Exercice 2. ($\heartsuit$) Résoudre dans $\mathbb{Z}$ les équations suivantes

1) $x-3|x+7$ 2) $x+2|x^2+2$

Correction - Dans les deux questions, on raisonne par analyse-synthèse (on laisse les détails de rédaction au lecteur).

1) Soit x est solution du problème alors, $x-3|x+7$ et $x-3|x-3$ donc $x-3|(x+7)-(x-3)=10$. Donc $x-3 \in \{-10,-5,-2,-1,1,2,5,10\}$. [.....]
$\boxed{\text{L'ensemble-solution est } \{-7,-2,1,2,4,5,8,13\}}$.

2) Soit x est solution du problème alors, $x+2|x^2+2$. De plus, $x+2|x+2$, alors $x+2|x^2+2-x(x+2)+2(x+2)=6$. Donc $x+2 \in \{-6,-3,-2,-1,1,2,3,6\}$. [...]
$\boxed{\text{L'ensemble-solution est } \{-8,-5,-4,-3,-1,0,1,4\}}$.

Exercice 6. ($*$) Montrer que dans la suite (u_n) de terme général $u_n = 2^n - 3$, il y a:

1) une infinité de termes divisibles par 5
2) une infinité de termes divisibles par 13
3) aucun terme divisible par 65.

Correction -

1) Remarquons que pour $k \in \mathbb{N}$, $2^{4k+3} = 16^k \times 8 \equiv 1^k \times 3\ [5] \equiv 3\ [5]$. Donc : $2^{4k+3}-3$ est divisible par 5, ce pour tout $k \in \mathbb{N}$.
$\boxed{\text{Il y a donc une infinité de } u_n \text{ divisibles par 5}}$.

2) Remarquons que pour $k \in \mathbb{N}$, $2^{12k+4} = 4096^k \times 16 \equiv 1^k \times 3\ [13] \equiv 3\ [5]$. Donc : $2^{12k+4}-3$ est divisible par 13, ce pour tout $k \in \mathbb{N}$.
$\boxed{\text{Il y a donc une infinité de } u_n \text{ divisibles par 13}}$.

3) Par l'absurde supposons qu'il existe $n \in \mathbb{N}$ tel que $65|u_n$. Alors en particulier $5|u_n$.
On montre qu'alors n est forcément de la forme $n = 4k+3$. Posons $n = 4k+r$ où $r \in \{0,1,2,3\}$, alors

$$2^n = 2^{4k+r} = 16^k \times 2^r \equiv 1^k \times 2^r\ [5] \equiv 2^r\ [5].$$

Or $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, le seul congru à 3 modulo 5 est le dernier.
Puis, on écrit $k = 3q+r$ où $r \in \{0,1,2\}$, alors :

$$2^{4k+3} = 2^{4(3q+r)+3} = 4096^q \times 2^{4r+3} \equiv 1^q \times 2^{4r+3}\ [13] \equiv 2^{4r+3}\ [13].$$

Or 2^{4r+3} vaut 8, 128 ou 2048 tous différents de 3 modulo 13. Donc, $2^{4k+3}-3$ n'est pas divisible par 13, donc ne peut être divisible par 65.
$\boxed{\text{Il n'y a donc aucun } u_n \text{ divisible par 65}}$

Exercice 7. ($*$) Montrer que le produit de k entiers consécutifs est divisible par $k!$.

Correction - On considère k entiers consécutifs, à partir de $n+1$, leur produit est :

$$P = (n+1)(n+2)\cdots(n+k) = \frac{(n+k)!}{n!} = k!\binom{n+k}{n}.$$

Donc $\boxed{k!|P}$.

Exercice 11. ($*$) Résoudre dans $\mathbb{N}^2$ l'équation $11(x \wedge y) + (x \vee y) = 203$ (E).

Correction - Analyse. Soit $(x,y) \in \mathbb{N}^2$ solution. Comme $x \wedge y | x \vee y$ alors $x \wedge y | 203 = 7 \times 29$. Donc $x \wedge y \in 1,7,29,203$.

