DIVISIBILITÉ DANS $\mathbb{Z}$

I - DIVISEURS ET MULTIPLES D'ENTIERS

Définition

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$
On dit que b est un diviseur de a ou que a est divisible par b, s'il existe $q \in \mathbb{Z}$ tel que $a = bq$

Vocabulaire

Si un entier a est divisible par un entier non nul b, on dit que a est un multiple de b

Conséquence

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$

- Si b divise a alors $-b$ divise a
- Les multiples de b sont les éléments de l'ensemble $b\mathbb{Z} = \{bq\ , q \in \mathbb{Z}\}$

Propriétés

Soit $(a;b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $c \in \mathbb{Z}$

- Si a divise b et b divise a alors $a = b$ ou $a = -b$
- Si a divise b et b divise c alors a divise c
- Si a divise b et a divise c alors a divise $\alpha b + \beta c$ pour tous entiers α et β

Démonstration

- a divise b $\Rightarrow$ il existe $q \in \mathbb{Z}$ tel que $b = qa$
  b divise a $\Rightarrow$ il existe $q' \in \mathbb{Z}$ tel que $a = q'b$
  Donc $a = qq'a \Rightarrow qq' = 1 \Rightarrow q = q' = 1$ ou $q = q' = -1$ alors $a = b$ ou $a = -b$
- a divise b $\Rightarrow$ il existe $q \in \mathbb{Z}$ tel que $b = qa$
  b divise c $\Rightarrow$ il existe $p \in \mathbb{Z}$ tel que $c = pb$
  Alors $c = pqa = p'a$ où $p' = pq \in \mathbb{Z}$ donc a divise c
- a divise b $\Rightarrow$ il existe $q \in \mathbb{Z}$ tel que $b = qa$
  a divise c $\Rightarrow$ il existe $n \in \mathbb{Z}$ tel que $c = na$
  Donc $\forall \alpha \in \mathbb{Z}, \beta \in \mathbb{Z}$, $\alpha b + \beta c = \alpha qa + \beta na = a(\alpha q + \beta n) = an'$ où $n' = (\alpha q + \beta n) \in \mathbb{Z}$
  Alors a divise $\alpha b + \beta c$

II - DIVISION EUCLIDIENNE DANS $\mathbb{Z}$

Définition (Rappel)

Pour tout réel x, il existe et unique entier n tel que $n \le x < n+1$. Cet entier est appelé partie entière de x, elle est notée $E(x)$

Définition

Soit $(a;b) \in \mathbb{Z} \times \mathbb{Z}^*$

On appelle quotient de a par b l'entier q défini de la manière suivante :

- q est le plus grand entier inférieur ou égal à $\frac{a}{b}$ si $b > 0$
- q est le plus petit entier supérieur ou égal à $\frac{a}{b}$ si $b < 0$

Exemples

Le quotient de 5 par 4 est égal à 1
Le quotient de 5 par -4 est égal à -1
Le quotient de -5 par 4 est égal à -2
Le quotient de -5 par -4 est égal à 2

Définition

Soit $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$

On appelle reste de a par b l'entier r tel que $r = a - bq$, où q est le quotient de a par b

Théorème

$\forall\, a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ il existe un unique couple d'entiers $(q;r)$ tel que $a = bq + r$ et $0 \le r < |b|$

Démonstration

Pour l'existante, il suffit de prendre le quotient de a par b et le reste de a par b
Prouvons l'unicité
Supposons qu'il existe deux couples d'entiers $(q;r)$ et (q',r') tels que

$a = bq + r$ et $0 \le r < |b|$ et $a = bq' + r'$ et $0 \le r' < |b|$

Il en résulte que $b(q - q') = r' - r \Rightarrow |b||q - q'| = |r - r'| < |b|$

Par suite $|b||q - q'| = 0 \Rightarrow q = q'$ et $r = r'$

Vocabulaire

L'écriture $a = bq + r$ et $0 \le r < |b|$ s'appelle division euclidienne de a par b, q est le quotient de a par b et r est le reste de a par b

Conséquence

Le reste de tout entier a dans la division euclidienne par un entier non nul b est un élément de l'ensemble $\{0;1;2.....;|b|-1\}$

III - CONGRUENCE MODULO n

Définition et notation

Soit $(a;b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}^*$

On dit que a est congru à b modulo n (ou a et b sont congrus modulo n) si $a - b$ est un multiple de n .On note alors $a \equiv b (\text{mod}\, n)$

