www.freemaths.fr

Maths Expertes
Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

Arithmétique, Synthèse 32

Correction

Partie A.

L'équation **(E)** est l'équation $25x - 108y = 1$.
Notons que les nombres 25 et 108 sont premiers entre eux. En effet, leurs décompositions en facteurs premiers $25 = 5^2$ et $108 = 2^2 \times 3^3$ n'ont aucun facteur premier commun.

1. Vérifions que le couple $(13\ ;\ 3)$ est solution de l'équation (E) :

$25 \times 13 - 108 \times 3 = 325 - 324 = 1$

Le couple $(13\ ;\ 3)$ est bien solution de l'équation (E).

2. Résolvons l'équation (E) :

NB. Soit *a, b, c* trois entiers relatifs non nuls, les entiers *a* et *b* étant premiers entre eux comme c'est le cas de 25 et 108.
La méthode générale de résolution dans l'ensemble $\mathbb{Z} \times \mathbb{Z}$ de l'équation $ax - by = c$ **(E)** quand on en connaît déjà un couple solution $(x_0,\ y_0)$ particulier est la suivante :

- Un couple $(x,\ y)$ est solution de **(E)** si et seulement si le couple $(x - x_0,\ y - y_0)$ est solution de l'équation $aX - bY = 0$ **(H)**, équation dite « homogène » ou « sans second membre » qui a pour solutions les couples de la forme $(kb,\ ka)$ *k* est un entier relatif[1].
- Les couples solutions de **(E)** sont les couples de la forme : $(x_0 + kb,\ y_0 + ka)$ où *k* est un entier relatif.

En l'occurrence, nous disposons du couple solution particulier $(x_0 = 13\ ;\ y_0 = 3)$.

Un couple $(x,\ y)$ est solution de l'équation **(E)** si et seulement si le couple $(X = x - 13,\ Y = y - 3)$ est solution de l'équation homogène $25X - 108Y = 0$, équation qui a pour solutions les couples de la forme $(108k,\ 25k)$ où *k* est un entier relatif.

[1] **Pour mémoire, résolution de l'équation homogène $aX - bY = 0$.** Soit (*X, Y*) un couple solution. L'entier *a* divise *bY* et est premier avec *b*, donc il divise *Y* (théorème de Gauss). Il existe un entier relatif *k* tel que $Y = ka$. De ce fait : $aX = b \times (ka)$ d'où on déduit, puisque *a* est non nul, $X = kb$. Le couple (X, Y) est nécessairement de la forme (ka, kb) où *k* est un entier relatif. Réciproquement, on vérifie sans peine qu'un couple de cette forme est solution de l'équation $aX - bY = 0$.

Un couple d'entiers relatifs $(x,\ y)$ est solution de l'équation **(E)** si et seulement s'il existe un entier relatif *k* tel que $\begin{cases} x-13=108k \\ y-3=25k \end{cases}$.

Les couples solutions de l'équation **(E)** sont les couples de la forme $(13+108k,\ 3+25k)$ où *k* est un entier relatif.

Partie B.

Dans cette partie, *c* et *g* sont deux entiers naturels vérifiant la relation $25g-108c=1$.

1. Montrons que, si *x* est congru à *a* modulo 7 et modulo 19, il est congru à *a* modulo 133 :

Notons que les entiers 7 et 19, en tant que nombres premiers distincts, sont des entiers premiers entre eux.

La congruence $x \equiv a\ [7]$ signifie que 7 divise $x-a$ ou, aussi bien, qu'il existe un entier relatif *k* tel que : $x-a=7k$.
La congruence $x \equiv a\ [19]$ signifie que 19 divise $x-a$ ou, aussi bien, qu'il existe un entier relatif *k'* tel que : $x-a=19k'$.
Nous en déduisons une relation entre *k* et *k'* : $7k=19k'$

Or, nous avons noté que 7 et 19 sont premiers entre eux. Les deux hypothèses du théorème de Gauss sont vérifiées, appliquons-le :
Puisque 19 divise $7k$ et qu'il est premier avec 7, il divise *k*. Il existe un entier relatif k_1 tel que $k=19k_1$.

