ARITHMÉTIQUE

♦ ***Exercice 1.*** [○]
Soit $(u_n)_{n\geqslant 1}$ la suite définie par la donnée de $u_1 = 2$ et de la relation de récurrence

$$\forall n \geqslant 1, \qquad u_{n+1} = u_n + \delta_n.10^n \qquad \text{où} \qquad \delta_n = \begin{cases} 2 & \text{si } 2^{n+1} \mid u_n \\ 1 & \text{sinon} \end{cases}$$

1. Démontrer que, pour tout $n \geqslant 1$, 2^n divise u_n.
2. En déduire que, pour tout $n \geqslant 1$, 2^n possède un multiple dont l'écriture décimale ne comporte que des 1 et des 2.

1. Pour tout $n \geqslant 1$, on pose $\mathscr{P}(n)$: $2^n \mid u_n$.

   Initialisation : $u_1 = 2$ est divisible par 2 donc $\mathscr{P}(1)$ est vraie.

   Hérédité : Fixons $n \geqslant 1$ tel que $\mathscr{P}(n)$ est vraie et démontrons $\mathscr{P}(n+1)$. On distingue deux cas.
   Si 2^{n+1} divise u_n, il existe $d \in \mathbb{N}$ tel que $u_n = 2^{n+1}d$, d'où $u_{n+1} = u_n + 2.10^n = 2^{n+1}d + +2.10^n = 2^{n+1}(d + 5^n)$, ce qui démontre que 2^{n+1} divise u_{n+1}.
   Si 2^{n+1} ne divise pas u_n, alors u_n est seulement divisible par 2^n (par H.R.), c'est-à-dire qu'il existe $d \in \mathbb{N}$ impair tel que $u_n = 2^n d$. D'où $u_{n+1} = u_n + 10^n = 2^n d + 10^n = 2^n(d + 5^n)$. Comme d et 5^n sont impairs, leur somme $d + 5^n$ est paire, ce qui permet d'affirmer qu'il existe $q \in \mathbb{N}$ tel que $d + 5^n = 2q$. On a donc $u_{n+1} = 2^{n+1}q$, ce qui démontre que 2^{n+1} divise u_{n+1}.
   Dans tous les cas, on voit que $\mathscr{P}(n+1)$ est vraie.

   Conclusion : D'après le principe de récurrence, $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}^*$, c'est-à-dire

   $$\boxed{\forall n \in \mathbb{N}^*, \qquad 2^n \mid u_n.}$$

2. Pour tout $n \geqslant 1$, on pose $\mathscr{Q}(n)$: « u_n est un entier composé de n chiffres valant chacun 1 ou 2 ».

   Initialisation : $u_1 = 2$ donc $\mathscr{Q}(1)$ est vraie.

   Hérédité : Fixons $n \geqslant 1$ tel que $\mathscr{Q}(n)$ est vraie et démontrons $\mathscr{Q}(n+1)$. Par hypothèse de récurrence, il existe $\delta_0, \delta_1, \ldots, \delta_{n-1} \in \{1; 2\}$ tels que $u_n = \overline{\delta_{n-1} \ldots \delta_1 \delta_0}$. Alors

   $$u_{n+1} = u_n + \delta_n.10^n = \overline{\delta_{n-1} \ldots \delta_1 \delta_0} + \overline{\delta_n \underbrace{0 \cdots 0}_{n \text{ zéros}}} = \overline{\delta_n \delta_{n-1} \ldots \delta_1 \delta_0},$$

   ce qui démontre que $\mathscr{Q}(n+1)$ est vraie.

   Conclusion : D'après le principe de récurrence, $\mathscr{Q}(n)$ est vraie pour tout $n \in \mathbb{N}^*$, c'est-à-dire que u_n est un entier composé de n chiffres valant chacun 1 ou 2.

   Comme u_n est un multiple de 2^n d'après 1, on en déduit que

   $$\boxed{\text{pour tout } n \geqslant 1,\ 2^n \text{ possède un multiple dont l'écriture décimale ne comporte que des 1 et des 2.}}$$

♦ ***Exercice 2.*** [★]
Soit $n \geqslant 1$. Démontrer que l'entier n admet un multiple de la forme $1 \cdots 10 \cdots 0$.

Considérons les restes respectifs r_j $(j = 1, 2, \ldots, n)$ des divisions euclidiennes par n des nombres $m_1 = 1,\ m_2 = 11,\ m_3 = 111,\ \ldots,\ m_n = 11 \cdots 11$ où le dernier de ces nombres possède n chiffres 1.

Ou bien l'un de ces restes est nul et le résultat tombe immédiatement.

Ou bien, aucun de ces restes n'est nul et l'on a donc obtenu n restes dans l'ensemble $[\![1; n-1]\!]$. Le principe des tiroirs impose alors qu'il y ait forcément deux restes égaux ; disons r_k et r_ℓ. Le nombre $|m_k - m_\ell|$ est alors un multiple de n et il est bien de la forme $11 \cdots 1100 \cdots 00$. Précisons que ce nombre possède au plus n chiffres.

En conclusion,

$$\boxed{n \text{ admet un multiple de la forme } 1\cdots10\cdots0.}$$

♦ ***Exercice 3.*** [⋆]
Soient $n \in \mathbb{Z}$, $a = 2n+3$ et $b = 5n-2$. En effectuant un algorithme de type Euclide, déterminer selon les valeurs de n le pgcd de a et b.

On a

quotients	restes	coefs de Bézout	
	$5n-2$	1	0
2	$2n+3$	0	1
2	$n-8$	1	-2
	19	-2	5

d'où $19 = -2(5n-2)+5(2n+3) = 5a-2b$, ce qui laisse deux possibilités :

$$a \wedge b = 1 \qquad \text{ou} \qquad a \wedge b = 19.$$

▷ Si 19 divise a alors $2n \equiv -3 \equiv 16$ [19], ce qui donne $n \equiv 8$ [19] puisque 2 est premier avec 19. Dès lors, on a $b = 5n-2 \equiv 0$ [19], ce qui prouve que 19 divise b. Dans ce cas, on a donc $a \wedge b = 19$.

▷ Si 19 ne divise pas a, alors $a \wedge b = 1$.

Donc

$$\boxed{a \wedge b = \begin{cases} 19 & \text{si } n \equiv 8 \text{ [19]}, \\ 1 & \text{sinon.} \end{cases}}$$

♦ ***Exercice 4.*** [○]
1. Résoudre dans $\mathbb{F}_{23}$ l'équation $5x = 2$.
2. Résoudre l'équation $15x \equiv 6$ [69] d'inconnue $x \in \mathbb{Z}$.
3. Résoudre l'équation $42x \equiv 84$ [121] d'inconnue $x \in \mathbb{Z}$.
4. Résoudre l'équation $3x \equiv 8$ [12] d'inconnue $x \in \mathbb{Z}$.

