Chapitre 3
Théorèmes d'arithmétique

I. PGCD de deux entiers

1) Diviseurs communs

Exemples :
- Les diviseurs de 12 sont : 1, 2, 3, 4, 6, 12 et leurs opposés.
- Les diviseurs de -9 sont : 1, 3, 9 et leurs opposés.

Notations :
- Pour tout entier naturel a, on note $\mathcal{D}(a)$ l'ensemble de ses diviseurs.
  Par exemple, $\mathcal{D}(1)=\{-1\,;1\}$ et $\mathcal{D}(0)=\mathbb{Z}$.
  $\mathcal{D}(a)$ contient toujours 1 et a.
  Lorsque $a\neq 0$, le plus grand élément de $\mathcal{D}(a)$ est a.
- Pour tous entiers naturels a et b non nuls, on note $\mathcal{D}(a\,;b)$, l'ensemble des diviseurs communs de a et b. Donc $\mathcal{D}(a\,;b)=\mathcal{D}(a)\cap\mathcal{D}(b)$.

Remarque :
Si a est un diviseur de b $\mathcal{D}(a)\subset\mathcal{D}(b)$

Propriété :
a et b sont deux entiers relatifs non tous les deux nuls.
L'ensemble $\mathcal{D}(a\,;b)$ admet un plus grand élément.

Démonstration :
Lemme : Toute partie finie, non vide de $\mathbb{Z}$ admet un plus grand élément.
L'ensemble $\mathcal{D}(a\,;b)$ est non vide : il contient toujours 1.
De plus, tous les nombres qu'il contient sont inférieurs ou égaux à $|a|$ et $|b|$.
Donc $\mathcal{D}(a\,;b)$ a un plus grand élément.

2) PGCD

Définition :
a et b sont deux entiers relatifs non tous les deux nuls.
Le plus grand élément de $\mathcal{D}(a\,;b)$ est le **Plus Grand Commun Diviseur** de a et b, noté PGCD($a\,;b$).

Exemples :
- $\mathcal{D}(6)=\{-6\,;-3\,;-2\,;-1\,;1\,;2\,;3\,;6\}$ et $\mathcal{D}(15)=\{-15\,;-5\,;-3\,;-1\,;1\,;3\,;5\,;15\}$.
  Donc $\mathcal{D}(6\,;15)=\{-3\,;-1\,;1\,;3\}$ et PGCD(6 ; 15)=3.
- PGCD(-9 ;12)=3

Remarques :

Si a et b sont deux entiers relatifs non tous les deux nuls.

- PGCD(a ;b) est un entier naturel.
- PGCD(a ;b)=PGCD(b ;a)=PGCD($|a|$; $|b|$). On se ramène donc, en général, à a et b positifs.
- PGCD(1 ;b)=1 et PGCD(0 ;b)= $|b|$.
- Si b est un diviseur positif de a, PGCD(a ;b)=b

3) Algorithme d'Euclide

Propriété :

Si a et b sont des entiers relatifs non tous les deux nuls.

$\mathcal{D}(a\,;b)=\mathcal{D}(a-kb\,;b)$ pour tout $k\in\mathbb{Z}$.

Démonstration :

- Si d divise a et b alors d divise a et $a-kb$ pour tout $k\in\mathbb{Z}$, donc d divise $a-kb$ et b.
  On vient de montrer que si $d\in\mathcal{D}(a\,;b)$ alors $d\in\mathcal{D}(a-kb\,;b)$, donc $\mathcal{D}(a\,;b)\subset\mathcal{D}(a-kb\,;b)$.
- Si d divise $a-kb$ et b alors d divise $a-kb$ et $(a-kb)+kb$ soit a, donc d divise a et b.
  On vient de montrer que si $d\in\mathcal{D}(a-kb\,;b)$ alors $d\in\mathcal{D}(a\,;b)$, donc $\mathcal{D}(a-kb\,;b)\subset\mathcal{D}(a\,;b)$.

