Divisibilité dans $\mathbb{Z}$, conguences

I Divisibilité dans $\mathbb{Z}$

Définition 1

Soit a et b deux entiers relatifs.
*On dit que b **divise** a s'il existe un entier k tel que $a = kb$. On note $b|a$.*
*On dit aussi que b **est un diviseur de** a ou que a **est un multiple de** b.*

Exemple

1) 3 divise 6 ; -5 divise 15, 7 divise -14.
2) Tous les diviseurs de 15 sont :
1,3,5,15 et $-1, -3, -5, -15$
3) Soit n un entier naturel, démontrer que n divise $n^2 - n$ pour tout n.
On a $n^2 - n = n(n-1)$, donc n divise $n^2 - n$.
4) Soit n un entier naturel, démontrer que $n-1$ divise $n^2 - 3n + 2$ pour tout n.
5) Trouver tous les couples d'entiers naturels $(x; y)$ tels que $x^2 - 2xy = 15$.

Propriété 1

Soient a, b et c trois entiers non nuls. On a :
(i) Si b divise a alors $-b$ divise a.
(ii) Si b divise a alors $|b| \leqslant |a|$.
(iii) Les seuls diviseurs de 1 et -1 dans $\mathbb{Z}$ sont 1 et -1.
(iv) Si $a|b$ et $b|c$, alors $a|c$.
(v) $a|b$ et $b|a$ équivaut à $a = b$ ou $a = -b$;
(vi) Si $c|a$ et $c|b$, alors pour tous entiers α et β, $c|\alpha a + \beta b$. (si c divise a et b alors c divise toute combinaison linéaire de a et b)

Remarque

Tout entier $a \neq \pm 1$ admet au moins 4 diviseurs : 1 ; -1 ; a et $-a$.

Exemple

1) Trouver tous les entiers relatifs tels que $(n-1)$ divise $(n+5)$.
2) Trouver tous les entiers relatifs tels que $(n-1)$ divise $n^2 - 4n + 8$.
3) k est un entier naturel, $a = 9k + 2$ et $b = 12k + 1$. Démontrer que les seuls diviseurs communs à a et b sont 1 et 5.

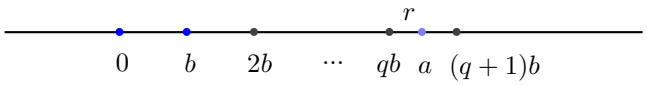
II Division euclidienne

II.1 Division euclidienne dans $\mathbb{N}$

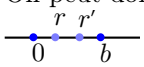
Théorème 1

Soit a un entier naturel et b un entier naturel non nul.
Il existe un unique couple $(q;r)$ d'entiers tels que :
$a = bq + r$ *et* $0 \leqslant r < b$.
q *est le* ***quotient*** *et* r *le* ***reste*** *de la* ***division euclidienne de*** a ***par*** b.

Preuve :



(i) Existence, Considérons l'ensemble $S = \{m \in \mathbb{N} / bm \leqslant a\}$. S est non vide car $0 \in S$ et majoré par $a+1$ (tout nombre plus grand que $a+1$ n'appartient pas à S), donc il admet un plus grand élément que nous noterons q. Cet entier vérifie donc la relation $qb \leqslant a < (q+1)b$.
Soit $r = a - bq$, on a d'après la relation ci-dessus $0 \leqslant r < b$. D'où le résultat.
(ii) Unicité. Supposons qu'il existe deux couples $(q;r)$ et $(q';r')$.
Ona donc $a = qb + r = q'b + r'$ et ainsi on obtient la relation $b(q - q') = r' - r$.
On peut donc en conclure que b divise $r' - r$. Or $0 \leqslant r < b$ et $0 \leqslant r' < b$



ce qui implique que $-b < r' - r < b$. b divise un $r' - r$ qui est strictement plus petit que lui en valeur absolue, donc $r' - r = 0$, ainsi $r = r'$ et $q = q'$ (car $b \neq 0$). ■

Exemple

1) La division euclidienne de 114 par 8 est $114 = 8 \times 14 + 2$ avec $0 \leqslant 2 < 8$.
2) La division euclidienne de 35 par 53 est $35 = 53 \times 0 + 35$ avec $0 \leqslant 35 < 53$
3) Déterminer la DE de 118 par 23.

