2-Structures algébriques

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

Ex 4 : Déterminer les entiers $n \in \mathbb{N}$ tels que : $(2n+8) \wedge (3n+15) = 6$.

Ex 5 : Montrer que $\ln(2)/\ln(3)$ est irrationnel.

Ex 6 : Soit n de la forme $3^p 5^q$ tel que le produit de ses diviseurs soit 45^{42}. Déterminer n.

Ex 7 : Résoudre dans $\mathbb{Z}^2$: $\left\{ \begin{array}{lcl} x \wedge y & = & x - y \\ x \vee y & = & 72 \end{array} \right.$.

Ex 8 :

1. Soit $a \in \mathbb{N}$. Montrer que le reste de la division euclidienne de a^2 par 8 est égal à $0, 1$ ou 4.
2. Soit $n \in \mathbb{N}$. Montrer que si $n \equiv 7[8]$, alors n ne peut pas être la somme de trois carrés d'entiers.

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

Ex 10 : (*) 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 11 : (*) Montrer qu'il existe un nombre infini de nombres premiers n tels que $n \equiv -1[4]$.

Ex 12 :

1. Soit $n \in \mathbb{N}^*$ tel que $n \wedge 10 = 1$. Montrer que : $n^4 \equiv 1 \ [10]$.

2. On suppose $a \wedge 10 = 1$ et $k \in \mathbb{N}$. Montrer que : $a^{4.10^k} \equiv 1 \ [10^{k+1}]$.

Ex 13 : Déterminer l'ensemble des entiers relatifs tels que : $n^{13} \equiv n[42]$.

Ex 14 : *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 15 : 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 16 : *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.
3. Soit $P \in \mathbb{Q}[X]$. Montrer que s'il existe $a, b, c \in \mathbb{C}^*$ tels que $P = (X-a)^p(X-b)^q(X-c)^r$, avec $0 < p < q < r$ des entiers, alors a, b, c sont dans $\mathbb{Q}$.

Ex 17 : 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 18 : (*) 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 19 : 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 20 : Soit $\mathcal{S}$ l'ensemble des couples $(P, Q) \in \mathbb{R}[X]^2$ tels que
$(X-1)^n Q(X) + X^n P(X) = 1$.

1. Montrer l'existence et l'unicité d'un couple $(P_0, Q_0) \in \mathbb{R}_{n-1}[X]^2$ dans $\mathcal{S}$.

2. Déterminer $\mathcal{S}$.

Ex 21 : (*) Quels sont les polynômes complexes P tels que $P(\mathbb{U}) \subset \mathbb{U}$ (en notant $\mathbb{U}$ le cercle unité) ?

Ex 22 : (*) 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 23 : ***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 24 : Soit $P \in \mathbb{R}[X]$ tel que : $\forall x \in \mathbb{R},\ P(x) \geqslant 0$.

1. Montrer que P peut se décomposer comme suit : $\displaystyle\prod_{i=1}^{n}(X-a_i)^{\alpha_i} \cdot \prod_{j=1}^{m}(X-\lambda_j)^{\beta_j} \cdot \prod_{k=1}^{m}(X-\bar{\lambda_j})^{\beta_j}$ avec α_i entier pair et $\lambda_j \in \mathbb{C} \setminus \mathbb{R}$.

2. Montrer que : $\exists A, B \in \mathbb{R}[X],\ P = A^2 + B^2$.

3. On note $Q = P + P' + P^{(2)} + \cdots + P^{(n)}$ où n est le degré de P. Montrer que Q vérifie : $\forall x \in \mathbb{R},\ Q(x) \geqslant 0$.

Ex 25 :

1. Résoudre dans $\mathbb{C}$ l'équation : $4x^4 + 3x^2 + 1 = 0$.

2. Factoriser dans $\mathbb{R}[X]$ le polynôme $4X^4 + 3X^2 + 1$.

3. Trouver deux diviseurs de 40301.

Ex 26 : 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 27 : 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 28 : Un sous-groupe H de $(G, \cdot)$ est dit <u>distingué</u> 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 jusqu'à la fin de l'exercice. 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 : (*) 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 30 : Le groupe $(\mathbb{Q},+)$ est-il engendré par une partie finie ?

Ex 31 : Démontrer que tout morphisme de $(\mathbb{Q},+)$ dans $(\mathbb{Z},+)$ est l'application nulle.

Ex 32 : *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 33 : (*) Déterminer les morphismes de groupes entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(\mathbb{Z}/m\mathbb{Z},+)$.

