1 Simplifier $7^{8n+1}+10(-1)^n$ modulo 17.
Montrer que $7^8 \equiv -1\ [17]$, d'où : $7^{8n+1} \equiv (-1)^n \times 7\ [17]$.

2 **a)** Observer que $3^2 \equiv 2\ [7]$ ce qui permet d'écrire $3^{2n+1}+2^{n+2} \equiv 2^n \times 3 + 2^{n+2}\ [7]$ et de factoriser par 2^n. (on peut aussi procéder par récurrence sur n en utilisant alors $3^2 \equiv 2\ [7]$ pour l'hérédité).

b) Même technique en commençant par observer que $2^6 \equiv -4\ [17]$ et que l'on a aussi $3^4 \equiv -4\ [17]$.

3
- *Méthode 1*. Par récurrence sur n.
- *Méthode 2*. On remarque que $5^4 \equiv 1\ [16]$ donc on raisonne modulo 4 pour n *i.e.* on distingue quatre cas : $n=4k$, $n=4k+1$, $n=4k+2$ et $n=4k+3$ et on vérifie pour chaque cas que 5^n (qui est congru à 5^0, 5^1, 5^2 ou 5^3 selon le cas considéré) est congru à $4n+1$ modulo 16

4 Faire un tableau de congruence modulo 6 en écrivant les valeurs de n, $n+2$, $7n-5$ pour chaque entier $0, 1, 2, 3, 4$ et 5.

5 Factoriser : $a^n - b^n = (a-b)\underbrace{\sum_{k=0}^{n-1} a^k b^{n-1-k}}_{S}$

puis montrer que n divise $a-b$ (facile) et que n divise S (calculer S modulo n uniquement en fonction de a en utilisant $b \equiv a\ [n]$).

6 Utiliser la méthode du cours :

a) On trouve $3^{10} \equiv -1\ [25]$ puis utiliser $3^{2189} = 3^{10\times 218+9}$.
Réponse : Le reste vaut 8.

b) Commencer par simplifier $3872 \equiv 2\ [5]$ puis observer par exemple que $2^2 \equiv -1\ [5]$.
Réponse : Le reste vaut 2.

7 Utiliser la méthode du cours pour simplifier toutes les puissances

a) On trouve $2^{10} \equiv 1\ [11]$ puis utiliser $2^{123} = 2^{12\times 10+3}$.
On trouve $3^5 \equiv 1\ [11]$ puis utiliser $3^{121} = 3^{24\times 5+1}$.

b) De même en utilisant $2^{10} \equiv 1\ [11]$ et $5^5 \equiv 1\ [11]$

c) De même en utilisant $2^{10} \equiv 1\ [11]$ et $5^5 \equiv 1\ [11]$

d) De même en utilisant $9^3 \equiv 1\ [7]$ et $4^3 \equiv 1\ [7]$

8 On démontre que $2^{4^n} \equiv 2\ [7]$ pour tout $n \in \mathbb{N}$.
Deux possibilités :
- Par récurrence , en utilisant $2^4 \equiv 2\ [7]$ pour l'hérédité.
- On constate que $2^3 \equiv 1\ [7]$.
En écrivant 4^n sous la forme $4^n = 3q + r$: $2^{4^n} = 2^r$.
Il suffit donc de calculer r. Pour cela simplifier 4^n modulo 3.

9 On simplifie $a = \displaystyle\sum_{k=1}^{10} 10^{10^k}$ modulo 7.

D'abord $10 \equiv 3\ [7]$ donc $a = \displaystyle\sum_{k=1}^{10} 3^{10^k}\ [7]$.

Il reste à simplifier les 3^{10^k} modulo 7.
Constater que $3^6 \equiv 1\ [7]$ donc reste à trouver le reste de la division euclidienne de 10^k modulo 6 (car si $10^k = 6q + r$ alors $3^{10^k} = (3^6)^q \times 3^r \equiv 1 \times 3^r\ [7]$).
On trouve que $10^k \equiv 4\ [6]$ donc $a \equiv 10 \times 4 \equiv 5\ [7]$.

