Arithmétique (partie 3)

1. PGCD de deux entiers

■ THÉORÈME :

Soient a et b deux entiers non nuls. L'ensemble des diviseurs communs à a et b admet un plus grand élément, appelé **Plus Grand Commun Diviseur** de a et b, noté $\text{pgcd}(a\,;b)$ ou $a \wedge b$.

Démonstration. L'ensemble des diviseurs de a est fini, ainsi que l'ensemble des diviseurs de b, donc leur intersection est finie. De plus elle est non vide, car 1 est diviseur commun à a et b. Donc l'ensemble des diviseurs communs à a et b admet un plus grand élément. □

■ DÉFINITION :

On dit que les entiers a et b sont **premiers entre eux** si $a \wedge b = 1$.

La méthode pour calculer le PGCD s'appelle l'**algorithme d'Euclide**, décrit par celui-ci au III$^{\text{e}}$ siècle avant J.-C. dans *Les Éléments*. Il est décrit et justifié dans le théorème suivant :

■ THÉORÈME :

a et b étant deux entiers naturels non nuls. La suite des divisions euclidiennes :

- de a par b : $a = bq_0 + r_1$ avec $0 \leqslant r_1 < b$
- de b par r_1 : $b = r_1q_1 + r_2$ avec $0 \leqslant r_2 < r_1$
- de r_1 par r_2 : $r_1 = r_2q_2 + r_3$ avec $0 \leqslant r_3 < r_2$
- ...
- de r_{n-1} par r_n (si $r_n \neq 0$) : $r_{n-1} = r_nq_n + r_{n+1}$ avec $0 \leqslant r_{n+1} < r_n$
- ...

est finie.
Si l'on note d le dernier reste non nul, alors $d = a \wedge b$.

Démonstration. Il découle de la définition des restes successifs que la suite des restes est une suite de nombres naturels strictement décroissante :

$$0 \leqslant \cdots < r_n < \cdots < r_2 < r_1 < b$$

Elle est donc finie et il existe un entier naturel k tel que $r_{k+1} = 0$.
On a alors $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{k-1} \wedge r_k = r_k \wedge r_{k+1} = r_k$ car $r_{k+1} = 0$. □

Exemples :

- Vérifier que 959 et 279 sont premiers entre eux et que 65 et 52 ne le sont pas.
  Pour 959 et 279 :

$$\begin{aligned} 959 &= 279 \times 3 + 122 \\ 279 &= 122 \times 2 + 35 \\ 122 &= 35 \times 3 + 17 \\ 35 &= 17 \times 2 + 1 \\ 17 &= 1 \times 17 + 0 \end{aligned}$$

  Donc $959 \wedge 279 = 1$, ils sont premiers entre eux.
  Pour 65 et 52 :

$$\begin{aligned} 65 &= 52 \times 1 + 13 \\ 52 &= 13 \times 4 + 0 \end{aligned}$$

  Donc $65 \wedge 52 = 13 \neq 1$, ils ne sont pas premiers entre eux.
- Montrer la propriété suivante : Si a et b sont deux entiers strictement positifs et si r est le reste dans la division euclidienne de a par b, alors, pour tout entier naturel d,

$$(d|a \text{ et } d|b) \Leftrightarrow (d|b \text{ et } d|r)$$

  Soit $a = bq + r$ avec $0 \leqslant r < b$.
  ($\Rightarrow$) Supposons que $d|a$ et $d|b$. Alors d divise $a - bq = r$. Donc $d|b$ et $d|r$.
  ($\Leftarrow$) Supposons que $d|b$ et $d|r$. Alors d divise $bq + r = a$. Donc $d|a$ et $d|b$.
  Par conséquent, les diviseurs communs à a et b sont exactement les diviseurs communs à b et r.
- En déduire que les diviseurs communs à 4 539 et 1 958 sont les diviseurs communs à 89. Quels sont les diviseurs positifs communs de 4 539 et 1 958 ? Que vaut alors $4\,539 \wedge 1\,958$?
  Appliquons l'algorithme d'Euclide :

$$\begin{aligned} 4\,539 &= 1\,958 \times 2 + 623 \\ 1\,958 &= 623 \times 3 + 89 \\ 623 &= 89 \times 7 + 0 \end{aligned}$$

D'après la propriété précédente :

- Les diviseurs communs à 4 539 et 1 958 sont les diviseurs communs à 1 958 et 623
- Les diviseurs communs à 1 958 et 623 sont les diviseurs communs à 623 et 89
- Les diviseurs communs à 623 et 89 sont les diviseurs communs à 89.

Comme 89 est premier, ses diviseurs positifs sont 1 et 89.
Donc les diviseurs positifs communs à 4 539 et 1 958 sont : 1 et 89.
Par conséquent, $4\,539 \wedge 1\,958 = 89$.

COROLLAIRE :
Tout diviseur commun de deux entiers naturels a et b est un diviseur de leur PGCD.

Exemples :

- Déterminer tous les diviseurs positifs communs à 3 247 043 et 5 934 251.