II.2 Division euclidienne dans $\mathbb{Z}$

Théorème 2

Soit a et b deux entiers relatifs avec $b \neq 0$.
Il existe un unique couple $(q;r)$ d'entiers tels que $a = bq + r$ et $0 \leqslant r < |b|$.
q *est le* ***quotient*** *et* r *est le* ***reste*** *de la division*

Exemple

Déterminer la DE de 118 par -23, de -118 par 23 et de -118 par -23

Propriété 2

Soit a un entier relatif et b un entier naturel avec $b \neq 0$. On a :
(i) b divise a si et seulement si la reste de la division euclidienne de a par b est 0.
(ii) Les seuls restes possibles dans la division euclidienne de a par b sont $0, 1, \ldots, b-1$.
Ainsi, tous les entiers relatifs a peuvent s'écrirent sous la forme $a = bq + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, 1, 2, \ldots, b-1\}$.

Exemple

1) En considérant la division euclidienne par 3.
Tout entier naturel n s'écrit $3p$ ou $3p+1$ ou $3p+2$.
2)En considérant la division euclidienne par 6.
Tout entier naturel n s'écrit $6p$ ou $6p+1$ ou $6p+2$ ou $6p+3$ ou $6p+4$ ou $6p+5$.
3) En considérant la division euclidienne par 3, démontrer que 3 divise $n^3 - n$ pour tout entier naturel n.
4) a et b sont des entiers tels que $a^2 - 2b^2 = 1$.
Prouver que a est impair, puis que b est pair.

III Congruences

Définition 2

Soient a et b deux entiers relatifs et n un entier naturel, $n \geqslant 2$.
*Dire que a **est congru à** b **modulo** n signifie que $a-b$ est un multiple de n (ou $a-b$ est divisible par n).*
On note alors : $a \equiv b\,[n]$ et on lit : "a congru à b modulo n".
Autrement dit : $a \equiv b\,[n] \Leftrightarrow$ Il existe un entier relatif k tel que $a - b = kn$.

Propriété 3

Soit n un entier naturel, $n \geqslant 2$, et a, b deux entiers relatifs.
$a \equiv b\,[n] \Leftrightarrow$ les divisions euclidiennes de a et de b par n ont le même reste.

Preuve :
Notons (q, r) et (q', r') les quotients et les restes respectifs des divisions euclidiennes de a et de b par n. On a donc $a = qn + r$ et $b = q'n + r'$ avec $0 \leqslant r < n$, $0 \leqslant r' < n$ et donc $-n < r - r' < n$.

$(\Rightarrow)$ $a \equiv b\,[n] \Rightarrow a - b$ est divisible par n
$\Rightarrow$ Il existe k tel que $a - b = kn$
$\Rightarrow qn + r - q'n - r' = kn$
$\Rightarrow r - r' = n(k - q + q')$
$\Rightarrow n$ divise $r - r'$ (or $-n < r - r' < n$))
$\Rightarrow r - r' = 0$
$\Rightarrow r = r'$

$(\Leftarrow)$ Si $r = r'$ alors $a - b = qn - q'n = (q - q')n$, donc n divise $a - b$. Ainsi, $a \equiv b\,[n]$. ■

Propriété 4

Soit n un entier naturel, $n \geqslant 2$, et a, b deux entiers relatifs.
(i) $a \equiv a\,[n]$.
(ii) $a \equiv b\,[n] \Leftrightarrow b \equiv a\,[n]$.
(iii) Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$.