Théorème et définition

Soit $n \in \mathbb{N}^*$

$\forall a \in \mathbb{Z}$ il existe un unique entier $r \in \{0;1;2...;n-1\}$ tel que $a \equiv r(\text{mod}\, n)$

On dit que r est le reste modulo n de a

Conséquence

Soit $n \in \mathbb{N}^*$

Deux entiers sont congrus modulo n, si et seulement si, ils ont le même reste modulo n

Démonstration

Soit $a = nq + r$ et $b = nq + r'$ où $0 \leq r < n$ et $0 \leq r' < n$

Si $r = r'$ alors $a - b = n(q - q') \Rightarrow n$ divise $a - b \Rightarrow a \equiv b(\text{mod}\, n)$

Réciproquement :

$a \equiv b(\text{mod}\, n) \Rightarrow$ il existe $k \in \mathbb{Z}$ tel que $a - b = nk$

Donc $r - r' = a - nq - b + nq' = a - b - n(q - q') = nk - n(q - q') = n(k - q + q')$

$\Rightarrow n$ divise $r - r'$ et puisque $0 \leq r < n$ et $0 \leq r' < n$ alors $|r - r'| < 0 \Rightarrow r - r' = 0 \Rightarrow r = r'$

Propriétés

Soit a, b et c trois entiers et n un entier naturel non nul

- $a \equiv a(\text{mod}\, n)$
- Si $a \equiv b(\text{mod}\, n)$ alors $b \equiv a(\text{mod}\, n)$
- Si $a \equiv b(\text{mod}\, n)$ et $b \equiv c(\text{mod}\, n)$ alors $a \equiv c(\text{mod}\, n)$

Démonstration

La preuve des deux premières propriétés est évidente

Dire que $a \equiv b(\text{mod}\, n)$ et $b \equiv c(\text{mod}\, n) \Rightarrow n$ divise $a - b$ et n divise $b - c$

$\Rightarrow n$ divise $a - b + b - c \Rightarrow n$ divise $a - c \Rightarrow a \equiv c(\text{mod}\, n)$

Propriétés

Soit a, b, c et d quatre entiers et n un entier naturel non nul

- Si $a \equiv b(\text{mod}\, n)$ et $c \equiv d(\text{mod}\, n)$ alors $a + c \equiv b + d(\text{mod}\, n)$ et $a \times c \equiv b \times d(\text{mod}\, n)$
- Si $a \equiv b(\text{mod}\, n)$ alors $\forall h \in \mathbb{Z}, ha \equiv hb(\text{mod}\, n)$ et $\forall p \in \mathbb{N}^*, a^p \equiv b^p(\text{mod}\, n)$

Démonstration

Soit a, b, c et d quatre entiers et n un entier naturel non nul

- Si $a \equiv b(\text{mod}\, n)$ et $c \equiv d(\text{mod}\, n)$ alors n divise $a - b$ et n divise $c - d$

$\Rightarrow n$ divise $(a - b) + (c - d) = (a + c) - (b + d) \Rightarrow a + c \equiv b + d(\text{mod}\, n)$

De même : si $a \equiv b(\text{mod}\, n)$ et $c \equiv d(\text{mod}\, n)$ alors n divise $a - b$ et n divise $c - d$

$\Rightarrow n$ divise $(a - b)c + (c - d)b \Rightarrow n$ divise $ac - bd \Rightarrow ac \equiv bd(\text{mod}\, n)$

- Si $a \equiv b(\text{mod}\, n) \Rightarrow n$ divise $a - b \Rightarrow n$ divise $h(a - b) \Rightarrow n$ divise $ha - hb \Rightarrow ha \equiv hb(\text{mod}\, n)$
- $\forall p \in \mathbb{N}^*$ $a^p - b^p = (a - b)\sum_{k=0}^{p-1} a^{p-1-k}b^k = (a - b)\alpha$ où $\alpha = \sum_{k=0}^{p-1} a^{p-1-k}b^k$, $\alpha \in \mathbb{Z}$

Donc $a \equiv b(\text{mod}\, n) \Rightarrow n$ divise $a - b \Rightarrow n$ divise $(a - b)\alpha \Rightarrow n$ divise $a^p - b^p \Rightarrow a^p \equiv b^p(\text{mod}\, n)$

Exercice :

Montrer que pour tous entiers naturels n, p et q $, 4^n + 4^p + 4^q \equiv 0(\text{mod}\, 3)$

