Université de Nice Sophia Antipolis
L2M&MI, Algèbre et Arithmétique 1, janvier 2014
Enseignant : Mohamed Elkadi — Série 1

**Exercice 1** *Calculer la somme des $n$ premiers entiers naturels impairs.*

**Exercice 2** *Soit $n \geq 2$.*

1. *Montrer que $u_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n} = \frac{2p+1}{2q}$, où $(p,q) \in \mathbb{N}^2$.*
2. *La fraction $u_n$ peut-elle être un entier ?*

**Exercice 3** *Montrer que*

1. *pour tout $n \in \mathbb{N}^*$, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$,*
2. *tout entier $n \geq 2$ est le produit de nombres premiers,*
3. *si $(a,b) \in \mathbb{R}^2$, $\forall n \in \mathbb{N}^*$, $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$, où $\binom{n}{i} = \frac{n!}{i!(n-i)!}$.*

**Exercice 4** *Soit $b \geq 2$ un entier.*

1. *Montrer que pour tout $n \in \mathbb{N}$, il existe $s \in \mathbb{N}$ tel que*
$$n = n_s b^s + \cdots + n_1 b + n_0$$
*avec $1 \leq n_s < b$ et $0 \leq n_0, \ldots, n_{s-1} < b$, et que cette expression (appelée l'écriture de $n$ en base $b$) est unique.*
2. *Montrer que $b^s \leq n < b^{s+1}$, et en déduire le nombre de "chiffres" $s+1$ qu'il faut pour écrire $n$ en base $b$ (en fonction de $n$ et $b$).*
3. *Décomposer 2014 dans les bases 2, 16, 60.*

**Exercice 5** *Existe-t-il un entier $n$ dont le reste de la division de 2003 par $n$ est 8 et le reste de la division de 3002 par $n$ est 27 ?*

**Exercice 6** *Calculer $\mathrm{pgcd}(12078, 12084)$, puis écrire ce pgcd comme combinaison linéraire de 12078 et 12084.*

**Exercice 7** *Soit $n \in \mathbb{N}$. La fraction $\frac{12n+1}{30n+2}$ est-elle toujours irréductible ?*

**Exercice 8** *Pour $i \in \mathbb{N}^*$, on note $p_i$ le $i$-ème nombre premier. Est-ce que pour tout $n \in \mathbb{N}^*$, le nombre $p_1 \ldots p_n + 1$ est toujours premier ?*

**Exercice 9** *1. Soit $n \geq 2$. Est-ce que l'un des entiers consécutifs $n! + 2, \ldots, n! + n$ est premier ?*

*2. En déduire qu'il est possible de trouver autant d'entiers consécutifs que l'on veut dont aucun n'est premier.*

**Exercice 10** *Existe-il $(x, y) \in \mathbb{N}^2$ tel que $2^x + 1 = y^3$ ?*

**Exercice 11** *Résoudre l'équation diophantienne $38x + 118y = 8$.*

**Exercice 12** *Trouver tous les couples d'entiers naturels $(m, n)$ tels que*

$$\begin{aligned} \mathrm{pgcd}(m,n) &= 5 \\ \mathrm{ppcm}(m,n) &= 30. \end{aligned}$$

**Exercice 13** *Soient $a$ et $b$ deux entiers strictement positifs tels que $a > b$.*

1. *Calculer $\mathrm{pgcd(a, b)}$ pour $b = 144$ et $a = 233$.*

2. *Si $\theta = \frac{1+\sqrt{5}}{2}$. On va montrer que le nombre d'étapes $n$ pour calculer $\mathrm{pgcd}(a, b)$ avec l'algorithme d'Euclide est au plus $1 + \frac{\ln(b)}{\ln(\theta)}$.*

   *(a) Montrer que l'on peut supposer $a$ et $b$ premiers entre-eux.*

   *(b) Si $r_0 = a, r_1 = b, \ldots, r_{n+1} = 0$ sont les restes dans l'algorithme d'Euclide, montrer (par récurrence descendante) que $\forall i = 1 \ldots n$, $r_i \geq \theta^{n-i}$. Puis, conclure.*

