Cours d'arithmétique

26 avril 2018

Définition

Soit a et b deux entiers relatifs. On dit que a divise b s'il existe un entier k tel que $b = a \times k$. Lorsque a divise b, on note $a \mid b$

On dit aussi que : a est un **diviseur** de b

b est **divisible** par a

b est un **multiple** de a

Remarque

0 est un multiple de tout entier : pour tout $n \in \mathbb{Z}, 0 \times n = 0$

Propriété

Soit a et b deux entiers

a) Si $a \mid b$ et $b \neq 0$ alors $|a| \leqslant |b|$

b) Tout entier b **non nul** a un nombre fini de diviseurs.

Propriété

Soit a et b deux entiers
a) Si $a \mid b$ et $b \neq 0$ alors $|a| \leqslant |b|$
b) Tout entier b **non nul** a un nombre fini de diviseurs.

Démonstration

a) Comme $a \mid b$, on peut écrire $b = k \times a$ avec $k \in \mathbb{Z}$ donc : $|b| = |k \times a| = |k| \times |a|$ mais $b \neq 0$ donc $k \neq 0$ et $|k| \geq 1$ et par conséquent :$|a| \leq |b|$
b) Soit b un entier non nul. Si a est un diviseur de b on a vu que : $|a| \leq |b|$ donc $-|b| \leq a \leq |b|$ et a peut prendre au maximum $2 \times |b|$ valeurs.
En revanche, 0 a une infinité de diviseurs car tous les entiers divisent 0.

Propriétés

Soit a, b et c trois entiers.

a) Si $a \mid b$ et $b \mid c$ alors $a \mid c$

b) $c \mid a$ si et seulement si $c \mid -a$

(L'ensemble des diviseurs de a est égal à l'ensemble des diviseurs de $-a$)

c)Si $c \mid a$ alors $c \mid ab$

d) Si $c \mid a$ et $c \mid b$ alors : 1) $c \mid a + b$

2) $c \mid a - b$

3) $c \mid au + bv$ avec u et v entiers

e) Soit a et b non nuls. Si $b \mid a$ et $a \mid b$ alors $a = b$ ou $a = -b$

Propriétés

Soit a, b et c trois entiers.

a) Si $a \mid b$ et $b \mid c$ alors $a \mid c$

b) $c \mid a$ si et seulement si $c \mid -a$

(L'ensemble des diviseurs de a est égal à l'ensemble des diviseurs de $-a$)

c)Si $c \mid a$ alors $c \mid ab$

d) Si $c \mid a$ et $c \mid b$ alors : 1) $c \mid a + b$

2) $c \mid a - b$

3) $c \mid au + bv$ avec u et v entiers

e) Soit a et b non nuls. Si $b \mid a$ et $a \mid b$ alors $a = b$ ou $a = -b$

Démonstration

b) Si $c \mid a$, il existe un entier k tel que : $a = k \times c$ et donc $-a = (-k) \times c$ soit $c \mid -a$

Si $c \mid -a$, il existe un entier k' tel que : $-a = k' \times c$ et donc $a = (-k') \times c$ soit $c \mid a$

Théorème

Soit a un entier et b un naturel non nul.
Il existe un unique entier q et un unique entier r tels que :

$$a = b \times q + r \text{ avec } 0 \leq r < b$$

Théorème

Soit a un entier et b un naturel non nul.
Il existe un unique entier q et un unique entier r tels que :

$$a = b \times q + r \text{ avec } 0 \leq r < b$$

Démonstration

On considère les multiples de b : $\ldots -2b, -b, 0, b, 2b, \ldots$
L'entier a est :
* soit multiple de b et dans ce cas il existe un unique entier q tel que : $a = b \times q$
* soit compris strictement entre deux multiples de b et donc il existe un unique entier q tel que :

$$bq < a < b(q+1)$$

Si on note $r = a - bq$ on a bien, dans les deux cas, $a = b \times q + r$ avec $0 \leq r < b$

Notation

a est le dividende, b est le diviseur, q est le quotient et r est le reste

Exemples

Déterminer le quotient et le reste de la division euclidienne de a par b avec :

a) $a = 325, b = 7$

b) $a = -113, b = 7$

Réponses

a) $325 = 7 \times 46 + 3$

b) $113 = 7 \times 16 + 1$ d'où $-113 = -7 \times 16 - 1$ puis $-113 = -7 \times 17 + 6$, $q = -17, r = 6$

Définition

Soit a et b deux entiers et n un entier naturel non nul.
On dit que a est **congru à** b **modulo** n si a et b ont le même reste dans la division euclidienne par n.