10 Appliquer l'algorithme d'Euclide étendu (on calcule le PGCD puis on « remonte » pour obtenir une relation de Bézout).

a) *Réponse :* $62 \wedge 43 = 1$ *et* $13 \times 43 - 9 \times 62 = 1$.

b) *Réponse :* $744 \wedge 516 = 12$ *et* $13 \times 516 - 9 \times 744 = 12$

c) *Réponse :* $720 \wedge 105 = 15$ *et* $2 \times 720 - 5 \times 105 = 15$.

11 Par récurrence à l'aide de la propriété $a \wedge b = b \wedge (a - bq)$

12 Procéder par double inclusion en commençant dans chaque cas par traduire soigneusement quelle est l'hypothèse de départ et ce que l'on cherche à montrer.

13 On suit la méthode du savoir faire SF 7

a) Une solution particulière est $(x_0, y_0) = (12, 20)$ (multiplier par 4 une relation de Bézout entre 42 et 25 par exemple).
Solutions : Les $(12 + 25k, 20 + 42k)$ *avec* $k \in \mathbb{Z}$

b) Une solution particulière est $(x_0, y_0) = (2, 0)$.
Solutions : Les $(2 - 5k, 3k)$ *avec* $k \in \mathbb{Z}$

c) Pas de solution.

d) Une solution particulière est $(x_0, y_0) = (-9, 13)$.
Solutions : Les $(-9 + 43k, 13 - 62k)$ *avec* $k \in \mathbb{Z}$

14 On suit la méthode du savoir faire SF 4

a) *Solutions : Les* $-5 + 28k$ *avec* $k \in \mathbb{Z}$

b) *Solutions : Les* $5 + 7k$ *avec* $k \in \mathbb{Z}$

c) Pas de solution.

15 Dans les deux cas, procéder par analyse-synthèse.

1. Dans l'analyse, écrire $x = 10x'$ et $y = 10y'$ où $x' \wedge y' = 1$ et $x' + y' = 10$.
Ne pas oublier l'étape de synthèse.
Solutions. $(10, 90)$, $(90, 10)$, $(30, 70)$ et $(70, 30)$.
2. Dans l'analyse, commencer par remarquer que $d = x \wedge y$ divise $75 \wedge 40 = 5$. Il y a donc deux valeurs plausibles pour d : $d = 1$ ou $d = 5$.
Pour chaque cas, écrire $x = dx'$ et $y = dy'$ où $x' \wedge y' = 1$.
On est ramené à un système « somme-produit » de la forme $\begin{cases} x' + y' = s \\ x'y' = p \end{cases}$ que l'on sait résoudre en se ramenant à une équation du second degré : vérifier que les solutions obtenues sont bien entières.
Solutions. $(15, 25)$ et $(25, 15)$.

16 Dans tous les cas, procéder par analyse-synthèse.

a) Dans l'analyse, montrer que $x \wedge y = 1$.
Solution. $(1, 1)$.

b) Dans l'analyse, montrer que $x \wedge y = 1$ ce qui permet d'écrire $x \vee y = xy$ et assure que x et y vérifient $xy - x - y + 1 = 0$.
Factoriser cette expression pour se ramener à un produit nul.
Solutions. Tous les couples $(1, k)$ et $(k, 1)$ pour $k \in \mathbb{N}$.

c) Dans l'analyse, poser $d = x \wedge y$ et écrire $x = dx'$ et $y = dy'$ où $x' \wedge y' = 1$ ce qui permet d'écrire $x' \vee y' = x'y'$ et assure que x' et y' vérifient $x'y' - 2x' - 3y' + 1 = 0$.

Factoriser cette expression pour se ramener à un produit égal à 5. Conclure en examinant les diviseurs de 5.
Solutions. Tous les couples $(4d, 7d)$ et $(8d, 3d)$ pour $d \in \mathbb{N}$.

17 **1.** A tâtons on trouve que -11 convient.
Il y a une méthode générale : on trouve une relation de Bézout entre 17 et 15 *i.e.* $u, v \in \mathbb{Z}$ tels que $17u + 15v = 1$.
L'entier $15v$ vérifie $15v \equiv 1\ [17]$ et $15v \equiv 0\ [15]$.
L'entier $17u$ vérifie $17u \equiv 0\ [17]$ et $17u \equiv 1\ [15]$.
Ainsi $x_0 = 4 \times 15v + 6 \times 17v$ est solution du système.

