Feuille de T.D. 4 - Structures algébriques - Arithmétique dans $\mathbb{Z}$ [1]

• Structures algébriques

Exercice 1 On considère la loi $\star$ définie sur $\mathbb{R}$ par $x \star y = x + y - xy$.

1. Cette loi est-elle commutative ? associative ? $(\mathbb{R}, \star)$ admet-il un élément neutre ?
2. $(\mathbb{R}, \star)$ est-il un groupe ?
3. Pour $x \in \mathbb{R}$, $n \in \mathbb{N}\backslash\{0\}$, calculer l'itéré $x^{(n)} = x \star x \star \cdots \star x$.
   Indication : on pourra remarquer que $x \star y = 1 + (1-x)(y-1)$.

Exercice 2

1. Soit $\star$ une loi de composition interne associative de neutre e sur un ensemble G. Soit x un élément admettant un inverse pour $\star$. Montrer alors que x est *simplifiable*, c'est-à dire que
$$\forall y, y' \in G, \quad x \star y = x \star y' \implies y = y'.$$
2. Soit $(G, \star)$ un groupe de neutre e. Montrer que si $x \star x = e$ pour tout $x \in G$ alors G est commutatif.

Exercice 3 Montrer que l'ensemble $\mathcal{U}_n$ des racines $n-$ièmes de l'unité forme un sous-groupe de $(\mathbb{C}, \times)$.

Exercice 4 Soit $(G, \star)$ un groupe non commutatif. On définit sur G la relation $\mathcal{R}$ par
$$x \mathcal{R} y \iff \exists a \in G,\ y = a \star x \star a^{-1}.$$
Montrer que $\mathcal{R}$ est une relation d'équivalence sur G, et déterminer la classe d'équivalence du neutre e.

Exercice 5 *(Anneau des entiers de Gauss)* On note $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$ (ensemble des nombres complexes dont les parties réelles et imaginaires sont des entiers).

1. Montrer que $(\mathbb{Z}[i], +, \times)$ est un sous-anneau de $\mathbb{C}$ (c'est-à-dire, montrer que c'est un sous-groupe de $(\mathbb{C}, +)$, stable pour la multiplication, et qui contient 1).
2. Déterminer les éléments inversibles de cet anneau.

• Arithmétique dans $\mathbb{Z}$

Exercice 6 Les questions sont indépendantes.

1. Donner le reste de 5^n dans la division euclidienne par 12 ($n \in \mathbb{N}$). En déduire le reste de 5^{789} dans la division euclidienne par 12.
2. Trouver le reste de la division par 7 de $a = 247^{349}$.
3. Démontrer que le nombre $7^n + 1$ est divisible par 8 si n est un entier naturel impair. Dans le cas n pair, donner le reste de sa division par 8.
4. Montrer que pour tout $n \in \mathbb{N}$, $3^{n+3} - 4^{4n+2}$ est un multiple de 11.

Exercice 7 Soit A l'ensemble des entiers naturels pairs et B l'ensemble des entiers naturels multiples de 3. Déterminer $A \cap B$ et $A \cup B$.

Exercice 8 Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $3x \equiv 7[9]$.
2. $4t \equiv 2[5]$.

Exercice 9 Soient x, y et z trois entiers solutions de l'équation de Fermat $x^3 + y^3 = z^3$. L'objectif est de montrer que l'un des entiers x, y ou z est divisible par 3.

1. Enseignant responsable du CM : G. Chagny. Chargés de TD : G. Chagny, J. Lemoine, L. Loukitch.

1. Supposons que a est un entier non divisible par 3. Montrer que $a^3 \equiv 1[9]$ ou $a^3 \equiv -1[9]$.
2. Conclure, en raisonnant par l'absurde.

Exercice 10 On considère dans $\mathbb{Z}^2$ l'*équation diophantienne* suivante : $62x + 43y = 3$ (E).

1. Déterminer le PGCD de 62 et 43 à l'aide de l'algorithme d'Euclide, ainsi qu'une relation de Bézout (vérifier le calcul du PGCD en le retrouvant également grâce aux décompositions en facteurs premiers de 62 et 43).
2. En déduire une solution particulière (x_0, y_0) de l'équation (E).
3. Résoudre l'équation (E).
4. Résoudre de la même façon l'équation $1665x+1035y = 45$ (commencer par simplifier l'équation !).

Exercice 11 Les questions sont indépendantes.

1. Déterminer, suivant les valeurs de $n \in \mathbb{Z}$, le PGCD de $5n - 9$ et $2n - 6$.
2. Quel est le PPCM de n et $2n + 1$, $n \in \mathbb{Z}$?

Exercice 12 Soient a, b et c trois entiers non nuls. Montrer les deux propriétés suivantes :

1. $a \wedge b = 1$ et $a \wedge c = 1 \iff a \wedge bc = 1$.
2. $a \wedge c = 1 \implies a \wedge (bc) = a \wedge b$.

Exercice 13

1. Soient a et b deux entiers naturels tels que $0 < a < b$. Montrer que
$$(a + b) \wedge (a \vee b) = a \wedge b.$$
2. Trouver a et b tels que $\begin{cases} a + b = 144 \\ a \vee b = 420. \end{cases}$

Exercice 14 On considère le trinôme $P(X) = X^2 + aX + b$, avec a, b entiers.

1. Montrer que si α est une solution rationnelle de l'équation $P(X) = 0$, alors α est un entier. *Indication :* on pourra écrire α sous sa forme irréductible $\alpha = p/q$ avec $p \wedge q = 1$.
2. Quels sont les entiers n tels que $\sqrt{n}$ est rationnel? *Indication :* on cherchera un trinôme P admettant $\sqrt{n}$ pour racine, et on utilisera 1..

Exercice 15 *(Nombres de Fermat)* Soit $m \in \mathbb{N}\backslash\{0\}$ tel que $a^m + 1$ soit premier. Montrer que m est de la forme $m = 2^n$, où $n \in \mathbb{N}$.
Indication : on pourra remarquer que $x^l + 1 = (x + 1)(x^{l-1} - x^{l-2} + \cdots + 1)$, $x \in \mathbb{R}$, $l \in \mathbb{N}$.

Exercice 16 *(Nombres de Mersenne)* Soient a et n deux entiers, $a, n \geq 2$.

1. Montrer que si $a^n - 1$ est premier, alors $a = 2$.
2. Montrer que si $M_n = 2^n - 1$ est premier, alors n est premier. La réciproque est-elle vraie? *Indication :* on pourra considérer M_{11}.

Exercice 17 *(Petit théorème de Fermat)* Soit p un nombre premier.

1. Montrer que p divise le coefficient binomial $\binom{p}{k}$ pour tout $k \in \{1, 2, \ldots, p - 1\}$.
2. Soient a et b des entiers. Montrer que $(a + b)^p - a^p - b^p$ est un multiple de p. En déduire que $(a + 1)^p - (a^p + 1)$ est un multiple de p.
3. Soit a un entier. Montrer par récurrence sur a que $a^p - a$ est un multiple de p. En déduire que pour p premier avec a, $p | a^{p-1} - 1$.