UNIVERSITÉ DE RENNES 1

Licence STS 2007-2008

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

Rattrapage du Partiel du 7 décembre 2007

2 heures

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits. Justifiez toutes vos réponses et soignez la prsentation ainsi que l'orthographe. L'énoncé comporte six exercices indépendants. Un barème est donné à titre indicatif pour chaque exercice.

EXERCICE 1 *(2 points)*

1) Donner la définition de l'ordre multiplicatif d'un entier a modulo un entier n.
2) Enoncer le théorème d'Euler.

EXERCICE 2 *(4 points)*

1) Déterminer si possible un couple (x, y) d'entiers relatifs tel que $30x + 12y = 1$. Peut-on trouver plusieurs couples solutions ?
2) Déterminer si possible un couple (x, y) d'entiers relatifs tel que $30x + 12y = 6$. Peut-on trouver plusieurs couples solutions ?
3) L'application $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x, y) \mapsto 30x + 12y$ est-elle surjective ? injective ?

EXERCICE 3 *(2 points)*

Calculer le pgcd(46 848,2379).

EXERCICE 4 *(4 points)*

Résoudre dans $\mathbb{Z}$ les équations
1) 17x= 5 mod 30
2) 15x=5 mod 30
3) 25x=5 mod 30

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 $5^{2^3} \equiv 4(mod 133)$.
2) Calculer $\varphi(133)$.
3) Calculer l'inverse de 25 modulo 108.
4) Gilles crée sa clé publique dans le cryptosystème RSA et la publie dans l'annuaire : $(n = 133, d = 25)$. Isabelle désire transmettre un message $m \in \{1, \dots 132\}$ (premier avec 133) 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 de Gilles.
5) Véronique intercepte le message M destiné à Gilles : $M = 5$. Expliquer comment elle calcule m et donner le résultat.

EXERCICE 6 *(5 points)*

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

$$\begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 9 \pmod{25} \end{cases}$$

2) Calculer $\varphi(25)$. En déduire le reste de la division euclidienne de 22^{20} par 25, puis celui de 22^{382} par 25.
3) Calculer 22^{382} modulo 4.
4) Déduire des trois questions précédentes le reste de la division euclidienne de 22^{261} par 100.
5) Calculer les deux derniers chiffres de 2222^{382}