3. *On va modifier la division euclidienne de $a$ par $b$, en posant comme quotient $q$ l'entier le plus proche de $\frac{a}{b}$. Si $\frac{a}{b}$ est à mi-distance de 2 entiers, on choisit le plus grand des 2 comme $q$. Montrer qu'il existe un unique couple $(q, r) \in \mathbb{N} \times \mathbb{Z}$ tel que $a = bq + r$ avec $-\frac{b}{2} \leq r < \frac{b}{2}$.*

4. *En déduire un algorithme pour calculer $\mathrm{pgcd(a, b)}$ en utilisant cette division, que l'on illustrera sur $b = 144, a = 233$. Puis, expliquer l'intérêt de cet algorithme par rapport à celui habituel dit d'Euclide.*

5. *Quel est le nombre maximal de divisions dans cet algorithme "d'Euclide modifié" pour calculer $\mathrm{pgcd(a, b)}$ (en fonction de $\log_2 b$) ?*

**Exercice 14** *1. Montrer que tout nombre de la forme $4n+3, n \in \mathbb{N}$ admet un diviseur premier de la forme $4m + 3, m \in \mathbb{N}$.*

*2. Montrer qu'il y a une infinité de premiers de la forme $4n + 3, n \in \mathbb{N}$.*

**Exercice 15** *Montrer que le n-ième nombre premier $p_n \leq 2^{2^{n-1}}$. (En fait, on sait que $p_n < 2^n$ pour $n \geq 2$).*

**Exercice 16**

1. *Montrer que $\sqrt{2}, \sqrt{3}, \sqrt{6}$ sont des nombres irrationnels.*
2. *Montrer que plus généralement, si $a \in \mathbb{N}$ et $n \geq 2$ , alors $\sqrt[n]{a}$ est un nombre rationnel (en fait un entier) si, et seulement si, a est une puissance $n^{ieme}$ d'un entier.*
3. *Le nombre $\frac{\ln 2}{\ln 3}$ peut-il être rationnel ?*

**Exercice 17** *Soit $A = \{4n + 1 : n \in \mathbb{N}\}$. Un élément $a \in A$ est dit A-premier si le nombre de ses diviseurs positifs dans A est 2.*

1. *Est-ce que les éléments A-premiers sont premiers ?*
2. *Montrer que tout entier de $A \setminus \{1\}$ est soit A-premier soit un produit de A-premiers.*
3. *Ecrire $693 \in A$ en produit de A-premiers. Est-ce que la décomposition précédente des entiers de A en A-premiers est unique ?*

**Exercice 18** *Soit $n \geq 2$ un entier. On s'intéresse au nombre de diviseurs de n. On suppose que la factorisation de n est connue : $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.*

1. *Déterminer le nombre $d(n)$ de diviseurs (positifs) de n.*
2. *Quels sont les entiers dont le nombre de diviseurs est impair ?*
3. *Quelle est la somme $\sigma(n)$ de tous les diviseurs de n ?*

**Exercice 19**

1. *Soient $a \geq 2$ et $n \geq 2$ deux entiers. Donner une condition nécessaire pour que $a^n - 1$ soit premier.*
2. *Est-ce que cette condition est suffisante ?*
3. *Pour $n \in \mathbb{N}^*$, $\sigma(n) := \sum_{d>0, d/n} d$. Montrer que si deux entiers r et s sont premiers entre-eux, alors $\sigma(rs) = \sigma(r)\sigma(s)$.*
4. *Un entier $n \geq 2$ est dit parfait si $\sigma(n) = 2n$ (i.e. la somme de tous les diviseurs d (positifs) de n, avec $d \neq n$, est exactement n).*

   *Montrer que si p est tel que $2^p - 1$ premier, alors $2^{p-1}(2^p - 1)$ est parfait.*

5. *Soit* $\alpha$ *un entier pair et parfait. Donc* $\alpha = 2^{n-1}m$ *avec* $n \geq 2$ *et* $m$ *impair.*

   (a) *Montrer que* $m$ *est un multiple de* $2^n - 1$.

