Groupe 2

Feuille d'Exercices

Arithmétique

Introduction

Soient $a \in \mathbb{N}, a \geq 2, (m,n) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $m \geq n$. On pose $m = qn + r$ avec $0 \leq r < n$.

1. Montrer que : $\exists b \in \mathbb{N}$; $a^m - 1 = (a^n - 1)b + a^r - 1$.
2. Montrer que : $(a^m - 1) \wedge (a^n - 1) = a^{m \wedge n} - 1$.
3. Montrer que : $(a^n - 1)$ divise $(a^m - 1) \iff n$ divise m
4. *Application* : Soit N_k le nombre qui s'écrit en base 10 avec k chiffres tous égaux 1. Montrer que : N_h divise $N_k \iff h$ divise k.

Exercice 1 : Nombres de Fermat ($F_n = 2^{2^n} + 1$)

1. Montrer que tous ces nombres sont premiers entre eux deux deux
2. Montrer que F_n est premier pour $n \in [|0,4|]$ mais F_5 ne l'est pas
3. Soit $a \in \mathbb{N}^*$ montrer que si $2^a + 1$ est premier alors a est une puissance de 2

A l'heure actuelle on ne connait pas nombre de Fermat premier autre que F_n o $n \in [|0,4|]$, mais on connait plusieurs qui ne le sont pas : F_{1945} qui a plus de 10582 chiffres est divisible par $2^{1947}5+1$ qui a exactement 587 chiffres.

Exercice 2 : Nombres de Mersenne ($M_p = 2^p - 1$ avec p premier.)

1. Montrer que les *Nombres de Mersenne* sont premiers entre eux deux deux.
2. Soit $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que : $a^b - 1$ est premier, montrer alors que : $a = 2$ et b premier.

Exercice 3b : Suite de Fibonnacci

Soit $(F_n)_{n \geqslant 0}$ la suite de Fibonacci ($F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geqslant 0$).

(i) Montrer que F_m et F_{m+1} sont premiers entre eux.

(ii) Montrer que $F_n = F_{m+1}F_{n-m} + F_mF_{n-m-1}$ pour $m < n$.

(iii) Soient m, n deux entiers naturels non nuls et soit d leur pgcd. Montrer que $\text{pgcd}(F_m, F_n) = F_d$.

Exercice 3 : Critère d'Eseinstein

1. Soient $(p,q) \in \mathbb{Z} \times \mathbb{N}$ tel que $p \wedge q = 1$ et $(a_i)_{0 \leq i \leq n} \in \mathbb{N}^{n+1}$.
   Montrer que si $\frac{p}{q} \in \mathbb{Q}$ est solution de l'ééquation : $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0 = 0$, alors : p divise a_0 et q divise a_n
2. Résoudre l'ééquation : $30X^3 - 37X^2 + 15X - 2 = 0$

Exercice 4 : Théorème de Wilson

Soit p un entier premier.

1. Montrer que $\forall \overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, $\exists \overline{b} \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $\overline{a}\overline{b} = \overline{1}$.
2. En déduire que : $(p-1)! \equiv -1 (\text{mod } p)$.

Exercice 5 : Petit Théorème de Fermat

Soit p un nombre premier.

1. Montrer que p divise $\binom{p}{k}$, $\forall k \in [\![1, p-1]\!]$. *Indication : Utiliser le théorème de Gauss.*
2. Montrer que pour tous $n, m \in \mathbb{N}^2$ on a : $(n+m)^p \equiv n^p + m^p \pmod{p}$
3. Que peut-on dire alors de l'application $\begin{array}{rccc} \phi :: & \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & \overline{x} & \mapsto & \overline{x}^p \end{array}$.
4. Montrer que : $\forall n \in \mathbb{N} : n^p \equiv n \pmod{p}$.

Exercice 6 : Problème de Bezout

Soient a, b, c trois entiers relatifs. On considère l'équation : $ax + by = c$, appelée problème de Bezout dont on recherche les solutions dans $\mathbb{Z}^2$.

