Cryptographie chapitre 3

Série A

Exercice 1. (4 pts)

$6\,x \equiv 9 \bmod 17$

Comme PGCD $(6\,;17) = 1$ et $1\,|\,9$, il existe des solutions entières pour cette équation.

a) $6\,x \equiv 1 \bmod 17$

$\Rightarrow\ x = 3$ est l'inverse de 6 modulo 17

b) En amplifiant par 9 : $x \equiv 27 \equiv 10 \bmod 17$

$\Rightarrow\ \boxed{x \equiv 10 \bmod 17}$

Série B

$6\,x \equiv 11 \bmod 17$

Comme PGCD $(6\,;17) = 1$ et $1\,|\,11$, il existe des solutions entières pour cette équation.

$6\,x \equiv 1 \bmod 17$

$\Rightarrow\ x = 3$ est l'inverse de 6 modulo 17

En amplifiant par 11 : $x \equiv 33 \equiv 16 \bmod 17$

$\Rightarrow\ \boxed{x \equiv 16 \bmod 17}$

Exercice 2. (7 pts)

$$\begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 4 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}$$

a) $m_1 = 4\ ;\ m_2 = 5\ ;\ m_3 = 7 \Rightarrow\ M = 140$

$M_1 = \frac{140}{4} = 35; M_2 = \frac{140}{5} = 28; M_3 = \frac{140}{7} = 20$

b) • $35\,x \equiv 1 \bmod 4$ $\quad 35 \equiv 3 \bmod 4$

$\Rightarrow 3\,x \equiv 1 \bmod 4$ $\quad \Rightarrow x_1 \equiv 3 \bmod 4$

• $28\,x \equiv 1 \bmod 5$ $\quad 28 \equiv 3 \bmod 5$

$\Rightarrow 3\,x \equiv 1 \bmod 5$ $\quad \Rightarrow x_2 \equiv 2 \bmod 5$

• $20\,x \equiv 1 \bmod 7$ $\quad 20 \equiv 6 \bmod 7$

$\Rightarrow 6\,x \equiv 1 \bmod 7$ $\quad \Rightarrow x_3 \equiv 6 \bmod 7$

c) $x = 1 \cdot 35 \cdot 3 + 4 \cdot 28 \cdot 2 + 3 \cdot 20 \cdot 6 = 689$

$\Rightarrow x \equiv 689 \equiv 129 \bmod 140$

$\Rightarrow\ \boxed{x \equiv 129 \bmod 140}$

$$\begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 3 \bmod 5 \\ x \equiv 4 \bmod 7 \end{cases}$$

$m_1 = 4\ ;\ m_2 = 5\ ;\ m_3 = 7 \Rightarrow\ M = 140$

$M_1 = \frac{140}{4} = 35; M_2 = \frac{140}{5} = 28; M_3 = \frac{140}{7} = 20$

• $35\,x \equiv 1 \bmod 4$ $\quad 35 \equiv 3 \bmod 4$

$\Rightarrow 3\,x \equiv 1 \bmod 4$ $\quad \Rightarrow x_1 \equiv 3 \bmod 4$

• $28\,x \equiv 1 \bmod 5$ $\quad 28 \equiv 3 \bmod 5$

$\Rightarrow 3\,x \equiv 1 \bmod 5$ $\quad \Rightarrow x_2 \equiv 2 \bmod 5$

• $20\,x \equiv 1 \bmod 7$ $\quad 20 \equiv 6 \bmod 7$

$\Rightarrow 6\,x \equiv 1 \bmod 7$ $\quad \Rightarrow x_3 \equiv 6 \bmod 7$

$x = 1 \cdot 35 \cdot 3 + 3 \cdot 28 \cdot 2 + 4 \cdot 20 \cdot 6 = 753$

$\Rightarrow x \equiv 753 \equiv 53 \bmod 140$

$\Rightarrow\ \boxed{x \equiv 53 \bmod 140}$

Exercice 3. (3 pts)

$$\begin{cases} x \equiv 4 \bmod 12 \\ x \equiv 3 \bmod 5 \\ x \equiv 8 \bmod 10 \end{cases}$$

- $x \equiv 4 \bmod 12 \Rightarrow \begin{cases} x \equiv 4 \equiv 1 \bmod 3 \\ x \equiv 4 \equiv 0 \bmod 4 \end{cases}$
- $x \equiv 3 \bmod 5$ OK
- $x \equiv 8 \bmod 10 \Rightarrow \begin{cases} x \equiv 8 \equiv 0 \bmod 2 \\ x \equiv 8 \equiv 3 \bmod 5 \end{cases}$
- $\Rightarrow \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 0 \bmod 4 \\ x \equiv 3 \bmod 5 \end{cases}$

$$\begin{cases} x \equiv 9 \bmod 20 \\ x \equiv 2 \bmod 3 \\ x \equiv 5 \bmod 6 \end{cases}$$

- $x \equiv 9 \bmod 20 \Rightarrow \begin{cases} x \equiv 9 \equiv 1 \bmod 4 \\ x \equiv 9 \equiv 4 \bmod 5 \end{cases}$
- $x \equiv 2 \bmod 3$ OK
- $x \equiv 5 \bmod 6 \Rightarrow \begin{cases} x \equiv 5 \equiv 1 \bmod 2 \\ x \equiv 5 \equiv 2 \bmod 3 \end{cases}$
- $\Rightarrow \begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 1 \bmod 4 \\ x \equiv 4 \bmod 5 \end{cases}$

Exercice 4. (6 pts)

- Variable : $x =$ le nombre de chevaux , $150 < x < 200$
- Système de congruences :

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 1 \bmod 4 \\ x \equiv 3 \bmod 5 \end{cases}$$

- Théorème chinois :

  - $m_1 = 3$; $m_2 = 4$; $m_3 = 5 \Rightarrow M = 60$

  $M_1 = \frac{60}{3} = 20; M_2 = \frac{60}{4} = 15; M_3 = \frac{60}{5} = 12$

  - $20\,x \equiv 1 \bmod 3 \quad 20 \equiv 2 \bmod 3$

  $\Rightarrow 2\,x \equiv 1 \bmod 3 \Rightarrow x_1 \equiv 2 \bmod 3$

  - $15\,x \equiv 1 \bmod 4 \quad 15 \equiv 3 \bmod 4$

  $\Rightarrow 3\,x \equiv 1 \bmod 4 \Rightarrow x_2 \equiv 3 \bmod 4$

  - $12\,x \equiv 1 \bmod 5 \quad 12 \equiv 2 \bmod 5$

  $\Rightarrow 2\,x \equiv 1 \bmod 5 \Rightarrow x_3 \equiv 3 \bmod 5$

  - $x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \bmod 60$

- Comme $150 < x < 200 \Rightarrow$ $\boxed{\text{L'éleveur possède 173 chevaux}}$
