Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. Soient $a, b, c \geq 1$ des entiers; on note $d = \mathrm{pgcd}(a, b)$. Montrer :
a) si $a \mid b$, alors $a^2 \mid b^2$;
b) si $a^2 \mid b^2$, alors $a \mid b$;
c) si $c \mid d$, alors $\mathrm{pgcd}(a/c, b/c) = d/c$.

Exercice 2. Montrer que le nombre $\sqrt[3]{5/3}$ n'est pas rationnel.

Exercice 3. Trouver toutes les solutions $x, y \in \mathbf{Z}$ de l'équation $10x + 16y = 18$.

Exercice 4. Pour tout entier $n \geq 0$ on note $x_n = 201 \cdot 2018^n + 8 \cdot 2019^n$. Montrer que, si n est pair, alors $11 \mid x_n$. Que peut-on dire des valeurs de $x_n \pmod{11}$ si n est impair ?

Exercice 5. Résoudre dans $\mathbf{Z}$ les systèmes suivants :
a) $x \equiv 3 \pmod{6}$, $x \equiv 3 \pmod{10}$, $x \equiv 3 \pmod{15}$.
b) $6x \equiv 9 \pmod{19}$, $7x \equiv 3 \pmod{15}$.
c) $6x \equiv 9 \pmod{21}$, $7x \equiv 3 \pmod{15}$.

Exercice 6. Montrer :
a) si $\mathrm{pgcd}(a, 6) = 1$, alors $a^2 \equiv 1 \pmod{24}$;
b) si $\mathrm{pgcd}(a, 30) = 1$, alors $a^4 \equiv 1 \pmod{240}$;
c) si $\mathrm{pgcd}(a, 10) = 1$, alors $a^{100} \equiv 1 \pmod{1000}$;
d) si $a \in \mathbf{Z}$, alors $a^{100} \equiv 0, 1, 376, 625 \pmod{1000}$.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.

Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. (a) Déterminer le nombre de diviseurs positifs de l'entier $n = 6000$.
(b) Résoudre dans $\mathbf{Z}$ la congruence $10x \equiv 18 \pmod{24}$.
(c) Résoudre dans $\mathbf{Z}$ le système suivant :

$$x \equiv 2 \pmod 7, \quad x \equiv 7 \pmod{11}, \quad x \equiv 6 \pmod{13}.$$

Exercice 2. Soit $n \geq 1$ un entier.
(a) Enoncer le théorème d'Euler.
(b) Exprimer la valeur de $\varphi(n)$ en termes de la décomposition $n = p_1^{r_1} \cdots p_k^{r_k}$ (où $p_1, \ldots, p_k$ sont des nombres premiers distincts, $k \geq 0$ et $r_i \geq 1$).
(c) Montrer : $\varphi(2n)/\varphi(n)$ est égal à 1 (resp. à 2) si n est impair (resp. si n est pair).
(d) Que se passe-t-il si l'on remplace $2n$ dans (c) par $3n$ (resp. par $6n$) ?

Exercice 3. (a) Soit $x \in \mathbf{Z}$. Montrer : si $7 \nmid x$ (resp. si $13 \nmid x$), alors on a $x^6 \equiv 1 \pmod 7$ (resp. $x^{12} \equiv 1 \pmod{13}$ et $x^6 \equiv \pm 1 \pmod{13}$).
(b) Déterminer les valeurs possibles de $x^{12} \pmod 7$, $x^{12} \pmod{13}$ et $x^{12} \pmod{91}$ pour $x \in \mathbf{Z}$.
(c) Idem pour x^6 à la place de x^{12}.
(e) Montrer : si $n \geq 1$ est un entier tel que $n \equiv 1 \pmod{12}$, alors on a $x^n \equiv x \pmod{91}$ pour tout $x \in \mathbf{Z}$.

Exercice 4. (a) Donner un exemple d'un groupe cyclique H d'ordre 6. Déterminer l'ordre de chaque élément de H et le nombre de générateurs de H.
(b) Soit $(G, *)$ un groupe. Si $g \in G$ est un élément d'ordre 24, déterminer l'ordre de g^k pour $k = 10, 15$ et 18.
(c) Plus généralement, si $g \in G$ est un élément d'ordre $m \geq 1$, déterminer l'ordre de g^k pour tout $k \geq 1$.

