| CORRECTION DU DEVOIR MAISON N° 8 | |
|---|---|
| ***Division euclidienne, congruences, théorème de Gauss et algorithme d'Euclide*** | ***Pour le 22 janvier 2008*** |

***Nouvelle-Calédonie, novembre 2007***

1) a) $6^{10} = 60466176 = 11 \times 5496925 + 1$ ; alors **le reste de la division euclidienne de $6^{10}$ par 11 est 1**.

b) $6^4 = 1296 = 259 \times 5 + 1$ ; alors **le reste de la division euclidienne de $6^4$ par 5 est 1**.

c) D'après la question 1) a), $6^{10} \equiv 1 \quad [11]$. On en déduit que $\left(6^{10}\right)^4 \equiv 1^4 \quad [11]$ (d'après les propriétés des congruences), c'est-à-dire que $\mathbf{6^{40} \equiv 1 \quad [11]}$.

D'après la question 1) b), $6^4 \equiv 1 \quad [5]$. On en déduit que $\left(6^4\right)^{10} \equiv 1^{10} \quad [5]$ (d'après les propriétés des congruences), c'est-à-dire que $\mathbf{6^{40} \equiv 1 \quad [5]}$.

d) Comme $6^{40} \equiv 1 \quad [11]$, alors $6^{40} - 1$ est divisible par 11 ; de même $6^{40} \equiv 1 \quad [5]$, alors $6^{40} - 1$ est divisible par 5.
Comme 5 et 11 divisent $6^{40} - 1$, et que 5 et 11 sont premiers entre eux, alors leur produit $5 \times 11$ divise $6^{40} - 1$ (corollaire du théorème de Gauss).
Par conséquent, **$6^{40} - 1$ est divisible par 55**.

2) a) Supposons qu'il existe des entiers relatifs a et b tels que $(a \ ; b)$ soit une solution de (*E*).
Alors $65a - 40b = 1$, d'où $5(13a - 8b) = 1$, c'est-à-dire à 5 divise 1 car $13a - 8b$ est un entier ; ce qui est impossible.
Par conséquent, **l'équation (*E*) $65x - 40y = 1$ n'a pas de solution**.

b) Par la méthode l'algorithme d'Euclide, on obtient :

| a | b | reste |
|---|---|---|
| 40 | 17 | 6 |
| 17 | 6 | 5 |
| 6 | 5 | 1 |
| 5 | 5 | 0 |

On en déduit que $\text{PGCD}(17 \ ; 40) = 1$, c'est-à-dire que 17 et 40 sont premiers entre eux.
**D'après le théorème de Bézout, on en déduit que l'équation (*E'*) admet au moins une solution**.

c) En remontant, on a :

$$1 = 6 - 5.$$

Or $5 = 17 - 2 \times 6$ ; alors :

$$1 = 6 - (17 - 2 \times 6) = 3 \times 6 - 17.$$

Or $6 = 40 - 2 \times 17$ ; alors :

$$1 = 3 \times (40 - 2 \times 17) - 17 = (-7) \times 17 - (-3) \times 40.$$

Par conséquent, **le couple $(-7\ ;\ -3)$ est un couple solution de (*E'*)**.

d) • D'après la question précédente, $17x-40y=1$ équivaut à $17x-40y=17\times(-7)-40\times(-3)$, ou encore à $17(x+7)=40\times(y+3)$ (*E''*).

On en déduit que 40 divise $17(x+7)$, et comme 10 et 47 sont premiers entre eux, d'après le théorème de Gauss, 40 divise $x+7$. Il existe donc un entier $k$ tel que $x+7=40k$, c'est-à-dire $x=-7+40k$.

En remplaçant $x$ par $-7+40k$ dans (*E''*), on obtient : $17\times 40k=40\times(y+3)$, soit $y+3=17k$.

Par conséquent, **les couples solutions de (*E'*) sont les couples $(-7+40k\ ;-3+17k)$ avec *k* un entier relatif**.

• Soit $(x_0\ ;\ y_0)$ soit une solution de (*E'*). Alors $17x_0=40y_0+1$, c'est-à-dire que $17x_0\equiv 1\ [40]$.

Or $x_0=-7+40k_0$ et comme $x_0$ est un entier naturel inférieur à 40, alors il faut que $k_0$ soit égal à 1. Dans ce cas, $\boldsymbol{x_0=33}$.

3) Soient $a$ et $b$ deux entiers naturels tels que $a^{17}\equiv b\ [55]$ et si $a^{40}\equiv 1\ [55]$.

D'après la question précédente, $17\times 33\equiv 1\ [40]$, c'est-à-dire que $17\times 33=40q+1$ avec $q$ un entier relatif.

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

Alors $a^{40q+1}\equiv b^{33}\ [55]$, ou encore $\left(a^{40}\right)^{q}\times a\equiv b^{33}\ [55]$.

Or $a^{40}\equiv 1\ [55]$, alors $\left(a^{40}\right)^{q}\times a\equiv 1^{q}\times \mathrm{a}\ [55]$, c'est-à-dire $\left(a^{40}\right)^{q}\times a\equiv \mathrm{a}\ [55]$.

On en déduit alors que $b^{33}\equiv a\ [55]$.

Par conséquent, **pour tout entier naturel *a*, si qu et si $\boldsymbol{a^{40}\equiv 1\ [55]}$, alors $\boldsymbol{b^{33}\equiv a\ [55]}$**.