Arithmétique, cours, Terminale, maths expertes

F.Gaudon

27 février 2024

Table des matières

1 Divisibilité dans l'ensemble des entiers relatifs

Définition :

Soi a et b deux entiers relatifs. On dit que :

- a est *multiple* de b s'il existe un entier relatif k tel que $a = kb$. On note $b|a$.
- Si $b \neq 0$, b est un *diviseur* de a s'il existe un entier relatif k tel que $a = kb$, c'est à dire si a est un multiple de b.

Si b est un diviseur de a, on dit aussi que b *divise* a et que a est *divisible* par b.

Exemple :

L'ensemble des diviseurs de 8 est l'ensemble $\{\pm 1; \pm 2; \pm 4 \pm 8\}$.

Remarques :

- On a les équivalences suivantes :

$$b|a \Leftrightarrow (-b)|a \Leftrightarrow b|(-a) \Leftrightarrow (-b)|(-a)$$

- Si n est un entier naturel non nul, tout diviseur positif de n est donc compris entre 1 et n : tout entier naturel a donc un nombre fini de diviseurs.

Propriétés :

Soient a, b et c trois entiers relatifs avec $c \neq 0$.

- Si c divise a et b, alors c divise $a + b$ et $a - c$.
  De manière plus générale, c divise toute *combinaison linéaire* de a et de b, c'est à dire tout entier relatif $am + bn$ où m et n sont deux entiers relatifs.
- On suppose en outre $b \neq 0$. Si c divise b et si b divise a, alors c divise a, propriété dite de *transitivité*.

Preuve :

- c divise a et c divise b. donc il existe des réels k_1 et k_2 tels que $a = k_1 c$ et $b = k_2 c$. Alors $a + b = (k_1 + k_2)c$ d'où c divise $a + b$.
  De même, $a - b = (k_1 - k_2)c$ donc c divise $a - b$.
  De même, pour tous les entiers relatifs m et n, $ma + nb = (mk_1 + nk_2)c$ donc c divise $ma + nb$.
- Si c divise b et b divise a, alors il existe deux réels k_1 et k_2 tels que $b = k_1 c$ et $a = k_2 b$. D'où $a = k_2 k_1 c$ donc c divise a.

Exemples d'application :

- Cherchons l'ensemble des entiers naturels n et p tels que $3n + 2np = 9$.
  L'équation s'écrit $n(3 + 2p) = 9$ ce qui signifie que n divise 9.
  Or l'ensemble des diviseurs positifs de 9 est $\{1; 3; 9\}$.
  Donc $n = 1$ ou $n = 3$ ou $n = 9$.
  Si $n = 1$ alors $3 + 2p = 9$ donc $2p = 6$ et $p = 3$.
  Si $n = 3$ alors $3 + 2p = 3$ donc $p = 0$.
  Si $n = 9$ alors $3 + 2p = 1$ donc $p = -1$ mais on cherche p entier naturel donc cette solution ne convient pas.
  On vérifie que $(n; p) = (1; 3)$ et $(n; p) = (3; 0)$ conviennent bien.
- Cherchons l'ensemble des entiers naturels n tels que $n + 1$ divise $2n + 5$.
  Comme $n + 1$ divise aussi $n + 1$ on peut affirmer que $n + 1$ divise $2(n + 1)$ donc $2n + 2$ et donc $2n + 5 - (2n + 2) = 3$.
  Donc $n + 1$ divise 3. Or, l'ensemble des diviseurs de 3 est $\{\pm 1; \pm 3\}$. Comme l'entier n cherché est un entier positif, $n+1$ aussi donc $n+1 = 1$ ou $n+1 = 3$ d'où $n = 0$ ou $n = 2$.
  On vérifie bien que si $n = 0$, alors $n + 1 = 1$ qui divise $2n + 5 = 7$ et si $n = 2$, alors $n + 1 = 3$ qui divise $2n + 5 = 9$.

2 Division euclidienne

Théorème et définition, théorème de la division euclidienne :
Soient a et b deux entiers naturels avec $b \neq 0$.
Il existe un unique couple $(q; r)$ d'entiers naturels tels que $a = bq + r$ avec $0 \leq r < b$.
On dit que a est le *dividende*, b est le *diviseur*, q le *quotient* et r le *reste* dans la *division euclidienne* de a par b.

Exemple :
La division euclidienne de 121 par 19 s'écrit $121 = 19 \times 6 + 7$.
121 est le dividende, 19 le diviseur, 6 le quotient et 7 le reste. Attention : la division euclidienne de 121 par 6 ne s'écrirait pas ainsi car 7 est supérieur à 6. Elle s'écrirait $121 = 6 \times 20 + 1$ où le reste 1 est bien inférieur au diviseur 6.

