Nouvelle-Calédonie – Décembre 2007 – Série S – Exercice

1. a. Quel est le reste de la division euclidienne de 6^{10} par 11 ? Justifier.

b. Quel est le reste de la division euclidienne de 6^4 par 5 ? Justifier.

c. En déduire que $6^{40} \equiv 1 \left[11\right]$ et que $6^{40} \equiv 1 \left[5\right]$.

d. Démontrer que $6^{40} - 1$ est divisible par 55.

2. Dans cette question, x et y désignent des entiers relatifs.

a. Montrer que l'équation

$$\left(E\right) \qquad 65x - 40y = 1$$

n'a pas de solution.

b. Montrer que l'équation

$$\left(E'\right) \qquad 17x - 40y = 1$$

admet au moins une solution.

c. Déterminer à l'aide de l'algorithme d'Euclide un couple d'entiers relatifs solution de l'équation $\left(E'\right)$.

d. Résoudre l'équation $\left(E'\right)$.

En déduire qu'il existe un unique entier naturel x_0 inférieur à 40 tel que $17x_0 \equiv 1 \left[40\right]$.

3. Pour tout entier naturel a, démontrer que si $a^{17} \equiv b \left[55\right]$ et si $a^{40} \equiv 1 \left[55\right]$ alors $b^{33} \equiv a \left[55\right]$.

Analyse

Théorème de Gauss, petit théorème de Fermat, propriétés de la relation de congruence sont « au programme » de cet exercice d'arithmétique qui propose, classiquement désormais, comme application des résultats intermédiaires un travail de décodage où la calculatrice peut être assez utile …

Résolution

Question 1.a.

On a : $6^2 = 36 = 3\times 11+3 \equiv 3\,[11]$. On en déduit : $6^{10} = \left(6^2\right)^5 \equiv 3^5\,[11]$.

Or : $3^5 = 243 = 11\times 22+1$. Donc $3^5 \equiv 1\,[11]$, d'où : $6^{10} \equiv 1\,[11]$.

Comme $0 \leq 1 < 11$, on en déduit finalement :

Le reste de la division euclidienne de 6^{10} par 11 est égal à 1.

Question 1.b.

On a cette fois : $6^2 = 36 = 7\times 5+1 \equiv 1\,[5]$. On en déduit immédiatement : $6^4 = \left(6^2\right)^2 \equiv 1^2\,[5]$, c'est-à-dire $6^4 \equiv 1\,[5]$.

Comme $0 \leq 1 < 5$, on en déduit finalement :

Le reste de la division euclidienne de 6^4 par 5 est égal à 1.

Question 1.c.

A la question 1.a., on a obtenu : $6^{10} \equiv 1\,[11]$. On en tire : $6^{40} = \left(6^{10}\right)^4 \equiv 1^4\,[11]$ soit $6^{40} \equiv 1\,[11]$.

A la question 1.b., on a obtenu : $6^4 \equiv 1\,[5]$. On en tire : $6^{40} = \left(6^4\right)^{10} \equiv 1^{10}\,[5]$ soit $6^{40} \equiv 1\,[5]$.

Ainsi, on a bien :

$6^{40} \equiv 1\,[11]$ et $6^{40} \equiv 1\,[5]$

Question 1.d.

D'après la question précédente, on a :

- $6^{40} \equiv 1\,[11]$, donc 11 divise $6^{40}-1$;
- $6^{40} \equiv 1\,[5]$, donc 5 divise $6^{40}-1$.

Ainsi, il existe un entier k tel que : $6^{40}-1=11k$. Ainsi 5 divise $11k$. Comme 5 et 11 sont premiers entre eux, le théorème de Gauss nous permet d'affirmer que 5 divise k : $k=5k'$, avec k' entier. Finalement : $6^{40}-1=11\times 5k'=55k'$. Le résultat est établi.

Remarque : les entiers 5 et 11 étant premiers entre eux, on peut aussi directement conclure. Plus généralement rappelons que si chacun des entiers $a_1, a_2, ..., a_n$ divise un entier n donné et que ces entiers sont deux à deux premiers entre eux alors leur produit divise n.

55 divise $6^{40}-1$.

Question 2.a.

On a : $65x-40y=1\Leftrightarrow 5(13x-8y)=1$. Cette égalité ne peut être vérifiée puisque 1 n'est pas un multiple de 5.

L'équation n'admet pas de solutions entières.

Question 2.b.

17 est un nombre premier et 40 n'est pas un multiple de 17 ; On en conclut immédiatement que 17 et 40 sont premier entre eux. D'après le théorème de Bézout, il existe donc deux entiers u et v tels que : $17u+40v=1$. On en tire immédiatement que le couple $(u\,;-v)$ est solution de l'équation (E').

L'équation (E') admet au moins une solution.

Question 2.c.

On a :

$$40=17\times 2+6$$
$$17=6\times 2+5$$
$$6=5\times 1+1$$

On multiplie alors les deux premières lignes, en commençant par la deuxième, par des coefficients entiers appropriés pour se débarrasser des deux premiers restes (6 et 5) :

$$40=17\times 2+6 \quad \times 3$$
$$17=6\times 2+5 \quad \times(-1)$$
$$6=5\times 1+1$$

En additionnant ces trois égalités membres à membres, on obtient alors :

$$3\times 40+(-1)\times 17+\cancel{6}=6\times 17+\cancel{3\times 6}+\cancel{(-2)\times 6}+\cancel{(-1)\times 5}+\cancel{1\times 5}+1$$

Soit : $17\times(-7)-40\times(-3)=1$.
Finalement :

Le couple $(-7\,;-3)$ est solution de l'équation (E').