Donc $\mathcal{D}(a\,;b)=\mathcal{D}(a-kb\,;b)$.

Propriété :

a, b, q et r désignent des nombres entiers relatifs non tous nuls.

Si $a=bq+r$ alors $\mathcal{D}(a\,;b)=\mathcal{D}(b\,;r)$ et par conséquent $PGCD(a;b)=PGCD(b;r)$.

Algorithme d'Euclide

Propriété :

Soient a et b des entiers relatifs non tous les deux nuls.

L'algorithme suivant, appelé **algorithme d'Euclide**, permet de calculer PGCD(a ;b).

```
Saisir a
Saisir b

r prend la valeur reste de la division euclidienne de a par b
        Tant que r ≠ 0 faire
                a prend la valeur b
                b prend la valeur r
                r prend la valeur reste de la division euclidienne de a par b
        Fin Tant que

Afficher b
```

Démonstration :

$a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, avec $a \geqslant b$.

Opération	Reste	Commentaire
On divise *a* par *b*	r_0	$0 \leqslant r_0 < b$ et $\mathcal{D}(a;b) = \mathcal{D}(b;r_0)$ et $PGCD(a;b) = PGCD(b;r_0)$
Si $r_0 \neq 0$, on divise *b* par r_0	r_1	$0 \leqslant r_1 < r_0$ et $\mathcal{D}(b;r_0) = \mathcal{D}(r_0;r_1)$ et $PGCD(b;r_0) = PGCD(r_0;r_1)$
Si $r_1 \neq 0$, on divise r_0 par r_1	r_2	$0 \leqslant r_2 < r_1$ et $\mathcal{D}(r_0;r_1) = \mathcal{D}(r_1;r_2)$ et $PGCD(r_0;r_1) = PGCD(r_1;r_2)$
…	…	…
Si $r_{n-1} \neq 0$, on divise r_{n-2} par r_{n-1}	r_n	$0 \leqslant r_n < r_{n-1}$ et $\mathcal{D}(r_{n-2};r_{n-1}) = \mathcal{D}(r_{n-1};r_n)$ et $PGCD(r_{n-2};r_{n-1}) = PGCD(r_{n-1};r_n)$
Si $r_n \neq 0$, on divise r_{n-1} par r_n	0	$PGCD(r_n;r_{n-1}) = r_n$

On construit ainsi une liste strictement décroissante r_0 , r_1 , r_2 , … d'entiers positifs.
Or il n'y a qu'un nombre fini d'entiers entre r_0 et 0.
Donc cette liste est finie : il existe un reste nul.
Il existe donc $n \geqslant 0$ tel que $r_n \neq 0$ et $r_{n+1} = 0$. Comme $r_{n+1} = 0$, l'algorithme s'arrête.
Il comporte donc bien un nombre fini d'étape.
Et, en remontant, $r_n = PGCD(r_n;r_{n-1}) = \ldots = PGCD(b;r_0) = PGCD(a;b)$.

<u>Exemple :</u>

Calculer le PGCD de 364 et 247 avec l'algorithme d'Euclide.

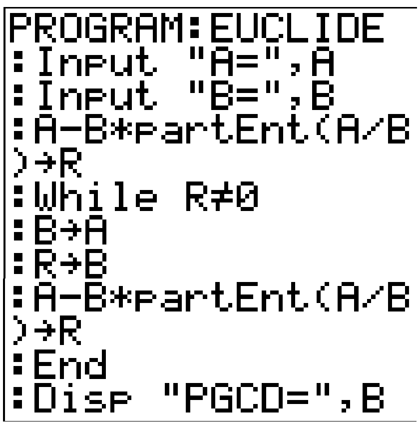
Étape	Opération	Reste	Commentaire
1	$364 = 247 \times 1 + 117$	117	$PGCD(364;247) = PGCD(247;117)$
2	$247 = 117 \times 2 + 13$	13	$PGCD(247;117) = PGCD(117;13)$
3	$117 = 13 \times 9 + 0$	0	$PGCD(117;13) = PGCD(13;0) = 13$

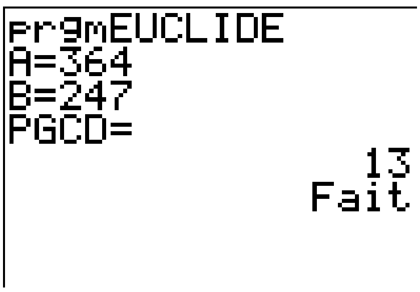
Donc, en remontant, $13 = PGCD(117;13) = PGCD(247;117) = PGCD(364;247)$.