- **Si** $x \wedge y = 1$. Alors $(E) \Leftrightarrow 11 + xy = 203 \Leftrightarrow xy = 192 = 2^6 \times 3$. Donc $(x,y) \in \{(1,192),(192,1),(64,3),(3,64)\}$.
- **Si** $x \wedge y = 7$. On pose $\begin{cases} x = 7x' \\ y = 7y' \\ x' \wedge y' = 1 \end{cases}$. Alors $(E) \Leftrightarrow 77 + \dfrac{xy}{7} = 203 \Leftrightarrow x'y' = 18 = 2 \times 3^2$. Donc $(x',y') \in \{(1,18),(18,1),(9,2),(2,9)\}$ donc $(x,y) \in \{(7,126),(126,7),(63,14),(14,63)\}$.
- **Si** $x \wedge y = 29$. Alors $11(x \wedge y) = 319 > 203$, donc pas de solution dans $\mathbb{N}^2$.
- **Si** $x \wedge y = 203$. Alors $11(x \wedge y) > 203$, donc pas de solution dans $\mathbb{N}^2$.

Synthèse. [...]
Conclusion. $\boxed{\mathcal{S}_{(E)} = \{(1,192),(192,1),(64,3),(3,64),(7,126),(126,7),(63,14),(14,63)\}}$.

Exercice 14. ($\heartsuit$) Résoudre dans $\mathbb{Z}^2$ les équations suivantes

1) $41x + 23y = 5$ (E_1)

2) $39x + 15y = 7$ (E_2)

Correction - Méthode classique. $\mathcal{S}_{(E_1)} = \{(45 - 23k, -80 + 41k) \ / \ k \in \mathbb{Z}\}$ et $\mathcal{S}_{(E_2)} = \emptyset$.

Exercice 15. ($*$) Soient a et b deux entiers non nuls premiers entre eux et un couple de Bezout $(u_0, v_0) \in \mathbb{Z}^2$ tel que $au_0 + bv_0 = 1$.

1) Déterminer les tous les couples d'entiers $(u,v) \in \mathbb{Z}^2$ tels que $au + bv = 1$ (E)

2) Si $(a,b) \in (\mathbb{N}^*)^2$. Montrer qu'il existe deux entiers $(u,v) \in \mathbb{Z}^2$ tels que $au + bv = 1$ et $\begin{cases} |u| \leqslant b \\ |v| \leqslant a \end{cases}$.

Correction -

1) Classique : $au + bv = 1 \Leftrightarrow au + bv = au_0 + bv_0 \Leftrightarrow a(u - u_0) + b(v - v_0) = 0 \Leftrightarrow a(u - u_0) = b(v_0 - v)$ [...].
Donc $\boxed{\mathcal{S}_{(E)} = \{(u_0 + kb, v_0 - ka) \ / \ k \in \mathbb{Z}\}}$.

2)

Exercice 17. ($*$) L'équation (E) $x^3 + x^2 + 2x + 1 = 0$ admet-elle des solutions rationnelles?

Correction - Soit $x = \dfrac{p}{q}$ une solution de (E) avec $(p,q) \in \mathbb{Z} \times N^*$ et $p \wedge q = 1$. Alors

$$\frac{p^3}{q^3} + \frac{p^2}{q^2} + 2\frac{p}{q} + 1 = 0 \quad \text{c'est-à-dire} \quad p^3 + p^2q + 2pq^2 + q^3 = 0 \quad \text{c'est-à-dire} \quad p^3 + p^2q + 2pq^2 = -q^3.$$

Donc $p|q^3$ or $p \wedge q = 1$ donc $p \wedge q^3 = 1$ ce qui contredit $p|q^3$ à moins que p ne soit égal à 1 ou -1.
Si $p = 1$, alors $1 + q + 2q^2 + q^3 = 0$ donc $q + q^3 = -1 - 2q^3$. Donc $q + q^3$ est impair, ce qui est absurde (distinguer q pair, q impair).
Si $p = -1$, alors $-1 + q - 2q^2 + q^3 = 0$ donc $q + q^3 = 1 + 2q^3$. Donc $q + q^3$ est impair, ce qui est absurde (distinguer q pair, q impair).
$\boxed{\text{Il n'y a donc pas de solutions rationnelles à } (E)}$.

Exercice 18. ($\heartsuit$) Montrer que pour tout $n \in \mathbb{N} \setminus \{0,1\}$, $\dfrac{1}{4}(n^3 + (n+2)^3)$ n'est pas premier.

Correction - Soit $n \in \mathbb{N}$, $n \geqslant 2$,

$$N = \frac{1}{4}(n^3 + (n+2)^3) = \frac{1}{4}(n + (n+2))(n^2 - n(n+2) + (n+2)^2) = \frac{1}{2}(n+1)(n^2 + 2n + 4).$$

Si $n = 2p$ où $p \geqslant 1$, alors $N = (n+1)(2p^2 + 2p + 2)$ donc N n'est pas pas premier ($n + 1 \geqslant 2$ et $2p^2 + 2p + 2 \geqslant 2$).
Si $n = 2p + 1$ où $p \geqslant 0$, alors $N = (p+1)(n^2 + 2n + 4)$ donc N n'est pas pas premier ($p + 1 \geqslant 2$ et $n^2 + 2n + 4 \geqslant 2$).
Donc dans tous les cas, $\boxed{N \text{ n'est pas premier}}$.

