Ex 1 : Montrer que $n = 1010...10101$, comptant $2p$ zéros, n'est pas premier.

Ex 2 : (*) Quel est le chiffre des unité de $2022^{2022^{2022}}$?

Ex 3 : (*) ***1.*** Démontrer que card$(\{1 \leq k \leq m$ tels que $q|k\} = \lfloor \frac{m}{q} \rfloor$.

2. En déduire que si q est premier, $\nu_q(m!) = \sum_{i=1}^{+\infty} \lfloor \frac{m}{q^i} \rfloor$.

Ex 4 : Soit p un nombre premier strictement supérieur à 3, montrer que $p^2 - 1$ est divisible par 12 et par 24.

Ex 5 : Déterminer les entiers $n \in \mathbb{N}$ tels que : $(2n + 8) \wedge (3n + 15) = 6$.

Ex 6 : Montrer que $\ln(2)/\ln(3)$ est irrationnel.

Ex 7 : Soit n de la forme $3^p 5^q$ tel que le produit de ses diviseurs soit 45^{42}. Déterminer n.

Ex 8 : Résoudre dans $\mathbb{Z}^2$: $\left\{ \begin{array}{rcl} x \wedge y & = & x - y \\ x \vee y & = & 72 \end{array} \right.$.

Ex 9 : Résoudre dans $\mathbb{Z}^2$: $544x - 944y = 160$.

Ex 10 : (*) Montrer qu'il existe un nombre infini de nombres premiers n tels que $n \equiv -1[4]$.

Ex 11 : (*) On définit sur $\mathbb{N}^*$ la fonction μ ainsi :

- Si $n = 1, \mu(n) = 1$;
- Si n a un facteur carré, $\mu(n) = 0$;
- Sinon, en notant $n = p_1...p_k$ la décomposition en facteurs premiers de n, on a $\mu(n) = (-1)^k$.

1. Montrer que pour tous entiers $n, m \in \mathbb{N}^*$ premiers entre eux, $\mu(mn) = \mu(m)\mu(n)$.

2. On considère désormais la fonction S définie sur $\mathbb{N}^*$ par $S(n) = \sum_{d|n} \mu(d)$. Montrer que pour $n \geq 2$, on a : $S(n) = 0$.

Ex 12 : ***1.*** Soit $n \in \mathbb{N}$. Montrer que si $2^n + 1$ est premier alors il existe $p \in \mathbb{N}$ tel que $n = 2^p$.
2. On note $f_p = 2^{2^p} + 1$. Montrer que, pour $p \neq q$, $f_p \wedge f_q = 1$.
3. En déduire qu'il y a une infinité de nombres premiers.

Ex 13 : Déterminer le pgcd dans $\mathbb{Q}[X]$ des polynômes A et B dans les cas suivants :

1) $A = 2X^4 + 3X^3 + 4X^2 + 2X + 1$ $\qquad$ $B = 3X^3 + 4X^2 + 4X + 1$;
2) $A = X^5 + X^4 + 2X^3 - 2X + 3$ $\qquad$ $B = X^4 + 3X^3 + 7X^2 + 8X + 6$.

Ex 14 : (*)

1. Soient $P \in \mathbb{Z}[X]$ de degré supérieur ou égal à 1 et $x \in \mathbb{Z}$. On pose $p = P(x)$. On suppose p premier.

- ***a.*** Montrer que : $\forall k \in \mathbb{Z}, P(x + kp) \equiv P(x)[p]$.
- ***b.*** Montrer qu'il existe $k \in \mathbb{Z}$ tel que $P(x + kp)$ n'est pas premier.
- ***c.*** Existe-t-il $P \in \mathbb{Z}[X]$ non constant tel que pour tout entier naturel n (ou à partir d'un certain rang), $P(n)$ est premier ?

2. Pour tout entier n, on note $\omega(n)$ le nombre de diviseurs premiers de n. Soit $P \in \mathbb{Z}[X]$; on pose $\Omega(P) = \{\omega(P(n)) | n \in \mathbb{N}, P(n) \neq 0\}$.

- ***a.*** On suppose $\Omega(P)$ borné et on note $N = max(\Omega(P))$. Soit $u \in \mathbb{N}$ tel que : $\omega(P(u)) = N$. On note $a = P(u)$. Montrer que : $\forall v \in \mathbb{Z}, P(u + a^2 v) \in \{-a, 0, a\}$.
- ***b.*** Conclure sur le nombre de diviseurs premiers de $P(n)$ pour $n \in \mathbb{N}$.

