CORRIGÉ – CHAPITRE 4

CONGRUENCES

Calculs de congruences

EXERCICE 1 ⋆

Rappel de méthode. Dire que $a \equiv x\ [9]$ signifie que $a - x$ est un multiple de 9. On commence donc par effectuer la division euclidienne de a par 9 : le reste r obtenu vérifie $a \equiv r\ [9]$ avec $0 \leqslant r \leqslant 8$. Si ce reste dépasse 4, on lui retranche 9 pour revenir dans l'intervalle demandé — ce qui est licite puisque r et $r - 9$ diffèrent d'un multiple de 9.

1. $11 = 9 \times 1 + 2$, donc $11 \equiv 2\ [9]$: $\boxed{x = 2}$
2. $24 = 9 \times 2 + 6$, donc $24 \equiv 6\ [9]$. Comme $6 > 4$, on écrit $6 \equiv 6 - 9 = -3\ [9]$: $\boxed{x = -3}$
3. $62 = 9 \times 6 + 8$, donc $62 \equiv 8 \equiv 8 - 9 = -1\ [9]$: $\boxed{x = -1}$
4. $85 = 9 \times 9 + 4$, donc $85 \equiv 4\ [9]$: $\boxed{x = 4}$
5. $-12 = 9 \times (-2) + 6$, donc $-12 \equiv 6 \equiv -3\ [9]$: $\boxed{x = -3}$
   Attention aux nombres négatifs : le reste d'une division euclidienne est toujours **positif**. On n'écrit pas $-12 = 9 \times (-1) - 3$ pour en déduire un reste de -3 ; on descend jusqu'au multiple de 9 immédiatement inférieur, ici -18.
6. $32 = 9 \times 3 + 5$, donc $32 \equiv 5 \equiv 5 - 9 = -4\ [9]$: $\boxed{x = -4}$

EXERCICE 2 ⋆

1. **Vrai.** C'est la compatibilité de la congruence avec les puissances (Proposition 1, avec $k = 2$).
2. **Faux.** Modulo 8, avec $a = 1$ et $b = 3$: $a^2 = 1$ et $b^2 = 9 \equiv 1\ [8]$, mais $1 \not\equiv 3\ [8]$ et $1 \not\equiv -3 \equiv 5\ [8]$. Le tableau des carrés modulo 8 de l'exercice 10 montre d'ailleurs que 1, 3, 5 et 7 ont tous le même carré.
3. **Faux.** Modulo 4, avec $a = 1$ et $b = 3$: $2a = 2$ et $2b = 6 \equiv 2\ [4]$, alors que $1 \not\equiv 3\ [4]$. On ne peut pas « simplifier » une congruence par un facteur comme une égalité.
4. **Faux.** Modulo 6, avec $a = 2$ et $b = 3$: $ab = 6 \equiv 0\ [6]$ alors que ni 2 ni 3 n'est congru à 0 modulo 6. L'affirmation devient vraie lorsque n est premier : c'est exactement le lemme d'Euclide du chapitre 1.
5. **Vrai.** D'après la Proposition 2, $a - b = 12k = 4 \times (3k)$ avec $k \in \mathbb{Z}$, donc $a \equiv b\ [4]$. Plus généralement, une congruence modulo n reste vraie modulo tout diviseur de n.
6. **Faux.** Avec $a = 6$ et $b = 0$: $6 \equiv 0\ [6]$ mais $6 \not\equiv 0\ [12]$. On ne peut pas passer à un multiple du module.

L'erreur la plus répandue est de croire que les congruences se manipulent exactement comme les égalités : les additions et multiplications sont permises (Proposition 1), mais pas les simplifications (questions 3 et 4).

EXERCICE 3 ⋆

Principe. Pour calculer le reste d'une puissance, on ne calcule jamais la puissance ! On réduit d'abord la base modulo n, puis on cherche un exposant pour lequel le résultat vaut 1 ou -1 : les puissances deviennent alors immédiates.

a) Division par 11

- $12 = 11 + 1$ donc $12 \equiv 1\ [11]$, d'où

$$12^{15} \equiv 1^{15} = 1\ [11] \qquad \Longrightarrow \qquad \boxed{\text{le reste de } 12^{15} \text{ est 1.}}$$

- $10 \equiv -1\ [11]$ (car $10 - (-1) = 11$), d'où

$$10^7 \equiv (-1)^7 = -1 \equiv 10\ [11] \qquad \Longrightarrow \qquad \boxed{\text{le reste de } 10^7 \text{ est 10.}}$$

  Le reste doit être compris entre 0 *et* 10 *: on remplace donc* -1 *par* 10*.*

- $78 = 11 \times 7 + 1$ donc $78 \equiv 1\ [11]$, d'où

$$78^{15} \equiv 1\ [11] \qquad \Longrightarrow \qquad \boxed{\text{le reste de } 78^{15} \text{ est 1.}}$$

- $13 \equiv 2\ [11]$. Cherchons les puissances de 2 :

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16 \equiv 5, \quad 2^5 \equiv 10 \equiv -1\ [11]$$

  Donc $2^{10} = \left(2^5\right)^2 \equiv (-1)^2 = 1\ [11]$, et

$$13^{12} \equiv 2^{12} = 2^{10} \times 2^2 \equiv 1 \times 4 = 4\ [11] \qquad \Longrightarrow \qquad \boxed{\text{le reste est 4.}}$$

- $(-2)^{19} = -2^{19}$, et $2^{19} = 2^{10} \times 2^9 \equiv 2^9\ [11]$. Or $2^9 = 2^5 \times 2^4 \equiv (-1) \times 5 = -5 \equiv 6\ [11]$, donc

$$(-2)^{19} \equiv -6 \equiv 5\ [11] \qquad \Longrightarrow \qquad \boxed{\text{le reste est 5.}}$$

b) Division par 7

- $351 = 7 \times 50 + 1$ donc $351 \equiv 1\ [7]$, et $85 = 7 \times 12 + 1$ donc $85 \equiv 1\ [7]$. La compatibilité du produit avec les congruences donne :

$$351^{12} \times 85^{15} \equiv 1^{12} \times 1^{15} = 1\ [7] \qquad \Longrightarrow \qquad \boxed{\text{le reste est 1.}}$$

- $16 = 7 \times 2 + 2$ et $23 = 7 \times 3 + 2$: ces deux nombres sont congrus au *même* entier 2 modulo 7. Donc $16^{12} \equiv 2^{12}$ et $23^{12} \equiv 2^{12}$, d'où

$$16^{12} - 23^{12} \equiv 2^{12} - 2^{12} = 0\ [7] \qquad \Longrightarrow \qquad \boxed{\text{le reste est 0.}}$$

  Inutile ici de calculer 2^{12} *:* il suffit de constater que les deux termes ont la même classe.

EXERCICE 4 ⋆

1. On cherche à chaque fois une puissance de 2 congrue à 1.
   - Modulo 3 : $2 \equiv -1$, donc $2^{100} \equiv (-1)^{100} = 1\ [3]$. Le reste est $\boxed{1}$.
   - Modulo 5 : $2^4 = 16 \equiv 1$, donc $2^{100} = \left(2^4\right)^{25} \equiv 1\ [5]$. Le reste est $\boxed{1}$.
   - Modulo 7 : $2^3 = 8 \equiv 1$ et $100 = 3 \times 33 + 1$, donc $2^{100} = \left(2^3\right)^{33} \times 2 \equiv 2\ [7]$. Le reste est $\boxed{2}$.
   - Modulo 9 : $2^6 = 64 = 63 + 1 \equiv 1$ et $100 = 6 \times 16 + 4$, donc $2^{100} \equiv 2^4 = 16 \equiv 7\ [9]$. Le reste est $\boxed{7}$.
2. On a $2026 = 7 \times 289 + 3$, donc $2026 \equiv 3\ [7]$. Les puissances de 3 modulo 7 sont 3, 2, 6, 4, 5, 1 : ainsi $3^6 \equiv 1\ [7]$. Comme $2026 = 6 \times 337 + 4$:

$$2026^{2026} \equiv 3^{2026} = \left(3^6\right)^{337} \times 3^4 \equiv 81 \equiv 4\ [7].$$

   Le reste est $\boxed{4}$. De même, $17 \equiv 2\ [5]$ et $2026 = 4 \times 506 + 2$, donc $17^{2026} \equiv 2^{2026} \equiv 2^2 = 4\ [5]$: le reste est $\boxed{4}$.

Divisibilité et chiffres

EXERCICE 5 ⋆

1. Calculons d'abord les puissances de 5 modulo 13 :

$$5^2 = 25 = 13 + 12 \equiv 12 \equiv -1\ [13]$$

$$5^4 = \left(5^2\right)^2 \equiv (-1)^2 = 1\ [13]$$

Par compatibilité avec les puissances, pour tout $k \in \mathbb{N}$:

$$5^{4k} = \left(5^4\right)^k \equiv 1^k = 1\ [13]$$

donc $5^{4k} - 1 \equiv 1 - 1 = 0\ [13]$:

$$\boxed{\text{pour tout } k \in \mathbb{N},\ 13 \text{ divise } 5^{4k} - 1.}$$

2. On traite séparément les deux termes modulo 11 :

$$5^{2n} = \left(5^2\right)^n = 25^n \qquad \text{et} \qquad 25 = 11 \times 2 + 3 \ \text{ donc } \ 25 \equiv 3\ [11]$$

$$14 = 11 + 3 \qquad \text{donc} \qquad 14 \equiv 3\ [11]$$

Ainsi $5^{2n} \equiv 3^n\ [11]$ et $14^n \equiv 3^n\ [11]$, d'où par différence :

$$5^{2n} - 14^n \equiv 3^n - 3^n = 0\ [11]$$

$$\boxed{\text{pour tout } n \in \mathbb{N},\ 11 \text{ divise } 5^{2n} - 14^n.}$$

L'idée à retenir : on ne cherche pas à calculer, on cherche à faire apparaître la **même** classe pour les deux termes.