   (b) *Puis, montrer que* $m = 2^n - 1$ *et que* $m$ *est premier.*

   (c) *En déduire la forme des nombres pairs et parfaits ?*

**Exercice 20** *Enoncer et prouver les tests de divisibilité par* 2, *par* 3, *par* 6, *par* 9, *par* 11.

**Exercice 21** *Résoudre l'équation diophantienne* $6x \equiv 0 \mod 9$.

**Exercice 22** *Résoudre le système*

$$\begin{aligned} 5x &\equiv 2 \mod 6 \\ 3x &\equiv 1 \mod 5 \\ 4x &\equiv 3 \mod 7. \end{aligned}$$

**Exercice 23** *Résoudre le système*

$$\begin{aligned} x &\equiv 2 \mod 12 \\ x &\equiv 6 \mod 10 \\ x &\equiv 11 \mod 45. \end{aligned}$$

**Exercice 24** *Pour $n = 6, 7, 8$,*

1. *dresser les tableaux d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$,*
2. *déterminer l'opposé de chaque élément de $\mathbb{Z}/n\mathbb{Z}$,*
3. *préciser (lorsqu'il existe) l'iverse de chaque élément de $\mathbb{Z}/n\mathbb{Z}$.*

**Exercice 25** *Déterminer l'inverse de $\overline{526}$ dans $\mathbb{Z}/561\mathbb{Z}$.*

**Exercice 26** *Pour chacune de ces opérations, étudier l'associativité, la commutativité, l'existence de l'élément neutre, l'existence du symétrique :*

1. *On définit sur $\mathbb{N}$, $n * m = n + 2m$.*
2. *On définit sur $\mathbb{N}^*$, $n * m = \mathrm{pgcd}(n, m)$.*
3. *On définit sur $\mathbb{N}^*$, $n * m = \mathrm{ppcm}(n, m)$.*

**Exercice 27** *L'ensemble des bijections d'un ensemble $E$ sur lui même est noté $\mathcal{B}(E)$.*

1. *Montrer que $\mathcal{B}(E)$ muni de la composition est un groupe.*
2. *Si $E$ est fini et son cardinal est $n$, on note $\mathcal{B}(E)$ par $\mathfrak{S}_n$ et on l'appelle le groupe des permutations à $n$ éléments. Quel est le cardinal de $\mathfrak{S}_n$ ?*
3. *Déterminer $\mathfrak{S}_3$.*
4. *Est-ce que le groupe $\mathfrak{S}_n$ es commutatif ? (commencer par $n = 3$).*

**Exercice 28** *Déterminer tous les sous-groupes de $\mathbb{Z}$.*

**Exercice 29** *Soient $G_1$ et $G_2$ deux groupes et $f : G_1 \to G_2$ un morphisme de groupes. On note $e_i$ l'élément neutre de $G_i$.*

1. *Vérifier que $f(e_1) = e_2$, et que si $x \in G_1$, $f(x^{-1}) = \big(f(x)\big)^{-1}$.*
2. *Montrer que si $f$ est bijectif, alors $f^{-1}$ est un isomorphisme de groupes.*
3. *Montrer que si $H_1$ est un sous-groupe de $G_1$, alors $f(H_1)$ est un sous-groupe de $G_2$. On note par $\mathrm{im}(f)$ le sous-groupe $f(G_1)$ de $G_2$.*

4. *Montrer que si $H_2$ est un sous-groupe de $G_2$, alors $f^{-1}(H_2)$ est un sous-groupe de $G_1$. Et, en déduire que* $\ker(f) := \{x \in G_1 : f(x) = e_2\}$ *est un sous-groupe de $G_2$.*

5. *Montrer que $f$ est injectif si, et seulement si,* $\ker(f) = \{e_1\}$.

