www.freemaths.fr

Maths Expertes
Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

ARITHMÉTIQUE, SYNTHÈSE 6

CORRECTION

1. a. a1. Vérifions que $8^7 \equiv 2\ [55]$:

Nous avons: $8^2 = 64$ et $64 = 9 + 55$.

D'où: $8^2 \equiv 9\ [55]$.

Dans ces conditions: $8^7 = 8 \times 8^6$

$= 8 \times (8^2)^3$

$\equiv 8 \times (9)^3\ [55]$.

Or: $9^3 = 729$

$= 14 + 13 \times 55$

$\equiv 14\ [55]$.

Donc: $8^7 \equiv 8 \times 14\ [55]$ **cad**: $8^7 \equiv 2\ [55]$ (car: $8 \times 14 = 2 + 2 \times 55$).

Ainsi, nous avons bien: $8^7 \equiv 2\ mod\ 55$.

1. a. a2. Déduisons-en le reste dans la division euclidienne par 55 de 8^{21}:

Nous avons: $8^{21} = (8^7)^3$.

D'où: $8^{21} \equiv 2^3\ [55]$ **cad**: $8^{21} \equiv 8\ [55]$.

Au total, nous avons: $8^{21} \equiv 8\ [55]$.

Donc le reste dans la division euclidienne par 55 de 8^{21} est: **8**.

1. b. b1. Vérifions que $8^2 \equiv 9\ [55]$:

Nous avons: $8^2 = 64$ et $64 = 9 + 55$.

D'où: $8^2 \equiv 9\ [55]$.

1. b. b2. Déduisons-en le reste dans la division euclidienne par 55 de 8^{23}:

Nous avons: $8^{23} = 8^2 \times 8^{21}$.

Or: • $8^2 \equiv 9\ [55]$

• $8^{21} \equiv 8\ [55]$.

D'où: $8^{23} \equiv 72\ [55]$ **cad**: $8^{23} \equiv 17\ [55]$.

Ainsi, le reste dans la division euclidienne par 55 de 8^{23} est: 17.

2. a. Justifions le fait que l'équation (E) admet au moins un couple solution:

Pour le justifier, nous allons appliquer le théorème de **BÉZOUT**.

D'après ce théorème: " Soient a et b deux entiers relatifs non nuls. a et b sont premiers entre eux ssi il existe deux entiers x et y tels que: $ax + by = 1$ ".

Ici l'équation (E) s'écrit: $23x - 40y = 1$, x et y étant des entiers relatifs.

$$(ax + by = 1)$$

Or: $a = 23$ et $b = -40$ sont premiers entre eux.

Donc d'après ce théorème, il existe bien deux entiers relatifs x et y tels que:

$$ax + by = 1 \iff 23x + (-40)y = 1.$$

Au total: l'équation (E) admet au moins un couple solution.

2. b. Donnons un couple, solution particulière de l'équation (E):

Nous pouvons prendre, par exemple, le couple: $(x\,;y) = (7\,;4)$.

En effet: $23 \times 7 - 40 \times 4 = 1$.

Au total, un couple solution particulière de l'équation (E) est: $x = 7$ et $y = 4$.

2. c. Déterminons tous les couples d'entiers relatifs solutions de l'équation (E):

• Soit un couple $(x\,;y)$ d'entiers relatifs vérifiant l'équation (E).

D'où: $23x - 40y = 1$.

Or nous savons que le couple (7; 4) est une solution particulière de l'équation (E).

D'où: $23 \times 7 - 40 \times 4 = 1$.

Nous pouvons ainsi écrire: $23x - 40y = 23 \times 7 - 40 \times 4$

$$\Leftrightarrow 23\,(x - 7) = 40\,(y - 4).$$

➔ Comme 23 et 40 sont premiers entre eux, d'après le théorème de **GAUSS**, l'entier 40 divise $x - 7$.

Par conséquent, il existe nécessairement un entier relatif p tel que:

$$x - 7 = 40 \times p \quad \textbf{cad}: \quad \boldsymbol{x = 7 + 40 \times p}.$$

➔ De même, comme 23 et 40 sont premiers entre eux, d'après le théorème de **GAUSS**, l'entier 23 divise $y - 4$.