Nous pouvons écrire : $x-a=7k=7\times(19k_1)=133k_1$

L'existence de cet entier k_1 caractérise le fait que 133 divise $x-a$ ou, aussi bien, que $x \equiv a\ [133]$.
Résumons :

Soit *x* et *a* deux entiers naturels tels que $x \equiv a\ [7]$ et $x \equiv a\ [19]$. Alors $x \equiv a\ [133]$

NB. Le résultat reste vrai si on suppose que *x* et *a* sont des entiers « relatifs ».

2.a. Montrons que si *a* n'est pas multiple de 7, a^6 et a^{108} sont congrus à 1 modulo 7 :

7 est un nombre premier et l'entier naturel *a* est par hypothèse un entier non divisible par 7.
Nous pouvons appliquer le petit théorème de Fermat, sachant que le prédécesseur « $7-1$ » de 7 figurant dans le théorème est l'entier 6. Nous obtenons :

$$a^6 \equiv 1\ [7]$$

D'après la compatibilité avec l'exponentiation de la relation de congruence modulo 7, la congruence $a^6 \equiv 1\ [7]$ implique pour tout entier naturel *k* la congruence $(a^6)^k \equiv 1^k\ [7]$, autrement dit la congruence suivante :

Pour tout entier naturel *k* : $a^{6k} \equiv 1\ [7]$.

.

C'est en particulier le cas en ce qui concerne l'entier $108=6\times18$ qui est un multiple de 6.

Nous obtenons en choisissant $k = 18$ dans la congruence générale précédente :

$$a^{108} \equiv 1 \ [7]$$

Déduisons-en qu'alors $(a^{25})^g \equiv a \ [7]$:

NB. Il faut bien lire « *a* puissance 25 élevé à la puissance *g* ».

Compte tenu de la relation liant les entiers *g* et *c* : $25g = 108c + 1$

Nous en déduisons : $(a^{25})^g = a^{25g} = a^{108c+1} = (a^{108})^c \times a$

Utilisons une congruence modulo 7 : $(a^{25})^g \equiv (a^{108})^c \times a \ [7]$

D'après le résultat précédent, $a^{108} \equiv 1 \ [7]$ donc pour tout entier naturel *c* : $(a^{108})^c \equiv 1 \ [7]$

En conséquence : $(a^{108})^c \times a \equiv a \ [7]$

En fin de compte, par transitivité :

Si *a* n'est pas un multiple de 7 : $(a^{25})^g \equiv a \ [7]$.

2.b. Montrons que si *a* est multiple de 7, la congruence $(a^{25})^g \equiv a \ [7]$ est encore vérifiée :

Si *a* est un multiple de 7, toutes ses puissances entières strictement positives sont aussi multiples de 7. L'entier *a* et toutes ses puissances entières strictement positives sont aussi congrues à 0 modulo 7.

Or, l'entier *g* est nécessairement un entier strictement positif (il est égal à $108c + 1$ avec *c* entier naturel) et il en est de même du nombre $25g$.

Les entiers *a* et a^{25g} sont tous deux congrus à 0 modulo 7.

La congruence $(a^{25})^g \equiv a \ [7]$ est encore vérifiée lorsque *a* est un multiple de 7.

3. Montrons que $(a^{25})^g \equiv a \ [133]$:

Les **questions B.2.a** et B.**2.b** ont montré que la congruence $(a^{25})^g \equiv a \ [7]$ était vérifiée quel que soit l'entier naturel *a*, qu'il soit multiple de 7 ou non.
D'autre part, l'énoncé nous fait admettre que pour tout entier naturel *a* : $(a^{25})^g \equiv a \ [19]$;

En conséquence, le nombre $(a^{25})^g$ est congru à *a* modulo 7 et modulo 19. En vertu du résultat de la **question B.1**, $(a^{25})^g$ est congru à *a* modulo 133.

