1 *Les cinq questions sont indépendantes.*
Pour chaque question une affirmation est proposée. Indiquer si elle est vraie ou fausse, en justifiant la réponse. Une réponse non justifiée ne sera pas prise en compte.
Toute justification complète sera valorisée.

Question 1
On considère l'équation (E) : $2x + 11y = 7$, où x et y sont des entiers relatifs.
Affirmation
Les seuls couples solutions de (E) sont les couples $(22k-2\ ;\ -4k+1)$, avec k appartenant à l'ensemble $\mathbb{Z}$ des entiers relatifs.

Question 2
On considère l'entier $N = 11^{2\,011}$.
Affirmation
L'entier N est congru à 4 modulo 7.

Question 3
a et b sont deux entiers relatifs quelconques, n et p sont deux entiers naturels premiers entre eux.
Affirmation
$a \equiv b\ (p)$ si et seulement si $na \equiv nb\ (p)$.
Question 4 *Affirmation :* Si un entier naturel n est congru à 1 modulo 7 alors le PGCD de $3n+4$ et de $4n+3$ est égal à 7.
Question 5 Soient a et b deux entiers naturels.
Affirmation : S'il existe deux entiers relatifs u et v tels que $au + bv = 2$ alors le PGCD de a et b est égal à 2.

2

1. On considère l'ensemble $\mathrm{A}_7 = \{1\ ;\ 2\ ;\ 3\ ;\ 4\ ;\ 5\ ;\ 6\}$
   a) Pour tout élément a de A_7 écrire dans le tableau figurant en annexe 2 l'unique élément y de A_7 tel que $ay \equiv 1 \pmod 7$.
   b) Pour x entier relatif, démontrer que l'équation $3x \equiv 5 \pmod 7$ équivaut à $x \equiv 4 \pmod 7$.
   c) Si a est un élément de A_7, montrer que les seuls entiers relatifs x solutions de l'équation $ax \equiv 0 \pmod 7$ sont les multiples de 7.
2. Dans toute cette question, p est un nombre premier supérieur ou égal à 3. On considère l'ensemble $\mathrm{A}_p = \{1\ ;\ 2\ ;\ \ldots\ ;\ p-1\}$ 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 $ax \equiv 1 \pmod p$.
   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 $ax \equiv 1 \pmod p$.
   c) Soient x et y deux entiers relatifs. Démontrer que $xy \equiv 0 \pmod p$ si et seulement si x est un multiple de p où y est un multiple de p.
   d) Application : $p = 31$. Résoudre dans A_{31} les équations : $2x \equiv 1 (\text{modulo} 31)$ et $3x \equiv 1 \pmod{31}$.
   À l'aide des résultats précédents, résoudre dans $\mathbb{Z}$ l'équation $6x^2 - 5x + 1 \equiv 0 \pmod{31}$.

DS 5 - Spé

I ① L'affirmation est fausse.

en effet le couple $(9,-1)$ est solution car $2\times(9)+11\times(-1)=7$

mais pourtant $(9,-1)$ ne fait pas partie des solutions données

car il n'existe pas $k\in\mathbb{Z}$ avec $\begin{cases} 9 = 22k-2 \\ -1 = -4k+1 \end{cases}$

② $N = 11^{2011} \equiv 4^{2011}\ (7)$

et $4^2 = 16 \equiv 2\ (7)$

$4^3 \equiv 8 \equiv 1\ (7)$.

or $2011 = 2010 + 1$ et 2010 multiple de 3 par critère $\Rightarrow 2010 = 3\times K$

d'où $N \equiv 4^{2011}\ (7)$

$\equiv 4^{3K+1} \equiv (4^3)^K \times 4 \equiv 4\ (7)$

L'affirmation est vraie

③ $a \equiv b\ (p) \Rightarrow na \equiv nb\ (p)$ par compatibilité des congruences avec le produit.

Réciproquement, si $na \equiv nb\ (p)$

alors $n(a-b) = kp$ pour $k\in\mathbb{Z}$

d'où $n \mid kp$ et $n \wedge p = 1$ donc d'après le th de Gauss $n \mid k$

et donc il existe $k'\in\mathbb{Z}$ tel que $k = k'n$.

On déduit $n(a-b) = nk'p$ et donc $a-b = k'p$

$\Rightarrow a \equiv b\ (p)$.

L'affirmation est vraie

④ $4n+3 = 3n+4 + n-1$

d'où $(4n+3) \wedge (3n+4) = (3n+4) \wedge (n-1)$

et $\begin{array}{r|l} 3n+4 & n+1 \\ 3n-3 & \hline 3 \\ \hline 7 & \end{array}$ d'où $3n+4 = 3(n+1)+7$

et donc $(3n+4) \wedge (n-1) = (n-1) \wedge 7$

finalement $(4n+3) \wedge (3n+4) = (n-1) \wedge 7$

et donc si $n-1$ multiple de 7 le pgcd vaut 7

donc si $n-1 \equiv 0\ (7)$, c.à.d $n \equiv 1\ (7)$ alors le PGCD vaut 7

L'affirmation est vraie.

⑤ L'affirmation est fausse.

En effet $3 \wedge 2 = 1$ donc il existe $u, v \in \mathbb{Z}$ tels que

$3u + 2v = 1$ d'après le Th de Bezout

et par produit par 2 on déduit $3 \times 2u + 2 \times 2v = 2$

c'est-à-dire $3u' + 2v' = 2$

pourtant $3 \wedge 2 \neq 2$!!

