Rectorat de Grenoble / Université Grenoble Alpes

Préparation à l'agrégation interne 2022-2023

Arithmétique

Parties du programme abordées : Parties 3.1 (extensions de la notion de nombre) et 3.2 (anneaux et corps).

Anneau $\mathbb{Z}$ des entiers relatifs. Division euclidienne. Sous-groupes additifs et idéaux de $\mathbb{Z}$. Nombres premiers. Décomposition en facteurs premiers. Plus grand commun diviseur et plus petit commun multiple. Théorème de Bachet-Bézout. Algorithme d'Euclide étendu. Congruences. Applications arithmétiques des anneaux quotients $\mathbb{Z}/n\mathbb{Z}$. Théorème chinois. Groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Applications à des problèmes de calendriers. Exemples de méthodes de codage et de cryptage. Équations diophantiennes $ax + by = c$.

Anneaux et corps : définition. Formule du binôme pour des éléments commutables. Idéaux d'un anneau commutatif. Anneaux quotients. Anneaux commutatifs intègres. Morphismes d'anneaux. Isomorphisme entre $\mathrm{Im}\,(f)$ et $A/\mathrm{Ker}\,(f)$ pour f morphisme d'anneaux de A dans A'. Anneaux principaux. Exemple des entiers de Gauss, applications. Sous-corps. Corps premier. Caractéristique d'un corps. Corps des fractions d'un anneau intègre. Éléments algébriques, transcendants sur un sous-corps. Dénombrabilité du corps des nombres algébriques sur $\mathbb{Q}$.

Références

COMBES, François, *Algèbre et géométrie*, Bréal.
DEMAZURE, Michel, *Cours d'algèbre*, Cassini.
FRANCINOU-GIANELLA, *Exercice de mathématiques pour l'agrégation, Algèbre 1*, Masson.
FRANCINOU-GIANELLA-NICOLAS, *Oraux X-ENS, algèbre 1 et 2*, Cassini.
KETRANE-ELINEAU, *Épreuve orale d'exemples et d'exercices*, Dunod.
DE KONINCK, MERCIER, *Introduction à la théorie de nombres*, Modulo.
MADERE, *Préparation à l'oral de l'agrégation*, Ellipses.
PERRIN, Daniel, *Cours d'algèbre*, ellipses.

Consigne de travail :
toutes les *définitions* des structures algébriques doivent être travaillées et connues.

Dans cette feuille, un anneau A est par défaut muni des lois $+$ et $\times$, avec les conventions usuelles de notation, les neutres sont notés 0 et 1, le groupe multiplicatif des éléments inversibles de A est noté A^* ou $U(A)$. **Tous les anneaux de cette feuille sont commutatifs.**

La notion de A-module (généralisant la notion de $\mathbb{K}$-espace vectoriel) n'est pas au programme de l'agrégation, mais il est intéressant de comprendre qu'un idéal d'un anneau A est exactement un sous-A-module : une partie stable pour l'addition et pour la multiplication par les éléments de A (scalaires).

On note $\mathrm{Div}\,(a)$ l'ensemble des diviseurs d'un élément a de A et aA l'ensemble de ses multiples, qui est l'idéal de A engendré par a (noté aussi (a)).

Pour tout entier $n \geq 2$, on note $\phi(n)$ le nombre l'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ (la fonction ϕ est l'indicatrice d'Euler).

I. Arithmétique dans les anneaux. Les fondamentaux.

Exercice 1 *Échauffement : les structures algébriques.*

1. Soient $A \subset B$ deux anneaux commutatifs. Soit $\omega \in B$. Décrire les éléments des ensembles suivants :

a. Le sous-groupe additif de B engendré par ω.

b. L'idéal de B engendré par ω.

c. Le sous-anneau de B engendré par ω.

d. Le sous-anneau de B engendré par A et ω.

e. (subsidiaire) Le sous-A-module de B engendré par ω.

f. La sous-A-algèbre de B engendré par ω.

2. Reprendre la question précédente avec $A = \mathbb{Z}$, $B = \mathbb{Q}$, $\omega = \frac{1}{2}$.

Exercice 2 *Le cas des anneaux finis*

Montrer que dans un anneau fini, tout élément non nul est soit un diviseur de zéro, soit un inversible. En déduire qu'un anneau fini est un corps si et seulement si il est intègre.