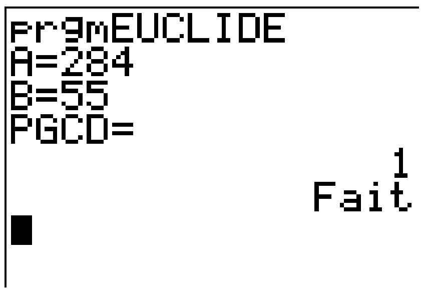
<u>Remarque :</u>

Lorsque *b* ne divise pas *a*, le PGCD de *a* et *b* est le **dernier reste non nul** dans l'algorithme d'Euclide.

<u>Calculatrice :</u> pour a e*t* b entiers naturels et $a > b$







Xcas : (pour *a* et *b* entiers relatifs quelconques)

```
Euclide(a,b):={
local r;
r:=irem(a,b);
tantque r>0 faire
a:=b;
b:=r;
r:=irem(a,b);
ftantque;
afficher b;
}
:;
```

```
// Interprete Euclide
// Success compiling Euclide
                                        Done
Euclide(247,364)
                                        13
```

Propriété :
a et *b* sont deux entiers relatifs non tous les deux nuls.
L'ensemble des diviseurs communs de *a* et *b* est l'ensemble des diviseurs de $PGCD(a;b)$.

Démonstration :
En suivant l'algorithme d'Euclide :
$\mathcal{D}(a;b)=...=\mathcal{D}(r_{n-1};r_n)=\mathcal{D}(r_n)$ et $r_n=PGCD(a;b)$.

Propriété (homogénéité) :
Soit *a* et *b* deux entiers relatifs non tous les deux nuls.
Pour tout $k\in\mathbb{N}^*$, $PGCD(ka;kb)=k\times PGCD(a;b)$.

Exemple :
$PGCD(150;100)=50\times PGCD(3;2)=50\times 1=50$

4) Nombres premiers entre eux

Définition :
Dire que deux entiers relatifs non tous les deux nuls sont **premiers entre eux** signifie que leur PGCD est égal à 1.

Propriété (caractéristique) :
Soit *a* et *b* deux entiers relatifs non tous les deux nuls et *k* un entier naturel.
$k=PGCD(a;b)$ si, et seulement si, $a=k\times a'$ et $b=k\times b'$ avec a' et b' premiers entre eux.

Démonstration :

- Si $k=PGCD(a;b)$, il existe a' et b' entiers tels que $a=k\times a'$ et $b=k\times b'$.
  Alors $PGCD(a;b)=PGCD(ka';kb')$ donc, par homogénéité, sachant que *k* est un entier naturel non nul, $PGCD(a;b)=k\times PGCD(a';b')$.
  Comme $PGCD(a;b)=k$ on en déduit que $PGCD(a';b')=1$ c'est-à-dire que a' et b' sont premiers entre eux.
- Réciproquement, si $a=k\times a'$ et $b=k\times b'$ avec a' et b' premiers entre eux et *k* entier naturel, alors $k\neq 0$ car *a* et *b* ne sont pas tous les deux nuls, donc par homogénéité, $PGCD(a;b)=k\times PGCD(a';b')=k\times 1=k$.

Exemple :
$90=9\times 10$ et $40=4\times 10$ avec 9 et 4 premiers entre eux donc $PGCD(90;40)=10$.

