

## CORRECTION DU DEVOIR MAISON N° 6

*PGCD et théorème de Bézout*

*Pour le 8 janvier 2008*

1) a) Comme 2003 est un nombre premier, alors 123 et 2003 sont premiers entre eux. Donc il existe deux entiers relatifs  $u$  et  $v$  tels que :  $123u + 2003v = 1$ .

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

a	b	reste
2003	123	35
123	35	18
35	18	17
18	17	1
17	1	0

En remontant, on a :

$$1 = 18 - 17.$$

Or  $17 = 35 - 18$  ; alors :

$$1 = 18 - (35 - 18) = 2 \times 18 - 35.$$

Or  $18 = 123 - 3 \times 35$  ; alors :

$$1 = 2 \times (123 - 3 \times 35) - 35 = 2 \times 123 - 7 \times 35.$$

Or  $35 = 2003 - 16 \times 123$  ; alors :

$$1 = 2 \times 123 - 7 \times (2003 - 16 \times 123) = 114 \times 123 - 7 \times 2003.$$

Donc,  $114 \times 123 - 7 \times 2003 = 1$ .

Par conséquent,  **$u = 114$  et  $v = -7$  sont deux entiers relatifs tels que  $123u + 2003v = 1$ .**

b) D'après la question précédente,  $114 \times 123 = 7 \times 2003 + 1$ , c'est-à-dire, comme 1 est inférieur à 2003, que :  **$123 \times 114 \equiv 1 \pmod{2003}$** .

c) • Supposons que  $123x \equiv 456 \pmod{2003}$  pour tout entier relatif  $x$ .

Par conséquent,  $114 \times 123x \equiv 456 \times 114 \pmod{2003}$

Or  $123 \times 114 \equiv 1 \pmod{2003}$ , alors,  $123 \times 114 \times x \equiv 1 \times x \pmod{2003}$ .

Donc, par transitivité, on obtient :  $x \equiv 456 \times 114 \pmod{2003}$ .

• Réciproquement, supposons que  $x \equiv 456 \times 114 \pmod{2003}$  pour tout entier relatif  $x$ .

Alors  $123x \equiv 123 \times 456 \times 114 \pmod{2003}$ .

Or  $123 \times 114 \equiv 1 \pmod{2003}$ , d'où  $123 \times 114 \times 456 \equiv 456 \pmod{2003}$ .

Par transitivité, on obtient :  $123x \equiv 456 \pmod{2003}$ .

Par conséquent, **pour tout entier relatif  $x$ ,  $123x \equiv 456 \pmod{2003}$  si, et seulement si,  $x \equiv 456k_0 \pmod{2003}$ .**

d) D'après la question précédente, pour tout entier relatif  $x$ ,  $123x \equiv 456 \pmod{2003}$  si, et seulement si,  $x \equiv 456 \times 114 \pmod{2003}$ , c'est-à-dire, si, et seulement si  $x \equiv 51984 \pmod{2003}$ .

Or  $51984 = 25 \times 2003 + 1909$ , c'est-à-dire  $51984 \equiv 1909 \pmod{2003}$ .

Donc,  $123x \equiv 456 \pmod{2003}$  si, et seulement si,  $x \equiv 1909 \pmod{2003}$ .

Par conséquent, **l'ensemble des entiers relatifs  $x$  tels que :  $123x \equiv 456 \pmod{2003}$  est l'ensemble des entiers relatifs  $x$  tels que  $x = 2003q + 1909$  avec  $q \in \mathbf{Z}$ .**

e) D'après la question précédente,  $123n \equiv 456 \pmod{2003}$  si, et seulement si,

$n = 2003q + 1909$  avec  $q \in \mathbf{N}$ .

Or  $1 \leq n \leq 2002$ , d'où  $1 \leq 2003q + 1909 \leq 2002$ .

Donc,  $-1908 \leq 2003q \leq 93$  ou encore  $-\frac{1908}{2003} \leq q \leq \frac{93}{2003}$ . Comme  $q$  est un entier naturel, alors

$q = 0$ .

Par conséquent, **le seul entier  $n$  tel que :  $1 \leq n \leq 2002$  et  $123n \equiv 456 \pmod{2003}$  est 1909.**

2) a) Comme  $a$  est un entier naturel compris entre 1 et 2002, que 2003 est un nombre premier et qu'un nombre premier est premier avec tous les entiers qu'il ne divise pas, alors  $a$  et 2003 sont premiers entre eux.

Par conséquent,  **$\text{PGCD}(a; 2003) = 1$ .**

Comme  $a$  et 2003 sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers  $m$  et  $v$  tels que  $am + 2003v = 1$ .

D'où,  $am = 1 + 2003 \times (-v)$ .

Comme  $(-v)$  est un entier, alors  $am \equiv 1 \pmod{2003}$ .

Par conséquent, **il existe un entier  $m$  tel que :  $am \equiv 1 \pmod{2003}$ .**

b) • Si  $ax \equiv b \pmod{2003}$ , alors  $amx \equiv mb \pmod{2003}$ .

Or  $am \equiv 1 \pmod{2003}$ , d'où  $amx \equiv x \pmod{2003}$ .

Par transitivité, on obtient :  $x \equiv mb \pmod{2003}$ .

Réciproquement, si  $x \equiv mb \pmod{2003}$ , alors  $ax \equiv amb \pmod{2003}$ .

Or  $am \equiv 1 \pmod{2003}$ , d'où  $amb \equiv b \pmod{2003}$ .

Par transitivité, on obtient :  $ax \equiv b \pmod{2003}$ .

Par conséquent,  **$ax \equiv b \pmod{2003}$  équivaut à  $x \equiv mb \pmod{2003}$ .**

• Soit  $r$  le reste de la division euclidienne de  $mb$  par 2003. Alors,  $bm \equiv r \pmod{2003}$ .

Par transitivité, on en déduit que  $x \equiv r \pmod{2003}$ .

De ce qui précède, on en déduit que  $ax \equiv b \pmod{2003}$  équivaut à  $x = r + 2003q$  avec  $q \in \mathbf{Z}$

Or  $0 \leq x \leq 2002$ , alors  $0 \leq r + 2003q \leq 2002$ .

D'où  $-\frac{r}{2003} \leq q \leq \frac{2002}{2003}$ .

Or  $0 \leq r < 2003$ , d'où  $-\frac{r}{2003} > -1$ , et,  $\frac{2002}{2003} < 1$ .

Donc,  $-1 < q < 1$ . Comme  $q$  est un entier, alors  $q = 0$ , c'est-à-dire  $x = r$  et  $r$  est unique.

Par conséquent, **pour tout entier  $b$ , il existe un unique entier  $x$  tel que :  $0 \leq x \leq 2002$  et  $ax \equiv b \pmod{2003}$ .**