L'arithmétique (propriété de divisibilité) se fait sur des anneaux commutatifs intègres qui ne sont pas des corps. La notion de diviseurs ou multiples dans un anneau fini, comme $\mathbb{Z}/n\mathbb{Z}$, sera donc peu utilisée. Cela n'empêche pas d'introduire des anneaux finis pour faire de l'arithmétique : la propriété de divisibilité par n dans $\mathbb{Z}$ se voit dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 3 *Éléments associés*

Soit A un anneau commutatif intègre. On dit que deux éléments a, a' de A sont associés s'il existe un inversible e de A tel que $a' = ea$. Cela définit une relation d'équivalence sur A, on la notera $\sim$.

1. Montrer l'équivalence entre les propriétés suivantes :

a. $a|a'$ et $a'|a$,

b. $aA = a'A$ (a et a' ont même multiples),

c. $\mathrm{Div}\,(a) = \mathrm{Div}\,(a')$ (a et a' ont mêmes diviseurs),

d. a et a' sont associés.

2. On note $A/\sim$ l'ensemble des classes d'équivalence de A pour la relation $\sim$.

a. Montrer que la relation $|$ sur A induit naturellement une relation $|$ sur $A/\sim$ qui est une relation d'ordre.

b. Déterminer $\mathbb{Z}/\sim$ et sa relation d'ordre $|$.

Dans l'anneau des polynômes $\mathbb{K}[X]$ sur un corps $\mathbb{K}$, on a l'habitude de prendre le polynôme unitaire comme représentant d'une classe de polynôme pour $\sim$, il est unique dans chaque classe d'équivalence.

Exercice 4 *Identité de Bezout dans un anneau principal*

Soit A un anneau principal. Soient $a, b, c \in A$.

1. Montrer l'équivalence suivante :

$$\mathrm{Div}\,(a) \cap \mathrm{Div}\,(b) = \mathrm{Div}\,(c) \;\Leftrightarrow\; aA + bA = cA.$$

(relation de "dualité" entre les diviseurs et les multiples.)

2. En déduire que toute ensemble fini d'éléments d'un anneau principal possède un p.g.c.d. Que peut-on dire de l'unicité du p.g.c.d. ?

Conclusion : On dit que a et b sont premiers entre eux si $\mathrm{Div}\,(a) \cap \mathrm{Div}\,(b) = \{1\}$. D'après la première question, dans un anneau principal, c'est donc équivalent à $aA + bA = A$, donc à $1 \in aA + bA$, c'est-à-dire à l'identité de Bezout.

Exercice 5 *Factorisation dans les anneaux principaux*

1. Factoriser le polynôme $X^4 - X^2 - 2$ en produit d'irréductibles dans les anneaux $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$.

2. Factoriser le polynôme $X^4 + X^2 + 1$ en produit d'irréductibles dans les anneaux $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$ et $\mathbb{F}_2[X]$. (indication : penser à la différence de deux carrés.)

3. Même question pour $X^4 + 1$.

Exercice 6 *Des anneaux non principaux*

1. Soit A un anneau commutatif. Montrer que $A[X]$ est principal si et seulement si A est un corps.

2. Donner des idéaux non principaux dans $\mathbb{R}[X, Y]$ et dans $\mathbb{Z}[X]$.

Les trois exercices suivants portent sur l'étude d'extensions de l'anneau des entiers $\mathbb{Z}$. Ils introduisent les outils et résultats de l'étude de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss (exercice 26).

Exercice 7 *Les anneaux $\mathbb{Z}[\frac{1}{2}]$ et $\mathbb{Z}[\frac{1}{10}]$*

On note $\mathbb{Z}[\frac{1}{2}] = \{P(\frac{1}{2}),\ P \in \mathbb{Z}[X]\}$.

1. Montrer que $\mathbb{Z}[\frac{1}{2}]$ est l'image d'un morphisme d'anneau défini sur $\mathbb{Z}[X]$ et que c'est un anneau commutatif intègre.

2. Montrer que tout polynôme à coefficients entiers ayant $\frac{1}{2}$ comme racine est divisible dans $\mathbb{Z}[X]$ par le polynôme $2X-1$. En déduire que $\mathbb{Z}[\frac{1}{2}] \simeq \mathbb{Z}[X]/(2X-1)$.