Remarque :
Une fraction est irréductible si son numérateur et son dénominateur sont premiers entre eux. Si *a* et *b* sont des entiers non nuls, on peut donc écrire $\frac{a}{b}$ sous forme irréductible $\frac{a'}{b'}$ en divisant *a* et *b* par $PGCD(a;b)$.

II. Le théorème de Bézout

1) *Identité de Bézout*

Propriété :
a et b désignent deux nombres entiers relatifs non nuls.
Si $d=PGCD(a\,;b)$, alors il existe des nombres entiers relatifs u et v tels que $au+bv=d$.

Démonstration :
E désigne l'ensemble des nombres entiers naturels de la forme $au+bv$ avec $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$.

- $E\neq\emptyset$ car $|a|$ appartient à E.
  En effet, si $a>0$, $|a|=a=1a+0b$ et si $a<0$, $|a|=-a=-1a+0b$, donc E admet un plus petit élément (toute partie non vide de $\mathbb{N}$ admet un plus petit élément). On le note c.
- Et on note $d=PGCD(a\,;b)$.
  On sait que d divise a et b, donc d divise toute combinaison linéaire de a et b, donc d divise c.
- En effectuant la division euclidienne de a par c, on obtient l'existence d'un unique couple de nombres entiers $(q\,;r)$ tel que $a=c\times q+r$ avec $0\leqslant r<c$.
  Comme $r=a-c\times q$, r est combinaison linéaire de a et c.
  Or c est combinaison linéaire de a et b, donc r est combinaison linéaire de a et b.
  On raisonne par l'absurde et on suppose que $r>0$. Alors r serait une combinaison linéaire strictement positive de a et b telle que $r<c$, ce qui est absurde car c est le plus petit élément de E. On en déduit que $r=0$ et ainsi c divise a.
  On démontre de même que c divise b. Ainsi, c est un diviseur commun de a et b, donc c divise d.

c divise d et d divise c, donc $c=d$ et donc le $PGCD$ de a et b est de la forme $au+bv$.

Exemple :
$PGCD(18\,;30)=6$.
On peut trouver un couple u et v tel que $18u+30v=6$, par exemple le couple $(2;-1)$ car $18\times 2+30\times(-1)=36-30=6$.

Remarques :

- Il n'y a pas unicité du couple $(u\,;v)$ trouvé. Dans l'exemple précédent, le couple $(-3;2)$ convient aussi.
- Ce théorème n'admet pas de réciproque ; en effet si $d=au+bv$, d n'est pas nécessairement le $PGCD$ des entiers a et b.
  Contre-exemple : $2=1+1$ et pourtant 2 n'est pas le $PGCD$ du couple $(1;1)$.
- Par contre, si $au+bv=d$ alors $\text{PGCD}(a\,;b)$ divise d.

Méthode :
$5=PGCD(35;55)$, donc il existe deux entiers relatifs u et v vérifiant $35u+55v=5$.
On pose $a=35$ et $b=55$.

$35=55\times 0+35$	donc	$35=35-0\times 55=a-0\times b=a$
$55=35\times 1+20$	donc	$20=55-1\times 35=b-1\times a=b-a$
$35=20\times 1+15$	donc	$15=35-1\times 20=a-1\times(b-a)=2a-b$
$20=15\times 1+5$	donc	$5=20-1\times 15=(b-a)-1\times(2a-b)=-3a+2b$

Ainsi, on a bien $-3\times 35+2\times 55=5$.

Remarque :
Pour calculer $PGCD(a;b)$ avec l'algorithme d'Euclide, les quotients ne sont pas utiles.
Par contre, pour calculer u et v ils sont indispensables.

