Chapitre

ARITHMÉTIQUE DANS $\mathbb{Z}$

I Divisibilité dans $\mathbb{Z}$

1 Définition

Définition

Soient a un entier relatif non nul et b un entier relatif. On dit que b est divisible par a dans $\mathbb{Z}$ ou que a divise b dans $\mathbb{Z}$ et on écrit $a|b$, s'il existe un entier relatif k tel que $b = ka$.

Dans ce cas, on dit que b est un multiple de a ou que a est un diviseur de b. L'ensemble des diviseurs de b est noté par $D(b) = D(|b|)$. Dans le cas contraire on écrit $a \nmid b$.

• Exemple

$2|6$ car $6 = 2 \times 3$
et on a : $D(6) = D(-6) = \{-6;-3;-2;-1;1;2;3;6\}$
$2 \nmid 7$ car $(\nexists k \in \mathbb{Z}) : 7 = 2k$.

Application

Soit a et b deux entiers relatifs non nuls. Montrer que : $b/a \longleftrightarrow |b| \leq |a|$.

Propriété

Soient a,b et c trois entiers relatifs, alors :

1. $a|a$ (avec $a \neq 0$).
2. Si $a|b$ et $b|c$, alors $a|c$.
3. Si $a|b$ et $b|a$, alors $|a| = |b|$ c'est à dire que $a = \pm b$.
4. Si $a|b$ et $c|d$, alors $ac|bd$.
5. Si $a|b$ et $a|c$, alors $a|mb+nc, \forall (m,n) \in \mathbb{Z}^2$
6. Si $a|b$, alors $(\forall c \in \mathbb{Z}^*); ac|bc$.

EXEMPLES

1. $a|a$ car $a = 1.a$.
2. On a $a|b$, alors $(\exists k \in \mathbb{Z}) : b = ka$.
   On a $b|c$, alors $(\exists k' \in \mathbb{Z}) : c = k'b$.
   Ainsi $c = (kk')a$, ce qui donne que $a|c$.
3. Si $a|b$ et $b|a$ alors $|a| \leq |b|$ et $|b| \leq |a|$, ainsi $|a| = |b|$ c'est à dire que $a = \pm b$.
4. On a $a|b$ alors $(\exists k \in \mathbb{Z}) : b = ka$.

On a $c|d$, alors $(\exists k' \in \mathbb{Z}) : d = k'c$.
Donc $bd = (ka).(k'c) = (kk').(ac)$, c'est à dire $ac|bd$

5 On a $a|b$ et $a|c$, alors $(\exists k \in \mathbb{Z}) : b = ka$ et $(\exists k' \in \mathbb{Z}) : c = k'a$.
Ainsi $(\forall (m,n) \in \mathbb{Z}^2, (\exists (k,k') \in \mathbb{Z}^2)) : mb + nc = mka + nk'a = (mk + nk')a$
ce qui donne que $a|mb + nc$,$(\forall (m,n) \in \mathbb{Z}^2)$.

6 Trivial

2 Division euclidienne

T Théorème

Soient a et b deux entiers relatifs, avec $b > 0$. Il existe un couple unique $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ vérifiant $a = bq + r$ et $0 \leq r < b$.
L'entier q s'appelle le quotient et l'entier r s'appelle le reste de la division euclidienne de a par b.

T Théorème

Soient a et b deux entiers relatifs, avec $b \neq 0$. Il existe un couple unique $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ vérifiant $a = bq + r$ et $0 \leq r < |b|$.

• Exemple

1 La division euclidienne de 18 par 6 est : $18 = 6 \times 3$ (le quotient est 3, le reste est 0).
2 La division euclidienne de 15 par 2 est : $15 = 2 \times 7 + 1$ (le quotient est 7, le reste est 1).

Application

1 Déterminer le quotient et le reste de la division euclidienne de b par a dans chacun des cas suivants :
- a $a = 5$ et $b = 67$
- b $a = -5$ et $b = 67$
- c $a = -5$ et $b = -67$
- d $a = 5$ et $b = -67$
- e $a = 12$ et $b = 56$

2 Les restes de la division euclidienne des nombres 4294 et 3512 par un entier naturel non nul a sont respectivment 10 et 12. Déterminer la valeur de a.