3. **a.** Caractériser les éléments de $\mathbb{Q}$ appartenant à $\mathbb{Z}[\frac{1}{2}]$.

b. Déterminer les éléments inversibles et les éléments irréductibles de $\mathbb{Z}[\frac{1}{2}]$.

c. Montrer que $\mathbb{Z}[\frac{1}{2}]$ est un anneau principal. Est-il euclidien ?

d. Décrire la décomposition des éléments de $\mathbb{Z}[\frac{1}{2}]$ en produit d'irréductibles.

4. Reprendre les questions précédentes pour l'anneau $\mathbb{Z}[\frac{1}{10}]$.

Exercice 8 *Les anneaux $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[i\sqrt{2}]$*

On considère $\mathbb{Z}[\sqrt{2}] = \{P(\sqrt{2}),\ P \in \mathbb{Z}[X]\}$.

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ est le sous-anneau de $\mathbb{C}$ engendré par $\sqrt{2}$ et que ses éléments sont de la forme $a+b\sqrt{2}$, $a, b \in \mathbb{Z}$.

2. Montrer que $\mathbb{Z}[\sqrt{2}]$ est un anneau commutatif intègre.

Pour tout $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, on note $\overline{a+b\sqrt{2}} = a-b\sqrt{2}$ et $N(a+b\sqrt{2}) = a^2-2b^2$.

3. Montrer que $x \mapsto \overline{x}$ et $x \mapsto N(x)$ sont des applications multiplicatives, de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{2}]$ et de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}$ respectivement.

4. Montrer que $x \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si $N(x) = \pm 1$.

5. Montrer qu'il y a une infinité d'éléments inversibles dans $\mathbb{Z}[\sqrt{2}]$.

6. Reprendre les questions précédentes en remplaçant $\sqrt{2}$ par $i\sqrt{2}$.

Exercice 9 *$\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel*

On considère l'anneau $\mathbb{Z}[i\sqrt{5}] = \{P(i\sqrt{5}),\ P \in \mathbb{Z}[X]\}$.

En s'inspirant de l'exercice précédent, définir une norme sur cet anneau et montrer que l'élément 9 possède deux écritures non équivalentes comme produit d'éléments irréductibles. En déduire que cet anneau n'est pas factoriel.

On étudiera plus loin l'anneau $\mathbb{Z}[i]$, appelé anneau des entiers de Gauss, pour étudier l'équation diophantienne $x^2+y^2=p$, avec p premier.

II. Les algorithmes de base et applications.

Exercice 10 *Algorithme d'Euclide étendu (théorie)*

Pour tous entiers $x, y \in \mathbb{Z}$, $y \neq 0$, on note $q(x,y)$ et $r(x,y)$ le quotient et le reste de la division euclidienne de x par y.

1. Montrer que pour tout $a, b \in \mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r(a,b)\mathbb{Z}$.

Soient a et b deux entiers tels que $a \geq b > 0$.

On considère les suites récurrentes $(r_n)_{n\geq -1}$, $(u_n)_{n\geq -1}$, $(v_n)_{n\geq -1}$, $(q_n)_{n\geq 1}$, définie de la manière suivante (algorithme d'Euclide étendu) :

1. $r_{-1} = a,\ r_0 = b, u_{-1} = 1,\ u_0 = 0,\ v_0 = 0,\ v_{-1} = 1$,
2. $\forall n \in \mathbb{N}$, si $r_n \neq 0$, alors
   (a) $q_{n+1} = q(r_{n-1}, r_n)$,
   (b) $r_{n+1} = r(r_{n-1}, r_n) = r_{n-1} - q_{n+1} r_n$,
   (c) $u_{n+1} = u_{n-1} - q_{n+1} u_n$,
   (d) $v_{n+1} = v_{n-1} - q_{n+1} v_n$,

   sinon $r_{n+1} = q_{n+1} = u_{n+1} = u_{n+1} = 0$.

2. Montrer que la suite $(r_n)_{n\geq -1}$ est strictement décroissante jusqu'à un rang N à partir duquel elle est identiquement nul.

3. Montrer que pour tout entier n compris entre -1 et N, on a $a\mathbb{Z}+b\mathbb{Z} = r_{n-1}\mathbb{Z}+r_n\mathbb{Z} = r_{N-1}\mathbb{Z}$.