2. Procéder par analyse-synthèse.
Dans l'analyse, si x est solution alors $17 \mid x - x_0$ et $15 \mid x - x_0$ et 15 et 17 sont premiers entre eux donc $x - x_0$ est un multiple de 15×17.
Il ne reste qu'à tester les candidats.

18 **a)** D'après le cours il suffit de montrer que $(2n+1) \wedge n = 1$ et $(2n+1) \wedge (n+1) = 1$.
Pour cela les trois méthodes du savoir faire **SF 9** sont possibles.
b) De même qu'au a)

19 Pour montrer que $(n+1) \mid \binom{2n}{n}$ utiliser la formule « sans nom » :

$$(n+1) \times \binom{2n+1}{n+1} = (2n+1) \times \binom{2n}{n}$$

puis le lemme de Gauss.

20 Poser $d = a \wedge c$ et $\delta = a \wedge (bc)$ et montrer que $d \mid \delta$ (il suffit de montrer que d divise a et bc) et que $\delta \mid d$ (il suffit de montrer que δ divise a et c)

21
- Si $a \wedge b = 1$, montrer que $a + b$ est premier avec a et avec b. Pour cela les trois méthodes du savoir faire **SF 9** sont possibles.
- Si $(a+b) \wedge ab = 1$, on peut montrer que $a \wedge b = 1$ en utilisant l'option 2 ou l'option 3 du savoir faire **SF 9**

22 **a)** A l'aide d'une relation de Bézout entre m et n, exprimer x en fonction de x^m et x^n.
b) Ecrire x sous forme irréductible $x = \frac{p}{q}$ avec $p \wedge q = 1$. Le fait que $x^n \in \mathbb{Z}$ assure que $q^n \mid p^n$ mais on sait aussi que $p^n \wedge q^n = 1$.

23 On peut tout montrer par récurrence, l'hypothèse de récurrence étant :

$$\text{il existe } a_n, b_n \in \mathbb{N} \text{ tels que } \begin{cases} (1+\sqrt{2})^n = a_n + b_n\sqrt{2} \\ a_n \wedge b_n = 1 \end{cases}$$

Pour l'hérédité, on développe

$$(1+\sqrt{2})(a_n + \sqrt{2}b_n) = (a_n + 2b_n) + \sqrt{2}(a_n + b_n)$$

Ne pas oublier de montrer que $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$ sont premiers entre eux (savoir faire **SF 9**).

24 **1.** Considérer l'ensemble des valeurs prises par r_k.
2. Fixer $k < \ell$ telq que $r_k = r_\ell$ et montrer que $a^{\ell - k} \equiv 1\ [n]$.
3. Montrer que $r_{k+N} \equiv r_k$ pour tout $k \in \mathbb{N}$, ce qui assure en fait l'égalité $r_{k+N} = r_k$ vu que l'on a affaire à des entiers de $[\![0, n-1]\!]$.

25 k divise $n! + k$ pour chaque $k \in [\![2, n]\!]$

26 **a)** $(a-1)$ divise $a^p - 1$: $a^p - 1 = (a-1) \times \sum_{k=0}^{p-1} a^k$
Or $a^p - 1$ n'a que deux diviseurs positifs : 1 et $a^p - 1$.
b) Exercice classique traité en cours (Mersenne).

27 **a)** Utiliser le petit théorème de Fermat (avec $n+1$ et avec n).
b) Il s'agit de montrer que $2p$ divise $N = (n+1)^p - (n^p + 1)$.
p et 2 sont premiers entre eux donc il suffit de montrer que 2 et p divisent N.
Avec la question a), il reste à montrer que $N \equiv 0\ [2]$.
On peut faire un tableau de congruence en calculant N modulo 2 selon que $n = 0$ ou $n = 1$.

