NETSCHOOL1
ACADEMY

Mathématiques

Classe : BAC

Chapitre : Divisibilité-Identité de Bézout

NETSCHOOL1
ACADEMY

Divisibilité dans $\mathbb{Z}$

Diviseurs et multiples d'un entier

Définition :
Soient a et b deux entiers relatifs tels que $b \neq 0$.

✓ On dit que b divise a sill existe un entier relatif q tel que : $a = bq$. On note $b|a$.

✓ On dit également que a est un multiple de b ou que b est un diviseur de a.

Remarque : si a n'est pas un multiple de b alors b ne divise pas a.
Conséquences :

✓ Tout entier a est divisible par 1 et -1 .

✓ Soit a un entier non nul. Si a divise 1 alors $a = 1$ ou $a = -1$

✓ Soit a et b deux entiers tels que $b \neq 0$. Si b divise a alors $\forall k \in Z$ et $\forall n \in \mathbb{N}^*, b$ divise ak et b divise a^n.

Propriétés :
Soient a , b et c trois entiers.

✓ Si $a|b$ et $b|a$ alors $a = \pm b$.

✓ Si $a|b$ et $b|c$ alors $a|c$

✓ si $c|a$ et $c|b$ alors $c|(au + bv)$ quels que soient u et v entiers relatifs.
On dit que c divise toute combinaison linéaire de a et de b a coefficients entiers.

Division euclidienne dans $\mathbb{Z}$

Théorème :
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe un unique couple (q, r) d'entiers relatifs tels que : $a = b \times q + r$ avec $0 \leq r < |b|$.
q est le quotient et r est le reste.
Détermination du quotient :

$$\text{Si } b > 0 \text{ alors } q = E\left(\frac{a}{b}\right) \quad \text{Si } b < 0 \text{ alors } q = -E\left(-\frac{a}{b}\right)$$

Congruence modulo n

Définition :
Soient a et b deux entiers relatifs et n un entier naturel non nul. On dit que a est congru à b modulo n ou que a et b sont congrus modulo n si $a - b$ est un multiple de n . On note $a \equiv b \pmod{n}$
Conséquences :
Soient a et b deux entiers relatifs et n un entier naturel non nul.

✓ $a \equiv b \pmod{n} \iff n$ divise $a - b$

✓ $a \equiv 0 \pmod{n} \iff n$ divise a

✓ Soit d un entier naturel non nul.
Si $a \equiv b \pmod{n}$ et d divise $n \Rightarrow a \equiv b \pmod{d}$

Théorème :
Soit n un entier naturel non nul. Pour tout entier a, il existe un unique entier r appartient a $\{0, 1, \ldots, n-1\}$ tel que $a \equiv r \pmod{n}$.
On dit que r est le reste modulo n de a.

Congruence modulo n (suite)

Propriété réciproque :
Soient a entier relatif et n entier naturel non nul.
Si $a \equiv r \pmod n$ et $0 \leq r < n$ alors r est le reste dans la division euclidienne de a par n.
Propriété :
Soient a, b et c trois entiers et n un entier naturel non nul.

✓ $a \equiv a \pmod n$.

✓ $a \equiv b \pmod n \Leftrightarrow b \equiv a \pmod n$

✓ $a \equiv b \pmod n \Leftrightarrow b \equiv a \pmod n$

✓ Si $a \equiv b \pmod n$ et $b \equiv c \pmod n$ alors $a \equiv c \pmod n$

Propriété :
Soient a, b, a' et b' quatre entiers relatifs et n entier naturel non nul. La congruence est compatible avec l'addition.

1. si $a \equiv b \pmod n$ et $a' \equiv b' \pmod n$ alors : $a + a' = b + b' \pmod n$
2. Quel que soit $c \in \mathbb{Z}$: si $a = b \pmod n$ alors : $a + c = b + c \pmod n$
3. Si $a = b \pmod n$ et $a' = b' \pmod n$ alors : $a \times a' = b \times b' \pmod n$
4. Quel que soit k entier naturel non nul: si $a \equiv b \pmod n$ alors : $a^k \equiv b^k \pmod n$
5. Quel que soit $c \in \mathbb{Z}$: si $a = b \pmod n$ alors : $a \times c = b \times c \pmod n$
   En particulier: si $a \equiv b \pmod n$ alors : $(-a) \equiv (-b) \pmod n$
6. si $a = b \pmod n$ et $a' = b' \pmod n$ alors : $a - a' = b - b' \pmod n$

Petit théorème de Fermat

Pour tout entier naturel a et pour tout nombre premier p ne divisant pas a. On a : $a^{p-1} \equiv 1 \pmod p$.
Remarque : si p est premier alors a est premier avec p si et seulement si p ne divise pas a