4. Montrer que pour tout $n \geq -1$, on a $r_n = u_n a + v_n b$. Laquelle de ces égalités est une identité de Bezout pour a et b ?

Exercice 11 *Algorithme d'Euclide étendu (application)*

1. Pour chacunes des familles suivantes dans $\mathbb{Z}$, déterminer le pgcd et une identité de Bezout :

a. 126 et 230. **b.** 427 et 715. **c.** 180, 606 et 750. **d.** 342, 405 et 720.

2. Pour chacunes des familles suivantes dans $\mathbb{R}[X]$, déterminer le pgcd unitaire et une identité de Bezout :

a. X^2+1 et X^2+X+1. **b.** $X^4+X^3-X^2-2X-2$ et $X^5+X^4+X^3-3X^2-3X-3$.

Exercice 12 *Deux algorithmes d'Euclide*

Soient $a, b \in \mathbb{N}$. Montrer que $\operatorname{pgcd}(X^a-1, X^b-1) = X^{\operatorname{pgcd}(a,b)}-1$.

Exercice 13 *Décomposition en facteurs premiers ou algorithme d'Euclide ?*

1. Trouver les factorisations en nombres premiers de 1961 et 2027. Donner le nombre de divisions euclidiennes effectuées. En déduire pgcd(1961,2027).

2. Comparer le nombre de divisions effectuées par cette méthode et par l'algorithme d'Euclide pour calculer le pgcd de ces deux nombres.

Exercice 14 *Coût de l'algorithme d'Euclide et suite de Fibonacci*

A. Une majoration simple.

Pour tous entiers $x, y \in \mathbb{N}\setminus\{0\}$, on note $r(x,y)$ le reste de la division euclidienne de x par y.

1. Montrer que si $x \geq y$, alors $r(x,y) < \frac{x}{2}$.

Soient a et b deux entiers tels que $a \geq b > 0$. On considère la suite récurrente suivante (algorithme d'Euclide pour calculer le pgcd de a et b) :

$$r_{-1} = a,\ r_0 = b$$
$$\forall n \in \mathbb{N}, \text{ si } r_n \neq 0, \text{ alors } r_{n+1} = r(r_{n-1}, r_n), \text{ sinon } r_{n+1} = 0.$$

2. Montrer que pour tout entier $k \geq 1$, on a $r_{2k} < \frac{b}{2^k}$.

On note N le nombre de divisions effectuées dans l'algorithme d'Euclide pour a et b, c'est-à-dire le plus petit entier k tel que $r_k = 0$ dans la suite définie précédemment, et L le nombre de chiffres de l'écriture en base 2 de b.

3. Montrer que $2^{L-1} \leq b < 2^L$ et que $N < 2L$.

Cette inégalité exprime que le temps de calcul d'un pgcd par l'algorithme d'Euclide contrôlé par le double du nombre de chiffres en écriture binaire du plus petit des deux entiers. La suite du problème améliore ce résultat à l'aide d'une majoration par la suite de Fibonacci.

B. Le théorème de Lamé, 1845 [Demazure, p.25].

On considère la suite de Fibonacci $(F_n)_{n\in\mathbb{N}}$ définie par :

$$F_0 = 1,\ F_1 = 1$$
$$\forall n \in \mathbb{N},\ F_{n+2} = F_n + F_{n+1}.$$

4. Montrer que pour tout n tel que $0 \leq n \leq N-1$, on a $r_n \geq F_{N-n}$. En déduire que $b \geq F_N$.

5. Sachant que $F_n = \frac{1}{\sqrt{5}}(\phi^n - (1-\phi)^n)$ avec $\phi = \frac{\sqrt{5}+1}{2}$, en déduire que $N \leq \frac{3}{2}L + 1$.

Exercice 15 *Calcul de puissance : exponentiation rapide vs théorème d'Euler*

A. Dans cete partie on se place dans l'anneau $\mathbb{Z}/91\mathbb{Z}$.

1. Calculer $\overline{2}^{1032}$ à l'aide de l'algorithme d'exponentiation rapide.

2. Montrer que $\overline{2}$ est inversible dans $\mathbb{Z}/91\mathbb{Z}$ et déterminer l'ordre de $\overline{2}$ dans le groupe $(\mathbb{Z}/91\mathbb{Z})^*$. Comment peut-on en déduire que 91 n'est pas un nombre premier ?