**Exercice 30** 1. *Montrer que le cercle $\{z \in \mathbb{C} : |z| = 1\}$ est un sous-groupe de $\mathbb{C}^*$.*

2. *Montrer que l'application*

$$\begin{array}{ccc} \mathbb{R} & \to & ]0, +\infty[ \\ x & \mapsto & e^x \end{array}$$

*est un morphisme de groupes et déterminer son inverse.*

**Exercice 31** 1. *Montrer qu'un corps (commutatif) est un anneau intègre.*

2. *Est-ce que la réciproque est vraie ?*

3. *Soit $A$ un anneau (commutatif et unitaire) fini et intègre. Montrer que $A$ est un corps.*

**Exercice 32** *Soit $n \geq 2$.*

1. *Supposons que $n$ est premier. Résoudre l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$.*

2. *Si $n$ est premier, montrer que $(n-1)! = -1 \mod n$.*

3. *Montrer que réciproquement si $(n-1)! = -1 \mod n$, alors $n$ est premier.*

**Exercice 33** *Soit $p$ un nombre premier.*

1. *Montrer que pour tout $k = 1, \ldots, p-1$, $p$ divise $\binom{p}{k} = \frac{p!}{k!(p-k)!}$.*

2. *Montrer que si $(m, n) \in \mathbb{N}^2, (m+n)^p \equiv m^p + n^p \mod p$.*

3. *En déduire que pour tout entier $a$, $a^p \equiv a \mod p$.*

**Exercice 34** *Soit $n \in \mathbb{N}^*$.*

1. *Si $d$ est un diviseur (positif) de $n$, on définit*

$$S_d = \{m : 1 \leq m \leq n, \mathrm{pgcd(m,n) = d}\}.$$

*Vérifier que les $S_d$ forment une partition de $\{1, \ldots, n\}$.*

2. *Quel est le cardinal de $S_d$ ?*

3. *En déduire $\sum_{d|n} \varphi(d) = n$.*

**Exercice 35** *Soit $A$ un anneau fini.*

1. *Montrer que si $a$ est un élément non nul de $A$, alors soit $a$ est diviseur de $0$, soit $a$ est inversible.*
2. *En déduire que si l'anneau $A$ est intègre, alors $A$ est un corps.*
3. *Est-ce que ce résultat est vrai si $A$ est infini ?*

**Exercice 36** *Soient $p$ et $q$ deux premiers distincts et $n$ leur produit. Montrer que si l'on connait $n$ et $\varphi(n)$, où $\varphi$ désigne l'indicatrice d'Euler, alors on peut déterminer $p$ et $q$*

**Exercice 37** *Soient $m$ et $n \geq 2$.*

1. *Expliquer comme peut-on munir $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau (commutatif et unitaire).*
2. *Déterminer l'ensemble des inversibles de cet anneau.*
3. *Montrer que*

$$\begin{array}{rcl} f : \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ {[x]_{mn}} & \mapsto & ([x]_m, [x]_n) \end{array}$$

   *est un morphisme d'anneaux.*
4. *Si $m$ et $n$ sont premiers entre-eux, montrer que $f$ est un isomorphisme.*
5. *En déduire que si $m$ et $n$ sont premiers entre-eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

**Exercice 38**

1. *Soient $n \in \mathbb{N}^*$ et $a \geq 2$. Montrer que si $a^n + 1$ est premier, alors $a$ est pair est $n = 2^m$ avec $m \in \mathbb{N}$.*

   *Les entiers $F_n = 2^{2^n} + 1$ sont appelés les nombres de Fermat.*
2. *Est-ce que $F_0, F_1, F_2, F_3, F_4$ sont premiers ?*
3. *Qu'en est-il pour $F_5$ ?*
   (a) *Quel est l'ordre de $2$ modulo $F_n$ ?*
   (b) *Soit $p$ un diviseur premier de $F_n$. Déterminer $\mathrm{ord}_p(2)$.*

(c) *Montrer que* $p = 1 + k2^{n+1}, k \in \mathbb{N}^*$.

(d) *Est-ce que* $F_5$ *est premier ?*

**Exercice 39** 1. *Est-ce que* 341 *est* 2*-pseudopremier ?*

2. *Est-ce que* 341 *est* 3*-pseudopremier ?*

**Exercice 40** *Montrer que si* $n$ *est* 2*-pseudopremier, alors* $2^n - 1$ *l'est aussi.*

**Exercice 41** 1. *Montrer que* 561 *et* 1729 *sont des nombres de Carmichäel.*

2. *Montrer que plus généralement, si* $n$ *est un entier dont la décomposition en premiers* $n = p_1 \dots p_r$ *(avec* $p_1, \dots, p_r$ *sont* 2 *à* 2 *distincts) est telle que pour tout* $i = 1 \dots r$*,* $p_i - 1$ *divise* $n - 1$*, alors* $n$ *est de Carmichäel.*

