Université Paris Est Créteil Val de Marne
Licences d'Informatique
2013-2014

Corrigé Contrôle continu 1 : Mathématiques discrètes pour l'informatique
Les documents et appareils électroniques ne sont pas autorisés.

[3pts] **Question 1** Déterminer l'ensemble des couples $(a,\, b) \in \mathbb{N}^2$ tels que :

$$a + b = 48 \qquad et \qquad \mathrm{pgcd}(a,\, b) = 6.$$

Réponse.
Nous avons :

$$\begin{cases} a = 6\,a' \\ b = 6\,b' \\ PGCD(a', b') = 1 \end{cases}$$

En remplaçant a et b dans la première equation, on obtient

$$\begin{cases} 6\,a' + 6\,b' = 48 \\ PGCD(a', b') = 1 \end{cases} \qquad \Longrightarrow \qquad \begin{cases} a' + b' = 8 \\ PGCD(a', b') = 1 \end{cases}$$

L'ensemble des couples possibles $(a',\, b')$ sont $\{(1,\, 7),\, (7,\, 1),\, (3,\, 5),\, (5,\, 3)\}$.
Ainsi, l'ensemble des couples $(a,\, b)$ sont $\{(6,\, 42),\, (42,\, 6),\, (18,\, 30),\, (30,\, 18)\}$.

[7pts] **Question 2**

On considère le chiffrement affine dans $\mathbb{Z}/26\mathbb{Z}$.

(a) Déterminer les éléments inversibles de $\mathbb{Z}/26\mathbb{Z}$.

(b) Trouver un couple $(a,\, b) \in \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ solution du système d'équations :

$$\begin{cases} 8\,a + b & = 12 \bmod 26 \\ \\ 19\,a + b & = 14 \bmod 26. \end{cases}$$

Réponse.

1. *(3 points)* les éléments inversibles de $\mathbb{Z}/26\mathbb{Z}$ sont
   ▶ Pour tout entiers $k \in \mathbb{Z}$, l'élément $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier à n.
   $\varphi(26) = 12$.
   $$\{1,\, 2,\, 3,\, 5,\, 7,\, 9,\, 11,\, 15,\, 17,\, 19,\, 21,\, 23,\, 25\}$$
2. *(4 points)*
   $$\begin{cases} 8\,a + b = 12 \pmod{26} \\ \\ 19\,a + b = 14 \pmod{26} \end{cases} \Longrightarrow 11\,a = 2 \pmod{26}.$$
   On doit déterminer l'inverse de 11 dans $\mathbb{Z}/26\mathbb{Z}$. D'après Bézout, $26u + 11v = 1$. Algorithme d'Euclide étendu

$$
\begin{aligned}
1 &= 4 - 3 \times 1 \\
&= 4 - (11 - 4 \times 2) \times 1 \\
&= 11 \times (-1) + 4 \times 3 \\
&= 11 \times (-1) + (26 - 11 * 2) \times 3 \\
&= 26 \times 3 + 11 \times (-7).
\end{aligned}
$$

D'où $u = 3$ et $v = -7 = 19$. Donc, l'inverse de 11 dans $\mathbb{Z}/26\mathbb{Z}$ est 19.
On obtient donc : $a \equiv 19 * 2 \pmod{26}$; $a \equiv 12 \pmod{26}$ et
$b \equiv 12 - 8 * 12 \pmod{26}$; $b \equiv -84 \pmod{26}$, $b \equiv 20 \pmod{26}$.

La solution du système est le couple (12, 20).