B. Dans cette partie on se place dans l'anneau $\mathbb{Z}/201\mathbb{Z}$.

3. Calculer à l'aide de l'algorithme d'exponentiation rapide $\overline{2}^{261}$.

4. **a.** Calculer $\phi(201)$.

b. Montrer que $\overline{2}$ est inversible dans $\mathbb{Z}/201\mathbb{Z}$, déterminer l'ordre de $\overline{2}$ dans le groupe $U(\mathbb{Z}/201\mathbb{Z})$ et calculer $\overline{2}^{261}$.

Exercice 16 *Théorème des restes chinois (1)*

On considère l'application suivante :

$$\begin{array}{rccc} \Phi & : \mathbb{Z}/20\mathbb{Z} & \to & \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ & \overline{x} & \mapsto & (\overline{x}, \overline{x}) \end{array}$$

où $\overline{x}$ désigne la classe de l'entier x dans l'anneau considéré.

1. Donner les images par Φ de tous les éléments de $\mathbb{Z}/20\mathbb{Z}$ et constater que Φ est bien une bijection.

2. Résoudre :

a. $\left\{ \begin{array}{rcll} x & \equiv & 2 & [4] \\ x & \equiv & 4 & [5] \end{array} \right.$ **b.** $\left\{ \begin{array}{rcll} x & \equiv & 1 & [4] \\ x & \equiv & 2 & [5] \end{array} \right.$

On rappelle que $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ muni des lois $+$ et $\times$ produits, définies par

$$(x, y) + (x', y') = (x + x', y + y'),\ (x, y) \times (x', y') = (x \times x', y \times y'),$$

est un anneau, dont les inversibles sont $U(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) = U(\mathbb{Z}/4\mathbb{Z}) \times U(\mathbb{Z}/5\mathbb{Z})$.

3. Déterminer les éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$ et ceux de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, et constater qu'ils sont en relation par Φ.

4. Trouver l'inverse de $\overline{13}$ dans $\mathbb{Z}/20\mathbb{Z}$ en utilisant l'image par Φ de $\overline{13}$ dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercice 17 *Théorème des restes chinois (2)*

1. Résoudre les systèmes suivants en $x \in \mathbb{Z}$:

a. $\left\{ \begin{array}{rcll} x & \equiv & 3 & [8] \\ x & \equiv & 6 & [27] \end{array} \right.$ **b.** $\left\{ \begin{array}{rcll} x & \equiv & 1 & [2] \\ x & \equiv & 2 & [3] \\ x & \equiv & 3 & [5] \\ x & \equiv & 4 & [7] \end{array} \right.$ **c.** $\left\{ \begin{array}{rcll} x & \equiv & 5 & [6] \\ x & \equiv & 7 & [9] \end{array} \right.$

d. $\left\{ \begin{array}{rcll} x & \equiv & 4 & [6] \\ x & \equiv & 7 & [9] \end{array} \right.$ **e.** $\left\{ \begin{array}{rcll} x & \equiv & 38 & [60] \\ x & \equiv & 14 & [42] \end{array} \right.$

2. Donner une condition nécessaire et suffisante pour que le système : $\left\{ \begin{array}{rcll} x & \equiv & a & [n] \\ x & \equiv & b & [m] \end{array} \right.$ ait une solution et décrire l'ensemble des solutions.

Exercice 18 *Le protocole RSA*

Soient p, q deux nombres premiers distincts.

1. Montrer que pout tout $a \in \mathbb{Z}$ non divisible par p ou q, on a $a^{(p-1)(q-1)} \equiv 1\ [pq]$.

2. Soit $d \in \{1, \ldots, (p-1)(q-1)\}$ premier avec $(p-1)(q-1)$. Montrer qu'il existe $e \in \{1, \ldots, (p-1)(q-1)\}$ tel que $ed \equiv 1\ [(p-1)(q-1)]$.

3. Montrer que pout tout $a \in \mathbb{Z}$, on a $a^{de} \equiv a\ [pq]$.

Exercice 19 *Indicatrice d'Euler et factorisation*

1. Déterminer $\phi(10836)$.

2. **a.** Soient p, q deux nombres premiers distincts et $n = pq$. Déterminer p et q en fonction de n et $\phi(n)$.

b. Sachant que $\phi(17063) = 16800$, factoriser 17063.