**Exercice 42** *Illustrer le cryptosystème RSA sur un exemple simple de votre choix.*

**EXERCICE 43** *Soit* $f(X) = X^5 + X^4 + X^3 + 15X^2 + 3X + 39 \in \mathbb{Z}[X]$.

1. *Effectuer la division de* $f(X)$ *par* $g(X) = X^2 + X + 1$.
2. *Pour quels* $m \geq 2$, *Le polynôme* $g(X)$ *divise* $f(X)$ *dans* $\big(\mathbb{Z}/m\mathbb{Z}\big)[X]$ *?*

**EXERCICE 44** *Pour quels premiers* $p$, *les polynômes* $X^6 + 2X^2 + X$ *et* $X^9 + 8X^3 + X$ *définissent la même application polynomiale sur* $\mathbb{F}_p$ *?*

**EXERCICE 45** *Soient* $A$ *un anneau commutatif et* $\mathcal{F}(A, A)$ *l'ensemble des applications de* $A$ *dans* $A$. *Si* $f(X) \in A[X]$, $\tilde{f}$ *désigne l'application polynomiale définie par* $f(X)$.

1. *Montrer que l'application*
$$\begin{array}{rcl} \mathcal{P} : A[X] & \rightarrow & \mathcal{F}(A, A) \\ f(X) & \mapsto & \tilde{f} \end{array}$$
*est un morphisme d'anneaux.*
2. *Si* $A$ *est fini, est-ce que* $\mathcal{P}$ *peut être injectif ?*
3. *Montrer que si* $A$ *est intègre, alors tout* $f(X) \in A[X]$ *admet au plus* $\deg f(X)$ *racines dans* $A$.
4. *Si* $A$ *est infini et intègre, montrer que* $\mathcal{P}$ *est injectif (donc un polynôme peut être confondu avec l'application polynomiale qu'il définit).*

**EXERCICE 46**

1. *Soit* $f(X) = a_d X^d + \cdots + a_0 \in \mathbb{Z}[X]$ *de degré* $d$. *Montrer que si* $\frac{\alpha}{\beta} \in \mathbb{Q}$ *est une racine de* $f(X)$, *alors* $\beta$ *divise* $a_d$ *et* $\alpha$ *divise* $a_0$.
2. *En déduire un algorithme pour calculer toutes les racines rationnelles d'un polynôme rationnel.*
3. *Trouver les racines du polynôme* $X^4 + X^3 + \frac{3}{4}X^2 - \frac{1}{4}X - \frac{1}{4}$.

**EXERCICE 47** *On note par* $\mathbb{R}_2[x] = \{P \in \mathbb{R}[x] : \deg P \leq 2\}$.

1. *Soient* $a_1, a_2, a_3$ *des nombres réels deux à deux distincts. Déterminer* 3 *polynômes* $L_1, L_2, L_3$ *de* $\mathbb{R}_2[x]$ *tels que pour tout* $i, j \in \{1, 2, 3\}$, $L_i(a_j) = \delta_{i,j}$, *où* $\delta_{i,j}$ *désigne le symbole de Kronecker.*

2. *Est-ce que* $(L_1, L_2, L_3)$ *est une base de* $\mathbb{R}_2[x]$ *?*

3. *Si oui, quelles sont les coordonnées d'un polynôme* $P$ *dans cette base.*

4. *Soient* $b_1, b_2, b_3$ *des valeurs réelles. Trouver un polynôme* $P \in \mathbb{R}_2[x]$ *qui vérifient* $P(a_1) = b_1, P(a_2) = b_2, P(a_3) = b_3$. *Est-ce qu'un tel polynôme est unique ?*

5. *Plus généralement, étant donnés* $n+1$ *nombres* $a_0, \dots, a_n$ *distincts deux à deux.*
   (a) *Montrer que pour tout* $i = 1 \dots n$, *il existe un seul polynôme* $L_i \in \mathbb{R}_n[x]$ *tel que* $L_i(a_i) = 1$ *et* $L_i(a_j) = 0$ *si* $j \neq i$.
   (b) *Montrer que la famille* $(L_0, \dots, L_n)$ *est une base de* $\mathbb{R}_n[x]$.
   (c) *Quelle est l'expression d'un polynôme dans cette base ?*
   (d) *Si* $b_0, \dots, b_n$ *sont des valeurs données, trouver un polynôme* $P$ *qui vérifie* $P(a_i) = b_i, i = 0 \dots n$.