EXERCICE 6 ⋆⋆

1. On a $3^{2n+1} = 3 \times 9^n$ et $9 \equiv 2\ [7]$, donc $3^{2n+1} \equiv 3 \times 2^n\ [7]$. D'autre part $2^{n+2} = 4 \times 2^n$. Ainsi :

$$3^{2n+1} + 2^{n+2} \equiv 3 \times 2^n + 4 \times 2^n = 7 \times 2^n \equiv 0\ [7].$$

Donc $\boxed{7 \text{ divise } 3^{2n+1} + 2^{n+2}}$ pour tout $n \in \mathbb{N}$.

2. On note $\mathcal{P}_n$: « 9 divise $4^n + 15n - 1$ ».
Initialisation : Pour $n = 0$, $4^0 + 0 - 1 = 0$, divisible par 9.
Hérédité : Si $4^k + 15k - 1 = 9m$, alors :

$$4^{k+1} + 15(k+1) - 1 = 4\left(4^k + 15k - 1\right) - 45k + 18 = 9(4m - 5k + 2).$$

Conclusion : Par récurrence, $\boxed{9 \text{ divise } 4^n + 15n - 1}$ pour tout $n \in \mathbb{N}$.

3. Les puissances de 4 modulo 9 valent 4, 7, 1 : $4^3 \equiv 1\ [9]$. Si $n = 3q + r$, alors $4^n \equiv 4^r$ et $15n = 45q + 15r \equiv 6r\ [9]$. On examine les trois cas :
   - $r = 0$: $4^n + 15n - 1 \equiv 1 + 0 - 1 = 0\ [9]$;
   - $r = 1$: $4^n + 15n - 1 \equiv 4 + 6 - 1 = 9 \equiv 0\ [9]$;
   - $r = 2$: $4^n + 15n - 1 \equiv 16 + 12 - 1 = 27 \equiv 0\ [9]$.

On retrouve le résultat. La récurrence est plus directe lorsque l'expression mêle puissances et termes polynomiaux, mais les congruences permettent de traiter un nombre fini de cas.

EXERCICE 7 ⋆⋆

Le chiffre des unités d'un entier est son reste dans la division par 10 *: tout le problème revient donc à travailler modulo* 10*.*

a) Puissances de 3 modulo 10 :

$$3^1 \equiv 3, \quad 3^2 = 9, \quad 3^3 = 27 \equiv 7, \quad 3^4 = 81 \equiv 1 \ [10]$$

Les restes se répètent donc par cycle de longueur 4. Comme $2025 = 4 \times 506 + 1$:

$$3^{2025} = \left(3^4\right)^{506} \times 3^1 \equiv 1^{506} \times 3 = 3 \ [10]$$

$$\boxed{\text{Le chiffre des unités de } 3^{2025} \text{ est 3.}}$$

b) Puissances de 7 modulo 10 :

$$7^1 \equiv 7, \quad 7^2 = 49 \equiv 9, \quad 7^3 \equiv 63 \equiv 3, \quad 7^4 \equiv 21 \equiv 1 \ [10]$$

Même cycle de longueur 4, et $2025 \equiv 1 \ [4]$:

$$7^{2025} \equiv 7^1 = 7 \ [10] \qquad \Longrightarrow \qquad \boxed{\text{le chiffre des unités est 7.}}$$

c) $13 \equiv 3 \ [10]$, donc $13^{2025} \equiv 3^{2025} \ [10]$, et l'on retrouve la question a) :

$$\boxed{\text{le chiffre des unités de } 13^{2025} \text{ est 3.}}$$

La tour de puissances. On cherche le chiffre des unités de

$$N = 7^{7^{7^{7^{7^{7}}}}}$$

Attention : une tour de puissances se lit **de haut en bas**. Le nombre N s'écrit 7^M, où $M = 7^{7^{7^{7^{7}}}}$ est lui-même une tour à six étages.

D'après la question b), le chiffre des unités de 7^M ne dépend que du **reste de** M **modulo** 4. Il suffit donc de connaître M modulo 4 — et non M lui-même, ce qui serait hors de portée.

Or $7 \equiv 3 \equiv -1 \ [4]$, donc pour tout exposant entier e :

$$7^e \equiv (-1)^e \ [4]$$

Comme M est une puissance de 7, c'est un nombre **impair**, donc

$$M \equiv (-1)^{\text{impair}} = -1 \equiv 3 \ [4]$$

En reportant dans le cycle des puissances de 7 modulo 10 :

$$N = 7^M \equiv 7^3 \equiv 3 \ [10]$$

$$\boxed{\text{Le chiffre des unités de } N \text{ est 3.}}$$

Ce qu'il faut retenir : pour une tour de puissances, on travaille modulo 10 à l'étage du bas, ce qui impose de connaître l'étage suivant modulo 4 — la longueur du cycle. C'est ce mécanisme « en cascade » qui rend le calcul possible.

EXERCICE 8 ⋆⋆

1. Comme $10 \equiv 1$ [9], on a $10^i \equiv 1$ [9] pour tout i (Proposition 1), donc $N \equiv a_k + \cdots + a_1 + a_0$ [9] : N est divisible par 9 si et seulement si la somme de ses chiffres l'est. De même, $10 \equiv -1$ [11] donne $10^i \equiv (-1)^i$ [11], donc $N \equiv a_0 - a_1 + a_2 - \ldots$ [11]. On retrouve les critères de l'exercice 28 du chapitre 1, sans récurrence : les congruences « absorbent » le calcul de $10^i - 1$.

2. On écrit $N = 100M + (10a_1 + a_0)$, où M est un entier. Comme $100 = 4 \times 25 \equiv 0$ [4], on a $N \equiv 10a_1 + a_0$ [4], d'où le critère.

3. On a $7 \times 11 \times 13 = 77 \times 13 = 1001$. Donc $1000 = 1001 - 1 \equiv -1$ [7], et de même modulo 11 et modulo 13. En découpant N en tranches de trois chiffres à partir de la droite, $N = t_0 + t_1 \times 1000 + t_2 \times 1000^2 + \cdots$, on obtient :

$$\boxed{N \equiv t_0 - t_1 + t_2 - t_3 + \cdots \ [7]}$$

Pour $N = 3\,214\,987\,608$: $t_0 = 608$, $t_1 = 987$, $t_2 = 214$, $t_3 = 3$, et $608 - 987 + 214 - 3 = -168 = 7 \times (-24)$. Donc $\boxed{N \text{ est divisible par } 7}$; en effet $N = 7 \times 459\,283\,944$. Le même calcul donne $-168 \equiv 1$ [13] : N n'est pas divisible par 13.

Tableaux de congruences et équations

EXERCICE 9 ⋆

1. Supposons qu'il existe des entiers x et y tels que $11x^2 - 7y^2 = 5$. Réduisons chaque coefficient modulo 5 :

$$11 = 5 \times 2 + 1 \equiv 1 \qquad -7 \equiv -7 + 10 = 3 \equiv -2 \qquad 5 \equiv 0 \ [5]$$

L'égalité $11x^2 - 7y^2 = 5$ donne donc, modulo 5 :

$$x^2 - 2y^2 \equiv 0 \ [5] \qquad \text{c'est-à-dire} \qquad \boxed{x^2 \equiv 2y^2 \ [5]}$$

2. Tout entier est congru à 0, 1, 2, 3 ou 4 modulo 5 : il suffit donc de tester ces cinq valeurs.

$x \equiv \cdots$ [5]	0	1	2	3	4
$x^2 \equiv \cdots$ [5]	0	1	4	4	1

$y \equiv \cdots$ [5]	0	1	2	3	4
$2y^2 \equiv \cdots$ [5]	0	2	3	3	2

Détail d'une case : pour $x \equiv 3$, on a $x^2 \equiv 9 \equiv 4$ [5] ; pour $y \equiv 2$, $2y^2 \equiv 2 \times 4 = 8 \equiv 3$ [5].

3. D'après le premier tableau, x^2 ne peut être congru qu'à 0, 1 ou 4 ; d'après le second, $2y^2$ ne peut l'être qu'à 0, 2 ou 3. Pour que l'égalité $x^2 \equiv 2y^2$ [5] soit possible, il faut une valeur commune aux deux listes :

$$\{0\,;1\,;4\} \cap \{0\,;2\,;3\} = \{0\}$$

La seule possibilité est donc $x^2 \equiv 0$ et $2y^2 \equiv 0$ [5]. En relisant les tableaux, cela impose $x \equiv 0$ [5] et $y \equiv 0$ [5] :

$$\boxed{x \text{ et } y \text{ sont des multiples de 5.}}$$

4. Écrivons $x = 5x'$ et $y = 5y'$ avec x' et y' entiers. En reportant :

$$11 \times 25x'^2 - 7 \times 25y'^2 = 5 \iff 25\left(11x'^2 - 7y'^2\right) = 5$$

Le membre de gauche est un multiple de 25, le membre de droite vaut 5. Or 25 ne divise pas 5 : c'est absurde.

$$\boxed{\text{L'équation } 11x^2 - 7y^2 = 5 \text{ n'admet aucune solution entière.}}$$

EXERCICE 10 ⋆

1. Tout entier est congru à l'un des huit entiers $0, 1, \ldots, 7$ modulo 8 :

$n \equiv \cdots\ [8]$	0	1	2	3	4	5	6	7
$n^2 \equiv \cdots\ [8]$	0	1	4	1	0	1	4	1

Détail : pour $n \equiv 3$, $n^2 \equiv 9 \equiv 1$; pour $n \equiv 5$, $n^2 \equiv 25 \equiv 1$; pour $n \equiv 6$, $n^2 \equiv 36 \equiv 4$ [8].

On remarque que le carré d'un entier ne peut être congru qu'à 0, 1 ou 4 modulo 8 : c'est une information très utile, dont on se sert souvent pour montrer qu'une équation n'a pas de solution.

2. L'équation s'écrit $(x+3)^2 \equiv 1$ [8]. Posons $m = x+3$: d'après le tableau, $m^2 \equiv 1$ [8] si et seulement si

$$m \equiv 1,\ 3,\ 5 \text{ ou } 7\ [8]$$

c'est-à-dire si et seulement si m est **impair**. Or $m = x+3$ est impair si et seulement si x est pair.

$$\boxed{S = \{x \in \mathbb{Z} \mid x \text{ est pair}\} = \{2k,\ k \in \mathbb{Z}\}}$$

Vérification : pour $x = 4$, $(4+3)^2 - 1 = 48 = 8 \times 6$. Pour $x = 1$, $(1+3)^2 - 1 = 15$, qui n'est pas divisible par 8.