III. Arithmétique des entiers.

Exercice 20

Soient $a, b \in \mathbb{N}$. Montrer que $2^a - 1$ divise $2^{ab} - 1$. En déduire que pour tout entier naturel p, si $2^p - 1$ est premier, alors p est premier.

Exercice 21

1. Quels sont les entiers relatifs de la forme $3k + 5l$, avec $k, l \in \mathbb{Z}$?

2. Montrer que tous les entiers supérieurs ou égaux à 8 sont de la forme $3k + 5l$, avec $k, l \in \mathbb{N}$.

Exercice 22

Soit $n \in \mathbb{N}$, $n \geq 1$. Quelle est la classe de $(n-1)!$ modulo n ?

Exercice 23

Montrer que $2^{2005} + 5^{2005}$ est divisible par 41.

Exercice 24 *Équations diophantiennes de degré 1.*

1. Résoudre les équations diophantiennes suivantes :

a. $7x - 9y = 1$ **b.** $11x + 17y = 5$ **c.** $21x - 49y = 12$ **d.** $21x - 49y = 14$.

2. Résoudre les équations suivantes dans $\mathbb{Z}/24\mathbb{Z}$:

a. $\overline{7}x = \overline{4}$ **b.** $\overline{15}x = \overline{5}$ **c.** $\overline{10}x = \overline{4}$.

Exercice 25 *L'équation diophantienne $x^2 - y^2 = n$.*

1. Résoudre l'équation diophantienne $x^2 - y^2 = p$ en $x, y \in \mathbb{Z}$, avec p premier.

2. Résoudre l'équation diophantienne $x^2 - y^2 = 15$ en $x, y \in \mathbb{Z}$.

Exercice 26 *L'équation diophantienne $x^2 + y^2 = p$. Entiers de Gauss.*

Le problème est de déterminer les entiers qui s'écrivent comme somme de deux carrés. Dans cet exercice on résoudra le cas des entiers premiers, le cas général s'en déduisant (voir [Perrin] p.56).

Soit $\Sigma = \{n \in \mathbb{N} \mid n = x^2 + y^2,\ x, y \in \mathbb{N}\}$.

1. Déterminer les carrés de $\mathbb{Z}/4\mathbb{Z}$ et en déduire que si $n \in \Sigma$, alors $n \not\equiv 3$ [4].

2. Montrer que $2 \in \Sigma$ et que 2 n'est pas irréductible dans $\mathbb{Z}[i]$.

Pour mimer la méthode de l'exercice précédent dans $\mathbb{Z}$, on est naturellement conduit à étudier les éléments irréductibles de $\mathbb{Z}[i]$.

A. *La norme et les inversibles de $\mathbb{Z}[i]$.*

On considère l'application $N : \mathbb{Z}[i] \to \mathbb{N}$, appelée "norme", définie par $N(a + ib) = a^2 + b^2$.

3. Montrer que N est multiplicative : pour tout $z, z' \in \mathbb{Z}[i]$, on a $N(z\,z') = N(z)\,N(z')$.

4. Déterminer $U(\mathbb{Z}[i])$.

5. En déduire qu'un nombre premier p appartient à Σ si et seulement si il n'est pas irréductible dans $\mathbb{Z}[i]$.

B. *L'anneau $\mathbb{Z}[i]$ est euclidien (donc principal, donc factoriel).*

6. Montrer que tout nombre complexe z est à distance euclidienne inférieure ou égale à $\frac{\sqrt{2}}{2}$ d'un élément de $\mathbb{Z}[i]$.

7. En déduire qu'il existe une division euclidienne dans $\mathbb{Z}[i]$ relativement à la norme N :

$$\forall a, b \in \mathbb{Z}[i],\ b \neq 0,\ \exists c, r \in \mathbb{Z}[i] \text{ tels que } a = bc + r \text{ et } N(r) < N(b)$$

(sans nécessairement unicité).

8. Faire la divisition euclidienne de $3 + 2i$ par $1 - 3i$ dans $\mathbb{Z}[i]$.

C. *Quotient par l'idéal engendré par un élément non irréductible.*

Soit p un nombre premier.

9. Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est intègre (indication : utiliser le fait que l'anneau $\mathbb{Z}[i]$ est euclidien, donc factoriel).

