

## Cryptographie chapitres 1 et 2

### Série A

**Exercice 1.** (1+1+1+2=5 pts)

1) proposition vraie pour  $n = 0$  :

$$7^{0+1} \equiv 1 \pmod{3} \text{ vraie car } 7 = 1 + 2 \cdot 3$$

2) hypothèse de récurrence :

$$7^{n+1} \equiv 1 \pmod{3} \text{ vraie pour } n \iff$$

$$\iff \exists k \in \mathbb{Z} \text{ tel que } 7^{n+1} = 1 + 3 \cdot k$$

3) conclusion :

$$7^{(n+1)+1} \equiv 1 \pmod{3}$$

4) raisonnement :

$$7^{n+2} = 7^{n+1} \cdot 7 \stackrel{\text{h.r.}}{=} (1 + 3k) \cdot 7 = 7 + 21k =$$

$$= 1 + 3 \cdot 2 + 3 \cdot 7k \stackrel{\text{mee}}{=} 1 + 3(2 + 3k) \iff$$

$$\iff 7^{n+2} \equiv 1 \pmod{3} \quad \text{CQFD}$$

### Série B

proposition vraie pour  $n = 0$  :

$$5^{0+1} \equiv 1 \pmod{4} \text{ vraie car } 5 = 1 + 1 \cdot 4$$

hypothèse de récurrence :

$$5^{n+1} \equiv 1 \pmod{4} \text{ vraie pour } n \iff$$

$$\iff \exists k \in \mathbb{Z} \text{ tel que } 5^{n+1} = 1 + 4 \cdot k$$

conclusion :

$$5^{(n+1)+1} \equiv 1 \pmod{4}$$

raisonnement :

$$5^{n+2} = 5^{n+1} \cdot 5 \stackrel{\text{h.r.}}{=} (1 + 4k) \cdot 5 = 5 + 20k =$$

$$= 1 + 4 \cdot 1 + 4 \cdot 5k \stackrel{\text{mee}}{=} 1 + 4(1 + 5k) \iff$$

$$\iff 5^{n+2} \equiv 1 \pmod{4} \quad \text{CQFD}$$

**Exercice 2.** (4 pts)

$$220 \cdot u + 21 \cdot v = 1$$

- Algorithme d'Euclide étendu :

$$220 = 10 \cdot 21 + 10 \Rightarrow 10 = 220 - 10 \cdot 21$$

$$21 = 2 \cdot 10 + 1 \Rightarrow 1 = 21 - 2 \cdot 10$$

$$10 = 10 \cdot 1 \Rightarrow \text{PGCD}(220; 21) = 1$$

- Par le théorème de Bézout, il existe deux entiers vérifiant cette équation.

- $1 = 0 \cdot 10 + 1 \cdot 1$

$$\Rightarrow 1 = 1 \cdot 21 - 2 \cdot 10$$

$$\Rightarrow 1 = (-2) \cdot 220 + 21 \cdot 21$$

$$\Rightarrow u = -2 \quad ; \quad v = 21$$

$$320 \cdot u + 31 \cdot v = 1$$

- Algorithme d'Euclide étendu :

$$320 = 10 \cdot 31 + 10 \Rightarrow 10 = 320 - 10 \cdot 31$$

$$31 = 3 \cdot 10 + 1 \Rightarrow 1 = 31 - 3 \cdot 10$$

$$10 = 10 \cdot 1 \Rightarrow \text{PGCD}(320; 31) = 1$$

- Par le théorème de Bézout, il existe deux entiers vérifiant cette équation.

- $1 = 0 \cdot 10 + 1 \cdot 1$

$$\Rightarrow 1 = 1 \cdot 31 - 3 \cdot 10$$

$$\Rightarrow 1 = (-3) \cdot 320 + 31 \cdot 31$$

$$\Rightarrow u = -3 \quad ; \quad v = 31$$

**Exercice 3.** (5 pts)

$$7 \cdot x + 3 \cdot y = 71$$

- Algorithme d'Euclide étendu :

$$7 = 2 \cdot 3 + 1 \Rightarrow 1 = 7 - 2 \cdot 3$$

$$3 = 3 \cdot 1 \Rightarrow \text{PGCD}(7; 3) = 1$$

- Comme  $1 \mid 71$ , il existe des solutions entières pour cette équation.

- $1 = 0 \cdot 3 + 1 \cdot 1$

$$\Rightarrow 1 = 1 \cdot 7 - 2 \cdot 3 \quad | \cdot 71$$

$$\Rightarrow 71 = 71 \cdot 7 - 142 \cdot 3$$

$$\Rightarrow (x_0; y_0) = (71; -142) \text{ est une solution particulière}$$

- $\Rightarrow (71 - 3k; -142 + 7k), k \in \mathbb{Z}$  est la solution générale

- Les solutions sont positives si  $\frac{142}{7} \leq k \leq \frac{71}{3}, k \in \mathbb{Z} \Rightarrow k \in \{21; 22; 23\}$

- $k = 21 \Rightarrow (x; y) = (8; 5)$   
 $k = 22 \Rightarrow (x; y) = (5; 12)$   
 $k = 23 \Rightarrow (x; y) = (2; 19)$

**Exercice 4.** (6 pts)

- Variables :

$x$  = le nombre de veaux

$y$  = le nombre de porcs

- Equation diophantienne :

$$80 \cdot x + 50 \cdot y = 810, \quad x < y$$

- Algorithme d'Euclide étendu :

$$80 = 1 \cdot 50 + 30 \quad \Rightarrow 30 = 80 - 50$$

$$50 = 1 \cdot 30 + 20 \quad \Rightarrow 20 = 50 - 30$$

$$30 = 1 \cdot 20 + 10 \quad \Rightarrow 10 = 30 - 20$$

$$20 = 2 \cdot 10 \quad \Rightarrow \text{PGCD}(80; 50) = 10$$

- Comme  $10 \mid 810$ , il existe des solutions entières pour cette équation.

- $10 = 0 \cdot 20 + 1 \cdot 10$

$$\Rightarrow 10 = 1 \cdot 30 - 1 \cdot 20$$

$$\Rightarrow 10 = (-1) \cdot 50 + 2 \cdot 30$$

$$\Rightarrow 10 = 2 \cdot 80 - 3 \cdot 50 \quad | \cdot 81$$

$$\Rightarrow 810 = 162 \cdot 80 - 243 \cdot 50$$

$$\Rightarrow (x_0; y_0) = (162; -243) \text{ est une solution particulière}$$

- $\Rightarrow (162 - 5k; -243 + 8k), k \in \mathbb{Z}$  est la solution générale

- Les solutions sont positives si  $\frac{243}{8} \leq k \leq \frac{162}{5}, k \in \mathbb{Z} \Rightarrow k \in \{31; 32\}$

- $k = 31 \Rightarrow (x; y) = (7; 5)$  mais  $7 > 5$

$$k = 32 \Rightarrow (x; y) = (2; 13) \text{ avec } 2 < 13$$

- Le fermier a acheté 2 veaux et 13 porcs.