Lycée J.P Vernant — Année scolaire 2010-2011
spéTS — Mathématiques

CORRECTION DU DEVOIR A LA MAISON N° 7

SUJET (a)

Exercice 1 :

1. (a) • On suppose que $3x \equiv 5$ [7] et $5 \equiv 12$ [7] (car 7 divise $5-12=-7$) donc $3x \equiv 12$ [7]. On en déduit que 7 divise $3x-12=3(x-4)$. Comme $PGCD(7,3)=1$ (car 3 et 7 sont premiers distincts) on peut utiliser le théorème de Gauss d'où 7 divise $(x-4)$. Cela signifie $x \equiv 4$ [7].

• On suppose que $x \equiv 4$ [7] donc $3x \equiv 12$ [7]. Or, on a justifié que $12 \equiv 5$ [7] d'où $3x \equiv 5$ [7].

Finalement, $3x \equiv 5$ [7] $\Leftrightarrow$ $x \equiv 4$ [7]

(b) On suppose que $ax \equiv 0$ [7] avec $a \in A_7$. Alors 7 divise ax. Comme $a \in A_7$, alors a est un strictement inférieur à 7 et non nul donc a n'est pas un multiple de 7. Vu que a est premier, cela implique que a et 7 sont premiers entre eux. D'après le théorème de Gauss, 7 divise x, ce qui signifie que x est un multiple de 7.

Réciproquement, si x est un multiple de 7, alors $x \equiv 0$ [7] donc $ax \equiv 0$ [7].

Finalement, les seules solutions de $ax \equiv 0$ [7] sont les multiples de 7.

2. (a) Comme a est dans A_p, c'est un nombre strictement inférieur à p et non nul donc il ne peut pas être un multiple de p. Vu que p est premier, cela implique que $PGCD(a\,;p)=1$. On peut alors utiliser le petit théorème de Fermat (p est premier, a et p sont premiers entre eux) pour affirmer que $a^{p-1} \equiv 1$ [p], c'est-à-dire que $a \times (a^{p-2}) \equiv 1$ [p]. Cela signifie que a^{p-2} est une solution de l'équation $ax \equiv 1$ [p].

(b) Si r est le reste de la division euclidienne de a^{p-2} par p, alors $r \equiv a^{p-2}$ [p]. Ainsi, $ar \equiv a \times a^{p-2}$ [p], c'est-à-dire que $ar \equiv a^{p-1}$ [p]. On a montré que $a^{p-1} \equiv 1$ [p] donc $ar \equiv 1$ [p] par transitivité. Cela signifie que r est solution de $ax \equiv 1$ [p]. De plus, $r \in A_p$ car par définition d'un reste dans une division euclidienne, $0 \leqslant r < p$ et $r \neq 0$ car p ne peut pas diviser a^{p-2} (en effet si c'était le cas, p apparaîtrait dans la décomposition en facteurs premiers de a^{p-2} et donc dans celle de a ; ce qui n'est pas le cas puisque $a < p$).

On suppose que b est une autre solution de $ax \equiv 1$ [p] tel que $b \in A_p$. Alors $ab \equiv ar$ [p] d'où $a(b-r) \equiv 0$ [p]. D'après la question 1b), on en déduit que $b-r$ est un multiple de p. Or, $1 \leqslant b < p$ et $1 \leqslant r < p$ donc $-p < -r \leqslant -1$ et donc par addition membre à membre $-p+1 < b-r < p-1$ donc $-(p-1) < b-r < p-1$. Le seul multiple de p de cet encadrement est 0 donc $b-r=0$ et $b=r$. Cela justifie que r est l'unique solution de $ax \equiv 1$ [p] dans A_p.

(c) • On suppose que $xy \equiv 0$ [p]. Alors p divise xy. Soit p divise x ; soit p ne divise pas x et dans ce cas là, $PGCD(p\,;x)=1$ (puisque p et premier) d'où p divise y d'après le théorème de Gauss. Finalement, x est multiple de p ou y est un multiple de p.

• On suppose que x est un multiple de p ou y est un multiple de p. Si x est un multiple de p, alors p divise x. Comme $y \in \mathbb{Z}$, alors x divise xy donc p divise xy par transitivité. Ainsi, $xy \equiv 0$ [p]. Le raisonnement est analogue si c'est y qui est un multiple de p.

Finalement, $xy \equiv 0$ [p] si et seulement si x est un multiple de p ou y est un multiple de p.

(d) D'après la question 2b) (31 est premier et 2 est un élément de A_{31}), l'unique solution dans A_{31} de $2x \equiv 1$ [31] est le reste de la division euclidienne de 2^{29} par 31. Or, $2^5 = 32 \equiv 1$ [31] et $29 = 5 \times 5 + 4$ donc $2^{29} = (2^5)^5 \times 2^4 \equiv 1^5 \times 2^4$ [31] soit $2^{29} \equiv 16$ [31]. Ainsi, 16 est l'unique solution de $2x \equiv 1$ [31] dans A_{31}.