1. L'algorithme d'Euclide donne

q_i	r_i	u_i	v_i
	23	1	0
4	5	0	1
1	3	1	-4
1	2	-1	5
2	1	2	-9
	0		

donc $2 \times 23 - 9 \times 5 = 1$, ce qui donne $-9 \times 5 \equiv 1$ [23] c'est-à-dire $-9 = 14$ est l'inverse de 5 dans $\mathbb{F}_{23}$. Dès lors, on a

$$5x = 2 \iff x = 2 \times 14 = 5,$$

donc

$$\boxed{\text{dans } \mathbb{F}_{23}, \text{ la solution de } 5x = 2 \text{ est } 5.}$$

2. On divise l'équation par 3, ce qui donne $5x \equiv 2$ [23]. On est ainsi ramené à la question précédente, donc

$$\boxed{\text{les solutions de } 15x \equiv 6 \text{ [69] sont les } x \in \mathbb{Z} \text{ tels que } x \equiv 5 \text{ [23]}}$$

3. Comme 42 et 121 sont clairement premiers entre eux (11 ne divise pas 42), on sait que 42 est inversible dans $\mathbb{Z}/121\mathbb{Z}$,donc

$$42x \equiv 84 \text{ [121]} \iff x \equiv 2 \text{ [121]}.$$

Donc

$$\boxed{\text{les solutions de } 42x \equiv 84 \text{ [121] sont les } x \in \mathbb{Z} \text{ tels que } x \equiv 2 \text{ [121]}}$$

4. Comme $3 \wedge 12 = 3$ et que 3 ne divise pas 8, on peut conclure tout de suite que

$$\boxed{\text{l'équation } 3x \equiv 8 \text{ [12] d'inconnue } x \in \mathbb{Z} \text{ n'a pas de solution.}}$$

♦ ***Exercice 5.*** [⋆]

1. Résoudre le système de congruences $(S_1)\begin{cases} x \equiv 2\ [23] \\ x \equiv 8\ [15] \end{cases}$ d'inconnue $x \in \mathbb{Z}$.
2. Résoudre le système de congruences $(S_2)\begin{cases} x \equiv 11\ [12] \\ x \equiv 8\ [15] \end{cases}$ d'inconnue $x \in \mathbb{Z}$.

1. On a la relation de Bézout suivante :

$$2 \times 23 - 3 \times 15 = 1.$$

On en déduit que $-45 \equiv 1\ [23]$ et $-45 \equiv 0\ [15]$, ce qui donne, après multiplication par 2,

$$-90 \equiv 2\ [23] \qquad \text{et} \qquad -90 \equiv 0\ [15].$$

On en déduit aussi que $46 \equiv 0\ [23]$ et $46 \equiv 1\ [15]$, ce qui donne, après multiplication par 8,

$$368 \equiv 0\ [23] \qquad \text{et} \qquad 368 \equiv 8\ [15].$$

En additionnant deux à deux ces égalités modulaires, on en déduit que

$$278 \equiv 2\ [23] \qquad \text{et} \qquad 278 \equiv 8\ [15],$$

ce qui signifie que

$$278 \text{ est une solution particulière du système de congruences.}$$

Alors

$$(S_1) \iff \begin{cases} x - 278 \equiv 0\ [23] \\ x - 278 \equiv 0\ [15] \end{cases} \iff x - 278 \equiv 0\ [345]$$

où la dernière équivalence découle du fait que 23 et 15 sont premiers entre eux. En conclusion,

$$\boxed{(S_1) \iff x \equiv 278\ [345].}$$

2. On a $12 \wedge 15 = 3$ et $3 \mid (11 - 8)$ donc tout roule. De plus, ici, il est clair que

$$23 \text{ est une solution particulière du système de congruences.}$$

Alors

$$(S_2) \iff \begin{cases} x - 23 \equiv 0\ [12] \\ x - 23 \equiv 0\ [15] \end{cases} \iff x - 23 \equiv 0\ [60]$$

où la dernière équivalence découle du fait que le ppcm de 12 et 15 est 60. En conclusion,

$$\boxed{(S_2) \iff x \equiv 23\ [60].}$$

♦ ***Exercice 6.*** [○]

Déterminer le nombre de manières de payer 641 euro en utilisant seulement des pièces de 2 euro et des billets de 5 euro.

Résolvons l'équation, d'inconnues $x, y \in \mathbb{Z}$,

$$2x + 5y = 641.$$

On commence par remarquer que $2 \wedge 5 = 1$ divise 641 et donc que l'équation admet, d'après le cours, une infinité de solutions.

On détermine ensuite un couple de coefficients de Bézout (α, β) tel que $2\alpha + 5\beta = 1$. On peut bien sûr appliquer l'algorithme d'Euclide mais il est plus simple de remarquer que $(\alpha, \beta) = (-2, 1)$ est une solution évidente. En multipliant alors par 641, on obtient que $2 \times (-1282) + 5 \times (641) = 641$.

On sait alors, d'après le cours, que l'ensemble $\mathscr{S}$ des solutions $(x, y) \in \mathbb{Z}^2$ de $2x + 5y = 641$ est

$$\mathscr{S} = \big\{(-1282 + 5k\,,\, 641 - 2k) : k \in \mathbb{Z}\big\}.$$

Déterminer le nombre de manières de payer 641 euro en utilisant seulement des pièces de 2 euro et des billets de 5 euro revient à déterminer le nombre de couples, contenus dans l'ensemble $\mathscr{S}$, dont les deux coordonnées sont positives ou nulles. Autrement dit, on recherche le nombre de valeurs de $k \in \mathbb{Z}$ telles que

$$-1282 + 5k \geqslant 0 \qquad \text{et} \qquad 641 - 2k \geqslant 0,$$

ce qui est équivalent à

$$\frac{1282}{5} \leqslant k \leqslant \frac{641}{2},$$

c'est-à-dire

$$257 \leqslant k \leqslant 320.$$

On obtient donc $320 - 257 + 1 = 64$ solutions, ce qui signifie qu'

il y a 64 manières de payer 641 euro en utilisant seulement des pièces de 2 euro et des billets de 5 euro.

♦ ***Exercice 7.*** [⋆]
Soient $n, a, b \in \mathbb{N}^*$. Démontrer que $(n^a - 1) \wedge (n^b - 1) = n^{a \wedge b} - 1$.

On propose deux démonstrations.

- ▷ Comme $a \wedge b$ divisent a et b, la formule de Bernoulli nous dit que

$$n^{a\wedge b} - 1 \mid n^a - 1 \qquad \text{et} \qquad n^{a\wedge b} - 1 \mid n^b - 1,$$

donc

$$n^{a\wedge b} - 1 \mid (n^a - 1) \wedge (n^b - 1).$$

▷ Posons $d = (n^a - 1) \wedge (n^b - 1)$. Plaçons nous dans $\mathbb{Z}/d\mathbb{Z}$. Comme d divise $n^a - 1$ et $n^b - 1$, on a $n^a = 1$ et $n^b = 1$ dans $\mathbb{Z}/d\mathbb{Z}$. Le théorème de Bézout nous dit qu'il existe $u, v \in \mathbb{Z}$ tels que $a \wedge b = au + bv$. Comme n est inversible dans $\mathbb{Z}/d\mathbb{Z}$ (puisque $n^a = 1$ nous dit que n^{a-1} est l'inverse de n), les éléments n^{au} et n^{bv} existent. Alors, dans $\mathbb{Z}/d\mathbb{Z}$, on a

$$n^{a\wedge b} = n^{au+bv} = (n^a)^u (n^b)^v = 1^u 1^v = 1.$$

Dans $\mathbb{Z}$, cela signifie que

$$(n^a - 1) \wedge (n^b - 1) \mid n^{a\wedge b} - 1.$$

On a donc $(n^a - 1) \wedge (n^b - 1) = n^{a\wedge b} - 1$.

- Soit $a = bq + r$ la division euclidienne de a par b. Alors

$$\begin{aligned} n^a - 1 &= n^{bq+r} - 1 \\ &= n^r(n^{bq} - 1) + n^r - 1 \qquad \text{Binet !} \\ &= n^r(n^b - 1)(\cdots) + n^r - 1 \qquad \text{Formule de Bernoulli} \end{aligned}$$

avec $n^r - 1 < n^b - 1$, ce qui démontre que le reste de la division euclidienne de $n^a - 1$ par $n^b - 1$ est $n^r - 1$. Il s'ensuit que

$$(n^a - 1) \wedge (n^b - 1) = (n^b - 1) \wedge (n^r - 1).$$

Notons $r_0 = a$, $r_1 = b$, r_2, r_3, …, $r_{N-1} = a \wedge b$ et $r_N = 0$ les restes dans l'algorithme d'Euclide. En itérant le résultat ci-dessus, on obtient

$$\begin{aligned} (n^a - 1) \wedge (n^b - 1) &= (n^{r_0} - 1) \wedge (n^{r_1} - 1) \\ &= (n^{r_1} - 1) \wedge (n^{r_2} - 1) \\ &= \cdots \\ &= (n^{a\wedge b} - 1) \wedge (n^0 - 1) \\ &= (n^{a\wedge b} - 1) \wedge 0 \\ &= n^{a\wedge b} - 1. \end{aligned}$$

En conclusion,

$$\boxed{(n^a - 1) \wedge (n^b - 1) = n^{a\wedge b} - 1.}$$

♦ ***Exercice 8.*** [○]
Soit $n \in \mathbb{N}^*$. Démontrer que $n!+1$ et $(n+1)!+1$ sont premiers entre eux.