Preuve :
(i) $a - a = 0$ est divisible par n.
(ii) $a \equiv b\,[n]$ donc $a - b$ est divisible par n, ce qui équivaut à $b - a$ est divisible par n et donc $b \equiv a\,[n]$.
(iii) $a \equiv b\,[n]$ et $b \equiv c\,[n]$ donc il existe k et k' tel que $a = b + kn$ et $b = c + k'n$. Ainsi, on a $a = c + k'n + kn = c + (k' + k)n$ et donc $a \equiv c\,[n]$. ■

Théorème 3
Soit n un entier naturel, $n \geqslant 2$, et a, b, a', b' des entiers relatifs.
Si $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$, alors :
(i) $a + b \equiv a' + b'\,|n|$ *et* $a - b \equiv a' - b'\,[n]$.
(ii) $ab \equiv a'b'\,[n]$.
(iii) *pour tout entier naturel p,* $a^p \equiv a'^p\,[n]$.

Preuve :
$a \equiv a'\,[n]$ et $b \equiv b'\,[n]$, donc il existe k et k' tel que $a = a' + kn$ et $b = b' + k'n$.
(i) $a + b = a' + kn + b' + k'n = a' + b' + (k + k')n$ donc $a + b \equiv a' + b'\,[n]$.
(ii) $ab = (a' + kn)(b' + k'n) = a'b' + a'k'n + b'kn + kk'n^2 = a'b' + (a'k' + b'k + kk'n)n$, donc $ab \equiv a'b'\,[n]$.
(iii) On le démontre par récurrence sur p.
Initialisation : pour $p = 0$, $a^0 = a'^0 = 1$, or $1 \equiv 1\,[n]$ donc $a^0 \equiv a'^0\,[n]$.
La propriété est vrai au rang 0.
Hérédité : On suppose la prépriété vrai au rang p c'est à dire $a^p \equiv a'^p\,[n]$.
Or par hypothèse, $a \equiv a'\,[n]$, ainsi $a^p \times a \equiv a'^p \times a'\,[n]$. Et donc, $a^{p+1} \equiv a'^{p+1}\,[n]$. Donc, la propriété au rang $p + 1$.
La propriété est donc héréditaire.
Conclusion : La propriété est initialisée et héréditaire, donc elle est vrai pour tout entier naturel p. ■

Remarque
Si $a \equiv b\,[n]$ alors pour tout c $ac \equiv bc\,[n]$.
La réciproque est fausse, $6 \equiv 0\,[6]$ c'est à dire $3 \times 2 \equiv 3 \times 0\,[6]$ par contre 2 n'est pas congru à 0 modulo 6.

IV Critères de divisibilité

Soit un entier naturel a. On effectue la division euclidienne de a par 10, on sait qu'il existe un unique couple $(q; r)$ tel que $a = 10q + r$ avec $0 \leqslant r < 10$. r est le reste de la division euclidienne mais c'est aussi le chiffre des unités dans l'écriture décimale de a.
• a est divisible par 10 équivaut à $a \equiv 0\,[10]$, ce qui équivaut à $r \equiv 0\,[10]$. Or $0 \leqslant r < 10$, donc $r = 0$.
a est divisible par 10 ssi le chiffre des unités est 0.
• a est divisible par 5 équivaut à $a \equiv 0\,[5]$, ce qui équivaut à $r \equiv 0\,[5]$. Or $0 \leqslant r < 10$, donc $r = 0$ ou $r = 5$.
a est divisible par 5 ssi le chiffre des unités est 0 ou 5.
• a est divisible par 2 équivaut à $a \equiv 0\,[2]$, ce qui équivaut à $r \equiv 0\,[2]$. Or $0 \leqslant r < 10$, donc $r = 0$ ou $r = 2$ ou $r = 4$ ou $r = 6$ ou $r = 8$.
a est divisible par 2 ssi le chiffre des unités est 0, 2, 4, 6, ou 8.