1. Donner une condition nécessaire et suffisante pour que cette équation admette une solution.
2. Soit (x_0, y_0) une solution particulière du problème de Bézout. Déterminer la forme générale des autres solutions (x, y) en fonction de $a, b, d = a \wedge b, x_0$ et y_0.
3. Résoudre dans $\mathbb{Z}^2$: $95x + 71y = 46$.

Exercice 7 : Théorème des reste chinois

Soient $a, b, n, m \in \mathbb{Z}$ avec $n \wedge m = 1$. On considère le système : $\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$ (S)

1. Justifier l'existence de $(u, v) \in \mathbb{N}^2$, tel que $\begin{cases} nu \equiv 1 \pmod{m} \\ mv \equiv 1 \pmod{n} \end{cases}$.
2. En déduire que $x_0 = amv + bnu$ est une solution particulière du système *(S)*.
3. Montrer que toutes les autres solutions sont congrues avec x_0 modulo nm.
4. Résoudre : $\begin{cases} x \equiv 2 \pmod{140} \\ x \equiv -3 \pmod{99} \end{cases}$
5. *Application.* Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces.
   Mais une rixe éclate et 6 pirates sont tus. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces.
   Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.
   Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ? **Réponse** : 785

Exercice 8 : Théorème de Fermat Euler

du théorème de Lagrange (l'ordre d'un élément divise l'ordre du groupe) dans la théorie des $\mathbb{Z}/n\mathbb{Z}$.

1) Montrer que si a et n sont deux entiers premiers entre eux alors $a^{\varphi(n)} = 1\ [n]$. Que se passe-t-il si n est premier ?

2) Soient $a \in \mathbb{N}^*$ et $n \geq 2$ tels que $a^{n-1} = 1\ [n]$ et $a^x \neq 1\ [n]$ pour tout diviseur strict x de $n-1$. Montrer que n est premier.

3) Soient a et n deux entiers naturels non nuls. Montrer que $n \mid \varphi(a^n - 1)$.

4) Soient a, n et m trois entiers naturels. On suppose que m est premier et que $n \mid a^m - 1$. Montrer que $n \mid a - 1$ ou $m \mid \varphi(n)$. En déduire que tout facteur premier du nombre de Mersenne $2^m - 1$ où $m > 2$ est congru à 1 modulo $2m$.

Exercice 9 : Nombres de Fermat (suites)

1) Soient $m \geq 2$ et $n \geq 1$ un entier. Monter que si $m^n + 1$ est premier, alors n est une puissance de 2 et m est pair.

Le nombre $x_n = 2^{2^n} + 1$ est appelé **le $n^{\text{ième}}$ nombre de Fermat**. Les nombres $x_0 = 3, x_1 = 5, x_2 = 17, x_3 = 257, x_4 = 65537$ sont premiers. Mais $x_5 = 641 \times 6700417$ ne l'est pas.

2) Montrer que si $n \neq m$ sont non nuls alors x_n et x_m sont premiers entre eux (on pourra considérer un diviseur premier commun à x_m que x_n ou alors, comme dans la question d, factoriser $x_n - 2 = 2^{2^n} - 1$). En déduire qu'il existe une infinité de nombres premiers.

3) Montrer que $x_{n+1} = (x_n - 1)^2 + 1$ pour $n \geq 0$.

4) En déduire que, pour $n \geq 1$,

$$x_n - 2 = \prod_{k=0}^{n-1} x_k \,.$$

En particulier, on obtient que $x_m \mid x_n - 2$ si $m < n$. Retrouver le résultat de la question b à savoir x_m et x_n sont premiers entre eux pour $n \neq m$ non nuls.

Dans les questions e et f , on considère $n \geq 1$ et p un diviseur premier de x_n. On suppose que $p \neq x_n$.

5) Montrer que $p = 2^{n+1}m + 1$ où m admet un diviseur premier impair.