Question 2.d.

On a, en utilisant l'égalité $17\times(-7)-40\times(-3)=1$ obtenue à la question précédente :

$$17x-40y=1\Leftrightarrow 17x-40y=17\times(-7)-40\times(-3)\Leftrightarrow 17\times(x+7)=40\times(y+3)$$

17 et 40 étant premiers entre eux, le théorème de GAUSS nous permet alors de conclure que 40 divise $x+7$. Il existe donc un entier k tel que $x+7=40k$, soit $x=-7+40k$.
On a alors :

$$17\times(x+7)=40\times(y+3)\Leftrightarrow 17\times 40k=40\times(y+3)\Leftrightarrow y+3=17k\Leftrightarrow y=-3+17k\,.$$

Ainsi, si $(x\,;y)$ est solution de l'équation (E') alors il existe un entier k tel que $x=-7+40k$ et $y=-3+17k$.
Réciproquement, on vérifie aisément que tout couple de la forme $(-7+40k\,;-3+17k)$ où k est un entier est solution de l'équation (E').
Finalement :

L'ensemble des solutions de l'équation (E') est :
$\{(-7+40k\,;-3+17k)\,/\,k\in\mathbb{Z}\}$

On cherche maintenant un entier naturel x inférieur à 40 tel que $17x\equiv 1[40]$.
Pour un tel entier, il existe donc un entier y tel que $17x=1+40y$. Ainsi, le couple $(x\,;y)$ est solution de l'équation (E'). L'entier x est donc, d'après le résultat précédent, de la forme : $-7+40k$. Puisque l'on veut : $0\leq x<40$, il vient :

$$\begin{cases}0\leq x<40\\ x\in\mathbb{N}\end{cases}\Leftrightarrow\begin{cases}0\leq -7+40k<40\\ x\in\mathbb{Z}\end{cases}\Leftrightarrow\begin{cases}7\leq 40k<47\\ x\in\mathbb{Z}\end{cases}$$

Le seul multiple de 40 compris entre 7 (largement) et 47 (strictement) est 40. On a donc $k=1$ et finalement : $x=-7+40\times 1=33$.

L'unique entier naturel x_0 inférieur à 40 et tel que $17x_0\equiv 1[40]$ est 33.

Question 3.

Comme $a^{17} \equiv b\,[55]$ alors $\left(a^{17}\right)^{33} = a^{17\times 33} \equiv b^{33}\,[55]$.

Mais d'après la question précédente, on a : $17\times 33 \equiv 1[40]$, soit $17\times 33 = 1+40k$ k étant un entier naturel (il ne peut être strictement négatif !).

On a donc : $a^{17\times 33} = a^{40k+1} = a^{40k}\times a \equiv b^{33}\,[55]$.

Par ailleurs, on a $a^{40} \equiv 1[55]$. Il vient alors : $\left(a^{40}\right)^{k} = a^{40k} \equiv 1^{k}\,[55]$, soit $a^{40k} \equiv 1[55]$ et enfin $a^{40k}\times a \equiv a\,[55]$.

Finalement, de $a^{40k}\times a \equiv b^{33}\,[55]$ et $a^{40k}\times a \equiv a\,[55]$, on tire immédiatement : $b^{33} \equiv a\,[55]$.

Le résultat est établi.

Pour tout entier naturel *a*, si $a^{17} \equiv b\,[55]$ et si $a^{40} \equiv 1[55]$ alors $b^{33} \equiv a\,[55]$.

Remarque : ce résultat est intéressant mais si la congruence $a^{17} \equiv b\,[55]$ ne constitue pas une contrainte (dès que *a* est donné, on peut trouver une infinité de *b* tels que $a^{17} \equiv b\,[55]$), il en va autrement de $a^{40} \equiv 1[55]$! Existe-t-il un entier naturel *a* tel que $a^{40} \equiv 1[55]$?

On l'aura peut-être oublié à la fin de l'exercice mais l'existence d'un tel entier est établie dans la première question où on a montré : $6^{40} \equiv 1[55]$. Ainsi, $a = 6$ convient !

Avec $a = 6$, on a : $6^3 = 216 \equiv -4\,[55]$ et donc $6^{15} = \left(6^3\right)^5 \equiv (-4)^5\,[55]$, soit $6^{15} \equiv -1\,024\,[55]$.

Mais comme $-1\,024 = -19\times 55 + 21$, on a : $6^{15} \equiv 21[55]$.

Il vient alors : $6^{17} = 6^{15}\times 6^2 \equiv 21\times 36\,[55]$. Comme $21\times 36 = 756 = 13\times 55 + 41$, on obtient finalement : $6^{17} \equiv 41[55]$. Ainsi, avec $a = 6$, on peut prendre : $b = 41$.

On peut alors en déduire : $41^{33} \equiv 6\,[55]$ (et on réfléchira à la taille, plus que respectable, du nombre 41^{33} … ☺).