Corrigé du devoir surveillé n°2

Exercice 1.

1. Le tableau suivant donne les restes modulo 7 :

Reste de x modulo 7	0	1	2	3	4	5	6
Reste de $2x$ modulo 7	0	2	4	6	1	3	5

On déduit de ce tableau que $2x \equiv 3$ [7] si et seulement si $x \equiv 5$ [7]. Ainsi, l'ensemble des entiers x tels que $2x \equiv 3$ [7] est $\{5 + 7k \mid k \in \mathbb{Z}\}$.

2. Le tableau suivant donne les restes modulo 7 :

Reste de x modulo 7	0	1	2	3	4	5	6
Reste de $2x^2$ modulo 7	0	2	1	4	4	1	2

On déduit de ce tableau que, quel que soit l'entier x, $2x^2 \not\equiv 3$ [7] donc l'ensemble des entiers x tels que $2x^2 \equiv 3$ [7] est $\varnothing$.

Exercice 2.

1. Étant donné que $2^{10} = 1024 = 24 + 10 \times 100$, $2^{10} \equiv 24 \pmod{100}$. Dès lors, $2^{20} = (2^{10})^2 \equiv 24^2 \pmod{100}$. Or, $24^2 = 576 = 76 + 5 \times 100$ donc $24^2 \equiv 76 \pmod{100}$. Par transitivité, on conclut que $\boxed{2^{20} \equiv 76 \pmod{100}}$.

2. Considérons, pour tout $n \in \mathbb{N}^*$, la proposition $\mathcal{P}(n)$: « $76^n \equiv 76 \pmod{100}$ ».
Puisque $76^1 = 76 \equiv 76 \pmod{100}$, la proposition $\mathcal{P}(1)$ est vraie.
Supposons que $\mathcal{P}(k)$ est vraie pour un certain $k \in \mathbb{N}^*$.
Alors, $76^k \equiv 76 \pmod{100}$ donc, en multipliant par 76, $76^{k+1} \equiv 76^2 \pmod{100}$. Or, $76^2 = 5776 = 76 + 57 \times 100 \equiv 76 \pmod{100}$ donc, par transitivité, $72^{k+1} \equiv 76 \pmod{100}$ donc $\mathcal{P}(k+1)$ est vraie.
On a donc démontré par récurrence que, $\boxed{\text{pour tout } n \in \mathbb{N}^*,\ 76^n \equiv 76 \pmod{100}}$.

3. Puisque $1000 = 20 \times 50$, grâce aux questions précédentes,

$$2^{1000} = 2^{20\times 50} = \left(2^{20}\right)^{50} \equiv 76^{50} \pmod{100} \equiv 76 \pmod{100}.$$

On conclut que $\boxed{\text{les deux derniers chiffres dans l'écriture décimale de } 2^{1000} \text{ sont 7 et 6}}$.

Exercice 3. — Soit $n \in \mathbb{N}$. Remarquons que $2017 = 2 + 403 \times 5 \equiv 2 \pmod 5$ et $2018 = 3 + 403 \times 5 \equiv 2 \pmod 5$ donc $A_n \equiv 2^n + 3^n \pmod 5$.

Ensuite, on constate que

$$\begin{array}{ccc} 2^1 \equiv 2 \pmod 5 & \text{et} & 3^1 \equiv 3 \pmod 5 \\ 2^2 \equiv 4 \pmod 5 & \text{et} & 3^2 \equiv 4 \pmod 5 \\ 2^3 \equiv 3 \pmod 5 & \text{et} & 3^3 \equiv 2 \pmod 5 \\ 2^4 \equiv 1 \pmod 5 & \text{et} & 3^4 \equiv 1 \pmod 5 \end{array}$$

Notons r le reste de n modulo 4. Alors, il existe un entier naturel q tel que $n = 4q + r$ donc

$$\begin{aligned} A_n &\equiv 2^{4q+r} + 3^{4q+r} \pmod 5 \equiv \left(2^4\right)^q \times 2^r + \left(3^4\right)^q \times 3^r \pmod 5 \\ &\equiv 1^q \times 2^r + 1^q \times 3^r \pmod 5 \equiv 2^r + 3^r \pmod 5. \end{aligned}$$

Ainsi,

- si $r = 0$, $A_n \equiv 2 \pmod 5$;
- si $r = 1$, $A_n \equiv 5 \pmod 5 \equiv 0 \pmod 5$;
- si $r = 2$, $A_n \equiv 8 \pmod 5 \equiv 3 \pmod 5$;
- si $r = 3$, $A_n \equiv 5 \pmod 5 \equiv 0 \pmod 5$.

On conclut donc que le reste de A_n modulo 5 est 2 si $n \equiv 0 \pmod 4$, 3 si $n \equiv 2 \pmod 4$ et 0 sinon (i.e. si n est impair).

Exercice 4.

1. Une solution simple de (E_1) est $(1\,;0\,;0)$ car $1^2 + 0^2 + 0^2 = 1 = 2^1 - 1$.

2. Une solution simple de (E_1) est $(1\,;1\,;1)$ car $1^2 + 1^2 + 1^2 = 3 = 2^2 - 1$.

3. **a.** Comme $n \geqslant 3$, $2^n = 2^3 \times 2^{n-3}$ avec $n - 3 \geqslant 0$ donc 2^{n-3} est un entier et ainsi $2^3 = 8$ divise 2^n. Il s'ensuit que $2^n \equiv 0$ [8] donc $2^n - 1 \equiv -1$ [8] et ainsi $\boxed{2^n - 1 \equiv 7\ [8]}$.

b.

Reste de m modulo 8	0	1	2	3	4	5	6	7
Reste de m^2 modulo 8	0	1	4	1	0	1	4	1

c. La question précédente montre que les restes possibles pour un carré modulo 8 sont 0, 1 et 4.

a^2 \ b^2	0	1	4
0	0	1	4
1	1	2	5
4	4	5	0

d. La question précédente montre que les restes possibles pour une somme de deux carrés modulo 8 sont 0, 1, 2, 4 et 5.

a^2+b^2 \ c^2	0	1	4
0	0	1	4
1	1	2	5
2	2	3	6
4	4	5	0
5	5	6	1

e. On constate que les restes possibles pour une somme de trois carrés modulo 8 sont 0, 1, 2, 3, 4, 5 et 6. Ainsi, 7 n'est pas un reste possible donc, d'après la question **a.**, pour tous entiers a, b et c, $a^2+b^2+c^2 \neq 2^n-1$. On conclut donc que l'équation (E_n) n'a pas de solution dans $\mathbb{N}^3$ pour $n \geqslant 3$.