6) Montrer que 2 est un carré modulo p. En déduire que $p = 2^{n+2}m + 1$. On pourra utiliser le calcul du symbole de Legendre

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \qquad et \qquad \left(\frac{2}{p}\right) = 2^{(p-1)/2}[p] \,.$$

Exercice 10 : Nombres de Carmichael

n non premier est dit de Carmichael si $a^{n-1} = 1\,[n]$ pour tout entier a premier à n.

1) Montrer qu'un nombre de Carmichael est sans facteur carré (regarder n modulo p^{k-1} si $n = p^k m$ avec $\text{pgcd}(m, p) = 1$) et produit d'au moins trois nombres premiers impairs.

2) Soit n un entier naturel supérieur strictement à 1. Montrer l'équivalence des propositions suivantes :

(i) n est de Carmichael

(ii) Pour tout entier a, on a $a^n = a\,[n]$.

(iii) n n'est pas premier, n est sans facteur carré et $p - 1$ divise $n - 1$ pour tout diviseur premier p de n.

3) Montrer que 561 est de Carmichael (c'est le plus petit nombre de Carmichael).

Exercice 11 : Divisibilité dans un anneau

Partie A:

Soient A un anneau commutatif (on ne suppose pas A intègre) et $a, b \in A$.

1) Montrer que les propriétés suivantes sont équivalentes

(i) il existe $c \in A$ tel que $ca = b$;

(ii) $b \in (a)$;

(iii) $(b) \subset (a)$;

Si ces conditions sont vérifiées, on dit que a *divise* b et on écrit $a \mid b$. On dit que a et b sont *associés* si $a \mid b$ et $b \mid a$

2) Montrer que a et b sont associés si et seulement si $(a) = (b)$. Montrer que être associés est une relation d'équivalence sur A.

On dit que a et b sont *fortement associés* s'il existe $u \in A^\times$ tel que $b = ua$.

3) Montrer que être fortement associés est une relation d'équivalence.

4) Montrer que des éléments fortement associés sont associés.

5) Montrer que dans un anneau intègre des éléments associés sont fortement associés.

Partie B:

1) Soient $a_1, \ldots, a_m \in A$. On dit que $d \in A$ est un ppcm de $a_1, \ldots, a_m$ si d vérifie les deux conditions suivantes

(i) $a_i \mid d$ pour tout $i \in \{1, 2, \ldots, m\}$ (i.e. d est un multiple commun des a_i) ;

(ii) pour tout $d' \in A$ vérifiant $a_i \mid d'$, on a $d \mid d'$ (i.e. d est "le" plus petit multiple commun).

2) Soient $a_1, \ldots, a_m \in A$. On dit que $d \in A$ est un pgcd de $a_1, \ldots, a_m$ si d vérifie les deux conditions suivantes

(i) $d \mid a_i$ pour tout $i \in \{1, 2, \ldots, m\}$ (i.e. d est un diviseur commun des a_i) ;

(ii) pour tout $d' \in A$ vérifiant $d' \mid a_i$, on a $d' \mid d$ (i.e. d est "le" plus grand diviseur commun).

Des éléments $a_1, \ldots, a_m$ dont le pgcd est 1 sont dit premiers entre eux.

3) Montrer que $a_1, \ldots, a_m \in A$ admet un ppcm si et seulement si l'idéal $(a_1) \cap \cdots \cap (a_m)$ est principal (on a ainsi un condition simple d'existence des ppcm : ce n'est pas le cas pour les pgcd).

4) On suppose que l'idéal $(a_1, \ldots, a_m)$ est principal. Montrer que $a_1, \ldots, a_m$ admettent un pgcd et qu'on a une relation de Bézout. Montrer que dans $k[X, Y]$, X et Y ont 1 comme pgcd mais que l'idéal (X, Y) n'est pas principal.

5) Montrer que $a_1, \ldots, a_m$ admettent un pgcd si et seulement si l'ensemble des idéaux **principaux** contenant $(a_1, \ldots, a_m)$ admet un élément plus petit élément.

6) Montrer que dans un anneau principal ppcm et pgcd existent toujours et qu'on dispose de relation de Bézout pour le pgcd.

