CORRECTION DE L'EXERCICE DONNÉ DANS LE DEVOIR COMMUN N° 1

Divisibilité, congruences, suites et dérivation	***Le 10 novembre 2007***

1) a) Soient a, b, c et d des entiers relatifs.
Si $a \equiv b \pmod 7$ et $c \equiv d \pmod 7$, alors il existe des entiers relatifs k et k' tels que $a = b + 7k$ et $c = d + 7k'$.
D'où $ac = (b+7k)(d+7k') = bd + 7(k + k' + 7kk') = bd + 7m$ avec $m = k + k' + 7kk'$.
Comme k et k' sont des entiers relatifs, alors m est un entier relatif.
Donc, $ac \equiv bd \pmod 7$.
Par conséquent, **si $a \equiv b \pmod 7$ et $c \equiv d \pmod 7$ alors $ac \equiv bd \pmod 7$**.

b) Soit a et b deux entiers relatifs non nuls tels que $a \equiv b \pmod 7$.
Soit $\mathscr{P}(n)$ la proposition : « pour tout n de $\mathbf{N}$, $a^n \equiv b^n \pmod 7$ »

$\rightarrow$ $a^0 = 1$ et $b^0 = 1$, alors $a^0 \equiv b^0 \pmod 7$; d'où on a $\mathscr{P}(0)$ qui est vraie.

$\rightarrow$ Montrons que pour tout $n \geq 0$, on a : $\mathscr{P}(n) \Rightarrow \mathscr{P}(n+1)$.
Soit $n \geq 0$. Supposons que $\mathscr{P}(n)$ est vraie. Alors : $a^n \equiv b^n \pmod 7$.
Comme $a \equiv b \pmod 7$, d'après la question 1) a), on en conclut que :
$a \times a^n \equiv b \times b^n \pmod 7$, c'est-à-dire $a^{n+1} \equiv b^{n+1} \pmod 7$.
On en déduit que $\mathscr{P}(n+1)$ est vraie.

On a alors prouvé :

$\mathscr{P}(0)$ et pour tout n supérieur ou égal à 0, $\mathscr{P}(n) \Rightarrow \mathscr{P}(n+1)$.

$\rightarrow$ Du principe de raisonnement par récurrence, on déduit :

pour tout n entier naturel, $a^n \equiv b^n \pmod 7$.

Par conséquent, **pour a et b entiers relatifs non nuls si $a \equiv b \pmod 7$ alors pour tout entier naturel n, $a^n \equiv b^n \pmod 7$**.

2) Déterminons les restes de 2^n et 3^n modulo 7 :

n	1	2	3	4	5	6
$2^n \equiv \ldots \pmod 7$	2	4	**1**	2	4	1
$3^n \equiv \ldots \pmod 7$	3	2	6	4	5	**1**

Donc, **le plus petit entier naturel n tel que $2^n \equiv 1 \pmod 7$ est 3, et le plus petit entier naturel n tel que $3^n \equiv 1 \pmod 7$ est 6**.

3) a) Soit a un entier naturel non divisible par 7. Les restes de la division euclidienne de a par sont alors : 1 ; 2 ; 3 ; 4 ; 5 ou 6.
On peut alors écrire que $a \equiv r \pmod 7$ avec $r \in \{1 ; 2 ; 3 ; 4 ; 5 ; 6\}$.
D'après la question 1) b), on en déduit que : $a^6 \equiv r^6 \pmod 7$.

C. Lainé

Or : $1^6 = 1$, alors $1^6 \equiv 1 \pmod 7$;

$2^6 = 64$, alors $2^6 \equiv 1 \pmod 7$ car $64 = 7 \times 9 + 1$;

$3^6 = 729$, alors $3^6 \equiv 1 \pmod 7$ car $729 = 7 \times 104 + 1$;

$4^6 = 4096$, alors $4^6 \equiv 1 \pmod 7$ car $4096 = 7 \times 585 + 1$;

$5^6 = 15625$, alors $5^6 \equiv 1 \pmod 7$ car $15625 = 7 \times 2232 + 1$;

$6^6 = 46656$, alors $6^6 \equiv 1 \pmod 7$ car $46656 = 7 \times 6665 + 1$;

Par conséquent, **si a un entier naturel non divisible par 7, alors $a^6 \equiv 1 \pmod 7$**.

b) • Il existe deux entiers uniques q et r tels que $6 = kq + r$ avec $0 \leq r < k$.

Alors $a^6 = a^{kq+r} = a^{kq} \times a^r = \left(a^k\right)^q \times a^r$.

D'où : $a^6 \equiv 1 \pmod 7$ équivaut à $\left(a^k\right)^q \times a^r \equiv 1 \pmod 7$.