Notons δ le pgcd de nos deux nombres. Alors δ divise $(n+1)(n!+1) - \big((n+1)!+1\big) = n$ et donc δ divise $n!$. Comme il divise aussi $n!+1$, δ divise 1, c'est-à-dire $\delta = 1$. Donc

$$\boxed{n!+1 \text{ et } (n+1)!+1 \text{ sont premiers entre eux.}}$$

♦ ***Exercice 9.*** [○]
Résoudre l'équation $(x \vee y) - (x \wedge y) = 9$, d'inconnues $x, y \in \mathbb{N}^*$ avec $x \geqslant y$.

Notons $\delta = x \wedge y$. Comme δ divise $x \vee y$ et $x \wedge y$, il est nécessaire que δ divise $9 = 3^2$ pour que l'équation admette des solutions. Donc $\delta \in \{1; 3; 9\}$.

- ▷ Si $\delta = 1$, l'équation devient $xy - 1 = 9$, c'est-à-dire $xy = 10 = 2 \times 5$, d'où $(x, y) = (10, 1)$ ou $(x, y) = (5, 2)$.
- ▷ Si $\delta = 3$, l'équation devient $xy/3 - 3 = 9$, c'est-à-dire $xy = 36 = 2^2 \times 3^2$, d'où $(x, y) = (12, 3)$.
- ▷ Si $\delta = 9$, l'équation devient $xy/9 - 9 = 9$, c'est-à-dire $xy = 162 = 2 \times 3^4$, d'où $(x, y) = (18, 9)$.

En conclusion,

$$\boxed{\text{les solutions } (x, y) \in \mathbb{N}^{*2} \text{ telles que } x \geqslant y \text{ de l'équation } (x \vee y) - (x \wedge y) = 9 \text{ sont } (10, 1), (5, 2), (12, 3) \text{ et } (18, 9).}$$

♦ ***Exercice 10.*** [⋆]
1. Soient $s, d \in \mathbb{N}^*$. Expliquer comment résoudre le système $\begin{cases} x + y = s \\ x \wedge y = d \end{cases}$ d'inconnues $x, y \in \mathbb{N}$.
   Traiter le cas $s = 360$ et $d = 10$.
2. Soient $p, d \in \mathbb{N}^*$. Expliquer comment résoudre le système $\begin{cases} xy = p \\ x \wedge y = d \end{cases}$ d'inconnues $x, y \in \mathbb{N}$.
   Traiter le cas $d = 48$ et $d = 2$.

1. Méthode
   Comme $x \wedge y$ divise $x + y$, il est nécessaire que $d \mid s$. Par conséquent, si d ne divise pas s, le problème n'a pas de solution. Sinon, si d divise s, on pose $X = x/d$, $Y = y/d$ et $S = s/d$ ce qui nous ramène au système
   $$\begin{cases} X + Y = S \\ X \wedge Y = 1 \end{cases}$$
   On constate (y réfléchir) que ce système est équivalent à
   $$\begin{cases} X + Y = S \\ X \wedge S = 1 \end{cases}$$
   Si $S = 1$, les seules solutions possibles sont $(X, Y) = (1, 0)$ ou $(X, Y) = (0, 1)$ et on n'en parle plus. Si $S \neq 1$, on veut les X de $[\![1; S]\!]$ qui sont premiers avec S. Pour cela, on décompose S en nombre premier puis on crible l'intervalle $[\![1; S]\!]$ par les multiples des nombres premiers de la décomposition primaire de S. Les nombres restants donnent les différents valeurs de X possibles. À chaque valeur de X trouvée correspond une valeur de Y donnée par $Y = S - X$. Comme $X \wedge S = 1$, on a aussi $X \wedge Y = 1$. Dès lors, en multipliant chaque couple (X, Y) ainsi déterminé par d, on obtient toutes les solutions.

   Exemple
   On veut résoudre le système
   $$(S) \begin{cases} x + y = 360 \\ x \wedge y = 10 \end{cases}$$
   On constate tout d'abord que 10 divise 360 donc ça roule. On divise tout par 10 en posant $X = x/10$ et $Y = y/10$, ce qui donne
   $$(S) \iff \begin{cases} X + Y = 36 \\ X \wedge Y = 1 \end{cases} \iff \begin{cases} X + Y = 36 \\ X \wedge 36 = 1 \end{cases}$$

Comme $36 = 2^2 \times 3^2$, on crible l'intervalle $[\![1;36]\!]$ par les multiples de 2 et 3, ce qui donne

1	~~2~~	~~3~~	~~4~~	5	~~6~~
7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~
19	~~20~~	~~21~~	~~22~~	23	~~24~~
25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~

donc

$$\begin{aligned}(S) &\iff X \in \{1;5;7;11;13;17;19;23;25;29;31;35\} \text{ et } Y = 36 - X \\ &\iff (X,Y) \in \left\{ \begin{array}{l} (1,35);(5,31);(7,29);(11,25);(13,23);(17,19); \\ (19,17);(23,13);(25,11);(29,7);(31,5);(35,1) \end{array} \right\}.\end{aligned}$$

En mutlipliant par 10, on obtient

$$\boxed{(S) \iff (x,y) \in \left\{ \begin{array}{l} (10,350);(50,310);(70,290);(110,250);(130,230);(170,190); \\ (190,170);(230,130);(250,110);(290,70);(310,50);(350,10) \end{array} \right\}.}$$

2. Méthode

Comme $(x \wedge y)^2$ divise xy, il est nécessaire que $d^2 \mid p$. Par conséquent, si d^2 ne divise pas p, le problème n'a pas de solution. Sinon, si d^2 divise p, on pose $X = x/d$, $Y = y/d$ et $P = p/d^2$ ce qui nous ramène au système

$$\left\{ \begin{array}{l} XY = P \\ X \wedge Y = 1 \end{array} \right.$$

On cherche donc des couples de diviseurs de P dont le produit fait P et qui n'ont pas de facteurs premiers en commun. Pour cela, on décompose P en facteurs premiers et l'on détermine tous les diviseurs X de P dont chacune des valuations p-adiques est ou bien nulle ou bien égale à la valuation p-adique de P. À chaque valeur de X trouvée correspond une valeur de Y donnée par $Y = P/X$. La condition sur les valuations p-adiques assurant que X et Y n'ont pas de facteurs premiers en commun donc qu'ils sont premiers entre eux. Dès lors, en multipliant chaque couple (X,Y) ainsi déterminé par d, on obtient toutes les solutions.