Exercice 5. Définir des isomorphismes d'anneaux suivants : $\alpha_1 : \mathbf{R}[X]/(X) \xrightarrow{\sim} \mathbf{R}$, $\alpha_2 : \mathbf{R}[X]/(X-1) \xrightarrow{\sim} \mathbf{R}$, $\alpha_3 : \mathbf{R}[X]/(X^2-1) \xrightarrow{\sim} \mathbf{R} \times \mathbf{R}$, $\alpha_4 : \mathbf{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbf{C}$, $\alpha_5 : \mathbf{R}[X]/(X^3-1) \xrightarrow{\sim} \mathbf{R} \times \mathbf{C}$. Expliquer pourquoi il s'agit bien des isomorphismes.

Exercice 6. (a) Construire un corps à 9 éléments. Expliquer pourquoi il s'agit bien d'un corps.
(b) Soit $A = (\mathbf{Z}/5\mathbf{Z})[X]/(X^3 - X + 2)$. Décrire explicitement l'ensemble de tous les éléments de l'anneau A. Déterminer le cardinal de A. L'anneau A est-il un corps (resp. un produit de corps) ? Pourquoi ?
(c) Idem pour l'anneau $B = (\mathbf{Z}/5\mathbf{Z})[X]/(X^3 - X + 1)$.

Les réponses doivent être justifiées.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.

Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. Déterminer le nombre de diviseurs positifs de l'entier $n = 2016000$.

Exercice 2. Soient $a, b \geq 1$ des entiers. Vrai ou faux (et pourquoi) :
(a) si $a^2 \mid b^3$, alors $a \mid b$;
(b) si $a^3 \mid b^2$, alors $a \mid b$;
(c) si $a^2 \mid b^2$, alors $a \mid b$.

Exercice 3. Pour tout entier $n \geq 0$ on note $x_n = 1018 \cdot 2018^n + 1026 \cdot 2019^n$. Que peut-on dire des valeurs de $x_n \pmod{13}$? Quand est-ce qu'on a $x_n \equiv 0 \pmod{13}$ (resp. $x_n \equiv 3 \pmod{13}$) ?

Exercice 4. Le nombre $(4/7)^{4/7}$ est-il rationnel ou pas ? Pourquoi ?

Exercice 5. Résoudre dans $\mathbf{Z}$ les systèmes suivants :
(a) $21x \equiv 33 \pmod{45}$, $15x \equiv 6 \pmod{66}$.
(b) $x \equiv 9 \pmod{15}$, $x \equiv 3 \pmod{16}$, $x \equiv 13 \pmod{17}$.

Exercice 6. Montrer :
(a) $[a \equiv b \pmod{m} \text{ et } a \equiv b \pmod{n}] \iff a \equiv b \pmod{\mathrm{ppcm}(m, n)}$.
(b) Si $\mathrm{pgcd}(a, 21) = 1$, alors $a^6 \equiv 1 \pmod{63}$.
(c) Déterminer les valeurs possibles de $a^6 \pmod{63}$, pour $a \in \mathbf{Z}$.

Exercice 7. Construire un corps F à 8 éléments. Expliquer pourquoi il s'agit bien d'un corps. Décrire explicitement l'ensemble de tous les éléments de F.

Les réponses doivent être justifiées.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.

Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. Déterminer l'ensemble de tous les entiers positifs n tels que $n^2 \mid 216000$. Déterminer leur nombre et leur somme.

Exercice 2. (a) Résoudre dans $\mathbf{Z}$ la congruence $64x \equiv 14 \pmod{100}$.
(b) Idem pour $65x \equiv 15 \pmod{100}$.

Exercice 3. Le nombre $(\sqrt[3]{40} - 3)/7$ est-il rationnel ou pas ? Pourquoi ?

Exercice 4. Déterminer toutes les valeurs possibles de $x^{16} \pmod{16}$, $x^{16} \pmod{17}$ et de $x^{16} \pmod{272}$ pour $x \in \mathbf{Z}$.

Exercice 5. Soient $a, b, c \in \mathbf{Z}$ des entiers non nuls. Vrai ou faux (et pourquoi) :
(a) si $a^3 \mid b^2$ et $b \mid c^2$, alors $a \mid c$;
(b) si $a^3 \mid b^2$ et $b^3 \mid c^4$, alors $a \mid c$.

Exercice 6. Résoudre dans $\mathbf{Z}$ le système suivant :

$$7x \equiv 11 \pmod{15}, \qquad 5x \equiv 3 \pmod{22}.$$

Les documents ne sont pas autorisés, les calculatrices non plus.