Ex 34 : 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 35 : Soit $f \in \mathbb{Z}[X]$ et $S_q = \displaystyle\sum_{\substack{0 \le a < q \\ a \wedge q = 1}} \sum_{n=0}^{q-1} e^{\frac{2i\pi a f(n)}{q}}$, pour $q \in \mathbb{N}^*$. Montrer que : $q \wedge q' = 1 \Rightarrow S_{qq'} = S_q S_{q'}$.

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 G un groupe. On note $\widehat{G}$ l'ensemble des morphismes de groupes de G dans $(\mathbb{C}^*,\times)$.

1. Montrer que $\widehat{G}$ est un groupe.

2. Déterminer $\widehat{G}$ dans le cas où $G = \mathbb{Z}/n\mathbb{Z}$.

Ex 38 : 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 39 : 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 40 : 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 41 : 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 42 : *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 43 : (*) 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 $n = \displaystyle\sum_{d|n} \varphi(d)$.

Ex 44 : 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 $\varphi : \left\{ \begin{array}{ccc} \mathbb{C} & \to & E \\ z & \mapsto & \begin{pmatrix} Re(z) & Im(z) \\ -Im(z) & Re(z) \end{pmatrix} \end{array} \right.$. Montrer que φ est un isomorphisme d'anneaux.

Ex 45 : Soit $P = X^3 - X - 1$.

1. Montrer que P admet une unique racine réelle α et que celle-ci est irrationnelle.

2. Soit $Q \in \mathbb{Q}[X]$, non nul, de degré au plus deux. Montrer que $P \wedge Q = 1$.

3. On note $\mathbb{Q}[\alpha] = \{R(\alpha),\ R \in \mathbb{Q}[X]\}$. Montrer que $\mathbb{Q}[\alpha]$ est un $\mathbb{Q}$-espace vectoriel de dimension 3.

4. Montrer que c'est un sous-corps de $\mathbb{R}$.

Ex 46 : On pose $u = 2+\sqrt{3}$ et $v = 2-\sqrt{3}$. Pour $n \in \mathbb{N}$, on note $M_n = 2^n - 1$ et $s_n = u^{2^n} + v^{2^n}$.

1. Montrer que si M_n est premier, alors n est premier.
2. Montrer que : $\forall n \in \mathbb{N},\ s_{n+1} = s_n^2 - 2$. Qu'en déduire sur la suite (s_n) ?
3. Soit q un nombre premier. On munit l'ensemble $B = (\mathbb{Z}/q\mathbb{Z})^2$ des deux lois de composition interne définies par :

$$(x,y)+(x',y') = (x+x', y+y') \quad \text{et} \quad (x,y).(x',y') = (xx'+3yy', xy'+x'y).$$

   (a) Montrer que les deux lois précédentes munissent B d'une structure d'anneau commutatif fini.

   (b) On note $A = \mathbb{Z}+\sqrt{3}\mathbb{Z}$. Montrer que l'application $\pi : \left\{\begin{array}{lcl} A & \to & B \\ a+\sqrt{3}b & \mapsto & (\overline{a}, \overline{b}) \end{array}\right.$ est bien défini et est un morphisme surjectifs d'anneaux.

4. On suppose n premier. Montrer que si M_n divise s_{n-2}, alors M_n est premier.
   Indication : on pourra raisonner par l'absurde en considérant le plus petit facteur premier q de M_n et déterminer l'ordre de $(\overline{2}, \overline{1})$ dans le groupe des éléments inversibles de l'anneau B.

Ex 47 : Soit $(A, +, \cdot)$ un anneau d'élément unité 1.

1. Soit a un élément de A tel qu'il existe un entier naturel non nul n tel que $a^n = 0$. Un tel élément est dit nilpotent.

   a. Montrer que $1-a$ est inversible et préciser son inverse.

   b. En déduire que $b = 1 + 2a + \cdots + na^{n-1}$ est inversible dans A et préciser son inverse.

2. Soit (a,b) dans A^2 tel que ab est nilpotent. Montrer que ba est nilpotent.

3. On suppose A commutatif. On note $\mathrm{Nil}(A)$ l'ensemble des éléments nilpotents de A. Montrer que $\mathrm{Nil}(A)$ est un idéal de A.

Ex 48 : Soit $A = \{m/n \in \mathbb{Q},\ \text{avec } n \text{ impair}\}$.

1. Montrer que A est un sous-anneau de $\mathbb{Q}$.

2. Quels sont les éléments inversibles de A ?

3. (*) Montrer que les idéaux non nuls de A sont de la forme $\{2^k x,\ x \in A\}$, avec $k \in \mathbb{N}$.