Exemple

On veut résoudre le système

$$(S) \left\{ \begin{array}{l} xy = 48 \\ x \wedge y = 2 \end{array} \right.$$

On constate tout d'abord que 2^2 divise 48 donc ça roule. On divise tout par 2 en posant $X = x/2$ et $Y = y/2$, ce qui donne

$$(S) \iff \left\{ \begin{array}{l} XY = 12 \\ X \wedge Y = 1 \end{array} \right.$$

Comme $12 = 2^2 \times 3$, on a

$$\begin{aligned}(S) &\iff X \in \{1;3;4;12\} \text{ et } Y = 12/X \\ &\iff (X,Y) \in \{(1,12);(3,4);(4,3);(12,1)\}.\end{aligned}$$

En mutlipliant par 2, on obtient

$$\boxed{(S) \iff (x,y) \in \{(2,24);(6,8);(8,6);(24,2)\}.}$$

♦ ***Exercice 11.*** [⋆]
Soient $a, b \in \mathbb{N} \setminus \{0;1\}$ tels que $ab-1 \in \mathbb{P}$. Résoudre l'équation $(x \wedge y) + (x \vee y) = ax + by$ d'inconnues $x, y \in \mathbb{N}$.

Si $x = 0$ et $y = 0$, on constate que $(x;y) = (0;0)$ est bien une solution. Dorénavant, on suppose que $x \neq 0$ ou $y \neq 0$.

▷ Analyse : Posons $\delta = x \wedge y$ qui est non nul. Alors

$$\begin{aligned}
& (x \wedge y) + (x \vee y) = ax + by \\
\iff \quad & \delta + \frac{xy}{\delta} = ax + by \\
\iff \quad & 1 + \frac{x}{\delta}\frac{y}{\delta} = a\frac{x}{\delta} + b\frac{y}{\delta} \\
\iff \quad & 1 + XY = aX + bY \qquad \text{en posant } X = \frac{x}{\delta} \text{ et } Y = \frac{y}{\delta} \\
\iff \quad & aX + bY - XY = 1 \\
\iff \quad & X(a-Y) + bY = 1 \\
\iff \quad & X(a-Y) + b(Y-a) + ab = 1 \qquad \text{Binet} \\
\iff \quad & (X-a)(a-Y) = 1-ab \\
\iff \quad & (X-a)(Y-b) = ab-1 \\
\iff \quad & \left\{\begin{array}{l} X-a = ab-1 \\ Y-b = 1 \end{array}\right. \text{ ou } \left\{\begin{array}{l} X-a = 1 \\ Y-b = ab-1 \end{array}\right. \text{ ou } \left\{\begin{array}{l} X-a = -ab+1 \\ Y-b = -1 \end{array}\right. \text{ ou } \left\{\begin{array}{l} X-a = -1 \\ Y-b = -ab+1 \end{array}\right. \\
\iff \quad & \left\{\begin{array}{l} X = a+ab-1 \\ Y = b+1 \end{array}\right. \text{ ou } \left\{\begin{array}{l} X = a+1 \\ Y = ab+b-1 \end{array}\right. \text{ ou } \underbrace{\left\{\begin{array}{l} X = a-ab+1 \\ Y = b-1 \end{array}\right.}_{\text{à rejeter car } X<0} \text{ ou } \underbrace{\left\{\begin{array}{l} X = a-1 \\ Y = b-ab+1 \end{array}\right.}_{\text{à rejeter car } Y<0} \\
\iff \quad & \left\{\begin{array}{l} x = \delta(a+ab-1) \\ y = \delta(b+1) \end{array}\right. \text{ ou } \left\{\begin{array}{l} x = \delta(a+1) \\ y = \delta(ab+b-1) \end{array}\right. .
\end{aligned}$$

ce qui démontre que les solutions sont de la forme

$$(x,y) = \big(n(a+ab-1), n(b+1)\big) \qquad \text{ou} \qquad (x,y) = \big(n(a+1), n(ab+b-1)\big)$$

où $n \in \mathbb{N}$.

▷ Synthèse : On a $(a+ab-1) - a(b+1) = -1$ donc $(a+ab-1) \wedge (b+1) = 1$ d'après Bézout. Il est alors facile de voir que le couple $(a+ab-1, b+1)$ est une solution de l'équation et d'en déduire que tous les couples $\big(n(a+ab-1), n(b+1)\big)$, pour n parcourant $\mathbb{N}$, sont solutions de l'équation.

De même, on démontre que tous les couples $\big(n(a+1), n(ab+b-1)\big)$, pour n parcourant $\mathbb{N}$, sont solutions de l'équation.

Donc l'ensemble $\mathscr{S}$ des solutions est

$$\boxed{\mathscr{S} = \big\{\big(n(a+ab-1), n(b+1)\big) : n \in \mathbb{N}\big\} \cup \big\{\big(n(a+1), n(ab+b-1)\big) : n \in \mathbb{N}\big\}}$$

♦ ***Exercice 12.*** [○]
Démontrer que si un nombre réel x est tel que ax et bx sont entiers, avec a et b entiers premiers entre eux, alors x est entier.

Comme $a \wedge b = 1$, le théorème de Bézout dit qu'il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$. En multipliant par x, il vient $x = uax + vbx \in \mathbb{Z}$. Donc

$$\boxed{x \in \mathbb{Z}.}$$

♦ ***Exercice 13.*** [○]
Soient $n, m \in \mathbb{N}^*$. Démontrer que $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}$.

Posons $\delta = n \wedge m$.

Comme $\delta \mid n$, il existe $q \in \mathbb{N}^*$ tel que $n = \delta q$. Alors si $z \in \mathbb{U}_\delta$, on a $z^\delta = 1$, ce qui donne $(z^\delta)^q = 1^1$, c'est-à-dire $z^n = 1$. Donc $z \in \mathbb{U}_n$. Cela démontre que $\mathbb{U}_\delta \subset \mathbb{U}_n$.
On démontre de même que $\mathbb{U}_\delta \subset \mathbb{U}_m$.
Donc $\mathbb{U}_\delta \subset \mathbb{U}_n \cap \mathbb{U}_m$.

Il existe des coefficients de Bézout $u, v \in \mathbb{Z}$ tels que $un + vm = \delta$. Alors, si $z \in \mathbb{U}_n \cap \mathbb{U}_m$ c'est-à-dire si $z^n = z^m = 1$, on a $z^\delta = z^{un+vm} = (z^n)^u (z^n)^v = 1^u 1^v = 1$, ce qui donne $z \in \mathbb{U}_\delta$. Donc $\mathbb{U}_n \cap \mathbb{U}_m \subset \mathbb{U}_\delta$.

En conclusion,

$$\boxed{\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}.}$$

♦ ***Exercice 14.*** [○]
Soient $p < q$ deux nombres premiers. Démontrer que p et q sont jumeaux (c'est-à-dire $q = p+2$) si, et seulement si, $pq + 1$ est un carré.

L'existence d'une infinité de nombres premiers jumeaux est un célèbre problème ouvert.

Si p et q sont jumeaux, on a $q = p + 2$, d'où $pq + 1 = p(p + 2) + 1 = p^2 + 2p + 1 = (p + 1)^2$ donc $pq + 1$ est un carré.

Réciproquement, supposons que $pq + 1$ est un carré, disons $pq + 1 = a^2$ où $a \in \mathbb{N}$. Alors $pq = a^2 - 1 = (a - 1)(a + 1)$ et, comme p et q sont premiers avec $p < q$, on a $p = a - 1$ et $q = a + 1$, d'où $q = p + 2$. Cela prouve que p et q sont jumeaux.
Donc

$$\boxed{p \text{ et } q \text{ sont deux nombres premiers jumeaux si, et seulement si, } pq + 1 \text{ est un carré.}}$$

♦ ***Exercice 15.*** [⋆] (Nombres de Mersenne et de Fermat)

1. Pour tout $n \in \mathbb{N}$, on considère le n-ème nombre de Mersenne $M_n = 2^n - 1$.
   Soit $k \in \mathbb{N}^*$. Démontrer que si M_k est premier, alors k est premier.
2. Pour tout $n \in \mathbb{N}$, on considère le n-ème nombre de Fermat $F_n = 2^{(2^n)} + 1$.
   a) Soit $k \in \mathbb{N}^*$. Démontrer que si $2^k + 1$ est premier, alors $2^k + 1$ est un nombre de Fermat.
   b) Démontrer que, pour tout $n \in \mathbb{N}^*$, on a $F_0 \times F_1 \times \cdots \times F_{n-1} = F_n - 2$ et en déduire que deux nombres de Fermat distincts sont premiers entre eux.

