Nouvelle-Calédonie décembre 2007

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 $6^{40} \equiv 1$ [11] et que $6^{40} \equiv 1$ [5].
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 (E) $65x - 40y = 1$ n'a pas de solution.
b. Montrer que l'équation (E′) $17x - 40y = 1$ admet au moins une solution.
c. Déterminer à l'aide de l'algorithme d'Euclide un couple d'entiers relatifs solution de l'équation (E′).
d. Résoudre l'équation (E′).
En déduire qu'il existe un unique naturel x_0 inférieur à 40 tel que $17x_0 \equiv 1$ [40].
3. Pour tout entier naturel a, démontrer que si $a^{17} \equiv b$ [55] et si $a^{40} \equiv 1$ [55], alors $b^{33} \equiv a$ [55].

CORRECTION

1. *a.*
$6^2 = 36 = 3 \times 11 + 3$ donc $6^2 \equiv 3$ [11]
$6^3 \equiv 3 \times 6$ [11] donc $6^3 \equiv 7$ [11]
$6^4 \equiv 6 \times 7$ [11] donc $6^4 \equiv 9$ [11]
$6^5 \equiv 6 \times 9$ [11] donc $6^5 \equiv -1$ [11]
$6^{10} = (6^5)^2$ donc $6^{10} \equiv (-1)^2$ [11] donc $6^{10} \equiv 1$ [11]
Le reste de la division euclidienne de 6^{10} par 11 est 1.

1. *b.* $6^2 = 36 = 7 \times 5 + 1$ donc $6^2 \equiv 1$ [5] or $6^4 = (6^2)^2$ donc $6^4 \equiv 1$ [5]
Le reste de la division euclidienne de 6^4 par 5 est 1.

1. *c.* $6^{10} \equiv 1$ [11] or $(6^{10})^4 = 6^{40}$ donc $6^{40} \equiv 1$ [11]
de même $6^4 \equiv 1$ [5] or $(6^4)^{10} = 6^{40}$ donc $6^{40} \equiv 1$ [5]

1. *d.* 11 et 5 divisent $6^{40} - 1$ or 11 et 5 sont premiers entre eux donc 11×5 divise $6^{40} - 1$
$6^{40} - 1$ est divisible par 55.

2. *a.* 5 divise 65 et 40 donc 65 et 40 ne sont pas premiers entre eux donc l'équation (E) $65x - 40y = 1$ n'a pas de solution d'après le théorème de Bézout.

2. *b.* 17 et 40 sont premiers entre eux donc, d'après le théorème de Bézout, l'équation (E′) $17x - 40y = 1$ admet au moins une solution.

2. *c.*

	u	v	$17u - 40v$	Quotient
	0	1	-40	
	1	0	17	-3
$L_3 = L_1 + 3L_2$	3	1	11	1
$L_4 = L_2 - L_3$	-2	-1	6	1
$L_5 = L_3 - L_4$	5	2	5	1
$L_6 = L_4 - L_5$	-7	-3	1	5
$L_7 = L_5 - 5L_6$	40	17	0	

donc $17 \times (-7) + 40 \times 3 = 1$ donc le couple $(-7 ; -3)$ est solution de $17x - 40y = 1$

2. *d.* $\begin{cases} 17x - 40y = 1 \\ 17 \times (-7) - 40 \times (-3) = 1 \end{cases}$ donc par différence membre à membre :
$17(x + 7) - 40(y + 3) = 0$
soit $17(x + 7) = 40(y + 3)$ donc 17 divise $40(y + 3)$ or 17 et 40 sont premiers entre eux donc d'après le théorème de Gauss, 17 divise $y + 3$. Il existe un entier relatif k tel que $y + 3 = 17k$ donc en remplaçant dans $17(x + 7) = 40(y + 3)$, $x + 7 = 40k$
donc $y = 17k - 3$ et $x = 40k - 7$
Vérification :
s'il existe un entier relatif k tel que $y = 17k - 3$ et $x = 40k - 7$ alors $17x - 40y = 17 \times 40k - 7 \times 17 - 40 \times 17k + 3 \times 40 = 1$
donc les solutions de (E') sont les couples $(40k - 7 ; 17k - 3)$ avec $k \in \mathbb{Z}$.

Si $17x \equiv 1$ [40], il existe un entier relatif y tel que $17x = 1 + 40y$ donc x est solution de (E') donc il existe un entier relatif k tel que : $x = 40k - 7$

$0 \le x \le 40 \Leftrightarrow 0 \le 40k - 7 \le 40 \Leftrightarrow \dfrac{7}{40} \le k \le \dfrac{47}{40} \Leftrightarrow k = 1$

Il existe un unique naturel x_0 inférieur à 40 tel que $17x_0 \equiv 1$ [40] : $x_0 = 40 - 7 = 33$

3. Si $a^{17} \equiv b$ [55] alors 55 divise $a^{17} - b$ et si $a^{40} \equiv 1$ [55] alors 55 divise $a^{40} - 1$
or $17 \times 33 - 40 \times 14 = 1$ donc $a^{17 \times 33} = b^{33}$ [55] donc $a^{1 + 40 \times 14} \equiv b^{33}$ [55]
or $a^{1 + 40 \times 14} = a^1 \times a^{40 \times 14} = a \times (a^{40})^{14}$ et $a^{40} \equiv 1$ [55], donc $a^{40 \times 33} \equiv 1$ [55] donc $a^{1 + 40 \times 14} \equiv a$ [55] donc $b^{33} \equiv a$ [55].