

Examen de seconde session du 26 juin 2014

Durée : 3 heures.

Sans document, ni calculatrice, téléphones mobiles éteints et rangés.

Le sujet comporte 1 page

Exercice 1 — Questions de cours.

1. Énoncer le théorème de la division euclidienne (dans \mathbb{N}).
2. Que dit le “petit théorème de Fermat” pour le nombre premier $p = 7$?
3. (a) Qu’est-ce qu’un isomorphisme d’anneaux ?
(b) Décrire deux anneaux à quatre éléments qui ne sont pas isomorphes. Justifier votre réponse.
4. (a) Énoncer le “Lemme chinois”.
(b) Donner un exemple d’utilisation de ce lemme.

Exercice 2

1. (a) Faire la division euclidienne de 64 par 7.
(b) Appliquer l’algorithme d’Euclide à 64 et 7 et en déduire des nombres entiers relatifs x et y tels que $64x + 7y = 1$.
(c) Décrire toutes les solutions en nombres entiers relatifs x et y de l’équation $64x + 7y = 3$. Justifier vos réponses.
2. Décomposer 721 en facteurs premiers.
3. Montrer que les nombres premiers divisant l’équation de congruence $x^2 \equiv 2 \pmod{11}$. Justifier votre réponse.
4. (a) Calculer le dernier chiffre de l’écriture décimale de 77^{77} . Justifier votre réponse.
(b) Calculer le reste de la division euclidienne de 77^{77} par 7. Justifier votre réponse.
5. Démontrer que tout groupe à sept éléments est cyclique.
6. (a) On pose $N = 721$; combien y-a-t-il de nombres entre 1 et 720 qui sont premiers avec 721 ?
(b) On suppose que la clé publique RSA modulo 721 de Minny est le nombre 5, et que la clé publique RSA modulo 721 de Spinoz est le nombre 7 ; quelles sont les clés secrètes de Minny et Spinoz ?
(c) Rappeler le principe de la méthode RSA pour l’écriture de messages secrets, lorsqu’on souhaite que le récepteur sache qui est l’expéditeur.
(d) Quel nombre envoie Minny à Spinoz afin que le message une fois décodé par Spinoz soit le chiffre 3 ?
7. Démontrer que tous les groupes abéliens à 14 éléments sont isomorphes entre eux.