1. Raisonnons par contraposition. On suppose que k admet un diviseur stricte a, de sorte que $k = ab$ où $a, b \in [\![2; k - 1]\!]$. Alors, d'après la formule de Bernoulli, on a

$$2^k - 1 = (2^a)^b - 1 = (2^a - 1)(\cdots),$$

ce qui prouve que $2^k - 1$ n'est pas premier. En conclusion,

$$\boxed{\text{si } M_k \text{ est premier, alors } k \text{ est premier.}}$$

2. a) Raisonnons par contraposition. On suppose que k admet un diviseur premier impair p, de sorte que $k = pq$ où $q \in \mathbb{N}^*$. Alors, d'après la formule de Bernoulli, on a

$$2^k + 1 = (2^q)^p - (-1)^p = (2^q + 1)(\cdots),$$

ce qui prouve que $2^k + 1$ n'est pas premier. En conclusion,

$$\boxed{\text{les seuls nombres premiers de la forme } 2^k + 1, \text{ avec } k \in \mathbb{N}^*, \text{ sont tels que } k = 2^n \text{ où } n \in \mathbb{N}.}$$

b) Démontrons par récurrence que, pour tout $n \in \mathbb{N}^*$, on a $\mathscr{P}(n) : F_0 \times F_1 \times \cdots \times F_{n-1} = F_n - 2$.

Initialisation : On a $F_0 = 2^{(2^0)} + 1 = 2^1 + 1 = 3$ et $F_1 - 2 = 2^{(2^1)} + 1 - 2 = 2^2 - 1 = 3$ donc $\mathscr{P}(1)$ est vraie.

Hérédité : Fixons $n \in \mathbb{N}^*$ et supposons que $\mathscr{P}(n)$ est vraie. On a

$$\begin{aligned} F_0 \times F_1 \times \cdots \times F_{n-1} \times F_n &= (F_n - 2) \times F_n \qquad \text{(par hyp. de réc.)} \\ &= \big(2^{(2^n)} - 1\big)\big(2^{(2^n)} + 1\big) \qquad \text{(par déf. de } F_n\text{)} \\ &= \big(2^{(2^n)}\big)^2 - 1 \\ &= 2^{2^{n+1}} - 1 \\ &= F_{n+1} - 2, \end{aligned}$$

donc $\mathscr{P}(n+1)$ est vraie.

Conclusion : D'après le principe de récurrence, $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}^*$, c'est-à-dire

$$\boxed{\forall n \in \mathbb{N}^*, \qquad F_0 \times F_1 \times \cdots \times F_{n-1} = F_n - 2.}$$

Soient $0 \leqslant k < n$. D'après la formule de la question a), on a $F_n - F_0 \times F_1 \times \cdots \times F_{n-1} = 2$, c'est-à-dire $F_n - mF_k = 2$ où $m = F_0 \times F_1 \times \cdots \times F_{k-1} \times F_{k+1} \times \cdots \times F_{n-1}$. D'après le théorème de Bézout, $F_n \wedge F_k$ divise 2. Comme F_n et F_k sont impairs, on en déduit que $F_n \wedge F_k = 1$. Donc

$$\boxed{\text{deux nombres de Fermat distincts sont premiers entre eux.}}$$

♦ ***Exercice 16.*** [○]

1. Soient $a, b \in \mathbb{N}$. Démontrer que si b^2 divise a^2 alors b divise a et a^2/b^2 est un carré.
2. Soit $m \in \mathbb{N}$. Démontrer que $\sqrt{m} \in \mathbb{Q}$ si, et seulement si, m est un carré.

1. Pour tout $p \in \mathbb{P}$, on a $v_p(a^2) \geqslant v_p(b^2)$, c'est-à-dire $2v_p(a) \geqslant 2v_p(b)$ ou encore $v_p(a) \geqslant v_p(b)$, donc b divise a. Par ailleurs, on a $v_p(a^2/b^2) = v_p(a^2) - v_p(b^2) = 2\big(v_p(a) - v_p(b)\big)$ ce qui prouve que toutes les valuations de a^2/b^2 sont paires, c'est-à-dire que a^2/b^2 est un carré. En conclusion,

$$\boxed{\text{si } b^2 \text{ divise } a^2 \text{ alors } b \text{ divise } a \text{ et } a^2/b^2 \text{ est un carré.}}$$

2. Si m est un carré, alors $\sqrt{m}$ est un entier et donc, a fortiori un rationnel.

   Réciproquement, supposons de $\sqrt{m} \in \mathbb{Q}$, c'est-à-dire $\sqrt{m} = a/b$ avec $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. En élevant au carré, il vient $mb^2 = a^2$, ce qui démontre que b^2 divise a^2. D'après la première question, on en déduit que $m = a^2/b^2$ est un carré.

   En conclusion,

$$\boxed{\sqrt{m} \in \mathbb{Q} \text{ si, et seulement si, } m \text{ est un carré.}}$$

♦ ***Exercice 17.*** [○]
Par combien de 0 se termine le nombre 100! ?

Cela revient à déterminer la plus grande puissance de 10 qui divise 100!

Entre 1 et 100, on trouve 50 nombres pairs ; 25 nombres divisibles par 4 ; 12 nombres divisibles par 8 ; 6 nombres divisibles par 16 ; 3 nombres divisibles par 32 et 1 nombre divisible par 64. Par conséquent, la puissance de 2 dans la décomposition en facteurs premiers de 100! est $50 + 25 + 12 + 6 + 3 + 1 = 97$.

De la même manière, on trouve 20 multiples de 5 et 4 multiples de 25. La puissance de 5 dans la décomposition en facteurs premiers de 100! est donc $20 + 4 = 24$.

On en déduit que 100! est divisible par 10^{24} et pas par 10^{25} et donc que

$$\boxed{100! \text{ se termine par 24 zéros.}}$$

♦ ***Exercice 18.*** [⋆]

Soit $n \geqslant 2$. On décompose n en facteurs premiers : $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ où les p_j sont des nombres premiers distincts deux à deux et $\alpha_j \in \mathbb{N}^*$.

1. Déterminer en fonction des α_j le nombre $\tau(n)$ de diviseurs de n.

   Quel sont les nombres inférieurs ou égaux à 100 qui admettent le plus grand nombre de diviseurs. Quelle remarque cela vous inspire ?
2. Déterminer en fonction des α_j et des p_j la somme $\sigma(n)$ de tous les diviseurs de n.
3. Vérifier que si $m \wedge n = 1$, on a $\tau(mn) = \tau(m)\tau(n)$ et $\sigma(mn) = \sigma(m)\sigma(n)$. On dit que τ et σ sont des fonctions arithmétiques *multiplicatives*.

