Arithmétique

MAGAZINE DE MATHEMATIQUES

Profs : *ÉQUIPE* ACADEMIQUE *MATHEMATIQUES*

Arithmétiques

Euclide, en grec ancien Εὐκλείδης *Eukleidês* (né vers -325, mort vers -265 à Alexandrie) est un mathématicien de la Grèce antique ayant probablement vécu en Afrique, auteur des *Éléments*, qui sont considérés comme l'un des textes fondateurs des mathématiques modernes.

Johann Carl Friedrich Gauß (traditionnellement transcrit **Gauss** en français) (30 avril 1777 — 23 février 1855) est un mathématicien, astronome et physicien allemand. Doté d'un grand génie, il a apporté de très importantes contributions à ces trois sciences. Surnommé « le prince des mathématiciens », il est considéré comme l'un des plus grands mathématiciens de tous les temps.

Bezout (Étienne), mathématicien, né à Nemours en 1730, m. en 1783, fut placé par M. de Choiseul en 1763 à la tête de l'instruction de la marine royale, fut chargé en 1768 de l'enseignement des élèves du corps de l'artillerie, et rédigea pour ses élèves des cours qui eurent un grand succès. Les principaux sont : *Cours de mathématiques à l'usage de l'artillerie*; *Cours de Mathématiques à l'usage de da marine*, 1764; *Théorie des équations algébriques*, 1779. Bezout est simple, clair, et sait se mettre à la portée des jeunes esprits : aussi ses ouvrages sont-ils restés classiques.

RESUME DU COURS

Divisibilité dans Z

1. Diviseurs et multiples d'entiers

Définition

Soit a un entier et d un entier non nul. On dit que :
d divise a $\Leftrightarrow$ il existe un entier k tel que $a = kd$

Remarque

Soit a un entier et d un entier non nul.
1/ Quand d divise a on dit aussi que a est un multiple de d.
2/ L'ensemble des multiples de d est $\{kd;\ k \in \mathbb{Z}\}$ noté $d\mathbb{Z}$.

Théorème

Soient a et b deux entiers non nuls et c un entier.
- ⊙ **si** b divise a **alors** $(-b)$ divise a
- ⊙ **si** b divise a **et** a divise b **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 $\alpha a+\beta c;\ \forall(\alpha,\beta) \in \mathbb{Z}^2$

2. Division euclidienne dans Z

Rappel

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

Définition

Soit a un entier et b un entier non nul.
• On appelle $\boxed{\texttt{quotient}}$ de a par b l'entier q défini par :

Premier cas : b divise a alors $q=\frac{a}{b}$

Deuxième cas : b ne divise pas a alors

Si $b > 0$ **alors** q est le plus grand entier inférieur ou égal à $\frac{a}{b}$.

autrement $q = E\left(\frac{a}{b}\right)$

Si $b < 0$ **alors** q est le plus petit entier supérieur ou égal à $\frac{a}{b}$.

autrement $q = E\left(\frac{a}{b}\right) + 1$.

• • On apelle **reste** de a par b l'entier $r = a - bq$ où q est le quotient de a par b.

Conséquence

Pour tout entier a et pour tout entier b non nul, il existe un couple unique d'entiers (q, r) tels que $a = qb + r$ et $0 \leqslant r < |b|$.

Remarque

$0 \leqslant r < |b| \iff r \in \{0;1;2;\ldots;|b|-1\}$.

3. Congruence dans Z

Définition

Soit n un entier naturel non nul et a et b deux entiers. On dit que a est congru à b modulo n (ou a et b sont congru modulo n)

$\Updownarrow$

il existe $k \in \mathbb{Z}$ tel que $a - b = kn$

On note $a \equiv b \pmod{n}$ ou aussi $a \equiv b \ [n]$

Théorème

Soient n un entier naturel non nul et a et b deux entiers.
Désignons par r et r' les restes respectifs de a et b dans la division euclidienne par n. On a:

$$a \equiv b \ [n] \iff r \equiv r' \ [n]$$

Théorème

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

- ⊙ **si** $a \equiv b \ [n]$ **alors** $b \equiv a \ [n]$
- ⊙ **si** $a \equiv b \ [n]$ **et** $b \equiv c \ [n]$ **alors** $a \equiv c \ [n]$
- ⊙ **si** $a \equiv b \ [n]$ **alors** $ca \equiv cb \ [n]$
- ⊙ **si** $a \equiv b \ [n]$ **alors** $a^m \equiv b^m \ [n]$ avec $m \in \mathbb{N}^*$.
- ⊙ **si** $a \equiv b \ [n]$ **et** $c \equiv d \ [n]$ **alors** $a + c \equiv b + d \ [n]$
- ⊙ **si** $a \equiv b \ [n]$ **et** $c \equiv d \ [n]$ **alors** $a \times c \equiv b \times d \ [n]$