IV-THÉORÈME DE FERMAT

Activité

Soit p un nombre premier

1) Montrer que p divise C_p^k , pour tout $k \in \{1;2.....;p-1\}$

2) En déduire que pour tout entier naturel n, p divise $(n+1)^p-(n^p+1)$

3) Montrer par récurrence que $\forall n \in \mathbb{N}$, $n^p \equiv n \pmod p$

4) En déduire que $\forall n \in \mathbb{N}$ tel que $n \wedge p = 1$, $n^{p-1} \equiv 1 \pmod p$

5) Montrer que $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod p$ et que si $a \wedge p = 1$, $a^{p-1} \equiv 1 \pmod p$

Réponse :

Soit p un nombre premier

1) Montrons que p divise C_p^k , pour tout $k \in \{1;2.....;p-1\}$

On a : $C_p^k = \dfrac{p(p-1)(p-2)...(p-k+1)}{k!} \Rightarrow k!C_p^k = p(p-1)...(p-k+1)$ donc p divise $k!C_p^k$ et puisque $k < p$ alors p ne divise aucun des entiers $k;(k-1),(k-2),....,1 \Rightarrow$ p ne divise pas k! donc p divise C_p^k

2) Déduisons que pour tout entier naturel n, p divise $(n+1)^p-(n^p+1)$

On a : $(n+1)^p = \sum_{k=0}^{p} C_p^k n^k = n^p+1+\sum_{k=1}^{p-1} C_p^k n^k$ donc $(n+1)^p-(n^p+1) = \sum_{k=1}^{p-1} C_p^k n^k$

Et puisque p divise C_p^k , pour tout $k \in \{1;2.....;p-1\}$ alors p divise $\sum_{k=1}^{p-1} C_p^k n^k$

Donc p divise $(n+1)^p-(n^p+1)$

3) Montrons par récurrence que $\forall n \in \mathbb{N}$, $n^p \equiv n \pmod p$

- Pour $n = 0$, $0^p \equiv 0 \pmod p$
- Soit $n \in \mathbb{N}$, Supposons que $n^p \equiv n \pmod p$ et montrons que $(n+1)^p \equiv n+1 \pmod p$
- On a par hypothèse $n^p \equiv n \pmod p \Rightarrow n^p+1 \equiv n+1 \pmod p$
  Et puisque p divise $(n+1)^p-(n^p+1)$ alors $(n+1)^p \equiv n^p+1 \pmod p$
  Donc $(n+1)^p \equiv n+1 \pmod p$

Conclusion : $\forall n \in \mathbb{N}$, $n^p \equiv n \pmod p$

4) Montrons que si $n \wedge p = 1$ alors $n^{p-1} \equiv 1 \pmod p$, $\forall n \in \mathbb{N}$

On a : $n^p \equiv n \pmod p \Rightarrow p$ divise $n^p-n = n(n^{p-1}-1)$ et puis que $n \wedge p = 1$ alors p divise $n^{p-1}-1 \Rightarrow n^{p-1} \equiv 1 \pmod p$

5) Montrons que $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod p$ et que si $a \wedge p = 1$, $a^{p-1} \equiv 1 \pmod p$

- Le cas où $a \in \mathbb{N}$ est déjà démontré
- Si $a \in \mathbb{Z}^*_-$ alors $(-a) \in \mathbb{N}^*$ donc :

Si $p = 2$ on a : $a^2-a = a(a-1) \Rightarrow 2$ divise a^2-a car $a(a-1)$ est pair

Si $p > 2$ alors p est impair .Donc d'après ce qui précède $(-a)^p \equiv -a \pmod p$ car $(-a) \in \mathbb{N}$

$\Rightarrow -a^p \equiv -a \pmod p \Rightarrow a^p \equiv a \pmod p$

Par suite $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod p$

En plus si : $\left.\begin{array}{l} a^p \equiv a \pmod p \\ a \wedge p = 1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} p \text{ divise } a^p-a \\ a \wedge p = 1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} p \text{ divise } a(a^{p-1}-1) \\ a \wedge p = 1 \end{array}\right\} \Rightarrow p$ divise $a^{p-1}-1$

$\Rightarrow a^{p-1} \equiv 1 \pmod p$

Propriété

Soit p un nombre premier
Pour tout $a \in \mathbb{Z}$, $a^p \equiv a(\mathrm{mod}\, p)$

Théorème de Fermat

Pour tout $a \in \mathbb{Z}$ et tout nombre premier p tel que $a \wedge p = 1$, $a^{p-1} \equiv 1(\mathrm{mod}\, p)$