Ex 49 : 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 50 : 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 51 : (*) Soit $a_1, \dots, a_r \in \mathbb{N}^*$, 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 $(y, x_1, \dots, x_r) \in \mathbb{Z}^{r+1}$, avec $0 \leqslant x_k < a_k$ pour tout k de $[\![1, r]\!]$, tel que : $\dfrac{b}{a_1 \dots a_r} = y + \sum_{k=1}^{r} \dfrac{x_k}{a_k}$.
3. Montrer que la décomposition précédente est unique (on pourra donner l'expression des x_k dans $\mathbb{Z}/a_k\mathbb{Z}$).

Ex 52 : Soit N une application de $\mathbb{Q}$ dans $\mathbb{R}^+$. On dit que N est une valeur absolue si et seulement si :

- $\forall x \in \mathbb{Q}, N(x) = 0 \Leftrightarrow x = 0$;
- $\forall x, y \in \mathbb{Q}^2, N(xy) = N(x)N(y)$;
- $\forall x, y \in \mathbb{Q}^2, N(x + y) \leq N(x) + N(y)$.

Une valeur absolue N est dite ultramétrique si : $\forall x, y \in \mathbb{Q}^2, N(x + y) \leq max(N(x), N(y))$.
N est dite triviale si elle est constante sur $\mathbb{Q}^*$.
Si p est un nombre premier, on note $\nu_p(n)$ la valuation p-adique définie sur les entiers. On pose par convention $\nu_p(0) = +\infty$.

1. Soit N une valeur absolue. Déterminer $N(1)$ et $N(-1)$.
2. Soit $q = \dfrac{a}{b} \in \mathbb{Q}^*$ où $a, b \in \mathbb{Z}^{*2}$, et p un nombre premier. Montrer que : $\nu_p(a) - \nu_p(b)$ ne dépend que de q. On le notera $\nu_p(q)$.
3. On définit pour $q \in \mathbb{Q}^*, |q|_p = p^{-\nu_p(q)}$. Montrer que $|.|_p$ est une valeur absolue ultramétrique.
4. (*) Soit N une valeur absolue ultramétrique non triviale. Montrer qu'il existe $\alpha \in \mathbb{R}_+^*$ et p premier tels que $N = |.|_p^\alpha$.

Ex 53 : Montrer que si n est produit de nombres premiers distincts, alors :
$\forall k \in \mathbb{N}, \forall a \in \mathbb{Z},\ a^{1+k\varphi(n)} \equiv a[n]$.

Ex 54 : Soit $n \in \mathbb{N}^*$. Montrer que $n | \varphi(2^n - 1)$.

Ex 55 : On note φ l'indicatrice d'Euler. Trouver les $n \in \mathbb{N}^*$ tels que $\varphi(n)$ divise n.

Ex 56 : Résoudre dans $\mathbb{Z}/143\mathbb{Z}$ l'équation suivante : $x^2 - 3x + 2 = 0$.

Ex 57 : (*) Soient p un nombre premier tel que $p \equiv 3[4]$ et $C = \{x \in \mathbb{Z}/p\mathbb{Z}, \exists y \in \mathbb{Z}/p\mathbb{Z},\ x = y^2\}$.

1. Rappeler l'énoncé du petit théorème de Fermat. Montrer que : $-1 \notin C$.
   On pose $\pi_x = \displaystyle\prod_{y \in C\setminus\{x\}} (x+y)$ et pour $x \in C \setminus \{0\}$ et $\pi = \displaystyle\prod_{\substack{x,y \in C \\ x \neq y}} (x+y)$.
2. Déterminer le cardinal de C.
3. Montrer que : $\forall x \in C \setminus \{0\},\ \pi_x = \pi_1$.
4. Calculer π.

Ex 58 : (*) Soit φ la fonction indicatrice d'Euler.

1. Calculer $\varphi(1176)$.

2. Soient $p_1, \dots, p_r$ 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 $E(q, p_1, \dots, p_r) = \left\{k \in \mathbb{N} \,\middle|\, 1 \leqslant k \leqslant q \text{ et } k \wedge p_1p_2\cdots p_r = 1\right\}$.

Ex 59 : 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 60 : Soit p un entier premier et $k \in \mathbb{N}$. Montrer que $\displaystyle\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$ est égal à 0 ou -1.

Ex 61 : (*) ***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 62 : ***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 63 : Dans $\mathbb{Z}/11\mathbb{Z}$, résoudre : $\left\{\begin{array}{lcl} x+y & = & \overline{4} \\ xy & = & \overline{10} \end{array}\right.$.

Ex 64 : ***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 : $9 | (2n^2 + 13n + 20)$.