3. On dresse le tableau des valeurs de $4x$ modulo 9 :

$x \equiv \cdots\ [9]$	0	1	2	3	4	5	6	7	8
$4x \equiv \cdots\ [9]$	0	4	8	3	7	2	6	1	5

La valeur 5 n'apparaît qu'une fois, pour $x \equiv 8$ [9] :

$$\boxed{S = \{8 + 9k,\ k \in \mathbb{Z}\}}$$

Vérification : $4 \times 8 = 32 = 9 \times 3 + 5$.

On remarque que chacun des neuf restes apparaît exactement une fois dans la seconde ligne : c'est parce que 4 et 9 n'ont aucun diviseur commun autre que 1, ce que l'étude du PGCD permettra d'expliquer. Si l'on avait résolu $3x \equiv 5$ [9], la seconde ligne n'aurait contenu que 0, 3 et 6, et l'équation n'aurait eu aucune solution.

EXERCICE 11 ⋆⋆

On remarquera d'emblée que $n = x^2 + x - 2 = (x+2)(x-1)$, *ce qui éclairera les résultats.*

1. n est divisible par 7 si et seulement si $n \equiv 0$ [7]. On teste les sept classes possibles pour x :

$x \equiv \cdots\ [7]$	0	1	2	3	4	5	6
$x^2 + x - 2 \equiv \cdots\ [7]$	5	0	4	3	4	0	5

Détail de deux cases : pour $x \equiv 3$, $9+3-2 = 10 \equiv 3$; pour $x \equiv 5$, $25+5-2 = 28 = 7 \times 4 \equiv 0$ [7].

La ligne s'annule pour $x \equiv 1$ et $x \equiv 5$ [7]. En remarquant que $5 \equiv -2$ [7] :

$$\boxed{E_7 = \{x \in \mathbb{Z} \mid x \equiv 1\ [7] \text{ ou } x \equiv -2\ [7]\}}$$

Ce résultat était prévisible : $n = (x+2)(x-1)$, et 7 étant premier, il divise ce produit si et seulement s'il divise $x+2$ ou $x-1$.

2. Même travail modulo 3 :

$x \equiv \cdots\ [3]$	0	1	2
$x^2 + x - 2 \equiv \cdots\ [3]$	1	0	1

$$\boxed{E_3 = \{x \in \mathbb{Z} \mid x \equiv 1\ [3]\}}$$

On remarque que les deux conditions $x \equiv 1$ et $x \equiv -2$ se confondent modulo 3, puisque $-2 \equiv 1\ [3]$: c'est pourquoi une seule classe apparaît ici.

3. Supposons $x = 1 + 21k$ ou $x = -2 + 21k$, avec $k \in \mathbb{Z}$. Comme $21 = 3 \times 7$, on a dans les deux cas :

$$x \equiv 1 \text{ ou } -2\ [7] \qquad \text{et} \qquad x \equiv 1 \text{ ou } -2 \equiv 1\ [3]$$

D'après les questions 1 et 2, n est donc divisible par 7 **et** par 3.

Il reste à traiter le facteur 2, que l'énoncé ne demande pas explicitement mais qui est indispensable, puisque $42 = 2 \times 3 \times 7$. Or :

$$n = x^2 + x - 2 = x(x+1) - 2$$

et $x(x+1)$ est le produit de deux entiers consécutifs, donc toujours pair. Ainsi n est pair.

Les entiers 2, 3 et 7 sont trois nombres premiers distincts qui divisent n. On écrit $n = 7m$; comme 3 divise $7m$ sans diviser 7, le lemme d'Euclide montre que 3 divise m, donc 21 divise n ; on recommence avec 2, qui divise $n = 21m'$ sans diviser 21. Ainsi le produit $2 \times 3 \times 7$ divise n.

$$\boxed{n \text{ est divisible par } 2 \times 3 \times 7 = 42.}$$

Vérification : pour $k = 1$ et $x = 22$, $n = 484 + 22 - 2 = 504 = 42 \times 12$.

Point de vigilance. On ne peut conclure « divisible par 3 et par 7 donc par 21 » que parce que 3 et 7 sont deux nombres premiers **distincts** (lemme d'Euclide). Un nombre divisible par 4 et par 6 n'est pas nécessairement divisible par 24 : par exemple 12.

EXERCICE 12 ⋆

1. $100 = 7 \times 14 + 2$, donc $\boxed{100 \equiv 2\ [7]}$.

Soit $(x\,;y)$ une solution de (E). Comme $10^{2n} = (10^2)^n = 100^n$, la compatibilité avec les puissances donne :

$$10^{2n} = 100^n \equiv 2^n\ [7]$$

Par ailleurs $7y^2 \equiv 0\ [7]$, puisque $7y^2$ est un multiple de 7. L'égalité $3x^2 + 7y^2 = 10^{2n}$ devient donc, modulo 7 :

$$3x^2 + 0 \equiv 2^n\ [7] \qquad \text{soit} \qquad \boxed{3x^2 \equiv 2^n\ [7]}$$

2. On teste les sept classes possibles pour x :

$x \equiv \cdots\ [7]$	0	1	2	3	4	5	6
$3x^2 \equiv \cdots\ [7]$	0	3	5	6	6	5	3

Détail : pour $x \equiv 2$, $3x^2 = 12 \equiv 5$; pour $x \equiv 3$, $3 \times 9 = 27 \equiv 6\ [7]$.

Les seules valeurs possibles de $3x^2$ modulo 7 sont donc

$$\boxed{0, \quad 3, \quad 5 \quad \text{et} \quad 6}$$

3. Calculons les puissances de 2 modulo 7 :

$$2^0 = 1, \qquad 2^1 = 2, \qquad 2^2 = 4, \qquad 2^3 = 8 \equiv 1\ [7]$$

Comme $2^3 \equiv 1$, les restes se répètent par cycle de longueur 3. En écrivant la division euclidienne de n par 3 sous la forme $n = 3q + r$ avec $r \in \{0\,;1\,;2\}$:

$$2^n = \left(2^3\right)^q \times 2^r \equiv 1^q \times 2^r = 2^r\ [7]$$

$\boxed{2^n \equiv 1,\ 2 \text{ ou } 4\ [7] \text{ selon le reste de } n \text{ dans la division par 3.}}$

Conclusion. Si (E) admettait une solution, on aurait $3x^2 \equiv 2^n\ [7]$. Or :

$$\underbrace{\{0\,;3\,;5\,;6\}}_{\text{valeurs de } 3x^2} \cap \underbrace{\{1\,;2\,;4\}}_{\text{valeurs de } 2^n} = \varnothing$$

Les deux membres ne peuvent jamais être congrus modulo 7 : c'est une contradiction.

$\boxed{\text{L'équation } (E) \text{ n'admet aucune solution entière, quel que soit } n.}$

C'est la démarche type de ce chapitre : pour prouver qu'une équation n'a pas de solution, on cherche un modulo bien choisi pour lequel les deux membres ne peuvent jamais coïncider.

EXERCICE 13 ⋆⋆

Dans chaque cas, on dresse le tableau des valeurs pour tous les restes possibles de x.

a) Modulo 7, $3x$ prend pour $x = 0, 1, \ldots, 6$ les valeurs 0, 3, 6, 2, 5, 1, 4. La valeur 4 est atteinte pour $x \equiv 6$ seulement : $\boxed{S = \{6 + 7k,\ k \in \mathbb{Z}\}}$.

b) Modulo 12, $5x$ prend pour $x = 0, \ldots, 11$ les valeurs 0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7. La valeur 2 est atteinte pour $x \equiv 10$: $\boxed{S = \{10 + 12k,\ k \in \mathbb{Z}\}}$. *Vérification :* $5 \times 10 = 50 = 48 + 2$.

c) Modulo 9, $6x$ prend les valeurs 0, 6, 3, 0, 6, 3, 0, 6, 3. La valeur 3 est atteinte pour $x \equiv 2$, 5 ou 8 [9], c'est-à-dire $\boxed{S = \{2 + 3k,\ k \in \mathbb{Z}\}}$.

d) Modulo 10, $4x$ ne prend que les valeurs paires 0, 4, 8, 2, 6 : la valeur 3 n'est jamais atteinte, et $\boxed{S = \varnothing}$. En effet, $4x - 3$ est impair et ne peut être un multiple de 10.

e) Modulo 7, x^2 prend les valeurs 0, 1, 4, 2, 2, 4, 1. Donc $\boxed{S = \{x \in \mathbb{Z} \mid x \equiv 3 \text{ ou } x \equiv 4\ [7]\}}$.

f) Modulo 6, $x^2 + x$ prend les valeurs 0, 2, 0, 0, 2, 0. Donc $\boxed{S = \{x \in \mathbb{Z} \mid x \equiv 0,\ 2,\ 3 \text{ ou } 5\ [6]\}}$.

Les cas b) et c) montrent qu'une équation $ax \equiv b\ [n]$ peut avoir une seule classe de solutions, plusieurs, ou aucune (cas d) : tout dépend des diviseurs communs à a et n, ce qu'éclairera l'étude du PGCD.

EXERCICE 14 ⋆⋆

1. On cherche les entiers x tels que $x \equiv 2\ [3]$, $x \equiv 3\ [5]$ et $x \equiv 2\ [7]$.

2. Dans $[\![0; 14]\!]$, les entiers congrus à 3 modulo 5 sont 3, 8 et 13, de restes respectifs 0, 2 et 1 modulo 3 : seul $\boxed{8}$ convient.
   Si $x \equiv 8\ [15]$, alors $x - 8$ est un multiple de 15, donc de 3 et de 5, et $x \equiv 8 \equiv 2\ [3]$, $x \equiv 8 \equiv 3\ [5]$.
   Réciproquement, si x vérifie les deux congruences, alors $x \equiv 8\ [3]$ et $x \equiv 8\ [5]$: on écrit $x - 8 = 3m$; comme 5 divise $3m$ et ne divise pas 3, le lemme d'Euclide montre que 5 divise m, donc 15 divise $x - 8$. Ainsi $\boxed{x \equiv 2\ [3] \text{ et } x \equiv 3\ [5] \iff x \equiv 8\ [15]}$.