Or $a^k \equiv 1 \pmod 7$, alors $\left(a^k\right)^q \equiv 1^q \pmod 7$ d'après la question 1) b), c'est-à-dire à $\left(a^k\right)^q \equiv 1 \pmod 7$.

D'après la question 1) a), $\left(a^k\right)^q \times a^r \equiv 1 \pmod 7$ équivaut alors à $a^r \equiv 1 \pmod 7$.

Donc $a^6 \equiv 1 \pmod 7$ équivaut à $a^r \equiv 1 \pmod 7$.

Par conséquent, **le reste r de la division euclidienne de 6 par k vérifie $a^r \equiv 1 \pmod 7$**.

• Comme k est le plus petit entier naturel non nul tel que $a^k \equiv 1 \pmod 7$, que $a^r \equiv 1 \pmod 7$ et que $0 \leq r < k$, alors r est égal à 0.
Par suite, ***k* divise 6**.

• On sait que 6 a quatre diviseurs positifs : 1 ; 2 ; 3 et 6.
Par conséquent, **les valeurs possibles de k sont 1 ; 2 ; 3 ou 6**.

c) D'après la question précédente, il suffit de calculer a, a^2, a^3 et a^6 pour chacun des entiers a compris entre 2 et 6.

a	$a^2 \equiv \ldots \pmod 7$	$a^3 \equiv \ldots \pmod 7$	$a^6 \equiv \ldots \pmod 7$	ordre de a
2	4	1	1	**3**
3	2	6	1	**6**
4	2	1	1	**3**
5	4	6	1	**6**
6	1	6	1	**2**

4) $A_{2006} = 2^{2006} + 3^{2006} + 4^{2006} + 5^{2006} + 6^{2006}$.

• $2006 = 3 \times 668 + 2$ (on a choisi de faire la division euclidienne de 2006 par 3 car l'ordre de 2 est 3), alors $2^{2006} = \left(2^3\right)^{668} \times 2^2$.

Or l'ordre de 2 est 3, d'où $2^3 \equiv 1 \pmod 7$; on en déduit que $\left(2^3\right)^{668} \times 2^2 \equiv 2^2 \pmod 7$.

Donc $2^{2006} \equiv 4 \pmod 7$.

- $2006 = 6 \times 334 + 2$ (on a choisi de faire la division euclidienne de 2006 par 6 car l'ordre de 3 est 6), alors $2^{2006} = \left(3^6\right)^{334} \times 3^2$.

Or l'ordre de 3 est 6, d'où $3^6 \equiv 1 \pmod 7$; on en déduit que $\left(3^6\right)^{334} \times 3^2 \equiv 3^2 \pmod 7$.

Donc $3^{2006} \equiv 2 \pmod 7$.

- $2006 = 3 \times 668 + 2$ (on a choisi de faire la division euclidienne de 2006 par 3 car l'ordre de 4 est 3), alors $4^{2006} = \left(4^3\right)^{668} \times 4^2$.

Or l'ordre de 4 est 3, d'où $4^3 \equiv 1 \pmod 7$; on en déduit que $\left(4^3\right)^{668} \times 4^2 \equiv 4^2 \pmod 7$.

Donc $4^{2006} \equiv 2 \pmod 7$.

- $2006 = 6 \times 334 + 2$ (on a choisi de faire la division euclidienne de 2006 par 6 car l'ordre de 5 est 6), alors $5^{2006} = \left(5^6\right)^{334} \times 5^2$.

Or l'ordre de 5 est 6, d'où $5^6 \equiv 1 \pmod 7$; on en déduit que $\left(5^6\right)^{334} \times 5^2 \equiv 5^2 \pmod 7$.

Donc $5^{2006} \equiv 4 \pmod 7$.

- $2006 = 2 \times 1003 + 0$ (on a choisi de faire la division euclidienne de 2006 par 2 car l'ordre de 6 est 2), alors $6^{2006} = \left(6^2\right)^{1003}$.

Or l'ordre de 6 est 2, d'où $6^2 \equiv 1 \pmod 7$; on en déduit que $\left(6^2\right)^{1003} \equiv 1 \pmod 7$.

Donc $6^{2006} \equiv 1 \pmod 7$.

En utilisant la propriété d'addition des congruences, on en déduit que :
$A_{2006} \equiv 4 + 2 + 2 + 4 + 1 \pmod 7$, c'est-à-dire $A_{2006} \equiv 13 \pmod 7$.
Or $13 \equiv 6 \pmod 7$, alors $\boldsymbol{A_{2006} \equiv 6 \pmod 7}$.