II NOMBRES PREMIERS

1 Nombres premiers

Définition

Soit $p \in \mathbb{Z}$. On dit que p est un nombre premier si : $|p| \neq 1$ et $D_p = \{-1; 1; -p; p\}$ où D_p désigne l'ensemble des diviseurs de p.

• Exemple

1. On a : $D_2 = \{-1; 1; 2; -2\}$; Donc 2 est un nombre premier.
2. les entiers : -2, 3 ; 5, -7,... sont des nombres premiers .
3. 0 n'est pas un nombre premier.
4. L'entier 2 est le seul nombre premier pair.

Application

1. Montrer que les nombres suivants ne sont pas premiers :
   4824 - 7281 - 111 - 25008 - 1111 - 437 - 990.
2. Montrer que tout nombre premier positif et distinct de 2 et 3 s'écrit sous la forme :
   $6p+1$ ou $6p+5$.

2 Détermination des nombres premiers

Proposition

Soit a un nombre non premier et différent de 1.
Le plus petit diviseur propre de a (c'est à dire distinct de 1 et a) est un nombre premier.

T Théorème

Soit n un entier non premier et supérieur ou égale à 2. alors, il existe au moins un diviseur premier p du nombre n et vérifiant $p^2 \leq n$.
(n est un nombre premier) $\leftrightarrow$ (n n'admet pas de diviseur premier dans $[2; \sqrt{n}] \cap \mathbb{N}$)

Application

1. Parmi les nombres suivants, lesquels sont des nombres premiers :
   127 - 1979 - 2024 - 13957 - 2309 - 232 - 2309.
2. En utilisant le rible d'Eratosthène, déterminer les nombres premiers qui existent entre 1 et 100.

Théorème

L'ensemble $\mathbb{P}$ des nombres premiers positifs est infini.

EXEMPLES

L'infinité des nombres premiers peut être démontrée en utilisant une preuve par l'absurde. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers $p_1, p_2, \ldots, p_n$. Ensuite, considérons le nombre $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Ce nombre n'est divisible par aucun des nombres premiers $p_1, p_2, \ldots, p_n$, car il laisse un reste de 1 dans chaque cas. Cela signifie que N est soit un nombre premier lui-même, soit divisible par un nombre premier qui n'est pas dans notre liste. Dans les deux cas, cela contredit notre hypothèse de départ, montrant ainsi qu'il doit y avoir une infinité de nombres premiers.

3 Décomposition en produit de facteurs premiers

Théorème

Tout entier relatif $n \neq 1$ et $n \neq -1$ peut être exprimé de manière unique (à l'ordre près des facteurs) sous la forme d'un produit de nombres premiers :

$$n = \varepsilon p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

où $p_1, p_2, \ldots, p_k$ sont des nombres premiers distincts et $a_1, a_2, \ldots, a_k$ sont des exposants positifs et $\varepsilon = \pm 1$.

• Exemple

1. Décomposition de 24 : $24 = 2^3 \cdot 3^1$
2. Décomposition de 60 : $60 = 2^2 \cdot 3^1 \cdot 5^1$
3. Décomposition de 126 : $126 = 2^1 \cdot 3^2 \cdot 7^1$
4. Décomposition de 240 : $240 = 2^4 \cdot 3^1 \cdot 5^1$
5. Décomposition de 385 : $385 = 5^1 \cdot 7^2$
6. Décomposition de 900 : $900 = 2^2 \cdot 3^2 \cdot 5^2$
7. Décomposition de 1024 : $1024 = 2^{10}$

Application

1. Décomposer les nombres suivants en produit de facteurs premiers : 10000 - 8200 - 1332 - -1777 - -51480.
2. Décomposer en produit de facteurs premiers le nombre : $a = 6^6 + 1$

III Plus grand commun diviseur, algorithme d'Euclide, plus petit commun multiple

1 Plus grand commun diviseur

Définition

Le Plus Grand Diviseur Commun (PGCD) de deux entiers relatifs non nuls a et b est le plus grand nombre entier positif qui divise à la fois a et b.