Quel que soit l'entier naturel *a* : $(a^{25})^g \equiv a \ [133]$.

Partie C.

1. Justifions que $r_1 \equiv a \ [133]$:

NB. Par leurs définitions respectives, *r* apparaît comme étant le reste de la division euclidienne de a^{25} par 133 et r_1 apparaît comme étant le reste de la division euclidienne de r^{13} par 133.

Confrontons les deux congruences dont nous disposons : $\begin{cases} a^{25} \equiv r \ [133] \\ r^{13} \equiv r_1 \ [133] \end{cases}$

Nous en déduisons la congruence : $(a^{25})^{13} \equiv r_1 \ [133]$;

Or, nous avons vu dans la **partie A** du problème que le couple (13, 3) était solution de l'équation (E), car $25 \times 13 - 108 \times 3 = 1$.

Autrement dit, le couple (13, 3) est un « couple (*g, c*) » au sens de la **partie B**, à savoir que $c = 3$ et $g = 13$ sont deux entiers naturels vérifiant la relation $25g - 108c = 1$.

En vertu des résultats de la **partie B** : $(a^{25})^{13} \equiv a \ [133]$.

.

Par transitivité de la relation de congruence modulo 133 :

$$a \equiv r_1 \ [133]$$

.

2. Décodons le message « 128 59 » :

Il s'agit de déterminer quels sont les entiers r_1 lorsque *r* prend les valeurs 128 puis 59.

Autrement dit, il s'agit de déterminer quels sont les restes des divisions euclidiennes de 128^{13} et de 59^{13} par 133.

Compte tenu de la « délicatesse » des calculs, déléguons allègrement les calculs à une calculatrice ou, encore mieux, à un logiciel de calcul formel. Il en est ainsi du logiciel TI-Nspire CAS qui est assez puissant pour traiter ce genre de choses.

Ce logiciel nous apprend (voir copie d'écran) que $128^{13} \equiv 2 \ [133]$ et que $59^{13} \equiv 3 \ [133]$

Le décodage du message « 128 59 » est le message « 2 3 »

NB. Il est possible d'aller plus loin avec le logiciel et de coder puis décoder tous les entiers de 1 à 26. C'est ce qu'exécute l'algorithme « **codecod** » qui renvoie une matrice à 3 lignes, les 26 premiers entiers, en dessous leur codage et en troisième ligne le décodage (copie d'écran page suivante). On constate bien que le décodage redonne exactement dans l'ordre la liste des 26 premiers entiers, ce qui a priori ne semblait pas gagné avec des congruences modulo 133.
On retrouve au passage que 128 et 59 sont les codages des entiers 2 et 3.

$\mathrm{mod}(128^{13},133)$ 2

$\mathrm{mod}(59^{13},133)$ 3

codecod()

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \\ 1 & 128 & 59 & 25 & 54 & 104 & 7 & 8 & 23 & 129 & 11 & 12 & 48 & 98 & 127 & 93 & 24 & 18 & 19 & 20 & 14 & 78 & 44 & 73 & 123 & 26 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \end{bmatrix}$$

Terminé

©L'instruction "mod(x, n)" utilisée ci–contre renvoie le reste de l division euclidienne de x par n. Le logiciel a assez de ressouces pour traiter le cas des puissances 25–èmes des 26 premiers entiers et de lapuissance 13–ème d'un entier comme 128 ou 129.

"codecod" enregistr. effectué

```
Define codecod()=
Prgm
Local a
Define t=newMat(3,26)
For a,1,26
  a→t[1,a]
EndFor
For a,1,26
  mod(a^25,133)→t[2,a]
EndFor
For r,1,26
  mod(t[2,r]^13,133)→t[3,r]
EndFor
Disp t
EndPrgm
```

NB. Le choix d'une congruence modulo 133 offre 132 restes non nuls possibles, nous avons de la marge puisque nous n'en utilisons que 26. Ce choix permettrait de coder, si on le souhaitait, non pas seulement les 26 lettres de l'alphabet mais tous les 128 caractères du code ASCII.