Ex 15 : ***1.*** Soit $P \in \mathbb{C}[X]$. Montrer que les racines de P sont simples si et seulement si $P \wedge P' = 1$.
2.Montrer que si P est irréductible sur $\mathbb{Q}[X]$, alors toutes les racines complexes de P sont simples.

Ex 16 : Soit $P = X^4 + X^2 + 1$. Est-il irréductible dans $\mathbb{C}[X]$? dans $\mathbb{R}[X]$? dans $\mathbb{Q}[X]$? Mêmes questions avec $Q = X^3 + 3X^2 + 2$ et $R = 8X^3 + 6X^2 - 9X + 24$.

Ex 17 : (*) Soit des entiers naturels $a_1, a_2, \ldots, a_n$, deux à deux distincts. On note $P = -1 + \prod_{i=1}^{n}(X - a_i)$. On suppose qu'on peut décomposer P en produit QR de polynômes à coefficients entiers, démontrer qu'un des deux polynômes est de degré n.

Ex 18 : On pose pour $n \in \mathbb{N}$ le polynôme $P_n = (X^2 - X + 1)^n - X^{2n} - X^n + 1$.

1. Déterminer n tel que $X^3 - X^2 + X - 1$ divise P_n.
2. Dans les cas où P_n n'est pas divisé, calculer le reste de la division euclidienne

---

Ex 19 : (*) Quels sont les polynômes complexes P tels que $P(\mathbb{U}) \subset \mathbb{U}$ (en notant $\mathbb{U}$ le cercle unité) ?

Ex 20 : (*) Soit $P \in \mathbb{C}[X]$ unitaire de degré au moins deux tel que : $P''|P$. Montrer que soit P est scindé à racines simples sur $\mathbb{C}$, soit il est de la forme $(X-a)^n$.

Ex 21 : ***1.*** Le polynôme X^4+4 est-il irréductible sur $\mathbb{R}$? Sur $\mathbb{Q}$?
2. En déduire les entiers n tels que n^4+4 est premier.

Ex 22 : Soit $P = (X+1)^7 - X^7 - 1$.

1. Calculer $P(j)$. En déduire la factorisation de P en facteurs irréductibles dans $\mathbb{R}[X]$.

2. Décomposer en éléments simples $\dfrac{(X^3-1)^4}{((X+1)^7-X^7-1)^2}$ dans $\mathbb{R}(X)$.

Ex 23 : Soit $\mathbf{K}$ le corps des nombres réels ou complexes. Soit $\dfrac{A}{B}$ une fraction rationnelle de $\mathbf{K}(X)$ dont le nombre α est pôle de degré 1. Montrer que le coefficient de $\dfrac{1}{(X-\alpha)^2}$ dans la décomposition en éléments simples de $\dfrac{A}{B^2}$ est $\dfrac{A(\alpha)}{B'(\alpha)^2}$.

Ex 24 : (*) Soit $n \in \mathbb{N}$, on note $(z_1, \dots, z_n)$ les racines de X^n+1.

1. Décomposer en éléments simples $\dfrac{X^k}{X^n+1}$ pour tout $k \in [\![0, n]\!]$.

2. Montrer que : $\forall P \in \mathbb{C}_n[X],\ XP'(X) = \dfrac{n}{2}P(X) + \dfrac{2}{n}\displaystyle\sum_{k=1}^{n} \frac{z_k P(z_k X)}{(z_k-1)^2}$.

Ex 25 : Soit $\omega_k = e^{\frac{2ik\pi}{n}}$ et $p \in [\![0, n-1]\!]$, avec $n \geq 2$. Mettre sous forme irréductible $\displaystyle\sum_{k=0}^{n-1} \frac{\omega_k^p}{X-\omega_k}$.

Ex 26 : Soit G un groupe fini non réduit à l'élément neutre et tel que : $\forall g \in G,\ g^2 = e$.

1. Montrer que G est commutatif.

2. Soit H un sous-groupe de G, avec $H \neq G$ et $a \in G \setminus H$. Montrer que $H \cup aH$ est un sous-groupe de G.