3. On écrit $x = 8 + 15k$ avec $k \in \mathbb{Z}$. Comme $15 \equiv 1\ [7]$, on a $x \equiv 8 + k \equiv 1 + k\ [7]$, et la condition $x \equiv 2\ [7]$ équivaut à $k \equiv 1\ [7]$, c'est-à-dire $k = 1 + 7j$ avec $j \in \mathbb{Z}$. Alors $x = 8 + 15 + 105j = 23 + 105j$:

$$\boxed{x \equiv 23\ [105]}$$

Vérification : $23 = 3 \times 7 + 2 = 5 \times 4 + 3 = 7 \times 3 + 2$.

4. Les solutions positives sont 23, 128, 233, ... : il y a $\boxed{128}$ objets.

La réponse donnée par le *Sunzi Suanjing* est bien 23, la plus petite solution positive. La méthode employée ici, qui consiste à résoudre les congruences deux par deux, est le principe du théorème des restes chinois.

Petit théorème de Fermat

EXERCICE 15 ⋆

1. $3^6 = 729 = 7 \times 104 + 1$, donc $3^6 \equiv 1\ [7]$, d'où pour tout $n \in \mathbb{N}$:

$$3^{6n} = \left(3^6\right)^n \equiv 1^n = 1\ [7] \qquad \Longrightarrow \qquad 3^{6n} - 1 \equiv 0\ [7]$$

$$\boxed{\text{pour tout } n \in \mathbb{N},\ 7 \text{ divise } 3^{6n} - 1.}$$

Autre lecture : 7 étant premier et ne divisant pas 3, le petit théorème de Fermat donne directement $3^{7-1} = 3^6 \equiv 1\ [7]$.

2. Factorisons l'expression :

$$3^{n+p} - 3^{n+1} = 3^{n+1}\left(3^{p-1} - 1\right)$$

en mettant en facteur la plus petite puissance, 3^{n+1} — on vérifie que $3^{n+1} \times 3^{p-1} = 3^{n+p}$.

Le nombre p étant premier et différent de 3, il ne divise pas 3. Le petit théorème de Fermat s'applique donc :

$$3^{p-1} \equiv 1\ [p] \qquad \text{c'est-à-dire} \qquad p \text{ divise } 3^{p-1} - 1$$

Par conséquent p divise le produit $3^{n+1}\left(3^{p-1} - 1\right)$:

$$\boxed{\text{pour tout } n \in \mathbb{N},\ p \text{ divise } 3^{n+p} - 3^{n+1}.}$$

L'hypothèse $p \neq 3$ est indispensable : pour $p = 3$, on aurait $3^{n+3} - 3^{n+1} = 3^{n+1} \times 8$, qui n'est divisible par 3 que grâce au facteur 3^{n+1} — le théorème de Fermat, lui, ne s'appliquerait pas.

EXERCICE 16 ⋆

1. 29 est un nombre premier, et 29 ne divise pas 4. Le petit théorème de Fermat donne donc :

$$4^{29-1} = 4^{28} \equiv 1\ [29] \qquad \Longrightarrow \qquad \boxed{29 \text{ divise } 4^{28} - 1.}$$

2. $4 = 3 + 1$, donc $4 \equiv 1\ [3]$, d'où pour tout $n \in \mathbb{N}$:

$$4^n \equiv 1^n = 1\ [3] \qquad \Longrightarrow \qquad \boxed{3 \text{ divise } 4^n - 1.}$$

3. **Divisibilité par 5 :** $4^2 = 16 = 3 \times 5 + 1$, donc $4^2 \equiv 1\ [5]$, d'où

$$4^{4k} = \left(4^2\right)^{2k} \equiv 1^{2k} = 1\ [5]$$

Divisibilité par 17 : $4^4 = 256 = 15 \times 17 + 1$, donc $4^4 \equiv 1\ [17]$, d'où

$$4^{4k} = \left(4^4\right)^k \equiv 1^k = 1\ [17]$$

$$\boxed{\text{pour tout } k \in \mathbb{N},\ 4^{4k} - 1 \text{ est divisible par 5 et par 17.}}$$

4. Comme $28 = 4 \times 7$, la question 3 s'applique avec $k = 7$: $4^{28} - 1$ est divisible par 5 et par 17. Il l'est aussi par 3 (question 2 avec $n = 28$) et par 29 (question 1).

$$\boxed{3, \quad 5, \quad 17 \quad \text{et} \quad 29 \text{ sont quatre diviseurs premiers de } 4^{28} - 1.}$$

Remarque. Ces quatre nombres premiers étant distincts, leur produit (lemme d'Euclide appliqué de proche en proche) $3 \times 5 \times 17 \times 29 = 7\,395$ divise également $4^{28} - 1$. La factorisation complète de ce nombre, qui vaut $72\,057\,594\,037\,927\,935$, comporte d'ailleurs d'autres facteurs premiers, comme 43, 113 et 127.

EXERCICE 17 ⋆

1. 13 est premier et ne divise pas 3, donc $3^{12} \equiv 1\ [13]$. Comme $100 = 12 \times 8 + 4$:

$$3^{100} = \left(3^{12}\right)^8 \times 3^4 \equiv 81 = 6 \times 13 + 3 \equiv 3\ [13].$$

Le reste est $\boxed{3}$.

2. 17 est premier et ne divise pas 2, donc $2^{16} \equiv 1\ [17]$. Comme $2026 = 16 \times 126 + 10$, $2^{2026} \equiv 2^{10} = 1024 = 17 \times 60 + 4\ [17]$. Le reste est $\boxed{4}$.

3. On a $2^{12} \equiv 1\ [13]$, donc $2^{70} = 2^{60} \times 2^{10} \equiv 2^{10} = 1024 = 13 \times 78 + 10 \equiv 10\ [13]$. Pour 3, il est plus rapide de remarquer que $3^3 = 27 \equiv 1\ [13]$, donc $3^{70} = \left(3^3\right)^{23} \times 3 \equiv 3\ [13]$. Ainsi $2^{70} + 3^{70} \equiv 10 + 3 = 13 \equiv 0\ [13]$: $\boxed{13 \text{ divise } 2^{70} + 3^{70}}$.

Le petit théorème de Fermat fournit un exposant qui convient toujours, $p - 1$, mais pas forcément le plus petit, comme le montre le cas de 3 modulo 13.

EXERCICE 18 ⋆

1. 5 est un nombre premier. Le petit théorème de Fermat, dans sa version valable pour *tout* entier n, affirme que

$$n^5 \equiv n\ [5]$$

donc $a = n^5 - n \equiv 0\ [5]$:

$$\boxed{a \text{ est divisible par } 5.}$$

Attention à la version employée. La forme $n^{p-1} \equiv 1\ [p]$ exige que p ne divise pas n ; la forme $n^p \equiv n\ [p]$, elle, est vraie sans aucune condition — c'est celle dont on a besoin ici, puisque n pourrait être un multiple de 5.

2. Factorisons :

$$a = n^5 - n = n\left(n^4 - 1\right) = n\left(n^2 - 1\right)\left(n^2 + 1\right)$$

en utilisant l'identité $n^4 - 1 = \left(n^2\right)^2 - 1^2 = (n^2 - 1)(n^2 + 1)$.

Or $n^2 - 1 = (n - 1)(n + 1)$, donc

$$a = (n - 1)\, n\, (n + 1)\left(n^2 + 1\right)$$

Le produit $(n - 1)\, n\, (n + 1)$ est celui de **trois entiers consécutifs** :

- parmi deux entiers consécutifs, l'un au moins est pair, donc 2 divise ce produit ;
- parmi trois entiers consécutifs, l'un exactement est un multiple de 3, donc 3 divise ce produit.

Ainsi a est divisible par 2 et par 3.

Les nombres 2, 3 et 5 sont des nombres premiers distincts qui divisent tous trois a : comme à l'exercice 11, le lemme d'Euclide montre que leur produit divise a.

$$\boxed{a \text{ est divisible par } 2 \times 3 \times 5 = 30.}$$

Vérification : pour $n = 2$, $a = 32 - 2 = 30$; pour $n = 3$, $a = 243 - 3 = 240 = 30 \times 8$.

EXERCICE 19 ⋆

1. (a) 7 étant premier, le petit théorème de Fermat donne $n^7 \equiv n\ [7]$ pour tout entier n, donc

$$\boxed{A = n^7 - n \text{ est divisible par } 7.}$$

(b) $A = n\left(n^6 - 1\right)$, et $n^6 - 1 = \left(n^3\right)^2 - 1^2 = (n^3 - 1)(n^3 + 1)$, d'où

$$\boxed{A = n\left(n^3 + 1\right)\left(n^3 - 1\right)}$$

En factorisant davantage, $n^3 - 1 = (n-1)\left(n^2 + n + 1\right)$ et $n^3 + 1 = (n+1)\left(n^2 - n + 1\right)$, donc A contient le produit

$$(n-1)\,n\,(n+1)$$

de trois entiers consécutifs. Comme à l'exercice 18, ce produit est divisible par 2 et par 3, donc A l'est aussi.

(c) 2, 3 et 7 sont des nombres premiers distincts qui divisent A, donc leur produit divise A (comme à l'exercice 11) :

$$\boxed{A \text{ est divisible par } 2 \times 3 \times 7 = 42.}$$

2. (a) **Divisibilité par 3 :** en écrivant $B = n^2\left(n^2+1\right)\left(n^2-1\right) = n \cdot \left[(n-1)\,n\,(n+1)\right] \cdot \left(n^2+1\right)$, on retrouve le produit de trois entiers consécutifs, donc 3 divise B.
Divisibilité par 5 : développons différemment,

$$B = n^2\left(n^4 - 1\right) = n^6 - n^2 = n\left(n^5 - n\right)$$

Or l'exercice 18 a montré que 5 divise $n^5 - n$: il divise donc B.