D'après la question 2b) (31 est premier et 3 est un élément de A_{31}), l'unique solution dans A_{31} de $3x \equiv 1$ [31] est le reste de la division euclidienne de 3^{29} par 31. Or, $3^3 = 27 \equiv -4$ [31] et $29 = 3 \times 9 + 2$ donc $3^{29} = (3^3)^9 \times 3^2 \equiv (-4)^9 \times 9$ [31].

Comme $(-4)^9 = -(2^2)^9 = -2^{18} = -2^{5\times3+3} = -(2^5)^3 \times 2^3$ alors $3^{29} \equiv -1^3 \times 8 \times 9$ [31] soit $3^{29} \equiv -72$ [31]. Or, $-72 = -3 \times 31 + 21$ alors $3^{29} \equiv 21$ [31]. L'unique solution de $3x \equiv 1$ [31] dans A_{31} est 21.

$P(x) = 6x^2 - 5x + 1$ admet pour discriminant $\Delta = 25 - 4 \times 6 = 1$ donc ce polynôme a deux racines : $x_1 = \dfrac{5-1}{12} = \dfrac{1}{3}$ et $x_2 = \dfrac{5+1}{12} = \dfrac{1}{2}$.
Ainsi $P(x) = 6(x - \dfrac{1}{3})(x - \dfrac{1}{2}) = 3(x - \dfrac{1}{3}) \times 2(x - \dfrac{1}{2}) = (3x-1)(2x-1)$.

Par conséquent, $6x^2 - 5x + 1 \equiv 0$ [31] $\Leftrightarrow$ $(3x-1)(2x-1) \equiv 0$ [31]. D'après la question 2c), cette congruence équivaut à $3x - 1 \equiv 0$ [31] ou $2x - 1 \equiv 0$ [31] soit $2x \equiv 1$ [31] ou $3x \equiv 1$ [31].

- On a justifié que $x_0 = 16$ est solution de $2x \equiv 1$ [31]. Si x est solution de $2x \equiv 1$ [31] alors $2x \equiv 2x_0$ [31] donc $2(x - x_0) \equiv 0$ [31]. Comme 31 divise $2(x - x_0)$ et que $PGCD(2\,;31) = 1$ (car 31 est impair), alors 31 divise $x - x_0$ d'après le théorème de Gauss donc il existe $k \in \mathbb{Z}$ tel que $x = x_0 + 31k = 16 + 31k$.

  Réciproquement, si $x = 16 + 31k$ avec $k \in \mathbb{Z}$, alors $x \equiv 16$ [31] donc $2x \equiv 32$ [31] soit $2x \equiv 1$ [31] par transitivité.
- On a justifié que $y_0 = 21$ est solution de $3x \equiv 1$ [31]. Si x est solution de $3x \equiv 1$ [31] alors $3x \equiv 3y_0$ [31] donc $3(x - y_0) \equiv 0$ [31]. Comme 31 divise $3(x - y_0)$ et que $PGCD(3\,;31) = 1$ (car 3 n'est pas multiplie du nombre premier 31), alors 31 divise $x - y_0$ d'après le théorème de Gauss donc il existe $k' \in \mathbb{Z}$ tel que $x = y_0 + 31k' = 21 + 31k'$.

  Réciproquement, si $x = 21 + 31k'$ avec $k' \in \mathbb{Z}$, alors $x \equiv 21$ [31] donc $3x \equiv 63$ [31] soit $3x \equiv 1$ [31] puisque $63 = 2 \times 31 + 1$.

L'ensemble des solutions est $\mathcal{S} = \{16 + 31k\,;\, 21 + 31k\,;\, k \in \mathbb{Z}\}$.

Exercice 2 :

1. (a) $363 = 3 \times 121 = 3 \times 11^2$ et $484 = 4 \times 121 = 2^2 \times 11^2$.
   Ainsi, $PGCD(363\,,\,484) = PGCD(3 \times 11^2\,,\,2^2 \times 11^2) = 11^2 = 121$.

   (b) $484 - 363 = 121 = PGCD(363\,,\,484)$ et $363 < 484$ donc le couple d'entiers naturels non nuls $(363\,,\,484)$ appartient à S.

2. Comme $(n+1) - n = 1$, on a trouve un couple $(u\,,\,v) = (-1\,,\,1)$ tel que $un + v(n+1) = 1$. D'après la réciproque du théorème de Bézout, on en déduit que $PGCD(n\,,\,n+1) = 1$. On sait que n et $n+1$ sont des entiers naturels non nuls, $n < n+1$ et $PGCD(n\,,\,n+1) = (n+1) - n$ donc $(n\,,\,n+1) \in S$.