Remarque

Le PGCD est souvent noté $\text{PGCD}(a,b)$ ou $\text{GCD}(a,b)$, et il satisfait les propriétés suivantes :

1. $\text{PGCD}(a,b) \leq a$ et $\text{PGCD}(a,b) \leq b$.
2. Si $\text{PGCD}(a,b) = 1$, alors a et b sont dits premiers entre eux (ou copremiers).
3. Si d est un diviseur commun de a et b, alors $d \leq \text{PGCD}(a,b)$.

Exemple

1. $\text{PGCD}(48,18) = 6$
2. $\text{PGCD}(72,90) = 18$
3. $\text{PGCD}(105,140) = 35$
4. $\text{PGCD}(240,64) = 16$
5. $\text{PGCD}(27,63) = 9$
6. $\text{PGCD}(15,17) = 1$ (car ils sont premiers entre eux)
7. $\text{PGCD}(0,5) = 5$ (par convention)
8. $\text{PGCD}(0,0)$ est indéfini (par convention)

Propriété

Soit a et b deux entiers relatifs non nuls et n un entier naturel non nul, Alors :

1. $a \wedge b = |a| \wedge |b|$
2. $a \wedge b = b \wedge a$
3. $a \wedge a = a \wedge 0 = |a|$
4. $a \wedge 1 = 1$
5. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
6. $a/b \leftrightarrow a \wedge b = |a|$
7. $a^n \wedge a = |a|$

EXEMPLES

- ☐ Les résultats 1), 2), 3), 4), et 7), sont des conséquences de la définition précédentes.
- ☐ Le résultat 5) découle de fait que : $(D_a \cap D_b) \cap D_c = D_a \cap (D_b \cap D_c)$.
- ☐ Pour le résultat 6) : On suppose que a/b, donc : $(\exists k \in \mathbb{Z}); b = ak$. Par conséquent : $D_a \cap D_b = D_a \cap D_{ka} = D_a$ car : $(D_a \subset D_{ka})$
  Il s'ensuit donc que : $a/b \rightarrow a \wedge b = |a|$
  Réciproquement, si $a \wedge b = |a|$ alors $|a|/b$, c'est à dire que : a/b
  D'où : $a/b \leftrightarrow a \wedge b = |a|$

2 Calcul pratique du P.G.C.D : L'algorithme d'Euclide

Proposition

Soient a et b deux nombres entiers positifs donnés avec $a > b$. Le but est de déterminer le Plus Grand Commun Diviseur (PGCD) de a et b en utilisant l'algorithme d'Euclide.

- ☐ **Initialisation :** Soit q_0 et r_0 les résultats de la division de a par b, c'est-à-dire $a = q_0 \cdot b + r_0$.
- ☐ Si $r_0 = 0$, alors le PGCD est b : $PGCD(a,b) = b$.
- ☐ **Sinon,** répéter les étapes suivantes jusqu'à ce que $r_k = 0$ pour un certain k.
  1. **Division :** Calculer q_{k+1} et r_{k+1} en effectuant la division de b par r_k, c'est-à-dire $b = q_{k+1} \cdot r_k + r_{k+1}$.
  2. **Mise à jour :** Réassigner b avec r_k et r_k avec r_{k+1}.
- ☐ Une fois $r_k = 0$ est atteint, le dernier r_{k-1} non nul avant cette étape est le PGCD recherché : $PGCD(a,b) = r_{k-1}$.

