Annamaria Iezzi
Antoine de Tarlé

Contrôle Continu

20/10/26

Consignes. *La durée du contrôle continu est 1h30. Il est constitué de trois exercices indépendants. Toute question non résolue peut être admise dans la suite. Les réponses doivent être correctement rédigées. Aucun document ni calculatrice n'est autorisé.*

Exercice 1.

(a) À l'aide de l'algorithme d'Euclide étendu, calculer le pgcd entre 83 et 57, et une identité de Bézout.

(b) En déduire deux entiers $u, v \in \mathbb{Z}$ tels que

$$\frac{1}{4731} = \frac{u}{57} + \frac{v}{83}. \tag{1}$$

(On remarquera que $4731 = 57 \times 83$.)

(c) Existe-t-il des entiers u, v tels que $\frac{1}{24} = \frac{u}{4} + \frac{v}{6}$? Justifier.

(d) Soient $m, n \geq 2$ et $k \in \mathbb{Z}$. Montrer qu'il existe $u, v \in \mathbb{Z}$ tels que

$$\frac{k}{mn} = \frac{u}{m} + \frac{v}{n}$$

si et seulement si $\mathrm{pgcd}(m, n)$ divise k.

Exercice 2. Soit $N \in \mathbb{Z}_{>0}$ un entier dont l'écriture en base 10 est

$$N = \sum_{i=0}^{k} c_i 10^i, \text{ avec } c_i \in \{0, \ldots, 9\}.$$

(a) Montrer que $N \equiv \sum_{i=0}^{k} c_i \pmod 9$. En déduire un critère de divisibilité par 9.

(b) Établir un critère de divisibilité par 11.

(c) Les entiers 123456789 et 20266202 sont-ils divisibles par 9 ? par 11 ?

(d) On dit que N est un *palindrome* si $c_i = c_{k-i}$ pour tout i. Montrer que tout palindrome ayant un nombre pair de chiffres est divisible par 11. Est-ce encore vrai pour un nombre impair de chiffres ?

Exercice 3. Pour $a, b \in \frac{\mathbb{Z}}{26\mathbb{Z}}$, on considère l'application

$$\begin{array}{rccc} f_{a,b}\colon & \frac{\mathbb{Z}}{26\mathbb{Z}} & \to & \frac{\mathbb{Z}}{26\mathbb{Z}} \\ & x & \mapsto & ax+b. \end{array}$$

(a) Déterminer les éléments inversibles de $\frac{\mathbb{Z}}{26\mathbb{Z}}$ et l'inverse de 7 modulo 26.

(b) Montrer que $f_{a,b}$ est bijective si et seulement si $\mathrm{pgcd}(a, 26) = 1$. Combien y a-t-il de couples (a, b) pour lesquels $f_{a,b}$ est bijective ?

(c) On suppose a inversible dans $\frac{\mathbb{Z}}{26\mathbb{Z}}$ et on note a^{-1} son inverse. Montrer que la réciproque $f_{a,b}^{-1}$ est encore de la forme $f_{a',b'}$, et exprimer a' et b' en fonction de a et b.

Application au chiffrement affine. On identifie maintenant les lettres A, B, …, Z aux éléments $0, 1, \ldots, 25$ de $\frac{\mathbb{Z}}{26\mathbb{Z}}$.

Soient $a, b \in \mathbb{Z}$ tels que $\mathrm{pgcd}(a, 26) = 1$. Le *chiffrement affine* de clé (a, b) remplace chaque lettre x par la lettre $f_{a,b}(x)$. La *fonction de déchiffrement* correspondante est la fonction $f_{a,b}^{-1}$.

Exemple. Prenons la clé $(a, b) = (15, 2)$, qui est valable car $\mathrm{pgcd}(15, 26) = 1$. Pour chiffrer la lettre C, on remplace C par son numéro $x = 2$, on calcule $f_{15,2}(2) = 15 \times 2 + 2 = 32 \equiv 6 \pmod{26}$. On revient aux lettres : 6 correspond à G. La lettre C est donc chiffrée en G. En procédant de même pour chaque lettre, le mot `CIAO` est chiffré en `GSCE`.

(d) Pour la clé $(a, b) = (7, 3)$, chiffrer le message `HELLO`.

(e) Le message `KSDUX` a été chiffré avec la clé $(7, 3)$. Après avoir déterminé la fonction de déchiffrement $f_{7,3}^{-1}$, le déchiffrer.

(f) On intercepte un message chiffré avec une clé inconnue, et on sait que les lettres E et S ont été chiffrées respectivement en B et en T. Retrouver la clé.

(g) Pour essayer de renforcer la sécurité, on chiffre un message avec la clé $(7, 3)$, puis on chiffre le résultat avec la clé $(5, 7)$. Montrer que l'on obtient le même résultat qu'avec un unique chiffrement affine, dont on donnera la clé. Ce double chiffrement est-il plus sûr ?