3. Montrer que le cardinal de G est une puissance de 2.

Ex 27 : Soit $(G, \cdot)$ un groupe commutatif fini, on note e l'élément neutre. Le groupe des automorphismes de G est supposé de cardinal 3.

1. Montrer que : $\phi : G \to G,\ x \mapsto x^{-1}$ est un automorphisme, puis que $\forall x \in G,\ x^2 = e$.

2. Montrer qu'il existe un sous-groupe V de G de cardinal 4, déterminer les automorphismes de V.

3. Montrer qu'il existe $r \in \mathbb{N}$ tel G soit isomorphe à $V \times (\mathbb{Z}/2\mathbb{Z})^r$, en conclure une absurdité.

Ex 28 : Un sous-groupe H de $(G,\cdot)$ est dit distingué lorsque

$$\forall x \in H,\ \forall a \in G,\ axa^{-1} \in H.$$

1. Montrer que le noyau d'un morphisme de groupes au départ de $(G,\cdot)$ est distingué.

2. Démontrer que H est distingué dans G si et seulement si pour tout $a \in G$, $Ha = aH$.

3. Soient H, K deux sous-groupes de $(G,\cdot)$. On suppose H distingué.
Montrer que l'ensemble $HK = \{xy\,;\, x \in H,\, y \in K\}$ est un sous-groupe de $(G,\cdot)$.

4. Considérons l'ensemble G/H des classes de G sous H (c'est-à-dire pour la relation $x\mathcal{R}y$ ssi $xy^{-1} \in H$). Démontrer qu'on le munit d'une structure de groupe en posant $Hx * Hy = Hxy$.

Ex 29 : Sur $\mathbb{R}^2$, on définit l'application $(a,b) \longmapsto a \top b = (a^3+b^3)^{\frac{1}{3}}$.

1. Démontrer que $(\mathbb{R}, \top)$ est un groupe commutatif.

2. Soit $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$, $a \longmapsto a^3$. Démontrer que φ est un isomorphisme du groupe $(\mathbb{R}, \top)$ sur le groupe $(\mathbb{R}, +)$.

Ex 30 : Soient Γ, Γ' des groupes finis et $\varphi : \Gamma \to \Gamma'$ un morphisme de groupes. Soit $H = \ker \varphi$.

1. Soit $\gamma' \in \Gamma'$. Démontrer que $\varphi^{-1}(\{\gamma'\})$ est vide ou de la forme $\gamma H = \{\gamma h \mid h \in H\}$ pour un certain $\gamma \in \Gamma$.

2. Démontrer que $\mathrm{card}(\Gamma) = \mathrm{card}(\varphi(\Gamma))\,\mathrm{card}(H)$

Ex 31 : (*) Soit $(G,.)$ un groupe commutatif fini de cardinal n et de neutre e. Pour $d \in \mathbb{N}^*$ divisant n, soit $G_d = \{x \in G,\ x^d = e\}$. On écrit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition de n en facteurs premiers.

1. Vérifier que G_d est un sous-groupe de G.

2. Montrer que $f : \left\{ \begin{array}{ccc} \prod_{i=1}^{r} G_{p_i^{\alpha_i}} & \to & G \\ (x_1, ..., x_r) & \mapsto & x_1 ... x_r \end{array} \right.$ est un isomorphisme.

On suppose désormais que pour tout diviseur d de n dans $\mathbb{N}^*$, on a : $|G_d| \leq d$.

3. Montrer que pour tout i dans $[\![1, r]\!]$, il existe g_i dans G d'ordre $p_i^{\alpha_i}$. En déduire que G est cyclique.

Ex 32 : Le groupe $(\mathbb{Q}, +)$ est-il engendré par une partie finie ?

Ex 33 : ***1.*** Démontrer que les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$ ne sont pas isomorphes.
2. Démontrer que les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ ne sont pas isomorphes.

Ex 34 : (*) Déterminer les morphismes de groupes entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/m\mathbb{Z}, +)$.

Ex 35 : Soient $\alpha \in \mathbb{C}^*$ et $\beta \in \mathbb{C}$ et on note $f_{\alpha,\beta} : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \alpha z + \beta \end{array} \right.$

1. Montrer que $\{f_{\alpha,\beta}, \alpha \in \mathbb{C}^*, \beta \in \mathbb{C}\}$ est un groupe pour la loi $\circ$. Est-il commutatif ?