(b) On dresse le tableau de congruence modulo 4 :

$n \equiv \cdots\ [4]$	0	1	2	3
$n^2 \equiv \cdots\ [4]$	0	1	0	1
$n^2 - 1 \equiv \cdots\ [4]$	3	0	3	0
$B = n^2\left(n^2+1\right)\left(n^2-1\right) \equiv \cdots\ [4]$	0	0	0	0

Lecture du tableau : si n est pair, c'est le facteur n^2 qui est congru à 0 ; si n est impair, c'est le facteur $n^2 - 1$. Dans les deux cas, le produit est nul modulo 4.

$$\boxed{B \text{ est divisible par } 4.}$$

(c) Dans la décomposition en facteurs premiers de B, le nombre 2 apparaît avec un exposant au moins égal à 2 (puisque $4 = 2^2$ divise B), et 3 et 5 apparaissent aussi : par unicité de la décomposition, $2^2 \times 3 \times 5$ divise B :

$$\boxed{B \text{ est divisible par } 3 \times 4 \times 5 = 60.}$$

Vérification : pour $n = 2$, $B = 4 \times 5 \times 3 = 60$; pour $n = 3$, $B = 9 \times 10 \times 8 = 720 = 60 \times 12$.

Exercices d'approfondissement

EXERCICE 20 ⋆⋆

1. On applique la relation de récurrence $u_{n+1} = 5u_n - 6$:

$$u_1 = 5 \times 14 - 6 = 64 \qquad u_2 = 5 \times 64 - 6 = 314$$

$$u_3 = 5 \times 314 - 6 = 1564 \qquad u_4 = 5 \times 1564 - 6 = 7814$$

Les deux derniers chiffres sont successivement 14, 64, 14, 64, 14 :

$$\boxed{\text{Conjecture : } u_n \text{ se termine par 14 si } n \text{ est pair, et par 64 si } n \text{ est impair.}}$$

2. Exprimons u_{n+2} en fonction de u_n :

$$u_{n+2} = 5u_{n+1} - 6 = 5\,(5u_n - 6) - 6 = 25u_n - 36$$

Or $25 \equiv 1\ [4]$ et $36 = 4 \times 9 \equiv 0\ [4]$, donc

$$u_{n+2} \equiv 1 \times u_n - 0 = u_n\ [4]$$

$$\boxed{\text{pour tout } n \in \mathbb{N},\ u_{n+2} \equiv u_n\ [4].}$$

Cette relation signifie que la classe de u_n modulo 4 ne change pas lorsqu'on avance de deux rangs : elle ne dépend donc que de la parité de n. Comme $u_0 = 14 = 4 \times 3 + 2 \equiv 2$ et $u_1 = 64 = 4 \times 16 \equiv 0\ [4]$, une récurrence immédiate de deux en deux donne :

$$\boxed{\text{pour tout } k \in \mathbb{N}, \quad u_{2k} \equiv 2\ [4] \quad \text{et} \quad u_{2k+1} \equiv 0\ [4].}$$

3. (a) Démontrons par récurrence la propriété

$$\forall n \in \mathbb{N}, \quad P_n : \text{« } 2u_n = 5^{n+2} + 3 \text{ »}$$

Initialisation : Pour $n = 0$: $2u_0 = 2 \times 14 = 28$ et $5^2 + 3 = 25 + 3 = 28$. Les deux membres coïncident, donc P_0 est vraie.

Hérédité : Soit $k \in \mathbb{N}$. Supposons P_k vraie, c'est-à-dire $2u_k = 5^{k+2} + 3$. Alors :

$$2u_{k+1} = 2\,(5u_k - 6) = 5 \times (2u_k) - 12 = 5\left(5^{k+2} + 3\right) - 12 = 5^{k+3} + 15 - 12 = 5^{k+3} + 3$$

C'est exactement P_{k+1}, qui est donc vraie.

Conclusion : Par principe de récurrence :

$$\boxed{\forall n \in \mathbb{N}, \quad 2u_n = 5^{n+2} + 3}$$

(b) Il suffit de connaître 5^{n+2} modulo 100. Or :

$$5^2 = 25, \qquad 5^3 = 125 \equiv 25, \qquad 5^4 = 625 \equiv 25 \ [100]$$

Plus généralement, si $5^m \equiv 25 \ [100]$ pour un $m \geqslant 2$, alors $5^{m+1} = 5 \times 5^m \equiv 125 \equiv 25 \ [100]$: la propriété se propage. Ainsi $5^{n+2} \equiv 25 \ [100]$ pour tout $n \in \mathbb{N}$, et

$$2u_n = 5^{n+2} + 3 \equiv 25 + 3 = 28 \ [100] \qquad \Longrightarrow \qquad \boxed{2u_n \equiv 28 \ [100]}$$

4. De $2u_n \equiv 28 \ [100]$, on déduit que $2u_n - 28$ est un multiple de 100, donc

$$2u_n - 28 = 100k \iff u_n - 14 = 50k \qquad (k \in \mathbb{Z})$$

Autrement dit $u_n \equiv 14 \ [50]$: les deux derniers chiffres de u_n valent donc 14 ou 64.

Attention : on ne peut pas diviser directement une congruence modulo 100 par 2 ; le module se divise lui aussi, et l'on obtient une congruence modulo 50 seulement. C'est précisément pourquoi deux possibilités subsistent.

Pour trancher, on utilise la question 2. Le nombre 14 est congru à 2 modulo 4, et 64 est congru à 0 modulo 4 :

$$\boxed{\begin{array}{l}\text{si } n \text{ est pair, } u_n \equiv 2 \ [4] \text{ : les deux derniers chiffres sont 14;} \\ \text{si } n \text{ est impair, } u_n \equiv 0 \ [4] \text{ : les deux derniers chiffres sont 64.}\end{array}}$$

La conjecture de la question 1 est donc démontrée.

EXERCICE 21 ⋆⋆

Partie A

1. $2009 = 16 \times 125 + 9$, donc $2009 \equiv 9 \ [16]$, d'où

$$2009^2 \equiv 9^2 = 81 = 16 \times 5 + 1 \equiv 1 \ [16]$$

$$\boxed{\text{Le reste de la division de } 2009^2 \text{ par 16 est 1.}}$$

2. On écrit $8001 = 2 \times 4000 + 1$, donc

$$2009^{8001} = \left(2009^2\right)^{4000} \times 2009 \equiv 1^{4000} \times 2009 = 2009 \ [16]$$

$$\boxed{2009^{8001} \equiv 2009 \ [16]}$$

Partie B

1. (a) $2009 = 5 \times 401 + 4$, donc $2009 \equiv 4 \ [5]$ et

$$u_0 = 2009^2 - 1 \equiv 4^2 - 1 = 15 \equiv 0 \ [5]$$

$$\boxed{u_0 \text{ est divisible par 5.}}$$

(b) Développons $(u_n + 1)^5$ à l'aide de la formule du binôme :

$$(u_n + 1)^5 = u_n^5 + 5u_n^4 + 10u_n^3 + 10u_n^2 + 5u_n + 1$$

d'où

$$u_{n+1} = (u_n + 1)^5 - 1 = u_n^5 + 5u_n^4 + 10u_n^3 + 10u_n^2 + 5u_n$$

En mettant u_n en facteur :

$$u_{n+1} = u_n \left(u_n^4 + 5u_n^3 + 10u_n^2 + 10u_n + 5\right)$$

et en factorisant 5 dans les quatre derniers termes :

$$\boxed{u_{n+1} = u_n \left[u_n^4 + 5\left(u_n^3 + 2u_n^2 + 2u_n + 1\right)\right]}$$

(c) Démontrons par récurrence la propriété

$$\forall n \in \mathbb{N}, \quad P_n : \text{« } u_n \text{ est divisible par 5 »}$$

Initialisation : C'est la question 1.(a) : u_0 est divisible par 5, donc P_0 est vraie.

Hérédité : Soit $k \in \mathbb{N}$. Supposons u_k divisible par 5. D'après la question précédente, $u_{k+1} = u_k \times A$ où A est un entier. Comme 5 divise u_k, il divise le produit $u_k \times A$, donc u_{k+1}. La propriété P_{k+1} est vraie.

Conclusion : Par principe de récurrence :

$$\boxed{\forall n \in \mathbb{N},\ u_n \text{ est divisible par 5.}}$$

2. (a) Montrons d'abord que $u_n + 1 = 2009^{2\times 5^n}$, par récurrence rapide : c'est vrai pour $n = 0$ puisque $u_0 + 1 = 2009^2$, et si $u_n + 1 = 2009^{2\times 5^n}$, alors

$$u_{n+1} + 1 = (u_n + 1)^5 = \left(2009^{2\times 5^n}\right)^5 = 2009^{2\times 5^{n+1}}$$

Pour $n = 3$: $2 \times 5^3 = 250$, donc

$$\boxed{u_3 = 2009^{250} - 1}$$

Montrons ensuite par récurrence que 5^{n+1} divise u_n. C'est vrai pour $n = 0$ (question 1.(a)). Si 5^{k+1} divise u_k, alors 5 divise u_k, donc aussi u_k^4, et le crochet $u_k^4 + 5\left(u_k^3 + 2u_k^2 + 2u_k + 1\right)$ est divisible par 5 ; d'après la question 1.(b), u_{k+1} est alors divisible par $5^{k+1} \times 5 = 5^{k+2}$. Pour $n = 3$, on obtient que $5^4 = 625$ divise u_3 :

$$2009^{250} - 1 \equiv 0\ [625] \qquad \text{soit} \qquad \boxed{2009^{250} \equiv 1\ [625]}$$

(b) On écrit $8001 = 250 \times 32 + 1$, donc

$$2009^{8001} = \left(2009^{250}\right)^{32} \times 2009 \equiv 1^{32} \times 2009 = 2009\ [625]$$

$$\boxed{2009^{8001} \equiv 2009\ [625]}$$

Partie C

D'après les parties A et B, le nombre $2009^{8001} - 2009$ est divisible par 16 *et* par 625. Dans la décomposition en facteurs premiers de cette différence, le nombre premier 2 apparaît donc avec un exposant au moins égal à 4, et le nombre premier 5 aussi (chapitre 1, exercice 16) ; par unicité de la décomposition, $2^4 \times 5^4$ divise cette différence :

$$16 \times 625 = 10\,000 \qquad \Longrightarrow \qquad 2009^{8001} \equiv 2009\ [10\,000]$$

Il ne reste qu'à écrire $8001 = 3 \times 2667$ pour faire apparaître un cube :

$$2009^{8001} = \left(2009^{2667}\right)^3$$

$$\boxed{n = 2009^{2667} \text{ convient : le cube de } n \text{ se termine par } 2\,009.}$$

L'idée de tout l'exercice est là : $10\,000 = 2^4 \times 5^4$, et l'on traite séparément la puissance de 2 (partie A) et la puissance de 5 (partie B) avant de recoller les deux résultats.

