   Indication de calcul : montrer que $5^{2^3} \equiv 4 \pmod{133}$.
2. Factoriser 133 et calculer $\varphi(133)$.
3. Quel est l'inverse de 13 modulo 108 ?
4. Soraya souhaite transmettre un message m à Matthieu en utilisant le cryptosystème RSA. Elle chiffre le message m en un message $M = 5$ puis envoie M à Matthieu.
   Sachant que la clé publique de Matthieu est $(n, e) = (133, 13)$, retrouver le message initial m.

EXERCICE 5

1. Résoudre le système
$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 5 \pmod{13} \end{cases}$$
2. Résoudre l'équation $x^2 + x + 9 \equiv 0 \pmod{11}$.
3. Résoudre l'équation $x^2 + x + 9 \equiv 0 \pmod{13}$.
4. Soit l'équation
$$(E)\ x^2 + x + 9 \equiv 0 \pmod{143}.$$
   Déduire des questions précédentes
   (a) une solution de (E) modulo 143 ;
   (b) le nombre de solutions de l'équation (E) modulo 143.