Théorème et définition, théorème de la division euclidienne dans $\mathbb{Z}$:
Soit a un entier *relatif* et b un entier *naturel* non nul.
Il existe un unique couple $(q;r)$ d'entiers *relatifs* tels que $a = bq + r$ avec $0 \leq r < b$.
On dit que a est le *dividende* , b est le *diviseur*, q le *quotient* et r le *reste* dans la *division euclidienne* de a par b.

Remarque :
b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Propriété :
Soit b un entier naturel supérieur ou égale à 2. Tout entier naturel s'écrit sous une, et une seule, des formes bq, $bq+1$, $bq+2$,...,$bq+(b-1)$ où q est un entier relatif.

Propriété :
Soit a un entier supérieur ou égal à 2.
Parmi a entiers consécutifs, l'un est multiple de a.

Preuve :
Soit n le premier de ces entiers. S'il n'est pas divisible par a, d'après la propriété de la division euclidienne, n s'écrit de manière unique sous une forme $n = aq + r$ avec r entier compris entre 1 et $a-1$ et q entier. Le dernier nombre s'écrit alors $n + a - 1 = aq + r + a - 1 = a(q+1) + r - 1$ et dans la série figure donc le nombre $a(q+1)$ qui est divisible par a.

Exemple :
Soit n un entier naturel, alors parmi les nombres n, $n+1$ et $n+2$, l'un est un multiple de 3.

3 Nombres premiers

Définition :
Un *nombre premier* est un nombre entier qui a exactement deux diviseurs : 1 et lui même.

Exemples :

- 5 est un nombre premier.
- 10 n'est pas premier car divisible par 2.
- 0 et 1 ne sont pas premiers.
- 2 est l'unique nombre premier pair.

Remarque :

Ne pas confondre un *nombre premier* avec des *nombres premiers entre eux* : deux nombres sont premiers entre eux lorsque leur seul diviseur commun est 1. Par exemple, 10 et 27 sont premiers entre eux car leur plus grand diviseur commun est 1 mais 10 n'est pas premier car divisible par 2 ou 5 et 27 n'est pas premier car divisible par 3.

Propriété :

Soit n un entier naturel non nul. Si n n'est pas premier, alors il est divisible par un *nombre premier*.

Preuve :

Si n n'est pas premier alors il admet un diviseur a_1 distinct de 1 et de n. a_1 est nécessairement strictement inférieur à n. Si a n'est pas premier, à nouveau il est divisible par un nombre a_2 strictement inférieur à a_1. Et ainsi de suite. Si aucun des nombres a_1, a_2, etc, n'était premier on pourrait construire une infinité de nombres tous distincts et de plus en plus petits et donc proche de 0 ce qui n'est pas possible car il n'y a qu'un nombre fini de nombres entre 0 et n. Par conséquent, l'un au moins des nombres a_1, a_2, etc. construit est un nombre premier et c'est en outre un diviseur de n.

Exemples :

100 n'est pas premier car divisible par 1, 100 et 10 par exemple. 2 en est un diviseur premier. 12 n'est pas premier, il est divisible par 2 qui est premier.

Propriété :

Soit n un entier naturel non nul. Si aucun nombre entier naturel différent de 1 et inférieur strictement à $\sqrt{n}$ n'est un diviseur de n, alors n est un *nombre premier*.

Preuve :

Supposons que n ne soit pas premier. Alors il existe a et b entiers naturels différents de 1 et n tels que $n = ab$. On peut supposer que $a \leq b$. Alors $ab \geq a^2$ et donc $n \geq a^2$ donc $\sqrt{n} \geq a$. Par conséquent, n admet un diviseur plus petit que $\sqrt{n}$. Par suite, on en déduit que si n n'admet aucun diviseur strictement inférieur à $\sqrt{n}$ alors n est premier.

Exemple [Savoir reconnaître si un nombre est premier] :

On considère le nombre 101.

$\sqrt{101} \approx 10$.

2, 3 et 5 ne sont pas des diviseurs de 101 de manière évidente (critères de divisibilité).

$101 \div 7 \approx 14,4$ Par conséquent, 101 est premier.

Programmation python : test de primalité :

```
def estPremier(n):
        k=0
        premier=true
        while(k<=Math.sqrt(n)) and (premier==true):
                if n%k=0:
                        premier=false
                k=k+1
        return premier
```

Propriété :

L'ensemble des nombres premiers est infini.