Corollaire

Soit p un nombre premier, quel que soit a entier naturel: $a^p \equiv a \pmod p$

Identité de Bezout

$PGCD$ de deux entiers

Soient a et b deux entiers naturels non nuls. Notons $D(a)$ l'ensemble des diviseurs de a et $D(b)$ celui des diviseurs de b.
L'ensemble de leurs diviseurs communs est noté: $D(a,b)$ avec $D(a,b) = D(a) \cap D(b)$.
1 divise a et b donc $D(a,b)$ n'est pas vide.
De plus, a et b admettant un nombre fini de diviseurs, leurs diviseurs communs sont en nombre fini.
$D(a,b)$ étant un sous ensemble fini et non vide de $\mathbb{N}$, il admet donc un plus grand élément d.
Définition du pgcd de deux entiers naturels non nuls :
Soient a et b deux entiers naturels non nuls. On appelle plus grand commun diviseurs de a et b l'entier naturel noté $d = \text{pgcd}(a,b)$ ou $d = a \wedge b$ tel que :

✓ d divise a et b

✓ Tout diviseur commun à a et b est un diviseur de d.

Remarque :
Soient a et b deux entiers naturels non nuls,

✓ si $a = bq + r$ avec q et r entiers naturels non nuls alors $pgcd(a,b) = pgcd(b,r)$

✓ si b divise a alors $pgcd(a,b) = b$.

✓ $a \wedge b$ est le dernier reste non nul dans la succession des divisions euclidiennes de l'algorithme d'Euclide de a par b.

PGCD de deux entiers (suite)

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

♠ d divise a et b.

♠ L'entier d est appelé plus grand commun diviseurs de a et b et noté $d = a \wedge b$ ou $d = \text{pgcd}(a,b)$

Conséquences :

✓ Pour tous entiers non nuls a et b , $a \wedge b$ est un entier naturel non nul.

✓ Pour tous entiers non nuls a et b , $\text{pgcd}(a,b) = \text{pgcd}(b,a)$.

✓ Si a et b sont des entiers relatifs non nuls: $p\text{gcd}(a,b) = p\text{gcd}(|a|,|b|)$

Propriétés :
soient a et b deux entiers non nuls

✓ si $b|$ a alors pgcd $(a,b) = |b|$.

✓ Si $a = bq + r$ avec q et r entiers naturels non nuls alors $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.

✓ $a \wedge b = b \wedge a$.

✓ Pour tout entier non nul $k, (ka) \wedge (kb) = |k|(a \wedge b)$.

✓ Pour tout entier non nul $c_s a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Nombres premiers

Définition :
Soit p un entier naturel. On dit que p est un nombre premier s'il admet exactement 2 diviseurs entiers naturels distincts. Diviseurs qui sont 1 et lui-même. (puisque 1 divise tout nombre et tout nombre est diviseur de lui-même.)
Remarque : A ce jour, il n'existe toujours pas de critère ou de formule qui permette instantanément de dire si un nombre quelconque est premier.
Théorème 1 :
Soit $n \in \mathbb{N}$ si $n \geq 2$ alors n admet au moins un diviseur premier.
Théorème 2 :
Soit $n \in \mathbb{N}$ avec $n \geq 2$. Si n n'est pas premier admet au moins un diviseur premier p tel que : $p \leq \sqrt{n}$
Théorème 3 : (contraposée du théorème 2) :
Si n n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$ alors n est premier.
Théorème 4 :
L'ensemble P des nombres premiers est infini.
Théorème 5 : (DECOMPOSITION D'UN ENTIER EN PRODUIT DE FACTEURS PREMIERS)
Tout entier $n \geq 2$ se décompose de façon unique sous la forme : $\text{n} = \text{p}_1^{\alpha_1}\text{xp}_2^{\alpha_2}\text{x}\ldots\text{xp}_\text{m}^{\alpha_\text{m}}$ *Où* : $p_1, p_2, \ldots p_m$ sont des nombres premiers tels que : $p_1 < p_2 < \ldots < p_m$ et $\alpha_1, \alpha_2, \ldots, \alpha_m$ sont des entiers naturels non nuls.
L'écriture de n sous cette forme est appelée décomposition de n en produit de facteurs premiers.

Nombres premiers entre eux

Définition :
Soient a et b deux entiers relatifs non tous nuls. a et b sont dits premiers entre eux si pgcd $(a,b) = 1$
Remarques :

1. Deux nombres premiers entre eux ont donc 1 pour seul diviseur positif commun.
2. Si a est un nombre premier et que a ne divise pas b alors a et b sont premiers entre eux.

Théorème :
Soient a et b deux entiers non nuls. pgcd $(a,b) = d \Leftrightarrow$ il existe a' et b ' entiers tels que:$a = da'$ et $b = db'$ avec pgcd $\left(a', b'\right) = 1$

Nombres premiers entre eux (suite)

Lemme de Gauss :
Soient a, b et c trois entiers relatifs non nuls.
Si a divise bc et a et b premiers entre eux alors a divise c.
Théorème :
Soient a et b deux entiers naturels non nuls et n un entier.

$$\text{Si} \quad \left.\begin{array}{c} a \wedge b = 1 \\ n = 0 (\text{mod}\, a) \\ n = 0 (\text{mod}\, b) \end{array}\right\} \quad \text{alors} \quad n = 0 (\text{mod}\, ab)$$

Conséquence :
Soient n et m deux entiers naturels non nuls et premiers entre eux . x et x_0 deux entiers.