Algorithme : recherche d'un couple (u,v) tel que $au+bv=d=PGCD(a;b)$

- Utiliser le calcul symbolique (Xcas par exemple) :

```
Bezout(a,b):={
  local r,A,B,R,m,n;
  m:=a;n:=b;
  supposons(A,symbol);supposons(B,symbol);supposons(R,symbol);
  r:=a-b*iquo(a,b);R:=A-B*iquo(a,b);
  tantque r>0 faire
    a:=b;A:=B;
    b:=r;B:=R;
    r:=a-b*iquo(a,b);R:=A-B*iquo(a,b);
  ftantque;
  afficher "pour A= "+m+" et B= "+n+" l'identité de Bezout est : "+simplifier(B)+"="+b;
}
:;
```

```
// Interprete Bezout
// Success compiling Bezout
Done
Bezout(71,19)
pour A= 71 et B= 19 l'identité de Bezout est : -4*A+15*B=1
```

- En utilisant le calcul numérique
  On utilise les suites (q_n) et (r_n) des quotients et des restes des divisions euclidiennes successives de l'algorithme d'Euclide et on construit deux suites d'entiers relatifs (u_n) et (v_n) tels que pour tout $n \in \mathbb{N}$:

$r_n = a \times u_n + b \times v_n$.

  - On choisit $r_0=a$ et $r_1=b$; $u_0=1$ et $u_1=0$; $v_0=0$ et $v_1=1$.
    On a donc bien $r_0=a\times u_0+b\times v_0$ et $r_1=a\times u_1+b\times v_1$.
  - À l'étape $n+1$, on a donc

$$r_n=r_{n+1}\times q_{n+1}+r_{n+2}\ .$$

Soit $r_{n+2}=a\times u_{n+2}+b\times v_{n+2}$ avec $\begin{cases} u_{n+2} = u_n - u_{n+1} \times q_{n+1} \\ v_{n+2} = v_n - v_{n+1} \times q_{n+1} \end{cases}$

```
Saisir a
Saisir b          (a>b)
r prend la valeur 1
u prend la valeur 1 ; v prend la valeur 0
x prend la valeur 0 ; y prend la valeur 1
     Tant que r>0 faire
          q prend la valeur du quotient de la division euclidienne de a par b
          r prend la valeur du reste de la division euclidienne de a par b
          a prend la valeur b
          b prend la valeur r
          s prend la valeur u−x×q ; u prend la valeur x ; x prend la valeur s
          t prend la valeur v−y×q ; v prend la valeur y ; y prend la valeur t
     Fin Tant que
Afficher a      PGCD(a;b)
Afficher u
Afficher v
```

Exemple :

Pour $a=71$ et $b=19$

	$a=71$; $b=19$	$r=1$ $u=1$; $v=0$ $x=0$; $y=1$	$r_0=71$; $r_1=19$ $u_0=1$; $u_1=0$ $v_0=0$; $v_1=1$
1	$71=3\times 19+14$	$q=3$; $r=14$ $a=19$; $b=14$ $s=1-0\times 14=1$; $u=0$; $x=1$ $t=0-1\times 3=-3$; $v=1$; $y=-3$	$q_1=3$ $r_0=r_1\times q_1+r_2$; $r_2=14$ $u_2=u_0-u_1\times q_1$; $u_2=1$ $v_2=v_0-v_1\times q_1$; $v_2=-3$ $r_2=a\times u_2+b\times v_2$ $14=71\times 1+19\times(-3)$
2	$19=14\times 1+5$	$q=1$; $r=5$ $a=14$; $b=5$ $s=0-1\times 1=-1$; $u=1$; $x=-1$ $t=1-(-3)\times 1=4$; $v=-3$; $y=4$	$q_2=1$ $r_1=r_2\times q_2+r_3$; $r_3=5$ $u_3=u_1-u_2\times q_2$; $u_3=-1$ $v_3=v_1-v_2\times q_2$; $v_3=4$ $r_3=a\times u_3+b\times v_3$ $5=71\times(-1)+19\times 4$
3	$14=5\times 2+4$	$q=2$; $r=4$ $a=5$; $b=4$ $s=1-(-1)\times 2=3$; $u=-1$; $x=3$ $t=(-3)-4\times 2=-11$; $v=4$; $y=-11$	$q_3=2$ $r_2=r_3\times q_3+r_4$; $r_4=4$ $u_4=u_2-u_3\times q_3$; $u_4=3$ $v_4=v_2-v_3\times q_3$; $v_4=-11$ $r_4=a\times u_4+b\times v_4$ $4=71\times 3+19\times(-11)$
4	$5=4\times 1+1$	$q=1$; $r=1$ $a=4$; $b=1$ $s=(-1)-3\times 1=-4$; $u=3$; $x=-4$ $t=4-(-11)\times 1=15$; $v=-11$; $y=15$	$q_4=1$ $r_3=r_4\times q_4+r_5$; $r_5=1$ $u_5=u_3-u_4\times q_4$; $u_5=-4$ $v_5=v_3-v_4\times q_4$; $v_5=15$ $r_5=a\times u_5+b\times v_5$ $1=71\times(-4)+19\times 15$
5	$4=1\times 4+0$	$q=4$; $r=0$ $a=1$; $b=0$ $s=3-(-4)\times 4=19$; $u=-4$; $x=19$ $t=(-11)-15\times 4=-71$; $v=15$; $x=-71$	$q_5=4$ $r_4=r_5\times q_5+r_6$; $r_6=0$ $u_6=u_4-u_5\times q_5$; $u_6=19$ $v_6=v_4-v_5\times q_5$; $v_6=-71$ $r_6=a\times u_6+b\times v_6$ $0=71\times 19+19\times(-71)$
$71\times(-4)+19\times 15=1$			

