UNIVERSITÉ DE RENNES 1
UFR Mathématiques

Licence STS 2007-2008

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

Partiel du 7 décembre 2007

2 heures

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

L'énoncé comporte six exercices indépendants. Un barème est donné à titre indicatif pour chaque exercice.

EXERCICE 1 *(3 points)*

1) Donner la définition d'un entier inversible modulo un entier non nul n.
2) A quelle condition un entier naturel x est-il inversible modulo un entier non nul n ? Comment alors déterminer un inverse ?
3) Enoncer le petit théorème de Fermat.

EXERCICE 2 *(3 points)*

1) Quel est le plus grand nombre premier plus petit que $\sqrt{250}$?
2) On appelle nombres premiers jumeaux, deux nombres premiers qui, comme 11 et 13, diffèrent de 2. A l'aide du crible d'Eratosthène, déterminer deux nombres premiers jumeaux compris entre 200 et 250.

EXERCICE 3 *(3 points)*

1) Le nombre entier 2 est-il un carré modulo 11 ?
2) Résoudre dans $\mathbb{Z}$ l'équation $x^2 + 4\,x + 2 \equiv 0 \pmod{11}$.

EXERCICE 4 *(4 points)*

Résoudre dans $\mathbb{Z}$ le système d'équations

$$\begin{cases} x \equiv 7 \pmod{17} \\ x \equiv 5 \pmod{30} \\ x \equiv 11 \pmod{7} \end{cases}$$

Suite au verso, TSVP

EXERCICE 5 *(5 points)*

Le but de cet exercice est de réussir à décrypter un message d'Isabelle envoyé à Gilles par le protocole du cryptosystème RSA.

1) Montrer que l'ordre multiplicatif de 30 modulo 403 est égal à 6.
2) En déduire 30^{149} modulo 403
3) Gilles crée sa clé publique dans le cryptosystème RSA et la publie dans l'annuaire : $(403, 29)$. Isabelle désire transmettre un message $m \in \{1, \dots 402\}$ à Gilles. Elle le chiffre à l'aide du protocole RSA en un message M et envoie M à Gilles.
Exprimer M en fonction de m et de la clé publique $(403, 29)$ de Gilles.
4) Véronique intercepte le message M destiné à Gilles : $M = 30$. Expliquer comment elle calcule m et donner le résultat.

EXERCICE 6 *(4 points)*

Le but de cet exercice est de calculer les deux derniers chiffres de 2222^{261}.

1) Résoudre dans $\mathbb{Z}$ le système

$$\begin{cases} x & \equiv & 0 & (\text{mod } 4) \\ x & \equiv & 22 & (\text{mod } 25) \end{cases}$$

2) Calculer $\varphi(25)$. En déduire le reste de la division euclidienne de 22^{20} par 25, puis celui de 22^{261} par 25.
3) Calculer 22^{261} modulo 4.
4) Déduire des trois questions précédentes le reste de la division euclidienne de 22^{261} par 100.
5) Conclure.