Preuve :

Par l'absurde : supposons qu'il n'existe qu'un nombre fini de nombres premiers p_1, p_2,..., p_n avec $n \in \mathbb{N}^*$ et $p_1 < p_2 < ... < p_n$.
On considère le nombre $M = p_1p_2...p_n + 1$. Comme $M > p_n$, M n'est pas un nombre premier. D'où M est divisible par un nombre premier d'après la propriété précédente. Soit p_k où $k \in \{1; 2; ...; n\}$ ce nombre. Il existe donc un entier d tel que $M = dp_k$. D'où $p_1p_2...p_k..p_n + 1 = dp_k$ donc $1 = p_k(d - p_1p_2..\widehat{p_k}.p_n)$ où la notation $\widehat{p_k}$ signifie que le nombre p_k ne figure pas dans le produit $p_1p_2...\widehat{p_k}...p_n$. Cette égalité montre que le nombre premier p_k diviserait 1 ce qui est absurde. Par conséquent, l'ensemble des nombres premiers est infini.

Théorème, théorème de la décomposition en facteurs premiers :
Tout entier naturel supérieur ou égal à 2 se décompose en un produit de nombres premiers. Cette décomposition est unique à l'ordre près des facteurs. On écrit

$$n = p_1^{n_1}p_2^{n_2}...p_k^{n_k}$$

où p_1, p_2,...,p_k sont des nombres premiers et n_1, n_2,...,n_k sont des nombres entiers naturels non nuls.
Le nombre de diviseurs de n est alors $(n_1 + 1)(n_2 + 1)...(n_k + 1)$.

Preuve :

Admise

Exemple :

$17\,640 = 2^3 \times 3^2 \times 5^1 \times 7^2$ donc $17\,640$ admet $4 \times 3 \times 2 \times 3 = 72$ diviseurs.

Théorème :
Soit n un entier naturel supérieur ou égal à 2 et soit $n = p_1^{n_1}p_2^{n_2}...p_k^{n_k}$ où p_1, p_2,...,p_k sont des nombres premiers et n_1, n_2,...,n_k la décomposition de n en facteurs premiers. Alors les diviseurs positifs de n dont les nombres entiers $p_1^{r_1}p_2^{r_2}...p_k^{r_k}$ où r_1, r_2,..., r_k sont des entiers naturels tels que $r_1 \leq n_1$, $r_2 \leq n_2$,..., $r_k \leq n_k$.

4 PGCD

Propriété et définition :

Soient a et b des entiers relatifs non nuls. L'ensemble des diviseurs communs à a et b admet un plus grand élément. On l'appelle le Plus Grand Commun Diviseur ou PGCD de a et de b. On le note $PGCD(a;b)$

Exemple :

Cherchons le PGCD de 12 et 78 :

L'ensemble des diviseurs de 12 est $\{\pm1;\pm2;\pm3;\pm4;\pm6;\pm12\}$.

L'ensemble des diviseurs de 78 est $\{\pm;\pm2;\pm3;\pm6;\pm13;\pm26;\pm39\}$.

Le plus grand diviseur commun à ces deux ensembles est 6.

Propriété :

Soient a et b des entiers relatifs non nuls.

- Si b est un diviseur de a, alors $PGCD(a;b)=b$.
- Pour tout entier relatif k, $PGCD(a;b)=PGCD(a-kb;b)$.
- Si $0<b\leq a$, $PGCD(a;b)=PGCD(b;r)$ où r est le reste de la division euclidienne de a par b.

Preuve :

- Immédiat car d est le plus grand élément de l'ensemble des diviseurs de lui-même donc des diviseurs communs à a et b.
- Si d divise a et d divise b alors d divise $a-bk$ pour tout entier k. Réciproquement, si d divise b et d divise $a-bk$ pour un entier relatif k alors d divise tout te combinaison linéaire de b et de $a-bk$ donc $a-bk+kb=a$. Donc l'ensemble des diviseurs communs à a et b est le même que l'ensemble des diviseurs communs à b et $a-bk$ ce qui assure que $PGCD(a;b)=PGCD(b;a-bk)$.
- D'après le théorème de la division euclidienne, il existe deux entiers q et r tels que $a=bq+r$. Si d divise a et b alors d divise $a-bq=r$. Réciproquement, si d divise b et $r=a-bq$ alors d divise $a-bq+bq=a$ donc l'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs communs à r et b. ce qui assure que $PGCD(a;b)=PGCD(b;r)$.