**Exercice 48** *Soient* $a_1, \dots, a_n$ *des nombres distincts* 2 *à* 2. *Le but de cet exercice est de caculer le déterminant de la matrice*

$$\begin{pmatrix} 1 & \dots & \dots & 1 \\ a_1 & \dots & \dots & a_n \\ \vdots & & & \vdots \\ a_1^{n-1} & \dots & \dots & a_n^{n-1} \end{pmatrix} \tag{1}$$

*pour* $n \geq 2$.

*Pour cela, on considère* $f(X) = \det \begin{pmatrix} 1 & \dots & \dots & 1 \\ a_1 & \dots & a_{n-1} & X \\ \vdots & & & \vdots \\ a_1^{n-1} & \dots & a_{n-1}^{n-1} & X^{n-1} \end{pmatrix}$.

1. *Montrer que* $f(X)$ *est un polynôme dont on déterminera le degré.*

2. *Trouver les racines de* $f(X)$.

3. *En raisonnant par récurrence sur* $n$, *calculer le déterminant (1).*

**Exercice 49** *Soient* $f(X) = 3X^3+4X^2+3$ *et* $g(X) = 3X^3+4X^2+3X+4$ *dans* $\mathbb{F}_5[X]$.

1. *Effectuer la division de* $f(X)$ *par* $g(X)$.
2. *Effectuer la division de* $g(X)$ *par* $f(X)$.
3. *Déterminer* $\operatorname{pgcd}\big(f(X), g(X)\big)$.

**Exercice 50** *Soient* $f(X) = X^6 - 1$ *et* $g(X) = X^4 - 1$ *dans* $\mathbb{Q}[X]$.

1. *Quel est le* $\operatorname{pgcd}\big(f(X), g(X)\big)$ *?*
2. *Ecrire ce pgcd comme combinaison de* $f(X)$ *et* $g(X)$.
3. *Calculer le* $\operatorname{ppcm}\big(f(X), g(X)\big)$.

**Exercice 51** *Pour quels réels* $a$*, les polynômes réels* $X^4 + X^2 + a$ *et* $X^2 - X + a$ *sont premiers entre-eux ?*

**Exercice 52** *Soit* $f(x) = x^2 + bx + c \in \mathbb{R}[x]$.

1. *Rappeler comment l'on résout* $f(x)$ *en justifiant votre réponse.*
2. *Notons* $\alpha$ *et* $\beta$ *les racines de* $f(x)$*. Montrer que le signe de* $\Delta = (\alpha-\beta)^2$ *détermine la nature de* $\alpha$ *et* $\beta$.
3. *Exprimer* $\Delta$ *en fonction des coefficients de* $f(x)$.
4. *Supposons que* $\Delta > 0$*. Montrer que l'on peut utiliser les coefficients de* $f(x)$ *pour précicer les signes des racines de* $f(x)$.

**Exercice 53** *Soit* $f(x) = x^3 + ax^2 + bx + c$ *un polynôme réel.*

1. *Montrer que* $f(x)$ *admet* 3 *racines (en comptant les multiplicités).*
2. *Déterminer la nature de ces racines.*
3. *Soient* $\alpha_1, \alpha_2, \alpha_3$ *les racines de* $f(x)$*. Notons*

$$\Delta = \big((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)\big)^2.$$

   *Montrer que la nature de* $\alpha_1, \alpha_2, \alpha_3$ *est donnée par le signe de* $\Delta$.

