UNIVERSITÉ DE RENNES 1

UFR DE MATHÉMATIQUES

Licence – portail MIPE

NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES, PERMUTATIONS (*A2*)

Examen du 24 novembre 2004 (1 heure)

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits.

PROBLÈME

1 Écrire 103 en base 2.

2 Décomposer 143 en facteurs premiers.

3 Calculer le pgcd d de 103 et 120 et déterminer des entiers u et v tels que $120u + 103v = d$.

4 Soit a et n des entiers relatifs. À quelle condition existe-t-il un entier x tel que $ax \equiv 1 \pmod{n}$?

5 Déterminer tous les entiers x compris entre 0 et 119 tels que $103x \equiv 1 \pmod{120}$.

6 Rappeler l'énoncé du « petit théorème de Fermat ».

7 Trouver $a \in \{0, 1, \ldots, 12\}$ tel que $27^{103} \equiv a \pmod{13}$.

8 Trouver $b \in \{0, 1, \ldots, 10\}$ tel que $27^{103} \equiv b \pmod{11}$.

9 Calculer le reste de la division euclidienne de 27^{103} par 143.

10 Juliette et Roméo ont lu dans la revue *Pour la Science* un article sur le principe de cryptographie RSA. Ils décident de le tester sur un exemple simple pour vérifier qu'ils ont compris. Pour cela, Juliette choisit la clef publique $(n = 143, c = 7)$; Roméo choisit alors un entier, compris entre 0 et 142, puis le code avant de transmettre à Juliette le résultat : 27.
Pouvez-vous aider Juliette à retrouver l'entier choisi par Roméo ? Justifiez soigneusement votre réponse ; en particulier, rappelez le principe du codage et du décodage et calculez la clef secrète qui permet le décodage.
Vous pourrez bien sûr utiliser les questions précédentes.