2. A quelle condition sur α, β, l'application $f_{\alpha,\beta}$ est d'ordre fini ?

Ex 36 : (*) Soit p un nombre premier. On pose $G_p = \left\{ z \in \mathbb{C} \,;\, \exists k \in \mathbb{N},\, z^{p^k} = 1 \right\}$.

1. Montrer que G_p est un sous-groupe de $(\mathbb{C}^*, \times)$.

2. Déterminer les générateurs de $(\mathbb{U}_n, \times)$, avec $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$.

3. Montrer que les sous-groupes de G_p différents de G_p sont cycliques et qu'aucun d'eux n'est maximal pour l'inclusion. *On pourra s'aider de* $\mathbb{U}_{p^k} = \{z \in \mathbb{C} \,;\, z^{p^k} = 1\}$.

4. Montrer que G_p n'est pas engendré par un système fini d'éléments.

Ex 37 : Soit $n \in \mathbb{N}$, avec $n \geq 3$ et $\omega = e^{\frac{2i\pi}{n}}$. Pour $k \in [\![0, n-1]\!]$, on pose $f_k : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \omega^k z \end{array} \right.$ et $g_k : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \omega^k \overline{z} \end{array} \right.$ On pose $G = \{f_k, g_k,\ k \in [\![0, n-1]\!]\}$.

1. Décrire géométriquement l'application f_k.

2. Montrer que $(G, \circ)$ est un groupe.

3. G est-il cyclique ?

4. Montrer que G est engendré par f_1 et g_0 et que $f_1 \circ g_0 = g_0 \circ f_1^{-1}$.

5. Soit H un groupe quelconque engendré par a et b, tels que a soit d'ordre n et b d'ordre 2 et $ab = ba^{-1}$. Montrer que G et H sont isomorphes.

Ex 38 : Soit G un groupe fini non réduit à un singleton. Montrer que $|G|$ est premier si et seulement si ses seuls sous-groupes sont $\{e\}$ et G.

Ex 39 : Soit $s \in \mathcal{S}_n$ un n-cycle. Soit G le sous-groupe de $\mathcal{S}_n$ engendré par s. Soit $\sigma \in G$. Montrer que σ engendre G si et seulement si σ est un n-cycle.

Ex 40 : Soit G l'ensemble des permutation de $\mathcal{S}_n$ telles que : $\forall k \in [\![1, n]\!],\ \sigma(n-k+1) = n - \sigma(k) + 1$. Montrer que G est un groupe.

Ex 41 : ***1.*** Soit $\sigma \in S_n$ et $a, b \in [\![1, n]\!]$ distincts. Déterminer $\sigma \circ (a, b) \circ \sigma^{-1}$.
2. Soit $\sigma \in S_n$ et $a_1, ..., a_p \in [\![1, n]\!]$ deux à deux distincts. Déterminer $\sigma \circ (a_1, ..., a_p) \circ \sigma^{-1}$.
3. En déduire que toute transposition (i, j) est la composée de transpositions du type $(1, k)$.
4. Montrer que $\{(1, k),\ k \in [\![2, n]\!]\}$ engendre $\mathcal{S}_n$.
5. En déduire que $\{(1, 2), (2, 3), ..., (n-1, n)\}$ engendre $\mathcal{S}_n$.
6.Soit $s \in S_n$ tel que : $\forall \sigma \in S_n,\ s \circ \sigma = \sigma \circ s$. Déterminer s.

Ex 42 : (*) Soit G un groupe cyclique de cardinal n, d'élément neutre e.

1. Soit H un sous-groupe de G. Montrer que H est cyclique. Montrer que le cardinal de H divise le cardinal de G.
2. Montrer qu'il y a $\varphi(d)$ éléments de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d, où φ désigne l'indicatrice d'Euler.
3. Montrer que $n = \sum_{d|n} \varphi(d)$.

Ex 43 : Soit $E = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix},\ a, b \in \mathbb{R} \right\}$.

1. Montrer que E est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$.
2. Soit $\varphi : \begin{cases} \mathbb{C} & \to & E \\ z & \mapsto & \begin{pmatrix} Re(z) & Im(z) \\ -Im(z) & Re(z) \end{pmatrix} \end{cases}$. Montrer que φ est un isomorphisme d'anneaux.

