FICHE DE RÉVISION ARITHMÉTIQUE

Exercice 1.

1. Donner les définitions de groupe, groupe commutatif, anneau, anneau commutatif.

2. Donner des exemples de groupes et anneaux commutatifs et groupes et anneaux non commutatifs.

Exercice 2. Soit $(A, +_A, \times_A)$ un anneau. On note A^* l'ensemble des éléments inversibles de A.

1. Rappeler à quelle condition $x \in A$ est inversible.

2. Peut-on avoir $0_A \in A^*$?

3. Quand A est-il un corps ?

4. Montrer que $(A^*, \times_A)$ est un groupe.

5. Déterminer $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{Z}^*$, $A[X]^*$ (où A est un anneau), $M_n(\mathbb{K})^*$ où $M_n(\mathbb{K})$ est l'anneau des matrices carrés à coefficients dans le corps $\mathbb{K}$.

Exercice 3.

1. Rappeler la définition d'un nombre premier.

2. Montrer qu'il existe une infinité de nombre premier.

Exercice 4. Soit n un entier strictement positif. Pour tout couple (a, b) de $\mathbb{Z}^2$, on pose $a \equiv_n b$ si et seulement si n divise $a - b$.

1. Montrer que $\equiv_n$ est une relation d'équivalence.

2. Pour $x \in \mathbb{Z}$, on note $[x]_n$ la classe d'équivalence de x relativement à $\equiv_n$. Rappeler la définition de $[x]_n$.

3. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\mathbb{Z}/\equiv_n$ des classes d'équivalences de $\equiv_n$. Montrer que les applications :

$$+_n : \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^2 & \to & \mathbb{Z}/n\mathbb{Z} \\ ([x]_n, [y]_n) & \mapsto & [x+y]_n \end{array} \quad \text{et} \quad \times_n : \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^2 & \to & \mathbb{Z}/n\mathbb{Z} \\ ([x]_n, [y]_n) & \mapsto & [x \times y]_n \end{array}$$

sont biens définies. On dit alors que la relation $\equiv_n$ est une congruence (elle préserve la structure de $\mathbb{Z}$)

4. Monter que $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$ est un anneau.

5. A quelle condition sur n, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il un coprs ?

Exercice 5.

1. Rappeler en terme de diviseur la définition de $\mathrm{pgcd}(a, b)$ pour $(a, b) \in \mathbb{Z}^2$.

2. Montrer que pour tout $(a, b) \in \mathbb{Z}^2$, on a $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, a)$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a + b, b)$.

3. On note r le reste de la division euclidienne de a par b. Montrer qu'on a $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r, b)$.

Exercice 6.

1. Soit P un polynôme de $\mathbb{Z}[X]$ montrer qu'un nombre premier p divise une racine x de P si et seulement si p divise $P(0)$.

2. Quels sont les racines dans $\mathbb{Z}$ de $6X^3 - 5X^2 - 3X + 2$.

3. Soit P un polynôme de $\mathbb{Q}[X]$ de coefficients $a_n, ..., a_0$ dans $\mathbb{Z}$. Montrer que la fraction irréductible $\frac{p}{q}$ est racine de P si et seulement si p divise a_0 et q divise a_p.

4. Quelles sont les racines dans $\mathbb{Q}$ de $6X^3 - 5X^2 - 3X + 2$?

5. Montrer que pour p premier, le polynôme n'a $X^2 - p$ n'a pas de racine dans $\mathbb{Q}$.

6. Montrer que pour p premier $\sqrt{p}$ n'est pas rationnel.

Exercice 7.

1. Montrer que pout tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

2. Soit G un sous-groupe de $\mathbb{Z}$. Montrer qu'il existe $n \in \mathbb{N}$ tel que $G = n\mathbb{Z}$.

Soient a et b deux entier de $\mathbb{Z}$.

3. Montrer que $G_{a,b} = a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

4. Montrer qu'on a $G_{a,b} = \mathrm{pgcd}(a,b)\mathbb{Z}$ (sans utiliser le théorème de Bezout).

5. Montrer, sans utiliser le théorème de Bezout, qu'in existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = \mathrm{pgcd}(a,b)$.

6. Réciproquement montrer que s'il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = d$ alors d est un multiple de $\mathrm{pgcd}(a,b)$.

Exercice 8. Soit n un entier strictement positif. On pose $X = \{[a]_n \mid \mathrm{pgcd}(a,n) = 1\}$.

1. Montrer l'inclusion $X \subseteq (\mathbb{Z}/n\mathbb{Z})^*$.

2. Montrer l'inclusion réciproque.

3. Déterminer les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour $n = 2, 3, 4, 5, 6, 7, 8, 9, 10$.

4. A quelle condition sur n, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il un coprs ? Justifier.

5. Quels sont les inverses de $[5]_{36}$ et $[13]_{36}$ dans $\mathbb{Z}/36\mathbb{Z}$?

Exercice 9. Pour $n \in \mathbb{N}$, on note $\varphi(n)$ le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$.

1. Déterminer $\varphi(p)$ pour p un nombre premier.

2. Déterminer $\varphi(pq)$ lorsque p et q sont des nombres premiers distincts.

Exercice 10. Soient $m_1, ..., m_k$ des nombres premiers entre eux deux à deux et $a_1, ..., a_k$ des entiers quelconques. On se propose de trouver tous les entiers x de $\mathbb{Z}$ vérifiant :

$$(S) \begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_k \mod m_k \end{cases}$$

1. Montrer que pour chaque $i \in \{1, ..., k\}$, les entiers m_i et $\hat{m}_i = \prod_{j \neq i} m_j$ sont premiers entre eux.

2. A l'aide du théorème de Bezout, montrer que pour tout $i \in \{1, ..., k\}$, il existe $e_i \in \mathbb{Z}$ tel que $e_i \equiv \delta_i^j \mod m_j$ pour tout $j \in \{1, ..., k\}$. On rappele que δ_i^j vaut 1 pour $i = j$ et 0 sinon.

3. En déduire une solution particulière x_0 de (S).

4. Montrer que les solutions de (S) sont les entiers x congrus à x_0 modulo $n = m_1 ... m_k$.

5. Quelles sont les solutions $x \in \mathbb{Z}$ du système congruentiel

$$(T) \begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}$$