**Exercice 54** *Soit* $f(X) = X^3 + pX + q \in \mathbb{R}[X]$.

1. *Montrer que* $\alpha \in \mathbb{C}$ *est une racine multiple de* $f(X)$ *si et seulement si* $f(\alpha) = f'(\alpha) = 0$.
2. *Donner une condition nécessaire et suffisante sur* $p$ *et* $q$ *pour que* $f(X)$ *ait une racine multiple.*
3. *Expliquer comment peut-on obtenir une condition nécessaire et suffisante sur les coefficients de* $X^3 + aX^2 + bX + c \in \mathbb{R}[X]$ *pour que ce polynôme ait une racine mulitple.*

**Exercice 55** *Soit* $\mathbb{K}$ *un corps commutatif.*

1. *Soit* $f(X) \in \mathbb{K}[X]$ *non constant. Montrer que si* $f(X)$ *n'est pas irréductible, alors il admet un diviseur irréductible de degré au plus* $[\frac{\deg f(X)}{2}]$.
2. *Déterminer les irréductibles de* $\mathbb{F}_2[X]$ *de degrés au plus* $4$.
3. *Est-ce que* $X^7 + X^5 + X^4 + X^2 + 1 \in \mathbb{F}_2[X]$ *est irréductible ?*

**Exercice 56** *Factoriser les polynômes*

1. $X^4 + 2, X^7 - X$ *dans* $\mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$,
2. $X^5 - 2i$ *dans* $\mathbb{C}[X]$,
3. $X^7 - X$ *dans* $\mathbb{F}_7[X]$.

**Exercice 57** *Les polynômes suivants ont-ils des facteurs multiples* $X^3 + X^2 - 8X - 12 \in \mathbb{Q}[X], X^5 + 2X^4 + 2X^2 + X + 1 \in \mathbb{F}_3[X]$ *?*

**Exercice 58** *Soit* $\mathbb{K}$ *un corps de caractéristique nulle. Etant donné un polynôme* $f(X)$ *dont la décomposition en irréductible est* $p_1(X)^{\alpha_1} \dots p_r(X)^{\alpha_r}$.

1. *Quelle est la décomposition en irréductible du* $\operatorname{pgcd}(f(X), f'(X))$ *?*
2. *Si* $f(X)$ *admet des facteurs multiples, déterminer un polynôme* $g(X)$ *ayant les mêmes facteurs que* $f$ *mais tous simples.*

**Exercice 59** *Est-ce que le polynôme* $X^4 - 3X^2 + X + 5$ *est irréductible dans* $\mathbb{Q}[X]$ *? (On pourra utiliser le lemme de Gauss).*

**EXERCICE 60** *On considère le polynôme*

$$f(X) = X^5 + 4X^4 + 2X^3 + 3X^2 - X + 5.$$

1. *Est-ce que* $f(X)$ *est irréductible dans* $\mathbb{F}_2[X]$ *?*
2. *Est-ce que* $f(X)$ *est irréductible dans* $\mathbb{F}_3[X]$ *?*
3. *Est-ce que* $f(X)$ *est irréductible dans* $\mathbb{Q}[X]$ *?*

**EXERCICE 61** *On considère le polynôme* $g(X) = 2X^3 - X^2 + X + 1$.

1. *Est-ce que* $g(X)$ *est irréductible dans* $\mathbb{F}_2[X]$ *?*
2. *Est-ce que* $g(X)$ *est irréductible dans* $\mathbb{Q}[X]$ *?*
3. *Que peut-on en déduire ?*

**EXERCICE 62** *Quels sont les degrés possibles des polynômes irréductibles de*

1. *de* $\mathbb{C}[X]$,
2. *de* $\mathbb{R}[X]$,
3. *de* $\mathbb{Q}[X]$ *?*

**EXERCICE 63** *Pour tout* $n \geq 2$, *on considère*

$$\varphi_n(X) = X^{n-1} + X^{n-2} + \cdots + X + 1 \in \mathbb{Q}[X].$$

1. *Supposons que* $n$ *est premier.*
   (a) *On introduit une nouvelle variable* $Y$ *et on définit le polynôme* $\psi_n(Y) = \varphi_n(Y+1)$. *Montrer que ce dernier polynôme est irréductible dans* $\mathbb{Q}[Y]$.
   (b) *Le polynôme* $\varphi_n(X)$ *est-il irréductible dans* $\mathbb{Q}[X]$ *?*
2. *Si* $n$ *n'est pas premier, que peut-on dire de l'irréductibilité de* $\varphi_n(X)$ *?*