Les réponses doivent être justifiées.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.

Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. Résoudre dans $\mathbf{Z}$ le système suivant :

$$21x \equiv 33 \pmod{48}, \qquad 4x \equiv 18 \pmod{35}.$$

Exercice 2. Trouver $b \in \{0, \ldots, 142\}$ tel que $2020^{2019} \equiv b \pmod{143}$.

Exercice 3. Déterminer le nombre de solutions $\pmod 8$ de la conguence $x^2 \equiv 1 \pmod 8$. Idem pour $x^2 \equiv 1 \pmod 9$ et $x^2 \equiv 1 \pmod{72}$.

Exercice 4. Soit a un entier qui n'est pas divisible par 5. Montrer que $a \pmod{25}$ est un générateur de $(\mathbf{Z}/25\mathbf{Z})^*$ si et seulement si $a^4, a^{10} \not\equiv 1 \pmod{25}$. Trouver un tel générateur.

Exercice 5. Les groupes suivants, sont-ils isomorphes ? Pourquoi ?
(a) $(\mathbf{Z}/3\mathbf{Z}, +) \times (\mathbf{Z}/2\mathbf{Z}, +)$ et $(\mathbf{Z}/6\mathbf{Z}, +)$.
(b) $(\mathbf{Z}/4\mathbf{Z}, +) \times (\mathbf{Z}/2\mathbf{Z}, +)$ et $(\mathbf{Z}/8\mathbf{Z}, +)$.
(c) $(\mathbf{Z}/6\mathbf{Z}, +)$ et $(\mathbf{Z}/7\mathbf{Z} \smallsetminus \{0\}, \cdot)$.

Exercice 6. (a) Définir un morphisme d'anneaux.
(b) Si $f : A \longrightarrow B$ est un morphisme d'anneaux, alors on a $f(A^*) \subset B^*$ et $f(a^{-1}) = f(a)^{-1}$ pour tout $a \in A^*$.
(c) Déterminer tous les morphismes d'anneaux $\mathbf{Z} \longrightarrow \mathbf{C}$.

Les documents ne sont pas autorisés, les calculatrices non plus.

Les réponses doivent être justifiées.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.

Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. Soit $n \geq 1$ un entier. On note $A_n = (5^n - 1)/4$ et $B_n = (5^n + 1)/2$. Montrer :
(a) A_n et B_n sont des entiers tels que $A_n \equiv n \pmod 4$ et $B_n \equiv 2n + 1 \pmod 8$.
(b) Si A_n est un nombre premier, alors n est un nombre premier.
(c) Si B_n est un nombre premier, alors $n = 2^k$ $(k \geq 0)$.

Exercice 2. Expliciter l'ensemble

$$\{n \in \mathbf{Z} \mid \text{ l'équation } 20x + ny = 14 \text{ admet une solution } x, y \in \mathbf{Z}\}.$$

Exercice 3. (a) Déterminer toutes les valeurs possibles de $x^{36} \pmod{999}$ $(x \in \mathbf{Z})$.
(b) Résoudre la congruence $x^{40} \equiv x^4 \pmod{999}$.

Exercice 4. Soit G un groupe, soit $g \in G$ un élément d'ordre fini $n \geq 1$. Donner une formule pour l'ordre de g^k $(k \geq 1)$. Démontrer cette formule.

Exercice 5. Les groupes suivants, sont-ils isomorphes ? Pourquoi ?
(a) $(\mathbf{Z}/14\mathbf{Z}, +) \times (\mathbf{Z}/15\mathbf{Z}, +)$ et $(\mathbf{Z}/10\mathbf{Z}, +) \times (\mathbf{Z}/21\mathbf{Z}, +)$.
(b) $(\mathbf{Z}/14\mathbf{Z}, +) \times (\mathbf{Z}/30\mathbf{Z}, +)$ et $(\mathbf{Z}/10\mathbf{Z}, +) \times (\mathbf{Z}/42\mathbf{Z}, +)$.
(c) $(\mathbf{Z}/13\mathbf{Z} \smallsetminus \{0\}, \cdot)$ et $(\mathbf{Z}/21\mathbf{Z} \smallsetminus \{0\}, \cdot)$.

Les documents ne sont pas autorisés, les calculatrices non plus.

Les réponses doivent être justifiées.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.

Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. Déterminer le nombre et la somme des diviseurs positifs de 36000.