Propriété, algorithme d'Euclide :

Soient a et b deux entiers tels que $0 < b \leq a$. Alors, l'algorithme suivant permet de calculer en un nombre fini d'étapes, le PGCD de a et b :

Calculer le reste dans la division euclidienne de a par b.
Tant que $r \neq 0$ faire :
| $a \leftarrow b$
| $b \leftarrow r$
Fin du tant que
$PGCD(a;b) = b$

Exemple :

Cherchons le PGCD de 1 554 et 136 :

$1554 = 136 \times 11 + 58$
$136 = 58 \times 2 + 20$
$58 = 20 \times 2 + 18$
$20 = 18 \times 1 + 2$
$18 = 2 \times 9 + 0$

Le dernier reste non nul donc le PGCD de 1 554 et 136 est 2.

Propriétés :

- Les diviseurs communs de a et de b sont les diviseurs de leur PGCD.
- Pour tout entier relatif k, $PGCD(ka;kb) = kPGCD(a;b)$

Programmation python : recherche du PGCD de a et b :

```
def PGCD(a,b):
    r=a%b
    while(r!=0):
        a=b
        b=r
        r=a%b
    return b
```

Définition :
Deux entiers relatifs sont dits *premiers entre eux* si leurs seuls diviseurs communs sont -1 et 1, c'est à dire si leur PGCD est 1.

Exemple :
12 et 25 sont premiers entre eux car leur PGCD est 1.
Attention : ce ne sont pas des nombres premiers.

Propriété :
Soient a et b deux entiers naturels non nuls et d le PGCD de a et b. Alors ils existe deux entiers naturels non nuls a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Preuve :
Soit d le PGCD de a et b. d étant un diviseur de a et de b, il existe donc deux entiers a' et b' tels que $a = da'$ et $b = db'$. D'après la propriété précédente, on a $PGCD(a;b) = PGCD(a'd;b'd) = dPGCD(a';b')$ et en outre on a $PGCD(a;b) = d$ d'où $PGCD(a';d') = 1$.

5 Théorème de Bezout et applications

Théorème, théorème de Bezout-Bachet :
Deux entiers a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que $au + bv = 1$.

Exemple de détermination de coefficients de Bezout à l'aide de l'algorithme d'Euclide :

Cherchons u et v tels que $47u + 39v = 1$.

Pour cela, on commence par appliquer l'algorithme d'Euclide à 47 et 39 :

$47 = 39 \times 1 + 8$ (1)

$39 = 8 \times 4 + 7$ (2)

$8 = 7 \times 1 + 1$ (3)

$7 = 1 \times 7 + 0$ (4)

Donc le PGCD de 47 et 39 est 1.

On « remonte » les calculs dans les égalités précédentes sauf la dernière en isolant à chaque fois le reste pour le substituer dans l'égalité d'avant :

En isolant le reste dans (3) on obtient ainsi $1 = 8 - 7 \times 1$.

Puis en isolant le reste dans (2) on a $7 = 39 - 8 \times 4$

ce qui donne donc en substituant dans (3) : $1 = 8 - (39 - 8 \times 4) \times 1$

donc $1 = 8 - 39 + 8 \times 4$ c'est à dire $1 = 8 \times 5 - 39$.

En isolant le reste dans (1) on obtient $8 = 47 - 39 \times 1$.

Puis en substituant dans l'égalité précédente on a :

$1 = (47 - 39 \times 1) \times 5 - 39$

c'est à dire $1 = 47 \times 5 - 39 \times 5 - 39$

donc $1 = 47 \times 5 - 39 \times 6$

D'où les coefficients $u = 5$ et $v = -6$.

Programmation python : recherche de u et v tels que $ua + bv = 1$:

```
def Bezout(a,b):
        u,v=1,0
        x,y=0,1
        while(r>0):
                q=b//a
                r=a%b
                a=b
                b=r
                s,u=u-x*q,x
                x=s
                t,v=v-q*y,y
                y=t
        return u,v
```

Corollaire :
Si d est le PGCD de a et de b, alors il existe des entiers u et v tels que $au + bv = d$.

Preuve :
D'après une propriété précédente, il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$. D'après le théorème de Bezout, il existe en outre deux entiers u et v tels que $ua' + b'v = 1$. D'où $ua'd + b'vd = d$ c'est à dire $ua + bv = d$.

6 Théorème de Gauss et applications

Théorème, théorème de Gauss :
Soit a, b et c trois entiers. Si a divise le produit bc et si a est premier avec b, alors a divise c.

Preuve :
D'après le théorème de Bezout, il existe deux entiers u et v tels que $au + bv = 1$. D'où $auc + bvc = c$. En outre, a divise bc donc il existe un entier k tel que $bc = ka$. D'où $auc + kav = c$ c'est à dire $a(uc + kv) = c$ donc a divise c.