II

① @ On essaye (de tête) de trouver l'inverse de chaque élément de A_7.

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

Rq: Si 2 inverse de 4 alors $2 \times 4 \equiv 1\ (7)$ et donc on a 4 inverse de 2 !

ⓑ $3x \equiv 5\ (7) \Rightarrow 5 \times 3x \equiv 5 \times 5\ (7)$ (par produit)

$\Rightarrow x \equiv 4\ (7)$.

Réciproquement si $x \equiv 4\ (7)$ alors par produit $3x \equiv 12\ (7)$

$\Leftrightarrow 3x \equiv 5\ (7)$

(c) $ax \equiv 0\ (7)$

$\iff 7 \mid ax$ et $a \in A_7$ avec 7 premier donc $a \wedge 7 = 1$

Donc $\left.\begin{array}{l} 7 \mid ax \\ 7 \wedge a = 1 \end{array}\right\}$ Th de Gauss $\Rightarrow$ $7 \mid x$ d'où $x \equiv 0\ (7)$

donc x multiple de 7.

Réciproquement si x multiple de 7, on a clairement $ax \equiv 0\ (7)$

donc finalement $ax \equiv 0\ (7) \iff x$ multiple de 7.

(2) (a) p est un nombre premier qui ne divise pas a car $a \in A_p = \{1, \dots p-1\}$

donc d'après le petit th de Fermat $a^{p-1} \equiv 1\ (p)$

d'où $a \times a^{p-2} \equiv 1\ (p)$ c'est-à-dire a^{p-2} solution de l'éq $ax \equiv 1\ (p)$

(b) La division euclidienne de a^{p-2} par p donne

$a^{p-2} = q \times p + r$ avec $0 \leq r < p$.

$0 \leq r < p \iff r \in A_p$ ainsi r est l'unique représentant dans A_p de a^{p-2}

c'est-à-dire $a^{p-2} \equiv r\ (p)$ et $r \in A_p$

on a $ax r \equiv ax a^{p-2} \equiv a^{p-1} \equiv 1\ (p)$.

Voir la remarque en fin de devoir pour une autre rédaction.

(c) $xy \equiv 0\ (p) \iff p \mid xy$

et comme p premier alors $p \mid x$ ou $p \mid y$

d'où $x \equiv 0\ (p)$ ou $y \equiv 0\ (p)$. La réciproque est évidente

(d) 31 premier.

$2x \equiv 1\ (31)$ alors $x = 2^{29}$ est solut° dans $\mathbb{Z}$

et cherchons la solut° dans A_{31}, c'-à-d le reste de la division de 2^{29} par 31

$2^5 = 32 \equiv 1\ (31)$ d'où $2^{29} = (2^5)^5 \times 2^4 \equiv 16\ (31)$

donc $2x \equiv 1\ (31) \iff x = 16\ (31)$.

16 est l'unique solut° de $2x \equiv 1\ (31)$ dans A_{31}

de même $3x \equiv 1\ (31)$ a pour solution dans $\mathbb{Z}$ $x = 3^{29}$

et $3^{29} \equiv 3^{3\times 9} \times 3^2 \equiv 27^9 \times 3^2 = (-4)^9 \times 9\ (31)$

$\equiv -2^{18} \times 9\ (31)$

$\equiv -2^{15} \times 2^3 \times 9\ (31)$

$\equiv -2 \times 36\ (31)$

$\equiv -10\ (31)$

$\equiv 21\ (31)$

D'où 21 est l'unique solution de $3x \equiv 1\ (31)$ dans A_{31}

$6x^2 - 5x + 1 \equiv 0\ (31)$

Soit $P(x) = 6x^2 - 5x + 1$

$\Delta = 1$ d'où P admet pour racines $x = \frac{5+1}{12} = \frac{1}{2}$ ou $x = \frac{5-1}{12} = \frac{1}{3}$

donc P admet pour factorisation

$P(x) = 6\left(x - \frac{1}{2}\right)\left(x - \frac{1}{3}\right)$ c.à.d $P(x) = (2x-1)(3x-1)$

D'où $6x^2 - 5x + 1 \equiv 0\ (31) \iff (2x-1)(3x-1) \equiv 0\ (31)$

$\iff 2x - 1 \equiv 0\ (31)$ ou $3x - 1 \equiv 0\ (31)$

d'après (2c)

$\iff x \equiv 16\ (31)$ ou $x \equiv 21\ (31)$

D'où $S = \{16 + 31k\ ;\ 21 + 31k\ ;\ (k \in \mathbb{Z})\}$.

Remarque : autre résolution pour (2b)

1) Soit r le reste de la division de a^{p-2} par p, alors $a^{p-2} \equiv r\ (p)$

d'où $a \times r \equiv a \times a^{p-2} \equiv a^{p-1} \equiv 1\ (p) \implies r$ est solut°.

2) Montrons l'unicité : si $r, r' \in A_p$ avec r, r' solutions de l'éq.

alors $ar \equiv 1\ (p)$; $ar' \equiv 1\ (p) \implies a(r - r') \equiv 0\ (p)$ (par différence)

d'où $p \mid a(r-r')$ et $a \wedge p = 1 \implies p \mid r - r'$ mais $0 \leq r < p$; $0 < r' < p$

d'où $-p < r - r' < p$ et donc il faut $r - r' = 0$ donc $r = r'$ donc r unique !