• Exemple

Soient $a = 48$ et $b = 18$. Nous allons utiliser l'algorithme d'Euclide pour calculer le PGCD de a et b.

$$a = 48, \quad b = 18$$
$$q_0 = \frac{a}{b} = \frac{48}{18} = 2, \quad r_0 = a - (q_0 \cdot b) = 48 - (2 \cdot 18) = 12$$

Étape 1 :

$$q_1 = \frac{b}{r_0} = \frac{18}{12} = 1, \quad r_1 = b - (q_1 \cdot r_0) = 18 - (1 \cdot 12) = 6$$

Étape 2 :

$$q_2 = \frac{r_0}{r_1} = \frac{12}{6} = 2, \quad r_2 = r_0 - (q_2 \cdot r_1) = 12 - (2 \cdot 6) = 0$$

Le PGCD est $r_1 = 6$, car le reste devient nul à l'étape 2.
Donc, le PGCD$(48, 18) = 6$

Application

Calculez le PGCD en utilisant l'algorithme d'Euclide :

1. $a = 72, b = 36$
2. $a = 105, b = 45$
3. $a = 210, b = 96$

Remplir les étapes de calcul suivantes :

1. **Paire de Nombres :** $a = 72, b = 36$

$$a = 72, \quad b = 36$$
$$q_0 = \frac{a}{b} = \quad , \quad r_0 = a - (q_0 \cdot b) =$$

Étape 1 :

$$q_1 = \frac{b}{r_0} = \quad , \quad r_1 = b - (q_1 \cdot r_0) =$$

Étape 2 :

$$q_2 = \frac{r_0}{r_1} = \quad , \quad r_2 = r_0 - (q_2 \cdot r_1) =$$

Le PGCD est $r_1 =$.

2. **Paire de Nombres :** $a = 105, b = 45$
3. **Paire de Nombres :** $a = 210, b = 96$

3 Plus petit commun multiple

Définition

Le Plus Petit Commun Multiple (PPCM) de deux nombres entiers positifs a et b est le plus petit multiple positif commun à la fois de a et de b.

Remarque

Si a et b sont différents de zéro, alors :

$$PPCM(a,b) \times PGCD(a,b) = a \times b$$

• Exemple

Par exemple, si $a = 4$ et $b = 6$, alors $PGCD(4,6) = 2$, et le PPCM est calculé comme suit :

$$PPCM(4,6) = \frac{4 \cdot 6}{2} = 12$$

Ainsi, le PPCM de 4 et 6 est 12.

Propriété

Soit a, b et c des entiers relatifs non nuls. ALors :

1. $a \vee b = |a| \vee |b|$
2. $a \vee b = b \vee a$
3. $a \vee a = |a|$
4. $a \vee 1 = |a|$
5. $(a \vee b) \vee c = a \vee (b \vee c)$
6. $a/b \leftrightarrow a \vee b = |b|$
7. $a \vee b / ab$

EXEMPLES

- ☐ Les résultats 1), 2), 3), et 4), sont des conséquences de la définition et la remarque précédentes.
- ☐ Le résultat 5) découle de fait que : $(a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z} = a\mathbb{Z} \cap (b\mathbb{Z} \cap c\mathbb{Z})$
- ☐ Pour le résultat 6) : On sait que : $a/b \leftrightarrow b\mathbb{Z} \subset a\mathbb{Z} \leftrightarrow a\mathbb{Z} \cap b\mathbb{Z} = b\mathbb{Z}$
  On en déduit donc que : $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^* = b\mathbb{Z} \cap \mathbb{N}^*$. Ainsi : $a/b \leftrightarrow a \vee b = |b|$
- ☐ Pour le résultat 7) : On a le produit ab est un multiple commun de a et b ; par définition de $a \vee b$, on en déduit que ab est un multiple de $a \vee b$, c'est à dire que : $a \vee b / ab$.

Application

1 Déterminer $a \vee b$ dans chacun des cas suivants :

1^{er} cas : $a \wedge b = 13$ et $ab = 221$; $2^{\text{ème}}$ cas : $a \wedge b = 17$ et $ab = -578$

2 Soit a et b deux éléments de $\mathbb{N}^*$.

Montrer que : $(\exists (a';b') \in \mathbb{N}^2)$; $\frac{1}{a} + \frac{1}{b} = \frac{a'+b'}{a \vee b}$

IV Congruence modulo n

1 Définition

Activité

☐ Objectif :

Faire découvrir et comprendre le concept de congruence modulo n tout en encourageant les participants à résoudre des énigmes et à collaborer.