$$\left.\begin{array}{c} x = x_0 (\text{mod}\, n) \\ x = x_0 (\text{mod}\, m) \end{array}\right\} \Longleftrightarrow x = x_0 (\text{mod}\, m.n)$$

PPCM de deux entiers

Théorème et définition :
Pour tous entiers non nuls a et b , il existe un unique entier naturel non nul M qui vérifie les deux conditions suivantes:

- M est un multiple de a et de b.
- Tout multiple de commun de a et b est un multiple de M .
  L'entier M ainsi défini est le plus petit commun multiple de a et b et est noté $a \vee b$

Conséquence :

- $a \vee b = |a| \vee |b|$.
- $a \vee b = d \cdot \left|a' \cdot b'\right|$ tels que $d = a \wedge b, a = a' \cdot d$ et $b = b' \cdot d$.
- $(a \vee b)(a \wedge b) = |a \cdot b|$

Propriétés :
Soient a et b deux entiers non nuls.

- si b divise a alors $a \wedge b = |a|$.
- Pour tout entier non nul k, $(ka) \vee (kb) = |k|(a \vee b)$.
- Pour tout entier non nul c, $a \vee (b \vee c) = (a \vee b) \vee c$

Théorème :
Soient a et b deux entiers non nuls tels que $b \geq 2$ et $a \wedge b = 1$.
Il existe un unique entier non nul u appartenant &$\{1, \ldots, b-1\}$ tel que $au \equiv 1 (\text{mod}\, b)$.
On dit que u est un inverse de a modulo b.
EXEMPLE : 3 est un inverse de 5 modulo 7.

Identité de Bezout

Théorème de Bezout :
Deux entiers non nuls a et b sont premiers entre eux, si et seulement si, il existe deux entiers u et v tels que $au + bv = 1$
Application :
Soient a, b et c trois entiers non nuls. Montrer que

✓ Si $a \wedge b = 1$ et $a \wedge c = 1$ alors $a \wedge (bc) = 1$.

✓ si $a \wedge b = 1$ alors $a \wedge b^2 = 1$

✓ Pour tout entier naturel n, si $a \wedge b = 1$ alors $a \wedge b^n = 1$

Corollaire :
Si a et b deux entiers non nuls et $d = a \wedge b$ alors il existe deux entiers u et v tels que $d = au + bv$.
Attention : La réciproque n'est pas vraie.

Définition :
Toute équation (E) du type : $ax+by=c$ où a,b et c sont des entiers relatifs et où les inconnues x et y sont des entiers relatifs est appelée équation diophantienne.
Théorème :
Soient a,b et c trois entiers et $d=a\wedge b$. L'équation $ax+by=c$ admet des solutions dans Z^2 si et seulement si, d divise c.

EQUATIONS DIOPHANTIENNES : EXISTENCE DE SOLUTIONS

Étape 1 :
A quelle condition (E) admet-elle au moins une solution?
L'équation $(E):ax+by=c$ admet au moins une solution si et seulement si $a\wedge b$ divise c.
Remarque :

1. La premiere chose a faire est évidemment de calculer le PGCD de a et de b
2. Si a et b sont premiers entre eux, (E) admet des solutions quel que soit c.

Étape 2 : Recherche d'une solution particulière.
Trois cas de figure sont possibles:

- Soit la solution particulière est donnée par le texte et il ne reste qu'a vérifier qu'elle est bien solution de (E).
- Soit il y a une solution particulière évidente.
- Soit il faut trouver cette solution par le calcul.

Prenons un exemple concret: $(E):616x+585y=12$

Première méthode
$616=585\times1+31$
$585=31\times18+27$
$31=27\times1+4$
$27=4\times6+3$
$4=3\times1+1$
$3=1\times3+0$

Le dernier reste non nul est 1 donc $pgcd(616,585)=1$. 1 divise 12 donc ce qui est certain c'est que l'équation a des solutions.
Voici maintenant la technique a adopter pour remonter la suite de divisions.

Exprimer le PGCD : $1=4-3\times1$
Remplacer le reste précédent : $1=4-(27-4\times6)\times1$
Factoriser : $1=4\times7-27\times1$
Remplacer le reste précédent : $1=(31-27\times1)\times7-27\times1$
Factoriser : $1=31\times7-27\times8$
Remplacer le reste précédent : $1=31\times7-(585-31\times18)\times8$
Factoriser : $1=31\times151-585\times8$ Remplacer le reste précédent : $1=(616-585\times1)\times151-585\times8$ Factoriser : $1=616\times151+585\times(-159)$
Multiplier par 12 : $12=616\times1812+585\times(-1908)$

Et vue la probabilité de se tromper dans ce genre de manipulation, il est conseillé de vérifier le résultat trouvé:
En effet, la calculatrice confirme que : $616\times1812+585\times(-1908)=12$
Une solution particulière de (E) est donc le couple ($1812;-1908$).

Deuxième méthode

		1	18	1	6	1	3
0	1	1	19	20	139	159	616
1	0	1	18	19	132	151	585