Ex 44 : Soient $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$ et on pose $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$. Par ailleurs on note : $\forall a, b \in \mathbb{Z},\ N(a + b\sqrt{2}) = a^2 - 2b^2$.

1. Montrer que $\mathbb{Q}[\sqrt{2}]$ a une structure de corps.
2. Dites brièvement pourquoi $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.
3. Montrer que l'application $\varphi : a + b\sqrt{2} \mapsto a - \sqrt{2}b$ est bien définie et que c'est un isomorphisme d'anneaux.
4. Montrer que : $\forall x, y \in \mathbb{Z}[\sqrt{2}],\ N(xy) = N(x)N(y)$.
5. Montrer que : $\forall x \in \mathbb{Z}[\sqrt{2}],\ x \in \mathcal{U}(\mathbb{Z}[\sqrt{2}]) \Leftrightarrow N(x) = \pm 1$.
6. Montrer que : $\forall n \in \mathbb{N},\ \pm(1 \pm \sqrt{2})^n$ est dans $\mathcal{U}(\mathbb{Z}[\sqrt{2}])$.
7. Soit $x = a + b\sqrt{2} \in \mathcal{U}(\mathbb{Z}[\sqrt{2}])$, avec $a, b \in \mathbb{N}$.
   a. Montrer que $a \neq 0$.
   b. Si $b = 0$, déterminer x.
   c. Si $b \neq 0$, montrer que l'on a : $b \leq a < 2b$.
   d. Montrer qu'il existe un entier n tel que $(1 + \sqrt{2})^n$. On pourra procéder par récurrence forte sur $a + b$ en distinguant les cas $b = 0$ et $b \neq 0$, et en calculant $\dfrac{x}{1 + \sqrt{2}}$ pour $b \neq 0$.
8. En déduire les éléments de $\mathcal{U}(\mathbb{Z}[\sqrt{2}])$.

Ex 45 : Soit A un anneau commutatif. Un idéal I de A est dit premier lorsque :
$\forall (a, b) \in A^2,\ ab \in I \Rightarrow (a \in I \ \text{ OU } \ b \in I)$.

1. On suppose $A \neq \{0\}$. Montrer que $\{0\}$ est premier si et seulement si A est intègre.
2. Trouver les idéaux premiers de $\mathbb{Z}$.
3. Soit $P \in \mathbb{K}[X]$ irréductible. Montrer que $P\mathbb{K}[X]$ est premier.
4. Soit I un idéal différent de A. Il est dit maximal lorsqu'on ne peut pas intercaler d'idéal strictement entre I et A. Montrer que $\{0\}$ est un idéal maximal si et seulement si A est un corps.
5. Déterminer les idéaux maximaux de $\mathbb{Z}$.
6. Montrer que tout idéal maximal de A est premier.

Ex 46 : On note $\mathbb{D} = \left\{ \frac{p}{10^n},\ p \in \mathbb{Z}, n \in \mathbb{N} \right\}$.

1. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2. Montrer que tout idéal de $\mathbb{D}$ est de la forme $a\mathbb{D}$, avec $a \in \mathbb{D}$.

Ex 47 : Soit $(A, +, x)$ un anneau commutatif non réduit à $\{0\}$. Démontrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0_A\}$ et A

Ex 48 : Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps.

1. Soit $x \in \mathbb{R}_+$. Montrer que $f(x) = (f(\sqrt{x}))^2$. En déduire que f est croissante.
2. Soit $(n, x) \in \mathbb{N} \times \mathbb{R}$. Montrer que $f(nx) = nf(x)$.
3. Soit $x \in \mathbb{Q}$, montrer que $f(x) = x$.
4. Montrer que $f = \mathrm{Id}_{\mathbb{R}}$.

Ex 49 : (*) Soit $a_1, \ldots, a_r \in \mathbb{N}^*$, deux à deux premiers entre eux. On pose, pour $1 \leqslant k \leqslant r, c_k = \prod_{\substack{i=1 \\ i \neq k}}^{r} a_i$.