EXERCICE 22 ⋆⋆

1. On calcule directement $u_n = 2^n + 3^n + 6^n - 1$:

n	1	2	3	4	5	6
u_n	10	48	250	1 392	8 050	47 448

2. Travaillons modulo 2. Pour $n \geqslant 1$, $2^n \equiv 0$ et $6^n \equiv 0$ [2], tandis que $3 \equiv 1$ [2] donne $3^n \equiv 1$ [2]. Donc
$$u_n \equiv 0 + 1 + 0 - 1 = 0 \ [2] \qquad \Longrightarrow \qquad \boxed{u_n \text{ est pair pour tout } n \in \mathbb{N}^*.}$$

3. Supposons n pair, avec $n \geqslant 2$. Alors :
   - 2^n est divisible par 4, puisque $n \geqslant 2$;
   - 6^n est divisible par 4, pour la même raison ($6^n = 2^n \times 3^n$) ;
   - $3^n - 1$: comme n est pair, $n = 2m$ et $3^n = 9^m$. Or $9 \equiv 1$ [4], donc $9^m \equiv 1$ [4] et $3^n - 1 \equiv 0$ [4].

   La somme des trois est donc divisible par 4 :
$$\boxed{\text{si } n \text{ est pair, } u_n \text{ est divisible par 4.}}$$
   Vérification : $u_2 = 48 = 4 \times 12$ et $u_4 = 1\,392 = 4 \times 348$.

4. On cherche si chacun de ces nombres premiers divise au moins un terme.
   - 2 divise $u_1 = 10$: $\boxed{2 \in E}$
   - 3 divise $u_2 = 48$: $\boxed{3 \in E}$
   - 5 divise $u_1 = 10$: $\boxed{5 \in E}$
   - 7 divise $u_5 = 8\,050 = 7 \times 1\,150$: $\boxed{7 \in E}$

5. (a) Soit p premier avec $p > 3$. Alors p ne divise ni 2 ni 3, et le petit théorème de Fermat s'applique :
$$2^{p-1} \equiv 1 \ [p] \qquad \text{et} \qquad 3^{p-1} \equiv 1 \ [p]$$
   On en déduit, en isolant astucieusement un facteur :
$$6 \times 2^{p-2} = 3 \times \left(2 \times 2^{p-2}\right) = 3 \times 2^{p-1} \equiv 3 \times 1 = 3 \ [p]$$
$$6 \times 3^{p-2} = 2 \times \left(3 \times 3^{p-2}\right) = 2 \times 3^{p-1} \equiv 2 \times 1 = 2 \ [p]$$
$$\boxed{6 \times 2^{p-2} \equiv 3 \ [p] \qquad \text{et} \qquad 6 \times 3^{p-2} \equiv 2 \ [p]}$$
   L'astuce consiste à répartir le facteur $6 = 2 \times 3$ *:* on en donne 2 à la puissance de 2 pour reconstituer 2^{p-1}, et 3 à la puissance de 3.

   (b) Multiplions u_{p-2} par 6 :
$$6\,u_{p-2} = 6 \times 2^{p-2} + 6 \times 3^{p-2} + 6 \times 6^{p-2} - 6$$
   Le troisième terme se simplifie : $6 \times 6^{p-2} = 6^{p-1} \equiv 1$ [p] par Fermat, puisque $p > 3$ ne divise pas 6. En reportant les trois congruences :
$$6\,u_{p-2} \equiv 3 + 2 + 1 - 6 = 0 \ [p] \qquad \Longrightarrow \qquad \boxed{6\,u_{p-2} \equiv 0 \ [p]}$$

6. La congruence précédente signifie que p divise le produit $6\,u_{p-2}$. Or p est premier et $p > 3$, donc p ne divise pas 6. D'après le lemme d'Euclide, p divise nécessairement l'autre facteur :
$$\boxed{p \text{ divise } u_{p-2}, \text{ donc } p \in E.}$$
   En rassemblant avec la question 4, tout nombre premier appartient à E : les nombres 2 et 3 y sont, et tout premier $p > 3$ également.
$$\boxed{E \text{ est l'ensemble de } \textit{tous} \text{ les nombres premiers ; il est donc infini.}}$$
   Remarque. Il faut $p - 2 \geqslant 1$, c'est-à-dire $p \geqslant 3$, ce qui est bien assuré par l'hypothèse $p > 3$.

EXERCICE 23 : NOMBRES DE POULET ⋆⋆⋆

1. Raisonnons par contraposée. **Supposons n premier.** Comme n est impair, on a $n \neq 2$, donc n ne divise pas 2. Le petit théorème de Fermat s'applique alors :

$$2^{n-1} \equiv 1\ [n]$$

ce qui contredit l'hypothèse $2^{n-1} \not\equiv 1\ [n]$.

$$\boxed{n \text{ n'est pas premier.}}$$

C'est un test de non-primalité : il permet d'affirmer qu'un nombre est composé **sans en connaître le moindre diviseur**, ce qui est remarquable.

2. Remarquons que

$$2^{10} = 1\,024 = 3 \times 341 + 1 \qquad \text{donc} \qquad 2^{10} \equiv 1\ [341]$$

Comme $340 = 10 \times 34$:

$$2^{340} = \left(2^{10}\right)^{34} \equiv 1^{34} = 1\ [341] \qquad \Longrightarrow \qquad \boxed{\text{le reste est 1.}}$$

Ce que cela signifie. Le nombre 341 vérifie donc la *conclusion* du petit théorème de Fermat, $2^{341-1} \equiv 1\ [341]$. Pourtant :

$$341 = 11 \times 31$$

n'est pas premier. Autrement dit, la réciproque du petit théorème de Fermat est fausse : la congruence $2^{n-1} \equiv 1\ [n]$ ne garantit pas la primalité de n. Le test de la question 1 ne fonctionne que dans un sens.

3. (a) Examinons quand le verdict est erroné.
   - Si n est premier, alors $2^{n-1} \equiv 1\ [n]$ et l'on annonce « premier » : le verdict est **correct**.
   - Si n n'est pas premier, deux cas se présentent. Ou bien $2^{n-1} \not\equiv 1\ [n]$ et l'on annonce « pas premier » : correct. Ou bien $2^{n-1} \equiv 1\ [n]$, c'est-à-dire n est un nombre de Poulet, et l'on annonce à tort « premier ».

   Les seuls cas d'erreur sont donc les 21 853 nombres de Poulet, sur les 25 milliards d'entiers considérés :

$$P(\text{erreur}) = \frac{21\,853}{25 \times 10^9} \approx 8{,}74 \times 10^{-7}$$

$$\boxed{\text{soit environ une chance sur 1,1 million.}}$$

   (b) On annonce « premier » lorsque $2^{n-1} \equiv 1\ [n]$, ce qui se produit pour les 1 091 987 405 nombres premiers *et* pour les 21 853 nombres de Poulet. En notant A l'événement « n est premier » et B l'événement « n est annoncé premier » :

$$P_B(A) = \frac{1\,091\,987\,405}{1\,091\,987\,405 + 21\,853} = \frac{1\,091\,987\,405}{1\,092\,009\,258}$$

$$\boxed{P_B(A) \approx 0{,}999\,98}$$

Interprétation. Le test se trompe environ deux fois sur cent mille annonces de primalité. C'est cette fiabilité — combinée à sa rapidité, puisque le calcul de 2^{n-1} modulo n est très rapide — qui rend ce type de test précieux en cryptographie, où l'on a besoin de fabriquer de très grands nombres premiers.

EXERCICE 24 : NOMBRES DE CARMICHAËL ⋆⋆

1. (a) On divise successivement par les premiers : $561 = 3 \times 187$, puis $187 = 11 \times 17$.

$$\boxed{561 = 3 \times 11 \times 17}$$

En particulier, $\boxed{561 \text{ n'est pas premier.}}$

(b) Ici $n - 1 = 560$, et l'on teste chaque facteur premier :

$$3 - 1 = 2 \text{ et } 560 = 2 \times 280 \qquad 11 - 1 = 10 \text{ et } 560 = 10 \times 56$$

$$17 - 1 = 16 \text{ et } 560 = 16 \times 35$$

$$\boxed{\text{Pour chaque facteur premier } p \text{ de } n,\ (p-1) \text{ divise } (n-1).}$$

(c) Soit a un entier premier avec 561, c'est-à-dire n'ayant aucun diviseur commun avec 561 autre que ± 1. Comme $561 = 3 \times 11 \times 17$, cela signifie qu'aucun des nombres premiers 3, 11 et 17 ne divise a. Le petit théorème de Fermat donne donc :

$$a^2 \equiv 1\ [3] \qquad a^{10} \equiv 1\ [11] \qquad a^{16} \equiv 1\ [17]$$

On élève alors chaque congruence à la puissance voulue, en utilisant les quotients de la question précédente :

$$a^{560} = \left(a^2\right)^{280} \equiv 1\ [3] \qquad a^{560} = \left(a^{10}\right)^{56} \equiv 1\ [11] \qquad a^{560} = \left(a^{16}\right)^{35} \equiv 1\ [17]$$