Dans toute la suite de l'exercice A est un anneau commutatif **intègre**.

7) Soit $a \neq 0$. Montrer que la famille $(a_1, \ldots, a_n)$ admet un ppcm si et seulement si la famille $(aa_1, \ldots, aa_n)$ en admet un. Donner le lien entre les deux ppcm.

8) Montrer que le résultat précédent n'est pas vrai pour les pgcd. Cependant, montrer qu'on a le résultat suivant : si le pgcd de la famille $(aa_1, \ldots, aa_n)$ existe, montrer que celui de la famille $(a_1, \ldots, a_n)$ existe et qu'on a la relation $\text{pgcd}(aa_1, \ldots, aa_n) = a\,\text{pgcd}(a_1, \ldots, a_n)$.

9) On suppose que x et y ont un ppcm. Montrer que $m \mid xy$. On écrit alors $xy = md$. Montrer que d est un pgcd pour x et y et que, pour tout $a \in A \setminus \{0\}$, $\text{pgcd}(ax, ay)$ existe et vaut ad (avoir un ppcm implique avoir un pgcd).

10) Montrer que si x, y et d sont tel que ad soit un pgcd de ax et ay pour tout $a \in A \setminus \{0\}$ alors on peut définir m tel que $md = xy$ et m est un ppcm de x et y. En déduire que (avoir un pgcd n'implique pas avoir un ppcm).

11) Montrer que si l'idéal (x, y) est principal alors $(x) \cap (y)$ l'est.

12) On dit que x et y sont *fortement premiers entre eux* si x et y ont un ppcm qui est xy. Montrer que des éléments qui sont fortement premiers entre eux sont premiers entre eux mais que la réciproque n'est pas vraie.

13) Montrer que si x et y sont fortement premiers entre eux et si $x \mid yz$ alors $x \mid z$ (le lemme d'Euclide ou de Gauss est vrai dans un anneau intègre sous l'hypothèse fortement premier entre eux).

14) Montrer que dans un anneau factoriel, des éléments sont fortement premiers entre eux si et seulement si ils sont premiers entre eux. En déduire que des éléments fortement premier entre eux ne sont pas forcément étrangers.

15) Soit A un anneau intègre. Montrer l'équivalence des propriétés suivantes

(i) L'intersection de deux idéaux principaux de A est un idéal principal.

(ii) Tout couple d'éléments de A admet un ppcm.

(iii) Tout couple d'éléments de A admet un pgcd.

Si les conditions précédentes sont vérifiées alors les produits xy et $\text{pgcd}(x, y)\,\text{ppcm}(x, y)$ sont associés ; deux éléments sont premiers entre eux si et seulement si ils sont fortement premiers entre eux. Tout élément irréductible est premier.

16) Montrer qu'un anneau intègre est factoriel si et seulement si tout élément irréductible est premier et il n'existe pas de suite infinie $(x_i)_{i\in\mathbb{N}}$ telle que pour tout $i > 0$ on a $x_i \mid x_{i-1}$ et x_i n'est pas associé à x_{i-1}.

17) Montrer qu'un anneau intègre est factoriel si et seulement si toute suite croissante d'idéaux principaux est stationnaire et l'intersection de deux idéaux principaux est principal.

18) Montrer qu'un élément p est irréductible si et seulement si $\text{pgcd}(a, p)$ existe et vaut 1 ou p pour tout $a \in A$.

19) Montrer qu'un élément irréductible p est premier si et seulement si $\text{ppcm}(a, p)$ existe, pour tout $a \in A$.

Partie C :

$\mathbb{Z}[i\sqrt{5}] = \{a + ib \quad 5, \quad a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

1) Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un sous-anneau de $\mathbb{C}$. Montrer qu'il est intègre (et noethérien).