Notation

a est congru à b modulo n se note au choix : $a \equiv b\,(n)$ ou $a \equiv b\,[n]$ ou $a \equiv b \mod n$

Exemple

86 et 23 ont pour reste 2 dans la division euclidienne par 7 donc $86 \equiv 23\,(7)$

Théorème

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

1) $a \equiv b\,(n)$ si et seulement si $a - b$ est un multiple de n

2) Si $a \equiv r\,(n)$ et si $0 \leq r < n$ alors r est le reste de la division de a par n.

3) Si $a \equiv b\,(n)$ et $b \equiv c\,(n)$ alors $a \equiv c\,(n)$

Théorème

Soit a, b, c et r entiers et n un entier naturel non nul.
1) $a \equiv b\,(n)$ si et seulement si $a - b$ est un multiple de n
2) Si $a \equiv r\,(n)$ et si $0 \leq r < n$ alors r est le reste de la division de a par n.
3) Si $a \equiv b\,(n)$ et $b \equiv c\,(n)$ alors $a \equiv c\,(n)$

Démonstration de 1)

★ Si $a \equiv b\,(n)$ alors la division par n donne : $a = nq + r$ et $b = nq' + r$ donc $a - b = n(q - q')$: n divise $a - b$
★ Si n divise $a - b$ il existe $k \in \mathbb{Z}$ tel que $a - b = nk$ soit $a = b + nk$
La division de a par n se traduit par : $a = nq + r$ avec $0 \leq r < n$.
On a alors $b + nk = nq + r$ donc $b = n(q - k) + r$ et $0 \leq r < n$ qui se traduit par : a et b ont le même reste dans la division par n

Congruences et opérations

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

1) Si $a \equiv b\,(n)$ alors $ac \equiv bc\,(n)$

2) Si $a \equiv b\,(n)$ et $c \equiv d\,(n)$ alors : 1) $a + c \equiv b + d\,(n)$
2) $a - c \equiv b - d\,(n)$
3) $ac \equiv bd\,(n)$

3) Si $a \equiv b\,(n)$ alors, pour tout naturel p, on a : $a^p \equiv b^p\,(n)$

Définition

Soit a et b deux entiers. On note $\Delta(a;b)$ l'ensemble des diviseurs communs à a et b. Si $b \mid a$ alors $\Delta(a;b)$ est égal à l'ensemble des diviseurs de b, qu'on note $\Delta(b)$

Propriété

Si a, b, q et r sont des entiers tels que : $a = bq + r$ alors $\Delta(a;b) = \Delta(b;r)$

Démonstration

Si $d \in \Delta(a;b)$ alors $d \mid r$ car $r = a - bq$ donc $d \in \Delta(b;r)$
Si $d \in \Delta(b;r)$ alors $d \mid a$ car $a = bq + r$ donc $d \in \Delta(a;b)$

Remarque : cas particulier

Si $a \in \mathbb{Z}, b \in \mathbb{N}^*$ et $a = bq + r, 0 \leq r < b$ est la division euclidienne de a par b alors : $\Delta(a;b) = \Delta(b;r)$

Définition

Si a et b sont deux entiers non tous les deux nuls alors $\Delta(a;b)$ est un ensemble fini et on appelle PGCD de a et b le **plus grand diviseur commun** de a et b.

Notation

$\text{pgcd}(a;b)$ ou $a \wedge b$

Propriétés du PGCD

Soit a, b et r entiers non nuls.

1) $\text{pgcd}(a;b) \geq 1$
2) $\text{pgcd}(a;b) = \text{pgcd}(b;a)$
3) $\text{pgcd}(a;a) = |a|$
4) $\text{pgcd}(a;b) = \text{pgcd}(-a;b) = \text{pgcd}(a;-b)$
5) Si $b \mid a$, $\text{pgcd}(a;b) = |b|$
6) Si $a = bq + r$ alors, $\text{pgcd}(a;b) = \text{pgcd}(b;r)$

Propriétés du PGCD

Soit a, b et r entiers non nuls.

1) $\text{pgcd}(a;b) \geq 1$
2) $\text{pgcd}(a;b) = \text{pgcd}(b;a)$
3) $\text{pgcd}(a;a) = |a|$
4) $\text{pgcd}(a;b) = \text{pgcd}(-a;b) = \text{pgcd}(a;-b)$
5) Si $b \mid a$, $\text{pgcd}(a;b) = |b|$
6) Si $a = bq + r$ alors, $\text{pgcd}(a;b) = \text{pgcd}(b;r)$

Principe de l'algorithme d'Euclide pour calculer le pgcd

Soit a et b deux entiers naturels non nuls tels que b ne divise pas a. Alors $\text{pgcd}(a;b)$ est le **dernier reste non nul** de la suite des divisions de l'algorithme d'Euclide.