10. En utilisant l'isomorphisme $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1)$ (voir exercice en fin de feuille), en déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{F}_p$.

11. En déduire pour tout nombre premier p impair l'équivalence des propriétés suivantes :

a. p appartient à Σ

b. -1 est un carré dans $\mathbb{F}_p$

c. $(-1)^{\frac{p-1}{2}} = 1$

d. $p \equiv 1\ [4]$.

Les nombres premiers qui appartiennent à Σ sont donc 2 et les nombres premiers p tels que $p \equiv 1\ [4]$.

Exercice 27 *Témoins de non primalité (1)*

Soit $(N_n = p_n q_n)_{n \in \mathbb{N}}$ une suite d'entiers produits de deux nombres premiers distincts p_n et q_n. On suppose que p_n et q_n tendent vers l'infini quand n tend vers l'infini. Montrer que la probabilité qu'un entier $a < N_n$ ne soit pas premier à N_n tend vers 0 quand n tend vers l'infini.

Exercice 28 *Témoins de Fermat (2) [Demazure]*

Soit $n \geq 2$ un entier. Montrer que soit n ne possède aucun témoin de Fermat, soit il en possède au moins $\frac{n}{2}$. (indication : utiliser un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$.)

Exercice 29 *Témoins de Fermat (3) [Demazure]*

Soit n un entier non premier. On dit que a est un *témoin de Fermat* de non-primalité de n si $n \wedge a = 1$ et $a^{n-1} \not\equiv 1\ [n]$.

On suppose que $n = pq$ où p et q sont deux nombres premiers distincts tels que $\text{pgcd}\,(p-1, q-1) = 2$. Montrer que 2 est un témoin de Fermat de n.

IV. Arithmétique et groupes

Exercice 30 *Sous-groupes finis de $\mathbb{K}^*$ (1) [FGN p.41]*

Soit G un groupe abélien fini. Pour tout $x \in G$, on note $\text{ord}\,(x)$ l'ordre de x dans G.

1. Soient $x, y \in G$, $m = \text{ord}\,(x)$, $n = \text{ord}\,(y)$. Montrer que si $\text{pgcd}\,(n, m) = 1$, alors $\text{ord}\,(xy) = nm$.

2. Soient $m, n \in \mathbb{N} \setminus \{0\}$. Montrer qu'il existe $m', n' \in \mathbb{N} \setminus \{0\}$ tels que $\text{pgcd}\,(n', m') = 1$ et $\text{ppcm}\,(n, m) = n'm'$.

3. Montrer qu'il existe $u \in G$ tel que $\text{ord}\,(u)$ est égal au ppcm des ordres des éléments de G (appelé exposant de G).

4. Montrer que tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.

Exercice 31 $n = \sum_{d|n} \psi(d)$

Soit $n \geq 2$ un entier. On va montrer que $n = \sum_{d|n} \psi(d)$ de deux manières différentes.

Comptage dans les groupes cycliques.

1. Montrer que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de cardinal un diviseur d de n.

2. Réciproquement, pour tout $d|n$, montrer qu'il existe un unique sous-groupe de cardinal d de $\mathbb{Z}/n\mathbb{Z}$, et que ce sous-groupe est cyclique.

3. Montrer que le groupe $\mathbb{Z}/d\mathbb{Z}$ possède exactement $\psi(d)$ générateurs.

4. En déduire que $n = \sum_{d|n} \psi(d)$.

5. Déterminer tous les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ et vérifier la formule précédente.

Comptage dans les nombres rationnels.

6. Énumérer de deux manières différentes l'ensemble $\{\frac{k}{n},\ 0 \leq k \leq n-1\}$ et retrouver la formule précédente.

Exercice 32 *Sous-groupes finis de $\mathbb{K}^*$ (2) [Perrin, p.74]*

Déduire de la formule de l'exercice précédent que tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.

V. Arithmétique des polynômes.

Exercice 33 *Anneau des polynômes sur le corps fini $\mathbb{F}_p$.*

Soit p un nombre premier.

1. Montrer l'égalité suivante dans l'anneau des polynômes à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}$:

$$\prod_{i=0}^{p-1} (X - \bar{i}) = X^p - X.$$

2. En déduire que $(p-1)! \equiv -1\ [p]$ (théorème de Wilson).

3. En déduire également que $(X + \overline{1})^p = X^p + \overline{1}$ (indication : montrer que $(X + \overline{1})^p - (X + \overline{1}) = X^p - X$).