Corollaires :

- Si un entier est divisible par des entiers a et b premiers entre eux, alors il est divisible par leur produit ab.
- Si un entier premier divise un produit de facteurs ab, alors il divise au moins l'une des facteurs a ou b.
- Si un entier premier divise un produit de nombres premiers, alors p est égal à l'un des deux.
- p est un entier premier avec les entiers a et b si et seulement si p est premier avec leur produit.

Exemple :

On considère l'équation $47x = 28y$ dans $\mathbb{Z}$. 47 divise $28y$ et 47 et 28 sont premiers entre eux donc d'après le théorème de Gauss, 47 divise y d'où $y = 47k$ où k est un entier relatif.

On obtient l'équation $47x = 28 \times 47k$ donc $x = 28k$.

On vérifie que les couples $(x; y)$ définis par $(28k; 47k)$ où k est un entier relatif sont solutions.

Les solutions sont donc les couples $(x; y)$ de la forme $(28k; 47k)$ où $k \in \mathbb{Z}$.

7 Congruences

Définition :

Soit m un entier naturel non nul. Deux entiers relatifs a et b sont dits congrus modulo m lorsque $b - a$ est multiple de m. On note $a \equiv b\,(m)$ ou $a \equiv b\,(\text{mod } m)$.

Théorème :

Soit m un entier naturel non nul. Deux entiers relatifs a et b sont congrus modulo m si et seulement si a et b ont le même reste dans la division euclidienne par m.

Preuve :

D'après le théorème de la division euclidienne, il existe deux entiers q_1 et r_1 tels que $a = mq_1 + r_1$ avec $0 \leq r_1 < m$ et deux entiers q_2 et r_2 tels que $b = mq_2 + r_2$ avec $0 \leq r_2 < m$.

On a donc $a \equiv b\,(m)$ si et seulement si il existe un entier k tel que $b - a = k(m)$ si et seulement si $mq_1 + r_1 - mq_2 - r_2 = km$ c'est à dire $m(k - q_1 - q_2) = r_1 - r_2$.

Comme $-m < r_1 - r_2 < m$, cela équivaut encore à $r_1 - r_2 = 0$ c'est à dire $r_1 = r_2$.

Propriétés :

Soit m un entier tel que $m \geq 2$. Soit a, b, a', b' et c des entiers relatifs.

- $a \equiv a(m)$;
- Propriété de transitivité :
  si $a \equiv b(m)$ et $b \equiv c(m)$ alors $a \equiv c(m)$.
- Compatibilité avec l'addition :
  si $a \equiv b\,(m)$ et $a' \equiv b'\,(m)$ alors $a + a' \equiv b + b'\,(m)$.
- Compatibilité avec la multiplication :
  si $a \equiv b\,(m)$ et $a' \equiv b'\,(m)$ alors $aa' \equiv bb'\,(m)$.
- Compatibilité avec les puissances :
  pour tout entier naturel n non nul, si $a \equiv b\,(m)$, alors $a^n \equiv b^n\,(m)$.
- Soit m un entier naturel tel que $m \geq 2$ et soit a un entier relatif a.
  a divisible par m si et seulement si $a \equiv 0\,(m)$.

Preuve :

- $a - a = 0m$ donc $a \equiv a\,(m)$.
- $a \equiv b\,(m)$ donc il existe un entier k_1 tel que $b - a = mk_1$
  $b \equiv c\,(m)$ donc il existe un entier k_2 tel que $c - b = mk_2$
  D'où $c - a = c - b + b - a = mk_2 + mk_1 = m(k_1 + k_2)$ donc $a \equiv c\,(m)$.
- $a \equiv b\,(m)$ donc il existe un entier k_1 tel que $b - a = mk_1$
  $b' \equiv a'\,(m)$ donc il existe un entier k_2 tel que $b' - a' = mk_2$
  D'où $b + b' - (a + a') = b - a + b' - a' = mk_1 + mk_2 = m(k_1 + k2)$ donc $a + a' \equiv b + b'\,(m)$

- $a \equiv b\,(m)$ donc il existe un entier k_1 tel que $b - a = mk_1$
  $b' \equiv a'\,(m)$ donc il existe un entier k_2 tel que $b' - a' = mk_2$
  D'où $bb' - aa' = bb' - ab' + ab' - aa' = b'(b-a) + a(b'-a') = mk_1b' + amk_2 = m(k_1b' + mk_2)$ donc $aa' \equiv bb'\,(m)$.
- Découle directement de $b^n - a^n = (b-a)\sum_{k=0} n - 1b^k a^{n-1-k}$.
- a est divisible par m si et seulement si il existe q tel que $a = mq$ c'est à dire $a - 0 = mq$ c'est à dire que $a \equiv 0\,(m)$.