28 $42 = 2 \times 3 \times 7$ et $2, 3$ et 7 sont deux à deux premiers entre eux donc il suffit de montrer que $n^7 - n \equiv 0\ [p]$ avec $p = 7$, $p = 2$ et $p = 3$.
Pour $p = 7$ c'est immédiat avec le petit théorème de Fermat.
Pour les deux autres on peut aussi partir de l'égalité fournie par Fermat pour obtenir le résultat voulu (par ex. pour $p = 2$ on part de $n^2 \equiv n\ [2]$ puis on multiplie par n jusqu'à obtenir n^7 à gauche de l'égalité en utilisant $n^2 \equiv n$ pour le membre de droite).
On peut aussi écrire $42 = 7 \times 6$ avec $7 \wedge 6 = 1$ et montrer que $7 \mid n^7 - n$ avec Fermat et que $6 \mid n^7 - n$ avec un tableau de congruences.

29 **1.** Par l'absurde supposer qu'aucun des facteurs premiers de N n'est congru à 3 modulo 4. Montrer qu'alors tous les facteurs premiers de N sont congrus à 1 modulo 4 et en déduire une contradiction sur N.
2. Procéder par l'absurde en supposant qu'ils sont en nombre fini et noter $p_1, \ldots, p_n$ tous les nombres premiers congrus à 3 modulo 4. Poser alors $N = 4p_1 \cdots p_n - 1$ et appliquer la question 1 à l'entier N.

30

31 **1.** Poser $\alpha = v_p(a)$ et $\beta = v_p(b)$, écrire a et b sous la forme :
$a = p^\alpha q$ et $b = p^\beta q'$ puis factoriser $a + b$ en supposant par exemple $\alpha \leq \beta$
2.
3. Reprendre la factorisation en supposant par exemple $\alpha < \beta$ et écrire $a + b$ sous la forme $p^\alpha q''$ où p ne divise par q''.

32 Si $a \mid b$ il suffit d'élever au carré l'égalité $b = ka$.
Si $a^2 \mid b^2$, c'est plus compliqué.
Au choix :
- On peut utiliser les décompositions en facteurs premiers en écrivant
$$a = p_1^{\alpha_1} \times \ldots p_n^{\alpha_n} \quad \text{et} \quad b = p_1^{\beta_1} \times \ldots p_n^{\beta_n}$$
Il s'agit alors de montrer que $\alpha_i \leq \beta_i$ pour tout $i \in [\![1, n]\!]$.
Pour cela traduire le fait que $a^2 \mid b^2$ à l'aide des décompositions de a^2 et b^2.

- On peut aussi utiliser les valuations p-adiques :
  - Il s'agit de montrer que $v_p(a) \leq v_p(b)$ pour tout $p \in \mathbb{P}$

- L'hypothèse est : $v_p(a^2) \leq v_p(b^2)$ pour tout $p \in \mathbb{P}$

Il suffit d'utiliser l'additivité des valuations p-adiques.

33 L'hypothèse est : $ab = c^2$ pour un $c \in \mathbb{Z}$.
Deux possibilités ensuite :

- *Utiliser les valuations p-adiques* L'hypothèse est que $v_p(c)$ est divisible par 2 pour tout $p \in \mathbb{P}$ et il s'agit de montrer que pour tout $p \in \mathscr{P}$, les valuations p-adiques de a et b sont divisibles par 2. Pour cela combiner :
  - La propriété d'additivité : $v_p(ab) = v_p(a) + v_p(b)$.
  - Le fait que si $v_p(a) \neq 0$ alors $v_p(b) = 0$ (car $a \wedge b = 1$).
- *Utiliser les décompositions en facteurs premiers*. Ecrire :
  $a = p_1^{\alpha_1} \times \ldots p_n^{\alpha_n}$ $\quad b = q_1^{\beta_1} \times \ldots q_m^{\beta_m}$ et $c = x_1^{\gamma_1} \times \cdots \times x_s^{\gamma_s}$
  où $\{p_1, \ldots, p_n\} \cap \{q_1, \ldots, q_m\} = \varnothing$ car $a \wedge b = 1$.
  Il s'agit alors de montrer que les α_i et β_i sont divisibles par 2.
  Pour cela écrire deux décompositions de ab :
  - $ab = p_1^{\alpha_1} \times \ldots p_r^{\alpha_r} q_1^{\beta_1} \times \ldots q_r^{\beta_r}$
  - $ab = c^2 = x_1^{2\gamma_1} \times \cdots \times x_s^{2\gamma_s}$

  L'unicité de la décomposition en facteurs premiers permet d'identifier les facteurs : tout $p_i^{\alpha_i}$ est un $x_j^{2\gamma_j}$ et de même pour les $q_i^{\beta_i}$.