Exercice 34 *(Construction de corps finis, [Skandalis, exercice 4.16])*

1. Montrer que tout corps fini est de cardinal p^α pour un nombre premier p et un entier $\alpha \geq 1$.

2. Soit K un corps fini à q éléments. Combien y a-t-il de polynômes irréductibles unitaires de degré 2 dans $K[X]$? de degré 3 ?

3. Déterminer les polynômes irréductibles unitaires de degre 2 et 3 dans $\mathbb{F}_2[X]$ et $\mathbb{F}_3[X]$.

4. **a.** Construire des corps à 4, 8, 9, 27 éléments.

b. Construire des corps à 25, 49, 121 éléments.

Exercice 35 *Racines d'un polynôme de $\mathbb{Z}[X]$ ou $\mathbb{Q}[X]$*

Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme de $\mathbb{Q}[X]$ dont les coefficients $a_0, \ldots, a_n$ sont entiers.

1. Montrer que si un rationnel $x = \frac{p}{q}$ est racine de P, où p et q sont des entiers premiers entre eux, alors p divise a_0 et q divise a_n.

2. Les polynômes suivants de $\mathbb{Q}[X]$ ont-ils des racines dans $\mathbb{Q}$?

a. $5X^3 + X^2 - 1$ **b.** $X^4 + 3X^3 - 3X^2 - 12X - 4$

Exercice 36 *Un algorithme de factorisation dans $\mathbb{Z}[X]$ [ref ?]*

On considère le polynôme $P(X) = X^5 + X^4 + 2X^2 - 1$.

1. Montrer que si P est irréductible dans $\mathbb{Z}[X]$, alors il existe un polynôme de degré au plus deux qui divise P dans $\mathbb{Z}[X]$.

2. Soit $Q \in \mathbb{Z}[X]$ un polynôme de degré au plus 2 et qui divise P. Calculer $P(0)$, $P(1)$ et $P(-1)$. En déduire toutes les valeurs possibles pour $Q(0)$, $Q(1)$ et $Q(-1)$, donc toutes les valeurs possibles de Q.

3. Factoriser P dans $\mathbb{Z}[X]$.

Exercice 37 *(irréductibilité par réduction modulo 2 et 3)*

On considère le polynôme $P(X) = X^5 - 6X^3 + 2X^2 - 4X + 5$ de $\mathbb{Z}[X]$.
En le réduisant modulo 2 et 3, montrer que ce polynôme est irréductible.

Exercice 38 *Anneau des polynômes sur un anneau non intègre et lemme chinois.*

1. Déterminer les racines du polynôme $X^2 - \overline{1}$ de $(\mathbb{Z}/15\mathbb{Z})[X]$, en remarquant qu'une racine est un élément de $U(\mathbb{Z}/15\mathbb{Z})$.

2. Soit n un entier impair, $n \geq 3$. Montrer que le nombre de racines du polynôme $X^2 - \overline{1}$ de $(\mathbb{Z}/n\mathbb{Z})[X]$ est 2^k où k est le nombre de facteurs premiers de la décomposition de n (indication : réduire l'équation $x^2 - 1 \equiv 0\ [n]$ aux diviseurs de n).

Exercice 39 *Isomorphismes et quotients.*

Pour tout $\omega \in \mathbb{C}$, on note $\mathbb{Z}[\omega] = \{P(\omega),\ P \in \mathbb{Z}[X]\}$.

1. Décrire les éléments de $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[j]$, $\mathbb{Z}[\pi]$.

2. Montrer que les anneaux suivants sont isomorphes :

a. $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[X]/(X^2 - 2)$. **b.** $\mathbb{Z}[i]$ et $\mathbb{Z}[X]/(X^2 + 1)$.

3. Décrire $\mathbb{Z}[j]$, $\mathbb{Z}[1 + i]$ comme des quotients de l'anneau $\mathbb{Z}[X]$.

4. Montrer les isomorphismes suivants pour p premier et d entier, $d \geq 1$:

$$\mathbb{Z}[i\sqrt{d}]/(p) \simeq \mathbb{Z}[X]/(X^2 + d, p) \simeq \mathbb{F}_p[X]/(X^2 + d).$$