1. Un nombre m est un diviseur de n si et seulement s'il s'écrit sous la forme $m = p_1^{\beta_1} \dots p_k^{\beta_k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour $i = 1, \dots, k$. Le nombre de diviseurs de n est donc en bijection avec le nombres de k-uplets $(\beta_1, \dots, \beta_k) \in \prod_{1 \leqslant i \leqslant k} [\![0; \alpha_i]\!]$, ce qui donne

$$\boxed{\tau(n) = \prod_{i=1}^{k} (\alpha_i + 1).}$$

   Pour avoir un maximum de diviseurs, un nombre n doit avoir un maximum de facteurs premiers. Comme $2 \times 3 \times 5 < 100 < 2 \times 3 \times 5 \times 7$, le nombre recherché doit donc être de la forme $n = 2^\alpha 3^\beta 5^\gamma 7^\delta$ avec $\alpha, \beta, \gamma, \delta \geqslant 1$. Pour augmenter le nombre de diviseurs, on essaye maintenant d'augmenter $\alpha, \beta, \gamma, \delta$ mais les possibilités sont limitées si l'on ne veut pas dépasser 100. On a $(\alpha, \beta, \gamma, \delta) = (2, 1, 1, 0)$ qui donne $n = 60$, $(\alpha, \beta, \gamma, \delta) = (3, 2, 0, 0)$ qui donne $n = 72$, $(\alpha, \beta, \gamma, \delta) = (2, 1, 0, 1)$ qui donne $n = 84$, $(\alpha, \beta, \gamma, \delta) = (1, 2, 1, 0)$ qui donne $n = 90$, $(\alpha, \beta, \gamma, \delta) = (5, 1, 0, 0)$ qui donne $n = 96$. Ces cinq nombres ont 12 diviseurs. Donc

> 60, 72, 84, 90 et 96 sont les cinq nombres, inférieurs ou égaux à 100, qui ont le plus grand nombre de diviseurs, à savoir 12.

   Un tel nombre est pratique pour découper les heures en minutes (et les minutes en secondes). Pour faire simple, on a choisi le plus petit de ces nombres, i.e. 60. Voilà pourquoi les heures comptent 60 minutes : pour être facilement divisibles sans tomber sur des nombres à virgule ! Avec 60 minutes dans une heure, une demi-heure compte 30 minutes, un tiers d'heure compte 20 minutes, un quart d'heure compte 15 minutes, un cinquième d'heure compte 12 minutes et un sixième d'heure compte 10 minutes. Ce n'est qu'à partir du septième d'heure que l'on trouve un nombre décimal de minutes. Le choix de découper les heures en 100 minutes, qui aurait davantage collé à notre système de numération en base dix, aurait posé un problème de division dès le tiers d'heure.
   La remarque vaut aussi pour les angles et le découpage du cercle trigonométrie en 360 degrés !
2. Avec les notations de la question précédente, on a

$$\sigma(n) = \sum_{(\beta_1, \dots, \beta_k) \in \prod\limits_{1 \leqslant i \leqslant k} [\![0; \alpha_i]\!]} p_1^{\beta_1} \dots p_k^{\beta_k} = \prod_{i=1}^{k} \sum_{\ell=0}^{\alpha_i} p_i^\ell = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

   Donc

$$\boxed{\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.}$$

3. Les quantités $\tau(n)$ et $\sigma(n)$ sont des produits sur l'ensemble des facteurs premiers de n. Si n et m sont premiers entre eux, leurs ensembles de facteurs premiers sont disjoints, donc le produit sur les facteurs premiers de nm est obtenu en multipliant le produit sur les facteurs premiers de n avec le produit sur les facteurs premiers de m, autrement dit $\tau(nm) = \tau(n)\tau(m)$ et $\sigma(nm) = \sigma(n)\sigma(m)$. Donc

> τ et σ sont des fonctions arithmétiques multiplicatives.

♦ ***Exercice 19.*** [⋆]
Soit $n \in \mathbb{N} \setminus \{0;1\}$. Déterminer une série de n nombres entiers consécutifs qui ne sont pas premiers.

Pour tout $k \in [\![2;n]\!]$, le nombre $n!+k$ est divisible par k donc n'est pas premier. La famille $(n!+k)_{k\in[\![2;n]\!]}$ constitue donc une série de $n-1$ nombres non premiers consécutifs. Comme n est quelconque, on en déduit bien que

on peut trouver des séries d'entiers consécutifs non premiers aussi longues qu'on le souhaite.

On ne peut évidemment pas espérer trouver des séries de nombres premiers consécutifs, puisque deux nombres premiers ne peuvent pas être consécutifs (sauf 2 *et* 3*) ! Toutefois, le théorème de Green–Tao (démontré en 2004) énonce qu'il existe des séries de nombres premiers en progression arithmétique aussi longues qu'on le souhaite.*

Par exemple, les nombres $43\,142\,746\,595\,714\,191 + 23\,681\,770\,223\,092\,870n$ *où* $n \in [\![0;25]\!]$ *forment une série de* 26 *nombres premiers en progression arithmétique.*

♦ ***Exercice 20.*** [⋆]
Le théorème de la progression arithmétique de Dirichlet énonce que si a et n sont deux entiers naturels non nuls premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo n. Le théorème d'Euclide traite le cas $n = 2$. L'objectif de cet exercice est de traiter le cas $n = 4$. La démonstration du théorème dans son cas général est très difficile.

1. Démontrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4. *Indication :* $N = 4p_1 \dots p_n - 1$
2. a) Soient $a \in \mathbb{Z}$ et p un nombre premier impair tel que p divise $a^2 + 1$. Démontrer que p est congru à 1 modulo 4. *Indication : Utiliser le petit théorème de Fermat.*
   b) Démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

1. Raisonnons par l'absurde en supposant qu'il existe un nombre fini de nombres premiers congrus à 3 modulo 4 et notons les $p_1, \dots, p_n$. On pose alors
$$N = 4p_1 \dots p_n - 1.$$
Notons que $N \equiv 3\ [4]$.
Par ailleurs, comme N est impair et premier avec tous les p_i, tous les diviseurs premiers de N sont congrus à 1 modulo 4. Un produit de nombres congrus à 1 modulo 4 étant lui-même congru à 1 modulo 4, le nombre N est donc lui-même congru à 1 modulo 4.
On a donc $3 \equiv 1\ [4]$, ce qui est absurde !
Donc
il existe une infinité de nombres premiers congrus à 3 modulo 4.

2. a) Raisonnons par l'absurde en supposant que p n'est pas congru à 1 modulo 4.
Alors p est congru à 3 modulo 4, c'est-à-dire qu'il existe $k \in \mathbb{N}$ tel que $p = 3 + 4k$. Dès lors, on a $a^{p-1} \equiv (a^2)^{1+2k} \equiv (-1)^{1+2k} \equiv -1\ [p]$.
Comme p divise $a^2 + 1$, les nombres a et p sont premiers entre eux. Dès lors, le petit théorème de Fermat nous dit que $a^{p-1} \equiv 1\ [p]$.
On a donc $1 \equiv -1\ [p]$, ce qui implique que $p = 2$. C'est absurde !
En conclusion,
p est congru à 1 modulo 4.

   b) Raisonnons par l'absurde en supposant qu'il existe un nombre fini de nombres premiers congrus à 1 modulo 4 et notons les $p_1, \dots, p_n$. On pose alors
$$N = (2p_1 \dots p_n)^2 + 1.$$
Comme N est impair et supérieur ou égal à 2, il admet un facteur premier impair p. La question a) nous dit que p est congru à 1 modulo 4. Par ailleurs, p divisant N, il est nécessairement distinct de $p_1, \dots, p_n$. C'est absurde ! Donc
il existe une infinité de nombres premiers congrus à 1 modulo 4.

♦ ***Exercice 21.*** [○]
Déterminer le plus petit entier naturel n dont le reste dans la division par 2 est 1, le reste dans la division par 3 est 2, le reste dans la division par 4 est 3, ..., le reste dans la division par 9 est 8.

Les hypothèses se traduisent par $n \equiv 1 \pmod 2$, $n \equiv 2 \pmod 3$, ..., $n \equiv 8 \pmod 9$, donc $n+1 \equiv 0 \pmod 2$, $n+1 \equiv 0 \pmod 3$, ..., $n+1 \equiv 0 \pmod 9$, ce qui signifie que $n+1$ est divisible par 2, par 3, ..., par 9 ou encore que $n+1$ est divisible par $2 \wedge 3 \wedge \cdots \wedge 9 = 2^3 \times 3^2 \times 5 \times 7 = 2520$. Comme $n+1$ est le plus petit nombre qui satisfasse cette propriété, on en déduit que $n+1 = 2520$ et donc aussi que

$$\boxed{n = 2519.}$$

♦ ***Exercice 22.*** [⋆]
Que vaut la somme des chiffres de la somme des chiffres de la somme des chiffres de 4444^{4444} ?