3. (a) - Supposons que $(x\,,\,y)$ appartient à S. Comme $PGCD(x\,,\,y) = y - x$, les nombres x et y sont divisibles par $y - x$. Il existe donc k et k' entiers naturels non nuls tels que $x = (y-x)k$ et $y = (y-x)k'$. On obtient : $y - x = (y-x)k' - (y-x)k = (y-x)(k'-k)$ donc $k' - k = \dfrac{y-x}{y-x} = 1$ ($y - x \neq 0$ car $y > x$) soit $k' = k + 1$. Ainsi, $x = k(y-x)$ et $y = (k+1)(y-x)$.
   - Réciproquement, on suppose qu'il existe un entier naturel k non nul tel qu'on puisse écrire $x = k(y-x)$ et $y = (k+1)(y-x)$. Alors

   $$PGCD(x\,,\,y) = PGCD\left(k(y-x)\,,\,(k+1)(y-x)\right) = |y-x|PGCD(k\,,\,k+1)$$

   Les entiers naturels non nuls x et y vérifient $x < y$ par hypothèse donc $|y - x| = y - x$. De plus, $PGCD(k\,,\,k+1) = 1$ d'après 2. Par conséquent, $PGCD(x\,,\,y) = y - x$. On en déduit que $(x\,,\,y) \in S$.

   Finalement, $(x\,,\,y) \in S$ si et seulement s'il existe k entier naturel non nul tel que $x = k(y-x)$ et $y = (k+1)(y-x)$.

   (b) Pour tout couple $(x\,,\,y) \in S$,

   $$PPCM(x\,,\,y) = PPCM\left(k(y-x)\,,\,(k+1)(y-x)\right) = (y-x)PPCM(k\,,\,k+1)$$

D'après la question 2, les nombres k et $k+1$ sont premiers entre eux, donc

$$PPCM(k\,,\,k+1) = \frac{k(k+1)}{PGCD(k\,,\,k+1)} = k(k+1)$$

Ainsi, $PPCM(x\,,\,y) = k(k+1)(y-x)$

4. (a) $228 = 2{\times}114 = 2^2{\times}57 = 2^2{\times}3{\times}19$. Le nombre 228 a donc $(2{+}1)(1{+}1)(1{+}1) = 3{\times}4 = 12$ diviseurs positifs. Ce sont les nombres de l'ensemble $D^+(228) = \{1\,,\,2\,,\,3\,,\,4\,,\,6\,,\,12\,,\,19\,,\,38\,,\,57\,,\,76\,,\,114\,,\,228\}$.

   (b) Si $(x\,,\,y) \in S$, $PPCM(x\,,\,y) = k(k+1)(y-x)$. On cherche donc à écrire le nombre 228 sous la forme $k(k+1)(y-x)$ avec $k \in \mathbb{N}^*$. Le nombre k correspond donc à un diviseur positif de 228.
   - Si $k = 1$, alors $k+1 = 2$ et $y - x = 114$. Or, k est défini par la relation $x = k(y-x)$ d'après 3.a) donc $x = 114$ et $y = 228$. Comme $x = 1 \times (y-x)$ et $y = 2 \times (y-x)$, d'après 3.a), le couple $(114\,,\,228)$ appartient à S. De plus, $PPCM(114\,,\,228) = 114\,PPCM(1\,,\,2) = 114 \times 2 = 228$.
   - Si $k = 2$, alors $k+1 = 3$ et $y - x = \dfrac{228}{6} = 38$. Ainsi, $x = k(y-x) = 2 \times 38 = 76$ et $y = (k+1)(y-x) = 3 \times 38 = 114$. D'après la question 3.a), $(x\,,\,y) \in S$.
     De plus, $PPCM(76\,,\,114) = 38\,PPCM(2\,,\,3) = 38 \times 2 \times 3 = 228$.
   - Si $k = 3$, alors $k+1 = 4$ puis $y - x = \dfrac{228}{12} = 19$. De plus, $x = 19 \times 3 = 57$ et $y = 4 \times 19 = 76$.
     D'après la question 3.a), $(x\,,\,y) \in S$. De plus, $PPCM(57\,,\,79) = 19\,PPCM(3\,,\,4) = 19 \times 3 \times 4 = 228$.
   - Si $k = 4, 6, 12, 19, 38, 57, 76, 114$ ou 228, alors $k+1$ ne fait pas partie des diviseurs de 228. On ne peut donc pas écrire 228 sous la forme $k(k+1)(y-x)$. Ces cas sont à exclure.