Ainsi $a^{560} - 1$ est divisible par 3, par 11 et par 17. Ces trois nombres premiers étant distincts, leur produit divise $a^{560} - 1$ (lemme d'Euclide, comme à l'exercice 11) :

$$\boxed{a^{560} \equiv 1\ [561]}$$

En multipliant par a, il vient $a^{561} \equiv a\ [561]$, c'est-à-dire que 561 divise $a^{561} - a$. Comme 561 n'est pas premier :

$$\boxed{561 \text{ est un nombre de Carmichaël.}}$$

2. On reprend le même raisonnement.

(a) $1\,105 = 5 \times 221 = 5 \times 13 \times 17$, donc $\boxed{1\,105 = 5 \times 13 \times 17 \text{ n'est pas premier.}}$

(b) $n - 1 = 1\,104$, et :

$$5 - 1 = 4 \text{ et } 1\,104 = 4 \times 276 \qquad 13 - 1 = 12 \text{ et } 1\,104 = 12 \times 92$$

$$17 - 1 = 16 \text{ et } 1\,104 = 16 \times 69$$

$$\boxed{\text{Là encore, } (p-1) \text{ divise } (n-1) \text{ pour chaque facteur premier.}}$$

(c) Soit a premier avec 1 105, c'est-à-dire non divisible par 5, 13 et 17. Par le petit théorème de Fermat appliqué à 5, 13 et 17 :

$$a^{1104} = \left(a^4\right)^{276} \equiv 1\ [5] \qquad a^{1104} = \left(a^{12}\right)^{92} \equiv 1\ [13] \qquad a^{1104} = \left(a^{16}\right)^{69} \equiv 1\ [17]$$

Les trois facteurs premiers étant distincts :

$$\boxed{a^{1104} \equiv 1\ [1\,105],\ \text{donc } 1\,105 \text{ est un nombre de Carmichaël.}}$$

3. Le petit théorème de Fermat affirme que si n est premier et a premier avec n, alors $a^{n-1} \equiv 1\ [n]$. La réciproque serait : « si $a^{n-1} \equiv 1\ [n]$ pour tout a premier avec n, alors n est premier. »

   Les nombres 561 et 1 105 vérifient l'hypothèse de cette réciproque **pour tout** a premier avec eux, et ne sont pourtant pas premiers.

   $$\boxed{\text{La réciproque du petit théorème de Fermat est fausse.}}$$

   Comparaison avec l'exercice 23. Un nombre de Poulet, comme 341, met le test en défaut pour la seule base $a = 2$: il suffirait d'essayer $a = 3$ pour le démasquer, car $3^{340} \not\equiv 1\ [341]$. Un nombre de Carmichaël est bien plus retors : *aucune* base première avec lui ne permet de le détecter. C'est pourquoi les tests de primalité modernes ne se contentent pas de la congruence de Fermat.

EXERCICE 25 ⋆⋆⋆

1. $S = 10\times 2+9\times 7+8\times 6+7\times 5+6\times 4+5\times 3+4\times 2+3\times 1+2\times 0+4 = 220 = 11\times 20$: le numéro est $\boxed{\text{valide}}$.
2. Les neuf premiers chiffres donnent $20+9+16+21+24+25+24+21+16 = 176 = 11\times 16 \equiv 0\ [11]$. La clé doit donc vérifier $a_{10} \equiv 0\ [11]$: $\boxed{a_{10} = 0}$.
3. Le chiffre a_i est affecté du poids $w = 11 - i \in [\![1; 10]\!]$. La nouvelle somme est $S' = S + w(b_i - a_i) \equiv w(b_i - a_i)\ [11]$. Si 11 divisait S', il diviserait le produit $w(b_i - a_i)$, donc, 11 étant premier, il diviserait w ou $b_i - a_i$ (lemme d'Euclide). C'est impossible, puisque $1 \leqslant w \leqslant 10$ et $1 \leqslant |b_i - a_i| \leqslant 10$. Donc $\boxed{S' \not\equiv 0\ [11]}$ et l'erreur est détectée.
4. Si l'on échange a_i et a_{i+1}, de poids w et $w-1$, la somme varie de

   $$(wa_{i+1} + (w-1)a_i) - (wa_i + (w-1)a_{i+1}) = a_{i+1} - a_i,$$

   qui est non nul et de valeur absolue au plus 10, donc non divisible par 11 : l'erreur est détectée.

Le choix du nombre premier 11 est essentiel : modulo 10, avec un poids 2, la modification d'un chiffre de 5 unités passerait inaperçue.

EXERCICE 26 ⋆⋆⋆

1. M = 12 donne $63 \equiv 11$ (L) ; A = 0 donne 3 (D) ; T = 19 donne $98 \equiv 20$ (U) ; H = 7 donne $38 \equiv 12$ (M) ; S = 18 donne $93 \equiv 15$ (P). Le mot chiffré est $\boxed{\text{LDUMP}}$.
2. On a $5\times 21 = 105 = 4\times 26+1$. Si $y \equiv 5x+3\ [26]$, alors $21(y-3) \equiv 105x \equiv x\ [26]$. Réciproquement, si $x \equiv 21(y-3)$, alors $5x + 3 \equiv 105(y-3) + 3 \equiv y\ [26]$. D'où l'équivalence.
3. X = 23 donne $21 \times 20 = 420 \equiv 4$ (E) ; O = 14 donne $21 \times 11 = 231 \equiv 23$ (X) ; A = 0 donne $21 \times (-3) = -63 \equiv 15$ (P) ; K = 10 donne $21 \times 7 = 147 \equiv 17$ (R) ; U = 20 donne $21 \times 17 = 357 \equiv 19$ (T). Le message est $\boxed{\text{EXPERT}}$.
4. Avec la clé $4x + 3$, les lettres A = 0 et N = 13 sont toutes deux chiffrées par 3 (D), puisque $4 \times 13 = 52 \equiv 0\ [26]$. Deux lettres différentes ayant le même code, le déchiffrement est ambigu.

Un nombre a convient comme clé lorsqu'il admet un « inverse » modulo 26, comme 21 pour 5 ; ce sera le cas exactement lorsque a n'a aucun diviseur premier commun avec 26, ce que l'étude du PGCD permettra de démontrer.

Pour aller plus loin

EXERCICE 27 ⋆⋆

1. $5^2 = 25 \equiv 1\ [8]$, donc $5^{2022} = \left(5^2\right)^{1011} \equiv 1\ [8]$: le reste est $\boxed{1}$.
2. (a) On a $(n+3)^3 = n^3 + 9n^2 + 27n + 27 \equiv n^3\ [9]$, et $7^3 = 343 = 9 \times 38 + 1 \equiv 1\ [9]$, donc $7^{n+3} = 7^n \times 7^3 \equiv 7^n\ [9]$.

   (b) D'après a), $7^{n+3} + (n+3)^3 \equiv 7^n + n^3\ [9]$: par récurrence, le reste ne dépend que du reste de n modulo 3. On calcule $7^0 + 0 = 1$, $7^1 + 1 = 8$ et $7^2 + 8 = 57 \equiv 3\ [9]$. Le reste vaut donc $\boxed{1,\ 8 \text{ ou } 3}$ selon que $n \equiv 0$, 1 ou 2 [3].

EXERCICE 28 ⋆⋆

1. On a $8(2x+3) = 16x+24 \equiv 5x+2\ [11]$: si 11 divise $2x+3$, il divise $5x+2$. Réciproquement, $7(5x+2) = 35x+14 \equiv 2x+3\ [11]$: si 11 divise $5x+2$, il divise $2x+3$. D'où $\boxed{11 \mid 2x+3 \iff 11 \mid 5x+2}$. Les facteurs 8 et 7 s'obtiennent en cherchant par quel nombre multiplier 2 (resp. 5) pour obtenir 5 (resp. 2) modulo 11.
2. Les carrés modulo 12 des entiers 0, …, 11 sont 0, 1, 4, 9, 4, 1, 0, 1, 4, 9, 4, 1. Ainsi :

$$\boxed{12 \mid x^2 - 1 \iff x \equiv 1,\ 5,\ 7 \text{ ou } 11\ [12]}$$

   c'est-à-dire si et seulement si x n'est divisible ni par 2 ni par 3. En revanche, 2 n'est jamais un carré modulo 12 : $\boxed{\text{aucun entier } x \text{ ne convient}}$ pour $x^2 - 2$.

EXERCICE 29 ⋆⋆

a) Les puissances de 2 modulo 5 sont 1, 2, 4, 3, puis se répètent ($2^4 \equiv 1$). On a $2^n \equiv 3\ [5]$ si et seulement si $\boxed{n \equiv 3\ [4]}$.

b) Les puissances de 2 modulo 13 pour $n = 0, \ldots, 12$ sont 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1 : elles se répètent avec la période 12 (Fermat), et la valeur 3 n'est atteinte que pour $n = 4$. Donc $\boxed{n \equiv 4\ [12]}$.

c) $65 = 5 \times 13$ avec 5 et 13 premiers distincts : 65 divise un entier si et seulement si 5 et 13 le divisent (lemme d'Euclide). Il faudrait donc $n \equiv 3\ [4]$ et $n \equiv 4\ [12]$. Mais la seconde condition donne $n \equiv 4 \equiv 0\ [4]$, ce qui contredit la première. $\boxed{\text{Aucun entier } n \text{ ne convient.}}$

EXERCICE 30 ⋆⋆

1. D'après le petit théorème de Fermat, $7^p \equiv 7$ et $8^p \equiv 8\ [p]$, donc $7^p + 8^p \equiv 15\ [p]$. Ainsi p divise $7^p + 8^p$ si et seulement si p divise 15, c'est-à-dire $\boxed{p \in \{3\,;5\}}$. *Vérification :* $7^3 + 8^3 = 855 = 3 \times 285$ et $7^5 + 8^5 = 49\,575 = 5 \times 9\,915$.
2. Modulo 11, Fermat donne directement $x^{11} \equiv x$. Modulo 3, Fermat donne $x^3 \equiv x$, donc $x^9 = \left(x^3\right)^3 \equiv x^3 \equiv x$ et $x^{11} = x^9 x^2 \equiv x^3 \equiv x\ [3]$. Ainsi 3 et 11 divisent $x^{11} - x$; ce sont deux nombres premiers distincts, donc (lemme d'Euclide) 33 divise $x^{11} - x$: $\boxed{x^{11} \equiv x\ [33]}$.

