Université Grenoble Alpes

08/12/2021 Licence 2 MIAGE, UE MAT 309

Devoir Surveillé MAT 309 n°2

Durée : 1h. Calculatrices et feuille manuscrite A4 recto-verso autorisées.
Toutes les réponses doivent être justifiées. La qualité de la rédaction sera prise en compte.

Exercice 1 : (*6 points*) On se place dans $\mathbb{Z}/13\mathbb{Z}$.

1. Quels sont les ordres possibles des éléments de $\mathbb{Z}/13\mathbb{Z}^*$.
2. Déterminer l'ordre de $\overline{10}$.
3. En déduire le reste dans la division euclidienne de 10^{139} par 13.
4. Montrer que $\overline{2}$ est un générateur de $\mathbb{Z}/13\mathbb{Z}^*$. Déterminer les autres générateurs.

Exercice 2 : (*6 points + Bonus*)

1. En utilisant l'algorithme d'exponentiation rapide, déterminer le reste dans la division euclidienne de 2^{90} par 91.
2. A quel test de primalité correspond ce résultat ? Quel témoin ou menteur vient-on d'exhiber pour 91 ?
3. a) Montrer que le système de congruence
$$\begin{cases} x \equiv 1[7] \\ x \equiv 12[13] \end{cases}$$
équivaut à une unique congruence modulo $7 \times 13 = 91$ que l'on déterminera.
   b) Vérifier que les restes dans les divisions euclidiennes de 2^{90} par 7 et 13 sont respectivement 1 et 12.
4. *Bonus :* On note $o(\overline{x})_n$ l'ordre d'un élément $\overline{x} \in \mathbb{Z}/n\mathbb{Z}^*$ pour $n \in \{7, 13, 91\}$. Montrer que
$$o(\overline{x})_{91} \mid \text{ppcm}(o(\overline{x})_7, o(\overline{x})_{13}).$$
En déduire que $\mathbb{Z}/91\mathbb{Z}^*$ n'admet pas de générateur.

Exercice 3 : (*6 points*) Un professeur P décide d'envoyer ses notes par mail au secrétariat S de l'Université en utilisant un codage RSA. La clé publique de chiffrement est $(c = 3, n = 33)$.

1. Quel message chiffré correspond à la note 13 ?
2. Vérifier que la clé privée de déchiffrement est 7.
3. Si S reçoit le message chiffré "9", à quelle note cela correspond ?
4. Supposons désormais que la clé publique de chiffrement soit $(c = 3, n = 55)$. Quelle est alors la clé privée de déchiffrement ?

Exercice 4 : (*6 points*)

1. Montrer que pour tout $n \in \mathbb{N}$, on a
   (a) $n^5 \equiv n[2]$,
   (b) $n^5 \equiv n[3]$,
   (c) $n^5 \equiv n[5]$.
   Indication : Pour chacune de ces questions, on pourra séparer les cas $\overline{n} = \overline{0}$ et $\overline{n} \neq \overline{0}$ dans $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$ respectivement.
2. En déduire que pour tout $n \in \mathbb{N}$,
$$n^5 \equiv n[30].$$