☐ Matériel

- ◇ Feuilles de papier avec des problèmes de congruence modulo n (variés en difficulté)
- ◇ Stylos
- ◇ Tableau blanc ou tableau noir
- ◇ Optionnel : petits prix pour les gagnants

☐ Déroulement

- ◇ Introduction (10 minutes) Commencez par expliquer brièvement ce qu'est la congruence modulo n à l'aide d'exemples concrets. Utilisez des chiffres simples pour illustrer comment deux nombres peuvent avoir le même reste lorsqu'ils sont divisés par n.
- ◇ Formation des équipes (5 minutes) Divisez les participants en petites équipes. Si possible, mélangez les niveaux d'aptitude mathématique pour favoriser la collaboration.
- ◇ Règles du jeu (5 minutes) Expliquez les règles de la "Chasse aux Trésors Modulo". Chaque équipe recevra une série d'énigmes liées à la congruence modulo n. Les équipes doivent résoudre ces énigmes pour trouver les indices menant à un "trésor" caché (peut être symbolique).
- ◇ Résolution des énigmes (30-40 minutes) Donnez à chaque équipe une série d'énigmes à résoudre. Chaque énigme devrait comporter des énoncés qui nécessitent l'application de la congruence modulo n pour trouver la solution. Les équipes doivent résoudre les énigmes pour découvrir des indices.
- ◇ Trouver le trésor (10 minutes) Une fois qu'une équipe a résolu suffisamment d'énigmes et obtenu tous les indices, elles devront suivre ces indices pour trouver le "trésor" caché dans la salle (ou un emplacement désigné). Cela pourrait être un mot-clé, un message secret, ou tout autre élément qui représente leur succès.
- ◇ Discussion et Explication (10 minutes) Une fois que toutes les équipes ont trouvé leurs "trésors", rassemblez-les pour une discussion. Demandez-leur de partager comment ils ont résolu les énigmes en utilisant la congruence modulo n. Discutez des concepts clés et clarifiez les points si nécessaire.

◇ Récompenses (5 minutes) Si vous le souhaitez, offrez des petits prix aux équipes qui ont résolu le plus grand nombre d'énigmes ou qui ont montré une compréhension exceptionnelle de la congruence modulo n.

• Exemple

☐ Énigme : Voyageur Modulaire

Un voyageur se déplace le long d'une route. Chaque jour, il parcourt une distance de 7 km. Cependant, il s'arrête pour la nuit à un endroit différent chaque jour. Si le voyageur commence son voyage le lundi, à quel jour de la semaine sera-t-il à 100 km de son point de départ ?

☐ Indice

Utilisez la congruence modulo 7 pour déterminer le jour de la semaine.

☐ Solution

L'utilisation de la congruence modulo 7 nous permet de répéter le cycle des jours de la semaine. Si nous exprimons 100 en termes de congruence modulo 7, nous avons $100 \equiv 2 \pmod 7$, ce qui signifie que le voyageur sera à 2 km de son point de départ après 100 km de voyage.

Le jour de la semaine correspondant à 2 jours après le lundi est le mercredi. Donc, le voyageur sera à 100 km de son point de départ un mercredi.

Définition

Soient a et b sont deux entiers, alors on dit que a est congru à b modulo n et on écrit $a \equiv b \ [n]$ si la différence $a-b$ est divisible par n, c'est-à-dire si $(a-b)$ est un multiple de n.
Formellement, on peut exprimer la congruence modulo n comme suit :

$$a \equiv b \ [n] \quad \text{si et seulement si} \quad \exists k \in \mathbb{Z} \text{ tel que } a-b=kn.$$

• Exemple

Exemples de Congruence :

☐ Exemple 1 : Congruence modulo 5

$$17 \equiv 2 \pmod 5$$

Cela signifie que 17 et 2 laissent le même reste lorsqu'ils sont divisés par 5.

☐ Exemple 2 : Congruence modulo 3

$$10 \equiv 1 \pmod 3$$

Cela signifie que 10 et 1 laissent le même reste lorsqu'ils sont divisés par 3.