EXERCICE 31 ⋆⋆⋆

D'après la Proposition 1, le reste de F_{n+2} modulo 8 ne dépend que des restes de F_{n+1} et F_n. On calcule les premiers restes :

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
F_n [8]	0	1	1	2	3	5	0	5	5	2	7	1	0	1

Comme $F_{12} \equiv F_0$ et $F_{13} \equiv F_1$ [8], une récurrence « à deux termes » montre que $F_{n+12} \equiv F_n$ [8] pour tout n : si $F_{k+12} \equiv F_k$ et $F_{k+13} \equiv F_{k+1}$, alors $F_{k+14} = F_{k+13} + F_{k+12} \equiv F_{k+1} + F_k = F_{k+2}$. Le reste de F_n est donc donné par le tableau, selon le reste de n modulo 12. *Vérification :* $F_{12} = 144 = 8 \times 18$ et $F_{13} = 233 = 8 \times 29 + 1$.

EXERCICE 32 ⋆⋆⋆

a) $2730 = 2 \times 1365 = 2 \times 3 \times 455 = \boxed{2 \times 3 \times 5 \times 7 \times 13}$.

b) Les nombres $p-1$ valent 1, 2, 4, 6 et 12, qui divisent tous 12.

c) Soit p l'un de ces nombres premiers. Si p divise x, alors $x^{13} \equiv 0 \equiv x$ [p]. Sinon, $x^{p-1} \equiv 1$ [p] d'après Fermat, et comme $12 = (p-1)m$ avec m entier, $x^{12} = \left(x^{p-1}\right)^m \equiv 1$, d'où $x^{13} \equiv x$ [p]. Ainsi les cinq nombres premiers distincts 2, 3, 5, 7, 13 divisent $x^{13} - x$, donc leur produit aussi (lemme d'Euclide appliqué de proche en proche) : $\boxed{x^{13} \equiv x \ [2730]}$.

L'énoncé original du poly écrit « $x^{13} \equiv n$ [2730] », ce qui est une coquille.

EXERCICE 33 ⋆⋆⋆

On raisonne par récurrence sur $k \in \{0, \dots, p-1\}$. Pour $k = 0$, $\binom{p-1}{0} = 1 = (-1)^0$. Si la propriété est vraie au rang $k-1$, avec $1 \leqslant k \leqslant p-1$, la formule de Pascal donne $\binom{p}{k} = \binom{p-1}{k} + \binom{p-1}{k-1}$. Or p divise $\binom{p}{k}$ (c'est le point clé de la démonstration du petit théorème de Fermat dans le cours), donc :

$$\binom{p-1}{k} \equiv -\binom{p-1}{k-1} \equiv -(-1)^{k-1} = (-1)^k \ [p].$$

Par récurrence, $\boxed{\binom{p-1}{k} \equiv (-1)^k \ [p]}$. *Vérification :* pour $p = 7$, la ligne $\binom{6}{k}$ vaut 1, 6, 15, 20, 15, 6, 1, congrue à 1, -1, 1, -1, 1, -1, 1 modulo 7.

EXERCICE 34 ⋆⋆⋆⋆

Étape 1. Modulo 3, les carrés valent 0 (si $x \equiv 0$) ou 1 (si $x \equiv 1$ ou 2). Si $x^2 + y^2 = 3z^2$, alors $x^2 + y^2 \equiv 0$ [3] ; or $x^2 + y^2$ est congru à 0, 1 ou 2, et ne vaut 0 que si $x^2 \equiv y^2 \equiv 0$, c'est-à-dire si 3 divise x et y. Alors 9 divise $x^2 + y^2 = 3z^2$, donc 3 divise z^2, puis z (lemme d'Euclide).

Étape 2. Supposons qu'il existe une solution non nulle, et choisissons-en une, (x, y, z), pour laquelle l'entier $|x| + |y| + |z| > 0$ est le plus petit possible. D'après l'étape 1, $x = 3x'$, $y = 3y'$ et $z = 3z'$; en divisant l'équation par 9, on obtient $x'^2 + y'^2 = 3z'^2$: (x', y', z') est une solution non nulle avec $|x'| + |y'| + |z'| = \frac{1}{3}(|x| + |y| + |z|)$, strictement plus petit. C'est absurde.

Donc $\boxed{(0,0,0) \text{ est la seule solution}}$. Ce raisonnement, dit de *descente infinie*, remonte à Fermat.

EXERCICE 35 ⋆⋆⋆⋆

a) Tout entier est congru à 0 ou 1 modulo 2, et $0^2 = 0$, $1^2 = 1$: tout x vérifie $x \equiv x^2$ [2].

b) Les carrés modulo 3 sont 0, 1 ; modulo 5 : 0, 1, 4 ; modulo 7 : 0, 1, 2, 4 (tableaux des exercices 9 et 13). Les carrés modulo 3 sont donc les $x \equiv 0$ ou 1 [3], et de même pour 5 et 7.

c) Si $x \equiv y^2$ [p] avec p ne divisant pas x, alors p ne divise pas y (sinon p diviserait y^2, donc x). Comme p est impair, $\frac{p-1}{2}$ est entier et, par Fermat, $x^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1$ [p].

d) Si $p \equiv 3$ [4], alors p est impair et $\frac{p-1}{2}$ est impair. Si -1 était un carré modulo p, la question c) donnerait $(-1)^{\frac{p-1}{2}} = -1 \equiv 1$ [p], donc p diviserait 2, ce qui est absurde.

e) Comme $n \geqslant 2$, $n!$ est pair, donc $(n!)^2 + 1$ est impair et $p \neq 2$. De plus $-1 \equiv (n!)^2$ [p] est un carré modulo p, donc d'après d), $p \not\equiv 3$ [4]. Un nombre impair étant congru à 1 ou 3 modulo 4, on a $\boxed{p \equiv 1 \text{ [4]}}$.

f) Si l'on avait $p \leqslant n$, p diviserait $n!$, donc $(n!)^2$, et donc $1 = ((n!)^2 + 1) - (n!)^2$, ce qui est absurde. Ainsi $\boxed{p > n}$.

g) Pour tout entier $n \geqslant 2$, il existe un nombre premier $p \equiv 1$ [4] strictement supérieur à n : l'ensemble de ces nombres premiers n'est donc pas majoré, il est $\boxed{\text{infini}}$.

La démarche des questions e) à g) reprend celle d'Euclide pour l'infinité des nombres premiers (Proposition 3 du chapitre 1), et celle de l'exercice 27 du chapitre 1 pour les nombres de la forme $6k + 5$.

EXERCICE 36 ⋆⋆⋆⋆

a) Pour $a \in \{1, \dots, p-1\}$, p ne divise ni a ni x, donc ne divise pas ax (lemme d'Euclide) : $r(a) \in \{1, \dots, p-1\}$. Si $r(a) = r(b)$, alors p divise $ax - bx = (a-b)x$, donc p divise $a-b$; comme $|a-b| < p$, on a $a = b$. L'application r est donc injective de $\{1, \dots, p-1\}$ dans lui-même ; un ensemble fini ayant autant d'éléments au départ qu'à l'arrivée, elle est bijective.

b) En multipliant les $p-1$ congruences $ax \equiv r(a)$ [p] (Proposition 1), on obtient $(p-1)!\, x^{p-1} \equiv \prod_{a=1}^{p-1} r(a)$ [p]. Comme r est une bijection, le produit des $r(a)$ est celui des entiers de 1 à $p-1$, soit $(p-1)!$. Ainsi p divise $(p-1)!\,(x^{p-1} - 1)$. Or p ne divise aucun des facteurs de $(p-1)!$, donc ne divise pas $(p-1)!$, et le lemme d'Euclide donne que p divise $x^{p-1} - 1$: $\boxed{x^{p-1} \equiv 1 \text{ [p]}}$.

Cette démonstration, due à Euler, n'utilise pas les coefficients binomiaux : c'est une alternative à celle du cours.

EXERCICE 37 ⋆⋆⋆⋆

a) **Existence.** D'après Fermat, $a \times a^{p-2} = a^{p-1} \equiv 1$ [p]. Le reste de a^{p-2} modulo p est donc un inverse de a ; il n'est pas nul, puisque son produit par a est congru à 1. **Unicité.** Si $ab \equiv ab' \equiv 1$ [p] avec b, b' dans $\{1, \dots, p-1\}$, alors p divise $a(b-b')$, donc $b-b'$ (lemme d'Euclide), d'où $b = b'$.

b) $i(a) = a$ équivaut à $a^2 \equiv 1$ [p], c'est-à-dire $p \mid (a-1)(a+1)$, soit $p \mid a-1$ ou $p \mid a+1$. Dans $\{1, \dots, p-1\}$, cela donne $a = 1$ ou $a = p-1$.

c) Pour $p = 2$, $(p-1)! = 1 \equiv -1$ [2]. Pour $p \geqslant 3$, on a $i(i(a)) = a$, et d'après b), les entiers 2, …, $p-2$ se regroupent en paires $\{a, i(a)\}$ d'éléments distincts dont le produit est congru à 1. Donc $2 \times 3 \times \cdots \times (p-2) \equiv 1$ [p], et $(p-1)! \equiv 1 \times 1 \times (p-1) \equiv -1$ [p] : $\boxed{(p-1)! \equiv -1 \text{ [p]}}$.
Vérification : $6! = 720 = 7 \times 103 - 1$.

d) Soit $a \in \{1, \dots, n-1\}$ et c le produit des autres éléments de $\{1, \dots, n-1\}$: $ac = (n-1)! \equiv -1$ [n], donc $a \times (-c) \equiv 1$ [n], et $-c$ est un inverse de a. Si n n'était pas premier, il s'écrirait $n = ab$ avec $1 < a < n$; en notant d un inverse de a, on aurait $ad - 1 = kn = kab$ avec $k \in \mathbb{Z}$, donc a diviserait 1, ce qui est absurde. Ainsi $\boxed{n \text{ est premier}}$.

Le théorème de Wilson fournit donc une caractérisation des nombres premiers : $n \geqslant 2$ est premier si et seulement si $(n-1)! \equiv -1\ [n]$. Elle est toutefois inutilisable en pratique, $(n-1)!$ étant gigantesque.