Exercice I

Affirmation 1 : $11^{13} \equiv 1\ (12)$: **Fausse** car : $11 \equiv -1\ (12)$ (en effet, $11-(-1)=12$ et $12|12$)

Donc $11^{13} \equiv (-1)^{13}\ (12)$ par compatibilité de la relation de congruence avec les puissances. Or, $(-1)^{13} = -1$

Donc $11^{13} \equiv -1\ (12)$ et $-1 \not\equiv 1\ (12)$, donc $11^{13} \not\equiv 1 (12)$.

Affirmation 2 : $\forall k \in \mathbb{Z}$, $11+20k$ est solution de $(S) : \begin{cases} n \equiv 1 (5) \\ n \equiv 3 (4) \end{cases}$: **Vraie** car :

$\forall k \in \mathbb{Z}$, $11+20k-1 = 10+20k = 5(2+4k)$ avec $2+4k \in \mathbb{Z}$, donc $11+20k-1 \equiv 0 (5)$ donc $11+20k \equiv 1 (5)$.

De même, $11+20k-3 = 8+20k = 4(2+5k)$ avec $2+5k \in \mathbb{Z}$, donc $11+20k-3 \equiv 0 (4)$ donc $11+20k \equiv 3(4)$.

Par suite, $\forall k \in \mathbb{Z}$, $11+20k$ est solution du système (S).

Affirmation 3 : Vraie. Si n est solution de (S), alors $5|n-1$ et $4|n-3$.

Or comme $5|10$, on a bien $5 | n-1-2\times 5$ i.e $5|n-11$.

De même : $\begin{cases} 4|n-3 \\ 4|8 \end{cases}$ donc $4|n-3-8$ donc $4|n-11$.

Par suite, $n-11$ est bien divisible par 5 et par 4.

Exercice II

a) $a \equiv \begin{vmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{vmatrix} [7]$, donc $a^2 \equiv \begin{vmatrix} 0^2 \\ 1^2 \\ 2^2 \\ 3^2 \\ 4^2 \\ 5^2 \\ 6^2 \end{vmatrix} (7)$.

$0^2 = 0$
$1^2 = 1$
$2^2 = 4$
$3^2 = 9$ et $9 \equiv 2 (7)$
$4^2 = 16$ et $16 \equiv 2 (7)$.
$5^2 = 25$ et $25 \equiv 4 (7)$.
$6^2 = 36$ et $36 \equiv 1 (7)$.

Par suite, $a^2 \equiv 0\ (7)$ ou $a^2 \equiv 1 (7)$ ou $a^2 \equiv 2 (7)$ ou $a^2 \equiv (4)\ (7)$.

$b^2 \equiv \cdots (7)$ / $a^2 \equiv \cdots (7)$	0	1	2	4
0	0 (*)	1	2	4
1	1	2	3	5
2	2	3	4	6
4	4	5	6	1

A l'intersection de chaque ligne et chaque colonne, on écrit à quel chiffre est congru a^2+b^2.

Ainsi: $7 \mid a^2+b^2 \iff a^2+b^2 \equiv 0 \ (7) \iff a^2 \equiv 0 \ (7)$ et $b^2 \equiv 0 \ (7)$ (case (*) du tableau).

$7 \mid a^2+b^2 \iff 7 \mid a$ et $7 \mid b$ ■ $\iff a \equiv 0 \ (7)$ et $b \equiv 0 \ (7)$ grâce à la première question où l'on a établi que $a^2 \equiv 0 \ (7) \iff a \equiv 0 \ (7)$

Exercice VI.

Partie A

① $a = 26$ et $b = 9$ en entrée.

	c	a	b	Test : $c \neq 0$
Entrée	X	26	9	X
Boucle 1	8	9	8	Vrai
Boucle 2	1	8	1	Vrai
Boucle 3	0	X	X	FAUX

$26 = 9 \times 2 + 8$

$9 = 8 \times 1 + 1$

$8 = 1 \times 8 + 0$

En sortie, l'algorithme affiche donc 1

② Il suffit, en sortie, de mettre le message suivant, à la place d'afficher b:

```
Si b=1,
Alors afficher "a et b premiers entre eux"
Sinon
  Afficher "a et b non premiers entre eux"
Fin Si
```

Partie B

① $p = 9$ et $q = 2$.

a) A la lettre V est associé l'entier $x = 21$. Or $px + q = 9 \times 21 + 2 = 191$

Ainsi $x' \equiv 191 \ (26)$ et $0 \leq x' \leq 25$. Vu que $191 \equiv 9 \ (26)$

$191 = 26 \times 7 + 9$

On a: $x' \equiv 9 \ (26)$ et $0 \leq 9 \leq 25$, donc $x' = 9$, auquel est associé la lettre J du tableau.

1b) Si $x' \equiv 9x + 2 \ (26)$,

Alors $3x' \equiv 3(9x+2) \ (26)$ (Compatibilité de la congruence avec la multiplication)

$3x' \equiv 27x + 6 \ (26)$

Donc $3x' + 20 \equiv 27x + 26 \ (26)$ → (Compatibilité de la congruence avec l'addition).

Vu que $26 \equiv 0 \ (26)$

$27 \equiv 1 (26)$, $27x \equiv x \ (26)$.

on a donc : $27x + 26 \equiv x \ (26)$.

Par suite, $\underline{3x' + 20 \equiv x \ (26)}$.

1c) Si $x \equiv 3x' + 20 \ (26)$, alors : $9x \equiv 9(3x'+20) \ (26)$.