Notons $\psi : \mathbb{N} \longrightarrow \mathbb{N}$ l'application qui, à un entier n, lui associe la somme de ses chiffres.

On a vu (principe de la preuve par 9) que $\psi(n) \equiv n$ [9]. Donc

$$\psi\big[\psi\big(\psi(4444^{4444})\big)\big] \equiv 4444^{4444} \equiv 7^{4444} \equiv 7^{3\times 1481+1} \equiv 7 \ \ [9]$$

où la première égalité modulaire vient d ufait que $4444 \equiv 7$ [9] et la dernière découle du fait que $7^3 \equiv 1$ [9].

Si a possède au plus n chiffres et b possède au plus m chiffres, c'est-à-dire si $a < 10^n$ et $b < 10^m$, alors on a $ab < 10^{n+m}$, ce qui signifie que ab possède au plus $n+m$ chiffres. Par conséquent, 4444^{4444} possède au plus $4 \times 4444 = 17\,776$ chiffres, ce qui donne $\psi(4444^{4444}) \leqslant 17\,776 \times 9 = 159\,984$. Avant 159 984, le nombre qui a la plus grande somme de chiffres est 99 999, donc $\psi\big(\psi(4444^{4444})\big) \leqslant 5 \times 9 = 45$. Avant 45, le nombre qui a la plus grande somme de chiffres est 39, donc $\psi\big[\psi\big(\psi(4444^{4444})\big)\big] \leqslant 3 + 9 = 12$.

En combinant les informations $\psi\big[\psi\big(\psi(4444^{4444})\big)\big] \equiv 7$ [9] et $\psi\big[\psi\big(\psi(4444^{4444})\big)\big] \leqslant 12$, on en déduit que $\psi\big[\psi\big(\psi(4444^{4444})\big)\big] = 7$. Donc

$$\boxed{\text{la somme des chiffres de la somme des chiffres de la somme des chiffres de } 4444^{4444} \text{ vaut } 7.}$$

♦ ***Exercice 23.*** [⋆]
Quel est le dernier chiffre du nombre $7^{7^{7^{7^{7}}}}$?

Demander le dernier chiffre de ce nombre, c'est demander sa classe modulo 10. Or $7^4 = 49^2 \equiv (-1)^2 \equiv 1$ [10], ce qui nous incite à regarder l'exposant modulo 4.

On a

$$7^7 = 49^3 \times 7 \equiv 1^3 \times 3 \equiv 3 \ \ [4]$$

donc il existe $k \in \mathbb{N}$ tel que

$$7^{7^7} = 7^{3+4k} = 49 \times 7 \times 49^{2k} \equiv 1 \times 3 \times 1^{2k} \equiv 3 \ \ [4].$$

Etc. Donc

$$7^{7^{7^{7^{7}}}} \equiv 3 \ \ [4]$$

Dès lors, il existe $\ell \in \mathbb{N}$ tel que

$$7^{7^{7^{7^{7^{7}}}}} = 7^{3+4\ell} = 49 \times 7 \times (7^4)^\ell \equiv -1 \times 7 \times 1^\ell \equiv -7 \equiv 3 \ \ [10].$$

En conclusion,

$$\boxed{\text{le dernier chiffre du nombre } 7^{7^{7^{7^{7}}}} \text{ est un 3.}}$$

♦ ***Exercice 24.*** [⋆]

1. Soit $a \in \mathbb{N}$ tel que $a \wedge 10 = 1$. Démontrer que $a^4 \equiv 1\ [10]$ et en déduire que, pour tout $k \in \mathbb{N}$, on a $a^{8\times 10^k} \equiv 1\ [10^{k+1}]$.
2. Déterminer un entier dont l'écriture décimale du cube se termine par 123456789.

1. Dans $\mathbb{Z}/10\mathbb{Z}$, on a $a \in \{1;3;7;9\}$, ce qui permet de vérifier sans mal que

$$\boxed{a^4 \equiv 1\ [10].}$$

Pour tout $k \in \mathbb{N}$, on pose $\mathscr{P}(k)$: $a^{8\times 10^k} \equiv 1\ [10^{k+1}]$.

Initialisation : $a^{8\times 10^0} = a^8 = (a^4)^2 \equiv 1^2 \equiv 1\ [10]$ donc $\mathscr{P}(0)$ est vraie.

Hérédité : Fixons $k \in \mathbb{N}$ tel que $\mathscr{P}(k)$ est vraie et démontrons $\mathscr{P}(k+1)$. D'après la formule de Bernoulli, on a

$$a^{8\times 10^{k+1}} - 1 = (a^{8\times 10^k})^{10} - 1 = (a^{8\times 10^k} - 1)\sum_{\ell=0}^{9} a^{8\ell\times 10^k}.$$

Par H.R., on a

$$10^{k+1} \mid a^{8\times 10^k} - 1.$$

Par ailleurs, comme $a^4 \equiv 1\ [10]$, on a

$$\sum_{\ell=0}^{9} a^{8\ell\times 10^k} = \sum_{\ell=0}^{9} (a^4)^{2\ell\times 10^k} \equiv \sum_{\ell=0}^{9} (1)^{2\ell\times 10^k} \equiv 10 \equiv 0\ \ [10],$$

c'est-à-dire

$$10 \ \Big|\ \sum_{\ell=0}^{9} a^{8\ell\times 10^k}.$$

Donc

$$10^{k+2} \mid a^{8\times 10^{k+1}} - 1,$$

ce qui signifie que $\mathscr{P}(k+1)$ est vraie.

Conclusion : D'après le principe de récurrence, $\mathscr{P}(k)$ est vraie pour tout $k \in \mathbb{N}$, c'est-à-dire

$$\boxed{\forall k \in \mathbb{N}, \qquad a^{8\times 10^k} \equiv 1\ \ [10^{k+1}].}$$

2. Posons

$$n = 123456789^{800000001/3}.$$

Alors

$$n^3 = 123456789^{800000001} = 123456789^{8\times 10^8+1} \equiv 123456789\ \ [10^9]$$

où la congruence découle du résultat de la question 1 puisque $123456789 \wedge 10 = 1$. Cela signifie bien que n^3 s etermine par 123456789. Donc

$$\boxed{\text{le cube de } 123456789^{800000001/3} \text{ se termine par } 123456789.}$$

♦ ***Exercice 25.*** [○]
Soient $a, b \in \mathbb{Z}$. Démontrer que $a^2 + b^2$ est divisible par 7 si, et seulement si, a et b le sont.

Si a et b sont divisibles par 7 alors $a^2 + b^2$ l'est aussi.

Si $a^2 + b^2$ est divisible par 7, on a $a^2 + b^2 = 0$ dans $\mathbb{F}_7$. Or dans $\mathbb{F}_7$, les seuls carrés sont 0, 1, 2 et 4, donc la seule façon de faire 0 en ajoutant deux carrés est $0 + 0$. Ainsi, on a $a = b = 0$ dans $\mathbb{F}_7$, ce qui signifie que a et b sont divisibles par 7.

En conclusion,

$$\boxed{a^2 + b^2 \text{ est divisible par 7 si, et seulement si, } a \text{ et } b \text{ le sont.}}$$

♦ ***Exercice 26.*** [⋆]
On considère 1975 entiers dont la somme est nulle. Démontrer que la somme de leurs puissances 37-èmes est un multiple de 399.