Calculatrice (pour *a* et *b* entiers naturels) :

```
PROGRAM:BEZOUT
:Input "A=",A
:Input "B=",B
:1→R
:1→U
:0→V
:0→X
:1→Y
:While R>0
:partEnt(A/B)→Q
:A-B*Q→R
:B→A
:R→B
:U-X*Q→S
:X→U
:S→X
:V-Y*Q→T
:Y→V
:T→Y
:End
:Disp "PGCD=",A
:Disp "U=",U
:Disp "V=",V
```

```
prgmBEZOUT
A=71
B=19
```

```
PGCD=
                1
U=
               -4
V=
               15
             Fait
```

```
prgmBEZOUT
A=30
B=18
```

```
PGCD=
                6
U=
               -1
V=
                2
             Fait
```

Xcas (pour *a* et *b* entiers relatifs quelconques) :

```
Prog   Edit   Configuration actuelle du CAS. Cliquer pour modifier        OK (F9)
Bézout(a,b):={
  local m,n,r,u,v,x,y,q,s,t ;
  m:=a;n:=b;
  r:=1;u:=1;v:=0;x:=0;y:=1;
  tantque r>0 faire
    q:=iquo(a,b); r:=irem(a,b);
    a:=b;b:=r;
    s:=u-x*q;u:=x;x:=s;
    t:=v-q*y;v:=y;y:=t;
  ftantque;
  afficher("PGCD("+m+";"+n+")="+a);
  afficher (m+"*"+u+"+"+n+"*"+v+"="+a)

  }
  :;
// Interprete Bézout
// Success compiling Bézout
                                   Done
Bézout(30,18)
PGCD(30;18)=6
30*-1+18*2=6
                                   1
Bézout(71,19)
PGCD(71;19)=1
71*-4+19*15=1
```

2) Théorème de Bézout

Propriété :
a et b désignent deux nombres entiers non nuls.
a et b sont premiers entre eux si, et seulement si, il existe des nombres entiers relatifs u et v tels que :

$$au+bv=1$$

Démonstration :

- Si a et b sont premiers entre eux, alors $PGCD(a;b)=1$.
  L'identité de Bézout permet alors de dire qu'il existe des nombres entiers relatifs u et v tels que $au+bv=1$.
- Réciproquement, s'il existe des nombres entiers relatifs u et v tels que $au+bv=1$, tout diviseur commun à a et b divise $au+bv$, donc 1. Donc $PGCD(a;b)=1$ et donc a et b sont premiers entre eux.