$9x \equiv 27x' + 180 \ (26)$

$9x + 2 \equiv 27x' + 182 \ (26)$.

Or $182 = 26 \times 7 + 0$

Donc $182 \equiv 0 \ (26)$.

et $27x' \equiv x' \ (26)$ (déjà vu).

donc $\underline{9x + 2 \equiv x' \ (26)}$

1d) Par double implication, grâce à 1b) et 1c) on a donc établi que :

$$\boxed{x' \equiv 9x + 2 \ (26) \Longleftrightarrow x \equiv 3x' + 20 \ (26).}$$

R est associé à $x' = 17$. Donc $\begin{cases} x \equiv 3\times17 + 20 \ (26) \\ \text{et } 0 \leq x \leq 25 \end{cases}$

$3\times17 + 20 = 71$

$71 = 26 \times 2 + 19$

Donc $71 \equiv 19 \ (26)$.

Donc $\begin{cases} x \equiv 19 \ (26) \\ \text{et } 0 \leq x \leq 25 \end{cases}$, donc $\underline{x = 19}$ auquel correspond la lettre $\underline{\underline{T}}$.

2) $q = 2$ et p inconnu.

J est codé en D : A : $x = 9$, on associe par ce codage : $x' = 3$.

Or $\begin{cases} x' \equiv px + q \ (26) \\ 0 \leq x' \leq 25 \end{cases}$, donc ici : $\begin{cases} 3 \equiv p\times9 + 2 \ (26) \\ 0 \leq 3 \leq 25 \end{cases}$ i.e $\begin{cases} 3 \equiv 9p + 2 \ (26) \\ 0 \leq 3 \leq 25 \end{cases}$

Donc : $9p \equiv 1 \ (26)$, donc $27p \equiv 3 (26)$, donc $\underline{p \equiv 3 (26)}$.

donc $\underbrace{26p}_{\equiv 0 (26)} + p \equiv 3 \quad (3)$

Par unicité de p, on a : $\underline{p = 3}$. (Ou bien : $p \equiv 3 (26)$ et $0 \leq p \leq 25$, donc $p = 3$).

3) $p = 13$ et $q = 2$

B : $x = 1$ donc $x' \equiv px + q \ (26)$

$x' \equiv 13\times1 + 2 \ (26)$

$\underline{x' \equiv 15 (26)}$ et $\underline{0 \leq 15 \leq 26}$, donc $\underline{x' = 15}$ auquel correspond la lettre $\underline{P}$.

D : $x = 3$ donc $x' \equiv 13 \times 3 + 2 \ (26)$

$x' \equiv 41 \ (26)$

$x' \equiv 15 \ (26)$ et $0 \leq 15 \leq 25$, donc $x' = 15 \rightsquigarrow P$.

Ainsi, à la lettre B est codée en P
la lettre D ——— P : Ce codage n'est donc pas lisible !

Plus exactement, il n'est pas possible avec un tel codage de déchiffrer, car deux lettres distinctes (B et D) sont codées en une même lettre P !

Exercice III a, b : CHIFFRES avec $b \neq 0$.

$N = a \times 10^3 + b$.

0) $\underline{N = \overline{a00b}^{(10)}}$.

1) $10 \equiv 3\,(7)$, donc $10^3 \equiv 3^3\,(7)$, donc $10^3 \equiv 27\,(7)$, donc comme $27 \equiv -1\,(7)$ (car $27-(-1)=28$ et $7 \mid 28$)

on a bien, par transitivité de $\equiv$: $\underline{10^3 \equiv -1\,(7)}$.

2) $N = a \times 10^3 + b$ et $10^3 \equiv -1\,(7)$, donc $a \times 10^3 \equiv -a\,(7)$ et $a \times 10^3 + b \equiv -a+b\,(7)$.

Donc $N \equiv -a+b\,(7)$

Par suite : $\underline{N \text{ est un multiple de } 7 \iff N \equiv 0\,(7) \iff -a+b \equiv 0\,(7) \iff a \equiv b\,(7)}$.

3) Si $a = b$, alors $a \equiv b\,(7)$.

donc il y a déjà :
$a=1$: $N = 1001$
$a=2$: $N = 2002$
$a=3$: $N = 3003$
$a=4$: $N = 4004$
$a=5$: $N = 5005$
$a=6$: $N = 6006$
$a=7$: $N = 7007$
$a=8$: $N = 8008$
$a=9$: $N = 9009$

Vu que $1 \leq a \leq 9$ et $0 \leq b \leq 9$ et que $7 \equiv 0\,(7)$, $a = 7$ et $b = 0$ convient : $N = 7000$.

$8 \equiv 1\,(7)$, donc $\left|\begin{array}{l} a = 8 \text{ et } b = 1 \\ \text{ou} \\ a = 1 \text{ et } b = 8 \end{array}\right.$ conviennent, donc $N = 8001$, $N = 1008$ sont solution.

Enfin, $9 \equiv 2\,(7)$, donc $\left|\begin{array}{l} a = 9 \text{ et } b = 2 \text{, donc } N = 9002 \\ \text{ou} \\ a = 2 \text{ et } b = 9 \text{ donc } N = 2009 \end{array}\right.$

Conclusion : $\boxed{S = \{1001 ; 1008 ; 2002 ; 2009 ; 3003 ; 4004 ; 5005 ; 6006 ; 7000 ; 7007 ; 8001 ; 8008 ; 9002 ; 9009\}}$.