Exercice 2. Déterminer toutes les solutions $x, y \in \mathbf{Z}$ de l'équation $42x + 26y = 4$.

Exercice 3. Montrer que le nombre $(\sqrt[3]{56} + 2)/5$ n'est pas rationnel.

Exercice 4. Déterminer l'ensemble

$$\{a \in \mathbf{Z} \mid \text{ la congruence } ax \equiv 6 \pmod{20} \text{ a une solution } x \in \mathbf{Z}\}.$$

Exercice 5. Résoudre dans $\mathbf{Z}$ le système suivant :

$$7x \equiv 24 \pmod{30}, \qquad 6x \equiv 4 \pmod{22}.$$

Les documents ne sont pas autorisés, les calculatrices non plus.

Les réponses doivent être justifiées.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.

Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. Résoudre dans $\mathbf{Z}$ le système suivant :

$$2x \equiv 24 \pmod{50}, \qquad 5x \equiv 2 \pmod{36}.$$

Exercice 2. Pour tout entier $n \geq 0$ on note $x_n = 5 \cdot 2022^n - 3 \cdot 2021^n$. Que peut-on dire des valeurs de $x_n \pmod{19}$? Quand est-ce qu'on a $x_n \equiv 0 \pmod{19}$ (resp. $x_n \equiv 2 \pmod{19}$) ?

Exercice 3. (a) Soit $a \in \mathbf{Z}$. Déterminer les valeurs possibles de $a^4 \pmod 5$, $a^4 \pmod{16}$ et $a^4 \pmod{80}$.
(b) Déterminer le nombre de solutions $x \pmod{80}$ de la congruence $x^2 \equiv 41 \pmod{80}$.

Exercice 4. Le groupe $(\mathbf{Z}/8\mathbf{Z})^*$ (resp. $(\mathbf{Z}/9\mathbf{Z})^*$) est-il cyclique ? Pourquoi ? Si c'est le cas, trouver tous les générateurs de ce groupe.

Exercice 5. Définir un corps (resp. un anneau intègre). Quand est-ce que $\mathbf{Z}/n\mathbf{Z}$ $(n \geq 1)$ est un corps (resp. un anneau intègre) ? Justifier la réponse.

Exercice 6. Construire un corps F à 27 éléments. Expliquer pourquoi il s'agit bien d'un corps.

Les documents ne sont pas autorisés, les calculatrices non plus.

Les réponses doivent être justifiées.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.

Il n'est pas nécessaire de tout faire pour avoir la note maximale.

Exercice 1. Soient $a, b \geq 1$ des entiers. Vrai ou faux (et pourquoi) :
(a) si $a^2 \mid b^3$, alors $a \mid b$;
(b) si $a^3 \mid b^2$, alors $a \mid b$;
(c) si $a^2 \mid b^2$, alors $a \mid b$.

Exercice 2. Pour tout entier $n \geq 0$ on note $a_n = 2019^n$, $b_n = 2022^n$, $c_n = 2010 \cdot 2019^n + 2024 \cdot 2022^n$. Que peut-on dire des valeurs de $a_n, b_n, c_n \pmod{17}$? Quand est-ce qu'on a $c_n \equiv 0 \pmod{17}$?

Exercice 3. Le nombre $(3/2)^{5/8}$ est-il rationnel ou pas ? Pourquoi ?

Exercice 4. Résoudre dans $\mathbf{Z}$ les systèmes suivants :
(a) $33x \equiv 24 \pmod{45}$, $30x \equiv 6 \pmod{72}$.
(b) $33x \equiv 24 \pmod{45}$, $30x \equiv 66 \pmod{72}$.

Exercice 5. Montrer :
(a) $[a \equiv b \pmod{m} \text{ et } a \equiv b \pmod{n}] \iff a \equiv b \pmod{\mathrm{ppcm}(m, n)}$.
(b) Si $\mathrm{pgcd}(a, 10) = 1$, alors $a^{20} \equiv 1 \pmod{400}$.

Exercice 6. (a) L'anneau $(\mathbf{Z}/5\mathbf{Z})[X]/(X^2 + 2X + 2)$ est-il un corps (resp. un produit de corps) ? Pourquoi ?
(b) Idem pour $(\mathbf{Z}/5\mathbf{Z})[X]/(X^2 + 2X + 3)$.

Les documents ne sont pas autorisés, les calculatrices non plus.

Les réponses doivent être justifiées.

Si vous citez un résultat du cours, vous devrez donner un énoncé précis.