MAT309 Université Grenoble Alpes
2019-2020

Contrôle continu 2

le 27 novembre 2019

Les documents, téléphones portables ainsi que tous les autres dispositifs électroniques sont strictement interdits. Une calculette et une feuille recto-verso manuscrite sont autorisées. **Toutes les réponses doivent être justifiées** *et la qualité de la rédaction sera prise en compte.*

Exercice n° 1

1. Que vaut $\varphi(15)$?
2. Quels sont les éléments inversibles de $\mathbb{Z}/15\mathbb{Z}$?
3. Pour chacun de ces éléments, donner leur ordre dans $(\mathbb{Z}/15\mathbb{Z})^*$.
4. Le groupe $(\mathbb{Z}/15\mathbb{Z})^*$ est-il cyclique ? *On rappelle qu'un groupe est cyclique s'il admet au moins un générateur.*

Exercice n° 2

1. Calculer le reste de la division euclidienne de 2^{26} par 53 à l'aide de l'algorithme d'exponentiation rapide. On détaillera les calculs.
2. Montrer que $\bar{2}$ est un générateur de $(\mathbb{Z}/53\mathbb{Z})^*$.

Exercice n° 3

On rappelle qu'un *menteur* de Fermat d'un entier n non premier est un entier $x \in \{0, \ldots, n-1\}$ tel que $x^{n-1} \equiv 1\ [n]$.

1. Justifier pourquoi un menteur de Fermat pour $n = 57$ est nécessairement premier avec 3 et 19.
2. Soit $x \in \{0, \ldots, 56\}$. Montrer en utilisant le théorème des restes chinois que x est un menteur de Fermat de 57 si et seulement si x est solution du système d'équations suivant :
$$\begin{cases} x^2 \equiv 1\ [3] \\ x^2 \equiv 1\ [19] \end{cases}$$
3. Quelles sont les solutions dans $\mathbb{Z}$ de l'équation $x^2 \equiv 1\ [3]$? et de $x^2 \equiv 1\ [19]$?
4. Déterminer l'ensemble des menteurs de Fermat de 57.