ENONCE

1. On considère l'ensemble $A_7 = \{1 ; 2 ; 3 ; 4 ; 5 ; 6\}$

a. Pour tout élément a de A_7 écrire dans le tableau figurant en annexe l'unique élément y de A_7 tel que $a\,y \equiv 1$ (modulo 7).

b. Pour x entier relatif, démontrer que l'équation $3\,x \equiv 5$ (modulo 7) équivaut à $x \equiv 4$ (modulo 7).

c. Si a est un élément de A_7, montrer que les seuls entiers relatifs x solutions de l'équation $a\,x \equiv 0$ (modulo 7) sont les multiples de 7.

2. Dans toute cette question, p est un nombre premier supérieur ou égal à 3.

On considère l'ensemble $A_p = \{1 ; 2 ; ... ; p - 1\}$ des entiers naturels non nuls et strictement inférieurs à p.

Soit a un élément de A_p.

a. Vérifier que a^{p-2} est une solution de l'équation $a\,x \equiv 1$ (modulo p).

b. On note r le reste dans la division euclidienne de a^{p-2} par p. Démontrer que r est l'unique solution x dans A_p, de l'équation $a\,x \equiv 1$ (modulo p).

c. Soient x et y deux entiers relatifs. Démontrer que $x\,y \equiv 0$ (modulo p) si et seulement si x est un multiple de p ou y est un multiple de p.

d. Application : $p = 31$. Résoudre dans A_{31} les équations : $2\,x \equiv 1$ (modulo 31) et $3\,x \equiv 1$ (modulo 31).

À l'aide des résultats précédents, résoudre dans $\mathbb{Z}$ l'équation $6\,x^2 - 5\,x + 1 \equiv 0$ (modulo 31).

Annexe :

a	1	2	3	4	5	6
y						6

CORRECTION

1. *a.* $4 \times 2 = 8$ donc $4 \times 2 \equiv 1$ (modulo 7)

$3 \times 5 = 15 = 2 \times 7 + 1$ donc $3 \times 5 \equiv 1$ (modulo 7)

$6 \times 6 = 36 = 7 \times 5 + 1$ donc $6 \times 6 \equiv 1$ (modulo 7)

a	1	2	3	4	5	6
y	1	4	5	2	3	6

b. $3\,x \equiv 5$ (modulo 7) $\Leftrightarrow 5 \times 3\,x \equiv 5 \times 5$ (modulo 7) or $15 \equiv 1$ (modulo 7) et $25 = 3 \times 7 + 4$ donc $25 \equiv 4$ (modulo 7)

$3\,x \equiv 5$ (modulo 7) $\Leftrightarrow x \equiv 4$ (modulo 7)

c. Si $a = 1$, $a\,x \equiv 0$ (modulo 7) $\Leftrightarrow x \equiv 0$ (modulo 7) $\Leftrightarrow x$ entier relatif multiple de 7

Si $a = 2$, $a\,x \equiv 0$ (modulo 7) $\Leftrightarrow 2\,x \equiv 0$ (modulo 7) $\Leftrightarrow 4 \times 2\,x \equiv 4 \times 0$ (modulo 7) $\Leftrightarrow x \equiv 0$ (modulo 7) $\Leftrightarrow x$ entier relatif multiple de 7

Si $a = 3$, $a\,x \equiv 0$ (modulo 7) $\Leftrightarrow 3\,x \equiv 0$ (modulo 7) $5 \times 3\,x \equiv 0$ (modulo 7) $\Leftrightarrow x \equiv 0$ (modulo 7) $\Leftrightarrow x$ entier relatif multiple de 7

Si $a = 4$, $a\,x \equiv 0$ (modulo 7) $\Leftrightarrow 4\,x \equiv 0$ (modulo 7) $\Leftrightarrow 2 \times 4\,x \equiv 0$ (modulo 7) $\Leftrightarrow x \equiv 0$ (modulo 7) $\Leftrightarrow x$ entier relatif multiple de 7

Si $a = 5$, $a\,x \equiv 0$ (modulo 7) $\Leftrightarrow 5\,x \equiv 0$ (modulo 7) $\Leftrightarrow 3 \times 5\,x \equiv 0$ (modulo 7) $\Leftrightarrow x \equiv 0$ (modulo 7) $\Leftrightarrow x$ entier relatif multiple de 7

Si $a = 6$, $a\,x \equiv 0$ (modulo 7) $\Leftrightarrow 6\,x \equiv 0$ (modulo 7) $\Leftrightarrow 6 \times 6\,x \equiv 0$ (modulo 7) $\Leftrightarrow x \equiv 0$ (modulo 7) $\Leftrightarrow x$ entier relatif multiple de 7

Si a est un élément de A_7, les seuls entiers relatifs x solutions de l'équation $a\,x \equiv 0$ (modulo 7) sont les multiples de 7.

2. *a.* p est un nombre premier, $1 \leq a \leq p - 1$ donc p et a sont premiers entre eux donc d'après le petit théorème de Fermat, $a^{p-1} \equiv 1$ (modulo p)

soit $a \times a^{p-2} \equiv 1$ (modulo p) donc a^{p-2} est une solution de l'équation $a\,x \equiv 1$ (modulo p).

b. r est le reste dans la division euclidienne de a^{p-2} par p, donc $0 \leq r < p$

p et a sont premiers entre eux donc p ne divise pas a donc $r \neq 0$ donc $1 \leq r \leq p - 1$ donc $r \in A_p$

$a^{p-2} = p\,q + r$ donc $a \times a^{p-2} = a\,p\,q + a\,r$ donc $a \times a^{p-2} \equiv a\,r$ (modulo p)

donc a^{p-2} étant solution de l'équation $a\,x \equiv 1$ (modulo p), $a\,r \equiv 1$ (modulo p) donc r est solution de l'équation $a\,x \equiv 1$ (modulo p).