Si $r_1, r_2, ..., r_n$ est la suite de restes non nuls, on a :

$\Delta(a;b) = \Delta(b;r_1) = ...\Delta(r_{n-1};r_n) = \Delta(r_n)$

Exemple 1

Calculer $\text{pgcd}(8820; 3150)$

Solution $8820 = 3150 \times 2 + 2520$

$3150 = 2520 \times 1 + 630$

$2520 = 630 \times 4 + 0$ donc $\text{pgcd}(8820; 3150) = 630$

Propriétés

Soit a et b deux entiers non nuls et $d = pgcd(a; b)$

1) L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de d

2) Il existe des entiers u et v tels que : $d = au + bv$

3) Pour $k \in \mathbb{N}^*$, $pgcd(ka; kb) = k \times pgcd(a; b)$

Démonstration

1)$\Delta(a;b) = \Delta(d)$ d'après l'algorithme d'Euclide.
2) Soit $E = \{au + bv \text{ avec } u, v \in \mathbb{Z}\}$
Si $u = 1, v = 0$, on voit que $a \in E$ Si $u = -1, v = 0$, on voit que $-a \in E$ Si $u = 0, v = 1$, on voit que $b \in E$
E contient au moins un entier strictement positif. Soit δ le plus petit d'entre eux ; il existe u_0 et v_0 entiers tels que : $\delta = au_0 + bv_0$
Soit $au + bv$ un élément quelconque de E La division euclidienne de cet élément par δ donne $au + bv = \delta q + r, 0 \leq r < \delta$ d'où :
$r = au + bv - q(au_0 + bv_0) = a(u - qu_0) + b(v - qv_0)$

Démonstration

1)$\Delta(a;b) = \Delta(d)$ d'après l'algorithme d'Euclide.
2) Soit $E = \{au + bv \text{ avec } u, v \in \mathbb{Z}\}$
Si $u = 1, v = 0$, on voit que $a \in E$ Si $u = -1, v = 0$, on voit que $-a \in E$ Si $u = 0, v = 1$, on voit que $b \in E$
E contient au moins un entier strictement positif. Soit δ le plus petit d'entre eux ; il existe u_0 et v_0 entiers tels que : $\delta = au_0 + bv_0$
Soit $au + bv$ un élément quelconque de E La division euclidienne de cet élément par δ donne $au + bv = \delta q + r, 0 \leq r < \delta$ d'où :
$r = au + bv - q(au_0 + bv_0) = a(u - qu_0) + b(v - qv_0)$
Par suite, $r \in E$ et $0 \leq r < \delta$, mais d'après la définition de δ :
$r = 0$ donc **tout élément de E est multiple de** δ.
$\delta \mid a$ et $\delta \mid b$ donc $\delta \mid d = pgcd(a;b)$.
Réciproquement, $d \mid a$ et $d \mid b$ donc aussi $d \mid au_0 + bv_0$
c'est-à-dire, $d \mid \delta$. Conclusion : $d = \delta$

Définition

Soit a et b deux entiers non nuls. On dit que a et b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$

Théorème

Soit a, b et d des entiers non nuls.
$\text{pgcd}(a, b) = d$ si et seulement si, il existe deux entiers non nuls a' et b' tels que : $a = da', b = db'$ et $a' \wedge b' = 1$

Définition

Soit a et b deux entiers non nuls. On dit que a et b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$

Théorème

Soit a, b et d des entiers non nuls.
$\text{pgcd}(a, b) = d$ si et seulement si, il existe deux entiers non nuls a' et b' tels que : $a = da', b = db'$ et $a' \wedge b' = 1$

Démonstration

Si $d = \text{pgcd}(a, b), d \mid a, d \mid b$ donc il existe $a', b' \in \mathbb{Z}^*$ tels que : $a = da', b = db'$
Soit $r = \text{pgcd}(a', b')$ alors $\text{pgcd}(da', db') = dr = d$ donc $dr = d$ avec $d \neq 0$ donc $r = 1$ et $a' \wedge b' = 1$
Réciproquement, si $a = da', b = db'$ et $a' \wedge b' = 1$ alors $\text{pgcd}(da', db') = d \times \text{pgcd}(a', b') = d$

Théorème de Bézout

Deux entiers non nuls a et b sont premiers entre eux si et seulement si, il existe des entiers u et v tels que : $au + bv = 1$

Théorème de Bézout

Deux entiers non nuls a et b sont premiers entre eux si et seulement si, il existe des entiers u et v tels que : $au + bv = 1$