☐ Exemple 3 : Congruence modulo 8

$$29 \equiv 5 \pmod 8$$

Cela signifie que 29 et 5 laissent le même reste lorsqu'ils sont divisés par 8.

☐ Exemple 4 : Congruence modulo 11

$$43 \equiv 9 \pmod{11}$$

Cela signifie que 43 et 9 laissent le même reste lorsqu'ils sont divisés par 11.

Application

Pour chaque paire de nombres suivante, déterminez si les deux nombres sont congruents modulo 4. Si c'est le cas, justifiez votre réponse en montrant que la différence entre les nombres est un multiple de 4.

1. 12 et 28
2. 9 et 21
3. 5 et 13
4. 20 et 36

Solution :

1. 12 et 28 :
   La différence entre 28 et 12 est $28-12=16$, qui est un multiple de 4 ($16=4\cdot 4$). Donc, 12 et 28 sont congruents modulo 4.
2. 9 et 21 :
   La différence entre 21 et 9 est $21-9=12$, qui est un multiple de 4 ($12=4\cdot 3$). Donc, 9 et 21 sont congruents modulo 4.
3. 5 et 13 :
   La différence entre 13 et 5 est $13-5=8$, qui n'est pas un multiple de 4. Donc, 5 et 13 ne sont pas congruents modulo 4.
4. 20 et 36 :
   La différence entre 36 et 20 est $36-20=16$, qui est un multiple de 4 ($16=4\cdot 4$). Donc, 20 et 36 sont congruents modulo 4.

2 Propriétés de la relation "Congruence modulo"

Proposition

Propriétés de la Congruence Modulo n

☐ Réflexivité

Pour tout entier a, on a $a \equiv a \pmod n$. Cela signifie qu'un nombre est toujours congruent à lui-même modulo n.

☐ Symétrie

Si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$. La congruence est une relation symétrique.

☐ Transitivité

Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$. La congruence est une relation transitive.

☐ Addition

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a+c \equiv b+d \pmod{n}$. Cela signifie que si deux paires de nombres sont congruentes modulo n, leur somme sera également congruente modulo n.

☐ Multiplication

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a \cdot c \equiv b \cdot d \pmod{n}$. Cela signifie que si deux paires de nombres sont congruentes modulo n, leur produit sera également congruent modulo n.

☐ Soustraction

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a-c \equiv b-d \pmod{n}$. Cela signifie que si deux paires de nombres sont congruentes modulo n, leur différence sera également congruente modulo n.

☐ Puissance

Si $a \equiv b \pmod{n}$, alors $a^k \equiv b^k \pmod{n}$ pour tout entier positif k. Cela signifie que si a et b sont congruents modulo n, alors leurs puissances correspondantes sont également congruentes modulo n.

• Exemple

1 Exemple 1 : Calcul par l'Addition

Supposons que nous voulions déterminer le reste de la somme $123+456$ lorsque divisé par 10. Utilisons la propriété d'addition de la congruence :

$$123 \equiv 3 \pmod{10}$$
$$456 \equiv 6 \pmod{10}$$

En utilisant la propriété d'addition, nous avons :

$$123+456 \equiv 3+6 \equiv 9 \pmod{10}$$

Donc, le reste de $123+456$ divisé par 10 est 9.

2 Exemple 2 : Calcul par la Multiplication

Si nous voulons déterminer le reste de $7 \times 8 \times 9$ lorsque divisé par 5, utilisons la propriété de multiplication de la congruence :

$$7 \equiv 2 \pmod{5}$$
$$8 \equiv 3 \pmod{5}$$
$$9 \equiv 4 \pmod{5}$$

En utilisant la propriété de multiplication, nous avons :

$$7 \times 8 \times 9 \equiv 2 \times 3 \times 4 \equiv 24 \equiv 4 \pmod 5$$

Donc, le reste de $7 \times 8 \times 9$ divisé par 5 est 4.

Application

V L'ensemble $\mathbb{Z}/n\mathbb{Z}$

1 Définition