Exercice 21. ($*$) Déterminer les nombres premiers p tels que $p^2 + 2$ soit lui-même premier.

Correction - On fait une disjonction selon le reste modulo 3.
Si $p = 3k$, p n'est premier que si $k = 1$, dans ce cas $p^2 + 2 = 11$ est premier.
Si $p = 3k + 1$, $p^2 + 2 = (9k^2 + 6k + 1) + 2 = 3(3k^2 + 2k + 1)$ donc $p^2 + 2$ n'est premier que si $k = 0$ (dans ce cas $p^2 + 2 = 3$), dans ce cas $p = 1$ n'est pas premier.
Si $p = 3k + 2$, $p^2 + 2 = (9k^2 + 12k + 4) + 2 = 3(3k^2 + 4k + 2)$ donc $p^2 + 2$ n'est pas premier.
Donc $\boxed{p = 3 \text{ est le seul nombre premier tel que } p^2 + 2 \text{ soit premier.}}$

Exercice 22. ($**$) Soit $n \in \mathbb{N}$. On note p_n le n-ième nombre premier.

1) Montrer que $p_{n+1} \leqslant p_1 p_2 \cdots p_n + 1$.

2) En déduire que $p_n \leqslant 2^{2^n}$.

3) Soit $x \in \mathbb{R}_+$. On note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x. Démontrer que pour x assez grand :

$$\ln(\ln(x)) - 1 \leqslant \pi(x) \leqslant x.$$

Correction -

1) Soit $n \in \mathbb{N}$. L'entier $p_1 p_2 \cdots p_n + 1$ est $\geqslant 2$ donc admet un diviseur premier qui n'est pas parmi $p_1, ldots, p_n$. En effet, supposons $p_k | p_1 p_2 \cdots p_n + 1$ où $1 \leqslant k \leqslant n$. Or $p_k | p_1 p_2 \cdots p_n$ donc $p_k | (p_1 p_2 \cdots p_n + 1) - p_1 p_2 \cdots p_n = 1$ absurde. Donc il existe un diviseur premier inférieur à $p_1 p_2 \cdots p_n + 1$ et supérieur à p_n. Par conséquent $\boxed{p_{n+1} \leqslant p_1 p_2 \cdots p_n + 1}$.

2) Posons pour $n \in \mathbb{N}$, $\mathcal{P}_n$: "$p_n \leqslant 2^{2^n}$".

- **Initialisation**. $p_0 = 2$ et $2^{2^0} = 2$ donc $p_0 \leqslant 2^{2^0}$.
- **Hérédité**. Soit $n \in \mathbb{N}$, supposons $\mathcal{P}_k$ vraie pour tout $k \in [\![0, n]\!]$, alors d'après 1) et l'HR :

$$p_{n+1} \leqslant 2^{2^0} 2^{2^1} \cdots 2^{2^n} + 1 = 2^{2^0 + \cdots + 2^n} + 1 = 2^{\frac{2^{n+1}-1}{2-1}} + 1 = 2^{2^{n+1}-1} + 1 \leqslant 2^{2^{n+1}}.$$

  Donc $\mathcal{P}(n+1)$ vraie.
- **Conclusion**. $\boxed{\text{Pour tout } n \in \mathbb{N},\ p_n \leqslant 2^{2^n}}$.

3) Soit $x \in \mathbb{R}_+$. On note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.
On a clairement, $\pi(x) \leqslant x$.
Puis $p_{\pi(x)} \leqslant x \leqslant p_{\pi(x)+1}$. D'après 2), $p_{\pi(x)+1} \leqslant 2^{2^{\pi(x)+1}}$ donc $x \leqslant 2^{2^{\pi(x)+1}}$. En appliquant deux fois ln qui est croissant,

$$\ln(\ln(x)) \leqslant \ln\left(2^{\pi(x)+1} \ln 2\right) = (\pi(x) + 1) \underbrace{\ln 2}_{\leqslant 1} + \underbrace{\ln(\ln 2)}_{<0} \leqslant \pi(x) + 1.$$

Donc $\pi(x) \geqslant \ln(\ln x) - 1$.
Finalement, $\boxed{\ln(\ln(x)) - 1 \leqslant \pi(x) \leqslant x.}$