Par conséquent, il existe nécessairement un entier relatif p' tel que:

$$y - 4 = 23 \times p' \quad \textbf{cad}: \quad \boldsymbol{y = 4 + 23 \times p'}.$$

• **Réciproque**:

Soient p et p' deux entiers relatifs et: $x = 7 + 40 \times p$ et $y = 4 + 23 \times p'$.

Dans ces conditions: $23x - 40y = 1 \iff 23(7 + 40 \times p) - 40(4 + 23 \times p') = 1$

$\iff 23 \times 40 \times (p - p') = 0$

$\iff \mathbf{p = p'}$.

Au total, les couples d'entiers relatifs solutions de l'équation (E) sont de la forme: $x = 7 + 40\,p$ et $y = 4 + 23\,p'$, avec $p = p'$.

Ils sont donc de la forme: $x = 7 + 40\,p$ et $y = 4 + 23\,p$.

2. d. Déduisons-en qu'il existe un unique entier " d " tel que $0 \leqslant d < 40$ et qui vérifie $23\,d \equiv 1\ [40]$:

• $23\,d \equiv 1\ [40]$ ssi il existe un entier relatif " w " tel que: $23\,d = 1 + 40 \times w$.

$23\,d = 1 + 40 \times w \iff 23\,d - 40\,w = 1$, $d \in \mathbb{Z}$ et $w \in \mathbb{Z}$.

D'après la question précédente, nous pouvons affirmer que:

$$\mathbf{d = 7 + 40\,p,\ p \in \mathbb{Z}}.$$

Dans ces conditions: $0 \leqslant d < 40 \iff 0 \leqslant 7 + 40\,p < 40$

$$\iff -\frac{7}{40} \leqslant p < \frac{33}{40}$$

$\iff \mathbf{p = 0}$ **car**: $\mathbf{p \in \mathbb{Z}}$.

D'où nécessairement: $d = 7 + 40 \times 0$ **cad**: $d = 7$.

• **Réciproque**:

Si $d = 7$: $23\,d = 161$ **ou encore**: $23\,d = 1 + 4 \times 40$ **cad**: $\mathbf{23\,d \equiv 1\ [40]}$.

Au total, il existe bien un unique entier **d** vérifiant les conditions: $d = 7$.

3. a. a1. Calculons N et n:

Ici: $p = 5$ et $q = 11$.

Or, d'après l'énoncé: $N = pq$ et $n = (p - 1)(q - 1)$.

D'où: $N = 55$ et $n = 40$.

3. a. a2. Vérifions que c = 23 est la bonne valeur:

D'après l'énoncé, le nombre " c " doit être un entier naturel et doit être premier avec $n = 40$.

Or ici:
- 23 est un entier naturel,
- 23 et 40 sont bien premiers entre eux.

Donc: $c = 23$ vérifie bien la condition voulue.

3. b. Déterminons la valeur du nombre crypté b, sachant que a = 8:

Ici: $a = 8$, $c = 23$ et $N = 55$.

D'où: $a^c = 8^{23}$

$\equiv 17\ [55]$, **d'après 1. b.**

Or, b correspond au reste dans la division euclidienne par N du nombre a^c.

Donc: $b = 17$, 17 étant le reste dans la division euclidienne par 55 du nombre 8^{23}.

4. a. Déterminons la valeur de " d ":

D'après la réponse à la question **2. d.**, nous pouvons dire que: $d = 7$.

4. b. Retrouvons le nombre en clair lorsque le nombre crypté est $b = 17$:

Nous avons: • $b^d = 17^7$,

et: • $17^7 \equiv -6 \times 17 \; [55]$.

D'où: $17^7 \equiv -102 \; [55]$

$\equiv 8 \; [55]$, car: $-102 = 8 - 2 \times 55$.

Au total, en appliquant la règle de décryptage, on trouve en clair: $a = 8$.