Supposons qu'il existe une seconde solution r' appartenant à A_p de l'équation $a\,x \equiv 1$ (modulo r)

$a\,r \equiv 1$ (modulo p) et $a\,r' \equiv 1$ (modulo p) donc par différence membre à membre : $a\,(r - r') \equiv 0$ (modulo p) donc p divise $a\,(r - r')$

p et a sont premiers entre eux donc d'après le théorème de Gauss p divise $r - r'$

or $|\,r - r'\,| < p$ donc si $r - r' \neq 0$ alors $r - r'$ et p sont premiers entre eux, ce qui n'est pas possibles donc $r - r' = 0$

donc r est l'unique solution x dans A_p, de l'équation $a\,x \equiv 1$ (modulo p).

c. Soient x et y deux entiers relatifs, soient r et r' les restes respectifs de la division de x et y par p

Si x est un multiple de p alors $x \equiv 0$ (modulo p) donc $x\,y \equiv 0$ (modulo p)

de même si y est un multiple de p

Si ni x ni y ne sont des multiples de p alors r et r' de A_p et $x \equiv r$ (modulo p) et $y \equiv r'$ (modulo p) alors $x\,y \equiv r\,r'$ (modulo p)
$x\,y \equiv 0$ (modulo p) $\Leftrightarrow r\,r' \equiv 0$ (modulo p) $\Leftrightarrow p$ divise $r\,r'$
$1 \leq r \leq p - 1$ donc r et p sont premiers entre eux donc d'après le théorème de Gauss, p divise r'
or $1 \leq r' \leq p - 1$ donc r' et p sont premiers entre eux donc il est impossible que $r\,r' \equiv 0$ (modulo p)
$x\,y \equiv 0$ (modulo p) si et seulement si x est un multiple de p où y est un multiple de p.

d. Deux méthodes : l'une basique :
D'après la question 2. *a*., si p est un nombre premier, l'équation a $x \equiv 1$ (modulo p) admet une unique solution dans A_p or 31 est un nombre premier donc $2\,x \equiv 1$ (modulo 31) admet une unique solution dans A_{31}
or $2 \times 16 = 31 + 1$ donc $2 \times 16 \equiv 1$ (modulo 31)
donc $x = 16$ est solution dans A_{31} de $2\,x \equiv 1$ (modulo 31)

de même $3\,x \equiv 1$ (modulo 31) admet une unique solution dans A_{31}
$3 \times 21 = 63 = 2 \times 31 + 1$ donc $3 \times 21 \equiv 1$ (modulo 31)
donc $x = 21$ est solution dans A_{31} de $3\,x \equiv 1$ (modulo 31)

Autre méthode utilisant plus l'énoncé.
Si p est un nombre premier et $a \in A_p$, a^{p-2} est solution de l'équation a $x \equiv 1$ (modulo p), donc ici 2^{29} est solution de l'équation $2\,x \equiv 1$ (modulo 31), et 3^{29} est solution de l'équation $3\,x \equiv 1$ (modulo 31).
D'après la question 2. *b*. si p est un nombre premier, si r le reste dans la division euclidienne de a^{p-2} par p alors r est l'unique solution x dans A_p, de l'équation a $x \equiv 1$ (modulo p).
donc 31 étant un nombre premier, le reste de la division de 2^{29} par 31 est l'unique solution x dans A_{31}, de l'équation $2\,x \equiv 1$ (modulo 31).
de même le reste de la division de 3^{29} par 31 est l'unique solution x dans A_{31}, de l'équation $3\,x \equiv 1$ (modulo 31).
$2^{29} \equiv 16$ (modulo 31) et $2^{29} \equiv 21$ (modulo 31) donc les solutions dans A_{31} de $2\,x \equiv 1$ (modulo 31) et de $3\,x \equiv 1$ (modulo 31) sont respectivement 16 et 21.

À l'aide des résultats précédents, résoudre dans $\mathbb{Z}$ l'équation $6\,x^2 - 5\,x + 1 \equiv 0$ (modulo 31).

Or $6\,x^2 - 5\,x + 1 = (2\,x - 1)(3\,x - 1)$
D'après la question 2. *c*. p étant un nombre premier, $x\,y \equiv 0$ (modulo p) si et seulement si x est un multiple de p ou y est un multiple de p
$(2\,x - 1)(3\,x - 1) \equiv 0$ (modulo 31) $\Leftrightarrow 2\,x - 1 \equiv 0$ (modulo 31) ou $3\,x - 1 \equiv 0$ (modulo 31)
$\Leftrightarrow 2\,x \equiv 1$ (modulo 31) ou $3\,x \equiv 1$ (modulo 31)
$\Leftrightarrow 16 \times 2\,x \equiv 16$ (modulo 31) ou $21 \times 3\,x \equiv 21$ (modulo 31)
$\Leftrightarrow x \equiv 16$ (modulo 31) ou $x \equiv 21$ (modulo 31)
$\Leftrightarrow x = 31\,k + 16$ ou $x = 31\,k + 21$ avec $k \in \mathbb{Z}$