Exercice 23. (**) Soit p un nombre premier supérieur ou égal à 3. Montrer que

$$\forall n \in \mathbb{Z}, \quad (n+1)^p - (n^p + 1) \equiv 0 \ [2p].$$

Correction - *On s'inspire de la démonstration du théorème de Fermat.*
Soit p un nombre premier supérieur ou égal à 3. Soit $p \in \mathbb{Z}$. D'après la formule du binôme de Newton,

$$(n+1)^p - (n^p + 1) = \sum_{k=1}^{p-1} \binom{p}{k} n^k.$$

Puis on utilise la formule de symétrie, $\binom{p}{k} = \binom{p}{p-k}$, on coupe la somme au milieu,

$$(n+1)^p - (n^p + 1) = \sum_{k=1}^{\frac{p-1}{2}} \left(\binom{p}{k} n^k + \binom{p}{p-k} n^{p-k} \right) = \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} (n^k + n^{p-k}).$$

Or $p | \binom{p}{k}$ (on utilise la formule du sélectionneur, comme dans la démo du th. de Fermat). Puis $2 | n^k + n^{p-k}$ en effet en distinguant n pair, n impair on obtient $n^k + n^{p-k}$ pair. Donc $2p | \binom{p}{k} (n^k + n^{p-k})$ et donc $2p | \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} (n^k + n^{p-k})$.

Conclusion : $\boxed{(n+1)^p - (n^p + 1) \equiv 0 \ [2p]}$.

Exercice 24. (*)

1) Résoudre dans $\mathbb{Z}^2$ le système $\begin{cases} x \equiv 7 \ [8] \\ x \equiv 1 \ [13] \end{cases}$.

2) Cas général. Soient deux entiers n_1 et n_2 premiers entre eux. Pour tout $(a_1, a_2) \in \mathbb{Z}^2$, montrer qu'il existe un entier $p \in \mathbb{Z}$ tel que pour tout $x \in \mathbb{Z}$, $\begin{cases} x \equiv a_1 \ [n_1] \\ x \equiv a_2 \ [n_2] \end{cases} \Leftrightarrow x \equiv p \ [n_1 n_2]$.

Correction -

1) Cette question est un cas particulier de la question 2).

2) Soient deux entiers n_1 et n_2 premiers entre eux et $(a_1, a_2) \in \mathbb{Z}^2$.

Analyse. Soit x solution de $\begin{cases} x \equiv a_1 \ [n_1] \\ x \equiv a_2 \ [n_2] \end{cases}$. Alors $\begin{cases} n_2 x \equiv n_2 a_1 \ [n_1 n_2] \\ n_1 x \equiv n_1 a_2 \ [n_1 n_2] \end{cases}$. Comme n_1 et n_2 sont premiers entre eux, d'après le théorème de Bezout, posons u_1, u_2 dans $\mathbb{Z}$ tels que : $n_1 u_1 + n_2 u_2 = 1$. On effectue alors la combinaison linéaire, $u_2 L_1 + u_1 L_2$,

$$u_2 n_2 x + u_1 n_1 x \equiv u_2 n_2 a_1 + u_1 n_1 a_2 \ [n_1 n_2] \qquad \text{donc} \qquad x \equiv u_2 n_2 a_1 + u_1 n_1 a_2 \ [n_1 n_2].$$

Avec $p = u_2 n_2 a_1 + u_1 n_1 a_2$, on a bien $x \equiv p \ [n_1 n_2]$.

Synthèse. Supposons $x \equiv p \ [n_1 n_2]$ avec $p = u_2 n_2 a_1 + u_1 n_1 a_2$ alors on a bien $\begin{cases} x \equiv u_2 n_2 a_1 \ [n_1] \\ x \equiv u_1 n_1 a_2 \ [n_2] \end{cases}$. Or $u_1 n_1 + u_2 n_2 = 1$ donc $u_1 n_1 \equiv 1 \ [n_2]$ et $u_2 n_2 \equiv 1 \ [n_1]$ et donc $\begin{cases} x \equiv a_1 \ [n_1] \\ x \equiv a_2 \ [n_2] \end{cases}$.

Conclusion. $\boxed{\text{Il existe un entier } p \in \mathbb{Z} \text{ tel que pour tout } x \in \mathbb{Z}, \quad \begin{cases} x \equiv a_1 \ [n_1] \\ x \equiv a_2 \ [n_2] \end{cases} \Leftrightarrow x \equiv p \ [n_1 n_2].}$.