Soient $a_1, \dots, a_{1975} \in \mathbb{Z}$ tels que $a_1 + \cdots + a_{1975} = 0$.
La décomposition primaire de 399 est $399 = 3 \times 7 \times 19$.
On a

$$\sum_{k=1}^{1975} {x_k}^{37} = \sum_{k=1}^{1975} {x_k}^{3^3+3^2+1} = \sum_{k=1}^{1975} \underbrace{\underbrace{\underbrace{\left(({x_k}^3)^3\right)^3}_{\equiv x_k \ [3]} \underbrace{({x_k}^3)^3}_{\equiv x_k \ [x_k]}}_{\equiv x_k \ [3]} x_k}_{\equiv x_k \ [3]} \equiv \sum_{k=1}^{1975} x_k \equiv 0 \ \ [3]$$

où les congruences découlent de Little Fermat (i.e. ${x_k}^3 \equiv x_k \ [3]$), donc

$$3 \ \Big| \ \sum_{k=1}^{1975} {x_k}^{37}.$$

On a

$$\sum_{k=1}^{1975} {x_k}^{37} = \sum_{k=1}^{1975} {x_k}^{7\times5+2} = \sum_{k=1}^{1975} \underbrace{({x_k}^7)^5}_{\equiv {x_k}^5 \ [7]} {x_k}^2 \equiv \sum_{k=1}^{1975} {x_k}^7 \equiv \sum_{k=1}^{1975} x_k \equiv 0 \ \ [7]$$

où les congruences découlent de Little Fermat (i.e. ${x_k}^7 \equiv x_k \ [7]$), donc

$$7 \ \Big| \ \sum_{k=1}^{1975} {x_k}^{37}.$$

On a

$$\sum_{k=1}^{1975} {x_k}^{37} = \sum_{k=1}^{1975} {x_k}^{19+18} = \sum_{k=1}^{1975} \underbrace{{x_k}^{19}}_{\equiv x_k \ [19]} {x_k}^{18} \equiv \sum_{k=1}^{1975} {x_k}^{19} \equiv \sum_{k=1}^{1975} x_k \equiv 0 \ \ [19]$$

où les congruences découlent de Little Fermat (i.e. ${x_k}^{19} \equiv x_k \ [19]$), donc

$$19 \ \Big| \ \sum_{k=1}^{1975} {x_k}^{37}.$$

Comme 3, 7 et 19 sont premiers entre eux, on en déduit que

$$3 \times 7 \times 19 \ \Big| \ \sum_{k=1}^{1975} {x_k}^{37},$$

c'est-à-dire

$$399 \ \Big| \ \sum_{k=1}^{1975} {x_k}^{37}.$$

En conclusion,

si 1975 entiers ont une somme nulle, la somme de leurs puissances 37-èmes est un multiple de 399.

♦ ***Exercice 27.*** [○]
Résoudre l'équation $x^2 - 2y^2 = 3$ d'inconnues $x, y \in \mathbb{Z}$. *Indication :* $\mathbb{Z}/8\mathbb{Z}$.

Dans $\mathbb{Z}/8\mathbb{Z}$, les seuls carrés sont 0, 1 et 4. Or

x^2	0	0	0	1	1	1	4	4	4
y^2	0	1	4	0	1	4	0	1	4
$x^2 - 2y^2$	0	6	0	0	7	1	4	2	4

donc $x^2 - 2y^2$ n'est jamais égal à 3 dans $\mathbb{Z}/8\mathbb{Z}$. Ainsi,

$x^2 - 2y^2 = 3$ n'a pas de solutions dans $\mathbb{Z}$.

♦ ***Exercice 28.*** [⋆]
Soit $k \in \mathbb{N} \setminus \{0;1\}$.

1. Soient $a, b \in \mathbb{Z}^*$ tels que $a \wedge b = 1$. On suppose que ab est la puissance k-ème d'un entier. Démontrer que a et b sont eux-mêmes des puissances k-èmes d'entiers.
2. Résoudre l'équation $x^2 + x = y^k$ d'inconnues $x, y \in \mathbb{Z}$.
3. Soit $p \in \mathbb{P}$. Résoudre l'équation $x^2 + px = y^2$ d'inconnue $x, y \in \mathbb{N}$. *Indication : Distinguer le cas où p divise x du cas contraire.*

1. Soit $p \in \mathbb{P}$. On a $k \mid v_p(ab)$ puisque ab est la puissance k-ème d'un entier. Or, comme a et b sont premiers entre eux, on a l'alternative $\big(v_p(a) = v_p(ab)$ et $v_b(b) = 0\big)$ ou $\big(v_p(a) = 0$ et $v_b(b) = v_p(ab)\big)$. En combinant ces informations, on voit que $k \mid v_p(a)$ et $k \mid v_p(b)$.
   Ce résultat étant vrai pour tout $p \in \mathbb{P}$, on en déduit que

   $$\boxed{a \text{ et } b \text{ sont des puissances } k\text{-èmes d'entiers.}}$$

2. On a $x^2 + x = y^k \iff x(x+1) = y^k$. Comme deux entiers consécutifs sont toujours premiers entre eux, la première question s'applique et permet d'affirmer que ou bien l'un des deux nombres x ou $x+1$ est nul, ou bien x et $x+1$ sont des puissances k-èmes. La seonde possibilité est impossible puiqu'il n'existe pas deux puissances k-èmes non nulles consécutives. Donc x ou $x+1$ est nul, c'est-à-dire $x = 0$ ou $x = -1$. Dans ces deux cas, on a $y = 0$. En conclusion,

   $$\boxed{\text{les solutions de } x^2 + x = y^k \text{ dans } \mathbb{Z} \text{ sont } (0;0) \text{ et } (-1;0).}$$

3. Si p divise x, alors $x = pa$ avec $a \in \mathbb{N}$. En reportant dans l'équation, cela donne $p^2a^2 + p^2a = y^2$. On en déduit que p^2 divise y^2 et donc que p divise y. On peut donc écrire $y = pb$ avec $b \in \mathbb{N}$. En reportant dans $p^2a^2 + p^2a = y^2$ et en simplifiant par p^2, on obtient $a^2 + a = b^2$. D'après la question précédente avec $k = 2$, cela impose $a = b = 0$.

   Si p ne divise pas x, alors x et $x+p$ sont premiers entre eux (sinon ils auraient un diviseur commun $d > 1$ qui diviserait leur différence p, ce qui imposerait $d = p$, ce qui n'est pas possible pour un diviseur de x). En réécrivant l'équation $x^2 + px = y^2$ sous la forme $x(x+p) = y^2$, on peut utiliser la première question pour affirmer que ou bien $x = 0$ ou bien x et $x+p$ sont des carrés. La possibilité $x = 0$ est à rejeter puisque p divise 0. Il reste donc la possibilité que $x = \alpha^2$ et $x + p = \beta^2$ avec $\alpha, \beta \in \mathbb{N}$. Mézalors, $p = \beta^2 - \alpha^2 = (\beta - \alpha)(\beta + \alpha)$ et comme le nombre premier p n'a pas d'autres diviseurs que 1 et p, cela impose $\beta - \alpha = 1$ et $\beta + \alpha = p$, c'est-à-dire $\alpha = (p-1)/2$ et $\beta = (p+1)/2$. Notons au passage que cela exclut la possibilité que p vaille 2. On conclut donc, dans ce cas, que pour $p \in \mathbb{P} \setminus \{2\}$, on a $x = (p-1)^2/4$ et $y = (p^2-1)/4$.

   En conclusion,

   $$\boxed{\text{pour } p \in \mathbb{P}, \text{ les solutions de } x^2 + px = y^2 \text{ dans } \mathbb{N} \text{ sont } (0;0) \text{ et, lorsque } p \neq 2, \left(\frac{(p-1)^2}{4}; \frac{p^2-1}{4}\right)}$$