2) Déterminer le groupe des éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{5}]$. On pourra introduire l'application

$$N : z = a + ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}] \longmapsto z\bar{z} = a^2 + 5b^2 \in \mathbb{Z}\,.$$

3) Montrer que $p = 2 + i\sqrt{5}$ est irréductible et que (p) n'est pas premier. En déduire que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

4) Montrer que 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm et que 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd dans $\mathbb{Z}[i\sqrt{5}]$.

Exercice 12 : Le Thoérème des Restes Chinois

Partie A:

(Idéaux étrangers). Soit A un anneau commutatif unitaire. Pour deux idéaux I et J de A, on dit que I et J sont *étrangers* si $I+J=A$ où $I+J=\{i+j\in A,\quad i\in I, j\in J\}$. Autrement dit I et J sont étrangers si et seulement si il existe $i\in I$ et $j\in J$ tel que $i+j=1$.

Soit A un anneau commutatif unitaire et $I_1,\dots,I_k$ des idéaux de A.

1) On suppose que les idéaux I_i pour $1\leq i\leq k$ sont deux à deux étrangers. Montrer que I_1 est étranger avec $I_2\cdots I_k$.

2) Montrer que pour tout $m,n\in\mathbb{N}$, les idéaux ${I_1}^m$ et ${I_2}^n$ sont étrangers (au fait c'est quoi ${I_1}^m$?).

3) Soit $\mathfrak{m}$ et $\mathfrak{m}'$ deux idéaux maximaux **distincts** de A. Montrer qu'ils sont étrangers. En déduire que $\mathfrak{m}^m$ et ${\mathfrak{m}'}^n$ sont étrangers pour tous $m,n\in\mathbb{N}$.

Partie B:

Soient A un anneau commutatif unitaire et I et J deux idéaux de A. On note $\pi_I: A\to A/I$ et $\pi_J: A\to A/J$ les surjections canoniques. On définit l'application

$$\begin{aligned}\varphi\colon A &\longrightarrow A/I\times A/J\\ x &\longmapsto (\pi_I(x),\pi_J(x))\end{aligned}$$

1) Vérifier que φ est un morphisme d'anneaux.

2) Calculer $\ker\varphi$.

3) Montrer que φ est surjectif si seulement si I et J sont étrangers. Construire explicitement un antécédent de $(a,b)=(\pi_I(x),\pi_J(y))\in A/I\times A/J$.

4) On définit $IJ:=\{\sum_{k=1}^n i_kj_k \mid n\in\mathbb{N}, i_k\in I, j_k\in J\}$. Montrer que $IJ\subset I\cap J$. Donner un exemple où $IJ\subsetneq I\cap J$.

5) On suppose que I et J sont étrangers. Montrer que $I\cap J=IJ$.

6) Conclure que si I et J sont étrangers alors φ induit un isomorphisme entre A/IJ et $A/I\times A/J$ donné par $\overline{x}\mapsto(\pi_I(x),\pi_J(x))$ où $\overline{x}$ désigne la classe de $x\in A$ modulo IJ.

Partie C :

Soient k un corps, E un k-espace vectoriel de dimension finie et u un endomorphisme de E dont le polynôme caractéristique est scindé.

1) **Décomposition de Dunford.** Montrer qu'il existe des endomorphismes d et n de E avec d diagonalisable, n nilpotent, $u=d+n$ et $dn=nd$. Montrer que d et n sont des polynômes en u et qu'un tel couple est unique. On pourra considérer P un solution du système

$$\begin{cases}P=\lambda_1 \mod (X-\lambda_1)^n\\ \quad\vdots\\ P=\lambda_r \mod (X-\lambda)^n\end{cases}$$

où les λ_i sont les valeurs propres distinctes de u.

2) Montrer que les projecteurs sur un sous-espace caractéristique de u parallèlement aux autres sous-espaces caractéristiques de u sont des polynômes en u. On pourra considérer P un solution du système

$$\begin{cases}P=1 \mod (X-\lambda_1)^n\\ P=0 \mod (X-\lambda_2)^n\\ \quad\vdots\\ P=0 \mod (X-\lambda_r)^n\end{cases}$$

où les λ_i sont les valeurs propres distinctes de u.