Identité de Bezout

1. PGCD de deux entiers

Définition

Soient a et b deux entiers non nuls.
Le plus grand élément de $D_a \cap D_b$ est dit le plus grand commun diviseur de a et b et il est noté $a \wedge b$.

Remarque:: $D_a \cap D_b = D_{|a|} \cap D_{|b|} \Rightarrow \boxed{a \wedge b = |a| \wedge |b|}$

Théorème

Soient a, b et k trois entiers non nuls et $d = a \wedge b$. On a :
k divise a et b $\Leftrightarrow$ k / d.

Propriétés

Soient a et b deux entiers non nuls.
- ⊙ **si** b divise a **alors** $a \wedge b = |b|$.
- ⊙ **si** $a \equiv c \ [b]$ et $c \in \mathbb{Z}^*$ **alors** $a \wedge b = b \wedge c$.
- ⊙ $a \wedge b = b \wedge a$.
- ⊙ Pour tout entier non nul k, $ka \wedge kb = |k| \ (a \wedge b)$.
- ⊙ $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

2. Entiers premiers entre eux

Définition

Soient a et b deux entiers non nuls.
a et b sont dits premiers entre eux $\Leftrightarrow$ $a \wedge b = 1$.

Remarque

Soient a et b deux entiers non nuls et $d = a \wedge b$. On a les entiers $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont premiers entre eux.

lemme de Gauss

$a \in \mathbb{Z}^*$, $b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}^*$. On a :
Si $a / (bc)$ **et** $a \wedge b = 1$ **alors** a / c

Théorème

Soient a et b deux entiers naturels non nuls et n un entier.

Si $\begin{cases} a \wedge b = 1 \\ n \equiv 0 \pmod{a} \\ n \equiv 0 \pmod{b} \end{cases}$ **alors** $n \equiv 0 \pmod{ab}$

3. PPCM de deux entiers

Théorème et **Définition**

Si a et b sont deux entiers non nuls **alors** il existe un unique entier **naturel** non nul m qui vérifie les deux conditions suivantes:

1. m est un multiple de a et b.

2. **Si** un entier k est un multiple commun a et b **alors** k est un multiple de m

★ L'entier m défini plus haut est noté $a \vee b$ et appelé le plus petit commun multiple de a et b.

Propriétés

Soient a et b deux entiers non nuls.

1) $a \vee b = |a| \vee |b|$
2) $(a \vee b) \times (a \wedge b) = |ab|$
3) **si** b divise a **alors** $a \vee b = |a|$.
4) $a \vee b = b \vee a$.
5) Pour tout entier non nul k, $ka \vee kb = |k|\,(a \vee b)$.
6) $a \vee (b \vee c) = (a \vee b) \vee c$.

4. Identité de Bezout

Théorème

Soit a et b deux entiers naturels non nuls tels que $b \geqslant 2$ et $a \wedge b = 1$.
Il existe un unique entier non nul u appartenant à $\{0, 1, 2, \dots, (b-1)\}$ tel que $ua \equiv 1 \pmod{b}$. On dit que u est l'inverse de a modulo b.

Théorème *(Identité de Bezout)*

Soient a et b deux entiers non nuls. On a:
$a \wedge b = 1 \iff$ Il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels que $au + bv = 1$.

Conséquence

Soient a et b deux entiers non nuls. On a:
$d = a \wedge b \iff$ Il existe deux entiers u et v tels que $au + bv = d$.

Théorème

Soient a, b et c trois entiers non nuls et $d = a \wedge b$. On a:
L'équation $ax + by = d$ admet des solutions dans $\mathbb{Z} \times \mathbb{Z}$ si et seulement si d divise c.