34 Deux possibilités :

- *Utiliser les valuations p-adiques*. Il suffit de montrer que pour tout $p \in \mathbb{P}$, $v_p(n)$ est divisible par 6. Pour cela, écrire $n = x^2$ et $n = y^3$ et utiliser les additivité des valuations p-adiques pour montrer que 2 divise $v_p(n)$ et que 3 divise $v_p(n)$.
- *Utiliser les décompositions en facteurs premiers de x et y*. Ecrire :
  $$x = p_1^{\alpha_1} \times \ldots p_n^{\alpha_n} \quad \text{et} \quad y = p_1^{\beta_1} \times \ldots p_n^{\beta_n}$$
  Donc
  $$n = x^2 = p_1^{2\alpha_1} \times \ldots p_n^{2\alpha_n}$$
  Il suffit de montrer que les α_i sont divisibles par 3.
  Pour cela écrire $n = y^3$ et identifier les facteurs premiers ; on obtient $2\alpha_i = 3\beta_j$ pour chaque i.
  Il reste à conclure à l'aide du lemme de Gauss.

35 Remarquer que $a_{n+1} = 2(2n+1)a_n$ puis utiliser la propriété d'additivité des valuations p-adiques : la suite $\big(v_2(a_n)\big)$ est arithmétique de raison 1.
Réponse : $v_2(a_n) = n$.

36 **1.** L'additivité des valuations p-adiques permet d'écrire
$$v_2(100!) = \sum_{k=1}^{100} v_2(k)$$
Séparer ensuite les termes d'indices pairs et d'indices impairs en utilisant :
$$v_2(2k) = 1 + v_2(k) \qquad \text{et} \qquad v_2(2k+1) = 0$$
ce qui donne : $v_2(100!) = 50 + \displaystyle\sum_{k=1}^{50} v_2(k)$.
En réitérant plusieurs fois le même raisonnement (séparation « pairs-impairs ») : $v_2(100!) = 50+25+12+6+3+1$

2. En adaptant le raisonnement ci-dessus $v_p(n!) = \displaystyle\sum_{k=1}^{n} v_p(k)$
La somme se réduit aux indices k multiples de p ($v_p(k) = 0$ si k n'est pas un multiple de p) *i.e.* les indices de la forme $k = p\ell$ pour tous les indices ℓ tels que $1 \leq \ell p \leq n$ *i.e.* tous les $\ell \in [\![1, \lfloor \frac{n}{p} \rfloor]\!]$ donc :
$$v_p(n!) = \sum_{\ell=1}^{\lfloor \frac{n}{p} \rfloor} v_p(p\ell) = \left\lfloor \frac{n}{p} \right\rfloor + \sum_{\ell=1}^{\lfloor \frac{n}{p} \rfloor} v_p(\ell)$$
Il suffit de réitérer le raisonnement en utilisant à chaque étape : $\left\lfloor \dfrac{\lfloor \frac{n}{p^k} \rfloor}{p} \right\rfloor = \left\lfloor \dfrac{n}{p^{k+1}} \right\rfloor$.

Pour plus de rigueur on peut poser $S_k = \displaystyle\sum_{\ell=0}^{\lfloor \frac{n}{p^k} \rfloor} v_p(\ell)$ et le raisonnement précédent permet de montrer que pour tout $k \in \mathbb{N}$: $S_k = \left\lfloor \dfrac{n}{p^{k+1}} \right\rfloor + S_{k+1}$. On peut par exemple conclure par télescopage : $\displaystyle\sum_{k=0}^{+\infty} S_k - S_{k+1} = S_0 = v_p(n!)$

37 Poser $\alpha = \displaystyle\max_{m \leq k \leq n} v_2(k)$ et montrer que k est atteinte une et une seule fois sur $[\![m, n]\!]$ pour en déduire que $\displaystyle\sum_{k=m}^{n} \frac{1}{k}$ est de la forme $\dfrac{p}{2^\alpha q}$ pour certains entiers p, q impairs.