1. Montrer qu'il existe $u_1, ...u_r$ dans $\mathbb{Z}$ tels que : $\sum_{i=1}^{r} c_i u_i = 1$.
2. Soit b dans $\mathbb{Z}$. Montrer qu'il existe $(y, x_1, \ldots, x_r) \in \mathbb{Z}^{r+1}$, avec $0 \leqslant x_k < a_k$ pour tout k de $[\![1, r]\!]$, tel que : $\frac{b}{a_1 \ldots a_r} = y + \sum_{k=1}^{r} \frac{x_k}{a_k}$.
3. Montrer que la décomposition précédente est unique (on pourra donner l'expression des x_k dans $\mathbb{Z}/a_k\mathbb{Z}$).

Ex 50 : On note φ l'indicatrice d'Euler. Trouver les $n \in \mathbb{N}^*$ tels que $\varphi(n)$ divise n.

Ex 51 : Montrer que si p est premier, $p > 5$, alors : $240 | (p^4 - 1)$.

Ex 52 : (*) Soit φ la fonction indicatrice d'Euler.

1. Calculer $\varphi(1176)$.
2. Soient $p_1, \ldots, p_r$ des nombres premiers distincts. Soit $a \in \mathbb{N}^*$ et on pose $q = ap_1p_2 \cdots p_r$. Calculer le cardinal de l'ensemble $E(q, p_1, \ldots, p_r) = \left\{ k \in \mathbb{N} \,\middle|\, 1 \leqslant k \leqslant q \text{ et } k \wedge p_1p_2 \cdots p_r = 1 \right\}$.

Ex 53 : Résoudre dans $\mathbb{Z}/143\mathbb{Z}$ l'équation suivante : $x^2 - 3x + 2 = 0$.

Ex 54 : Soit p un nombre premier et $G = (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ qui est un groupe muni de $+$. Combien il y a-t-il d'éléments d'ordre p ? d'ordre p^2 ?

Ex 55 : (*) Soit p un nombre premier impair. Résoudre $x^2 = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$, puis montrer que $(p-1)! \equiv -1 \ \ [p]$.

Ex 56 : Soit p un entier premier et $k \in \mathbb{N}$. Montrer que $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$ est égal à 0 ou -1.

Ex 57 : Résoudre dans $\mathbb{Z}/41\mathbb{Z}$ l'équation $x^3 - 21x^2 + 29x - 9 = 0$.

Ex 58 : (*) ***1.*** Soit p un nombre premier impair.
Montrer que le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$ est $\dfrac{p+1}{2}$.
2. Montrer que : $\{x^2,\ x \in (\mathbb{Z}/p\mathbb{Z})^*\} \subset \{x \in \mathbb{Z}/p\mathbb{Z},\ x^{\frac{p-1}{2}} = \overline{1}\}$.
3. Montrer que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est somme de deux carrés.

Ex 59 : Dans $\mathbb{Z}/n\mathbb{Z}$, avec $n \in \mathbb{N}^*$, on considère l'équation $(E) : \overline{x}^2 = \overline{x}$.

1. Résoudre (E) si n est premier.

2. Même question avec $n = p^k$, avec $k \in \mathbb{N}^*$ et p un nombre premier.

3. Quel est le nombre de solutions dans le cas général ?

4. Soit $\overline{x}$ une solution de (E). On pose $\alpha = n \wedge x$ et $\beta = n \wedge (x-1)$. Montrer que $\alpha\beta = n$.

5. Étudier la réciproque.

Ex 60 : ***1.*** Démontrer que $(\mathcal{U}(\mathbb{Z}/12\mathbb{Z}), \times)$ est isomorphe au groupe additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Est-il cyclique ?
2. $(\mathcal{U}(\mathbb{Z}/10\mathbb{Z}), \times)$ est-il cyclique ?

Ex 61 : Dans $\mathbb{Z}/11\mathbb{Z}$, résoudre : $\left\{ \begin{array}{lcl} x+y & = & \overline{4} \\ xy & = & \overline{10} \end{array} \right.$.

Ex 62 : ***1.*** Déterminer les éléments non inversibles de $\mathbb{Z}/p^2\mathbb{Z}$, avec p un nombre premier.
2. Trouver les entiers naturels n tels que : $9 | (2n^2 + 13n + 20)$.

Ex 63 : ***1.*** Soit a un nombre impair positif et n un entier supérieur à 3. Montrer que : $a^{2^{n-2}} \equiv 1 \ [2^n]$.
2. En déduire les entiers naturels non nuls n pour lesquels le groupe des inversibles de l'anneau $\mathbb{Z}/2^n\mathbb{Z}$ est cyclique.