Exemples :

- $a=4$ et $b=-9$ sont premiers entre eux car on a $4\times(-2)+(-9)\times(-1)=1$
- Deux entiers consécutifs sont toujours premiers entre eux car pour tout entier n, $n\times(-1)+(n+1)\times 1=1$.
- Pour tout entier naturel n non nul, $3\times(5n+7)-5\times(3n+4)=1$, donc d'après le théorème de Bézout, $5n+7$ et $3n+4$ sont premiers entre eux.

Remarque :
La propriété se formule également de la façon suivante :
a et b désignent deux nombres entiers non nuls.

$$\text{PGCD}(a;b)\neq 1 \Leftrightarrow \forall (u,v)\in\mathbb{Z}^2,\ au+bv\neq 1$$

III. Le théorème de Gauss

1) Le théorème

Propriété :
a, b et c désignent trois nombres entiers relatifs non nuls.
Si ***a*** **divise le produit** ***bc*** et si ***a*** **et** ***b*** **sont premiers entre eux**, alors ***a*** **divise** ***c***.

Démonstration :
a et b sont premiers entre eux donc, d'après le théorème de Bézout, il existe des nombres entiers relatifs u et v tels que $au+bv=1$.
En multipliant chaque membre de l'égalité par c, on obtient $auc+bvc=c$.
a divise auc et, par hypothèse, a divise bc donc bvc, donc a divise $auc+bvc$, c'est-à-dire a divise c.

Remarque :
Il est essentiel de vérifier que a est premier avec b, car a peut diviser bc en ne divisant ni b ni c.
Par exemple, $300=15\times 20$ or 6 divise 300 sans diviser ni 15, ni 20.

Exemples :

- Si 4 divise $3^{10}\times n$, comme 4 et 3^{10} sont premiers entre eux, on sait alors que 4 divise *n*.
- Résolution de l'équation $7x=11y$ avec $x\in\mathbb{Z}$ et $y\in\mathbb{Z}$.
    - Si $7x=11y$, alors 11 divise $7x$. Or 7 et 11 sont premiers entre eux, donc d'après le théorème de Gauss, 11 divise *x*.
      Par conséquent, il existe un nombre entier relatif *k* tel que $x=11k$.
      Alors de $7x=11y$, on déduit que $7\times 11k=11y$ soit $y=7k$.
    - Réciproquement, tous les couples $(11k;7k)$ sont solutions de l'équation $7x=11y$.
      En effet, $7\times 11k=11\times 7k$.
    - Conclusion :
      Les solutions de l'équation $7x=11y$ sont les couples $(11k;7k)$ avec $k\in\mathbb{Z}$.

2) Conséquence

Propriété :
a, *b* et *c* désignent trois nombres entiers relatifs non nuls.
Si ***b* et *c* sont premiers entre eux** et **divisent *a***, alors ***bc* divise *a***.

Démonstration :
b divise *a* donc il existe un nombre entier relatif *k* tel que $a=kb$.
c divise *a* donc il existe un nombre entier relatif k' tel que $a=k'c$.
Ainsi $kb=k'c$.
On en déduit alors que *b* divise $k'c$.
b et *c* étant premiers entre eux, on déduit d'après le théorème de Gauss, que *b* divise k' c'est-à-dire qu'il existe un nombre entier relatif k'' tel que $k'=k''b$.
De $a=k'c$, on déduit alors $a=k''bc$ donc bc divise *a*.

Exemples :

- Comme 4 et 7 divise 700 et 4 et 7 sont premiers entre eux alors $4\times 7=28$ divise 700.
- Le nombre 1573875 est divisible par 5 (car le chiffre des unités est 5) et il est divisible par 9 (car la somme de ses chiffres est divisible par 9).
  Or 9 et 5 sont premiers entre eux, donc 1573875 est divisible par 5×9 soit 45.
- Le produit $n(n+1)(n+2)$ de trois nombres entiers naturels consécutifs est divisible par 2 et par 3.
  Ce produit est donc divisible par 6 puisque 2 et 3 sont premiers entre eux.