Démonstration

Si a et b premiers entre eux, $\text{pgcd}(a, b) = 1$ et donc il existe deux entiers u et v tels que $au + bv = 1$
Réciproquement, si $au + bv = 1$ et $d \mid a$ et $d \mid b$ alors $d \mid au + bv$ donc d divise 1. Les seuls diviseurs communs à a et b sont -1 et 1 et $a \wedge b = 1$

Théorème

Soit a, b_1 et b_2 des entiers non nuls.
Si $a \wedge b_1 = 1$ et $a \wedge b_2 = 1$ alors $a \wedge (b_1 b_2) = 1$

Théorème

Soit a, b_1 et b_2 des entiers non nuls.
Si $a \wedge b_1 = 1$ et $a \wedge b_2 = 1$ alors $a \wedge (b_1 b_2) = 1$

Démonstration

Si $a \wedge b_1 = 1$ il existe u, v tels que $au + b_1 v = 1$
Si $a \wedge b_2 = 1$ il existe u', v' tels que $au' + b_2 v' = 1$
donc :
$(au + b_1 v)(au' + b_2 v') = 1 = a(auu' + b_2 uv' + b_1 u' v) + (b_1 b_2)(vv')$
donc $a \wedge (b_1 b_2) = 1$

Théorème de Gauss

Soit a, b, c entiers avec a, b non nuls.
Si a divise bc et a premier avec b alors a divise c.

Théorème de Gauss

Soit a, b, c entiers avec a, b non nuls.
Si a divise bc et a premier avec b alors a divise c.

Démonstration

Comme $a \wedge b = 1$ il existe u, v tels que $au + bv = 1$ donc
$cau + cbv = c$
a divise acu et bcv donc a divise c.

Théorème

Un entier n divisible par a et b tels que $a \wedge b = 1$ est divisible par ab.

Théorème

Un entier n divisible par a et b tels que $a \wedge b = 1$ est divisible par ab.

Démonstration

Si $a \mid n$ il existe un entier k tel que $n = ak$.
Si $b \mid n$ alors $b \mid ak$ et comme $a \wedge b = 1$, d'après Gauss, $b \mid k$. Il existe donc k' tel que $k = bk'$ et on a alors $n = ak = abk'$ donc n est divisible par ab

Définition

Un entier naturel est dit **premier** s'il admet exactement deux diviseurs positifs (1 et lui-même)

Remarque

1 n'est pas premier.

Théorème

Tout $n \in \mathbb{N}$ avec $n \geq 2$ admet au moins un diviseur premier.
Si n n'est pas premier et $n \geq 2$ alors il admet un diviseur premier compris entre 2 et $\sqrt{n}$

Théorème

Tout $n \in \mathbb{N}$ avec $n \geq 2$ admet au moins un diviseur premier.
Si n n'est pas premier et $n \geq 2$ alors il admet un diviseur premier compris entre 2 et $\sqrt{n}$

Démonstration

Si n est premier, il admet bien un diviseur premier : lui-même.
Si n n'est pas premier alors il admet un plus petit diviseur positif $p \neq 1$. p est premier sinon p aurait lui-même un diviseur positif différent de 1 qui serait un diviseur de n, mais plus petit que p.
De plus, n peut s'écrire $n = p \times r$ avec $p \leq r$ donc $p^2 \leq p \times r$ soit $p^2 \leq n$ et $p \leq \sqrt{n}$

Remarque

On utilise ce théorème de la manière suivante :
Si un naturel $n \geq 2$ n'admet pas de diviseur premier compris entre 2 et $\sqrt{n}$ alors n est premier.

Exemple

Pour savoir si 631 est premier, il suffit de tester tous les nombres premiers inférieurs à $\sqrt{631} \approx 25,12$

Théorème

Il existe une infinité de nombres premiers.

Démonstration **ROC**

On suppose qu'il existe un nombre fini de nombres premiers $p_1, p_2, ..., p_n$

Soit $N = p_1 \times p_2 \times .... \times p_n + 1$

N n'est pas premier car pour tout i de 1 à n, $N > p_i$.

N admet donc un diviseur premier dans la liste $p_1, p_2, ..., p_n$.

Soit p_k ce diviseur premier de N.

p_k divise N et p_k divise $p_1 \times p_2 \times .... \times p_n$ donc

p_k divise $N - p_1 \times p_2 \times .... \times p_n$, soit p_k divise 1 : la seule possibilité est que $p_k = 1$ qui est impossible car p_k est premier.

Théorème

Tout entier naturel strictement supérieur à 1 admet une décomposition, unique à l'ordre des facteurs près, en produit de nombres premiers.

Exemple

$72 = 2^3 \times 3^2$