  Appliquons l'algorithme d'Euclide :

$$\begin{aligned} 5\,934\,251 &= 3\,247\,043 \times 1 + 2\,687\,208 \\ 3\,247\,043 &= 2\,687\,208 \times 1 + 559\,835 \\ 2\,687\,208 &= 559\,835 \times 4 + 447\,868 \\ 559\,835 &= 447\,868 \times 1 + 111\,967 \\ 447\,868 &= 111\,967 \times 4 + 0 \end{aligned}$$

  Donc $3\,247\,043 \wedge 5\,934\,251 = 111\,967$.

  Les diviseurs positifs communs à 3 247 043 et 5 934 251 sont tous les diviseurs positifs de 111 967.

- Programmer l'algorithme d'Euclide en Python.

```
Lire a
Lire b
Tant que (b ≠ 0)
  r ⟵ a % b
  a ⟵ b
  b ⟵ r
Afficher "Le PGCD est : "
Afficher a
```

2. Théorème de Bézout

Exemple :
Considérons l'algorithme d'Euclide appliqué aux entiers 1 958 et 4 539.

$$\begin{aligned} 4\,539 &= 1\,958 \times 2 + 623 \\ 1\,958 &= 623 \times 3 + 89 \\ 623 &= 89 \times 7 + 0 \end{aligned}$$

On en tire :

$$\begin{aligned} 89 &= 1\,958 - 3 \times 623 \\ &= 1\,958 - 3(4\,539 - 1\,958 \times 2) \\ &= -3 \times 4\,539 + 7 \times 1\,958 \end{aligned}$$

Donc $4\,539 \wedge 1\,958$ est une combinaison linéaire (à coefficients entiers) de 4 539 et 1 958.

THÉORÈME : Identités de Bézout [1]
Soient a et b deux entiers non nuls. Il existe deux entiers relatives u et v tels que $au + bv = a \wedge b$.

Démonstration. Soit S l'ensemble des entiers naturels strictement positifs de la forme $ax + by$ où x et y sont des entiers relatifs.
Comme $a = 1 \times a + 0 \times b$, a est un élément de S si $a > 0$ et $-a = (-1) \times a + 0 \times b$, donc $-a \in S$ si $a < 0$.
Ainsi $|a| \in S$, qui n'est donc pas l'ensemble vide.
S est donc une partie non vide de $\mathbb{N}^*$ admettant, d'après l'axiome du plus petit élément, un plus petit élément $d \neq 0$ et il existe donc deux entiers relatifs u et v tels que $au + bv = d$.
Observons que $a \wedge b$ étant un diviseur de a et de b, il est un diviseur de la combinaison linéaire $au + bv$ et donc $a \wedge b$ divise d.
De plus, si l'on note q et r respectivement le quotient et le reste dans la division de a par $d \neq 0$, on a : $a = qd + r$ avec $0 \leqslant r < d$, d'où comme $au + bv = d$:

$$r = a - qd = a - q(au + bv) = a(1 - qu) + b(-qv)$$

où $(1 - qu)$ et $(-qv)$ sont des entiers relatifs.
Ceci montre que $r \in S$ avec $0 \leqslant r < d$, ce qui, si $r \neq 0$, contredit la minimalité de d. Donc $r = 0$ et donc $d|a$.
On montre de manière analogue que $d|b$. Si $d|a$ et $d|b$, alors $d|a \wedge b$.
Ainsi : $a \wedge b|d$ et $d|a \wedge b$ donc $d = a \wedge b$ et donc il existe bien deux entiers u et v tels que $au + bv = a \wedge b$. □

1. Étienne Bézout, mathématicien français (1730-1783)

Remarque : Le couple $(u\,;\,v)$ n'est pas unique : par exemple $89 = 503 \times 4\,539 + (-1\,166) \times 1\,958$.
En pratique, on procède comme dans l'exemple précédent.
On peut aussi **programmer** l'algorithme d'Euclide étendu, qui donne $a \wedge b$ ainsi qu'un couple d'entiers $(u\,;\,v)$ tels que $au + bv = a \wedge b$.
On observe en effet, avec les notations de l'algorithme d'Euclide, que si l'on suppose connus deux entiers u_i et v_i tels que $r_i = au_i + bv_i$, comme $r_{i-1} = r_i q_i + r_{i+1}$, on obtient

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i q_i \\ &= (au_{i-1} + bv_{i-1}) - (au_i + bv_i)q_i \\ &= a(u_{i-1} - u_i q_i) + b(v_{i-1} - v_i q_i) \end{aligned}$$

D'où : $\begin{cases} u_{i+1} = u_{i-1} - u_i q_i \\ v_{i+1} = v_{i-1} - v_i q_i \end{cases}$

Remarque : Cet algorithme fournit aussi une preuve **constructive** de l'identité de Bézout.

Algorithme d'Euclide étendu

```
Lire a
Lire b
r ⟵ a
u ⟵ 1
v ⟵ 0
r' ⟵ b
u' ⟵ 0
v' ⟵ 1
Tant que (r' ≠ 0)
   q ⟵ Partie_Entière(r / r')
   rs ⟵ r
   us ⟵ u
   vs ⟵ v
   r ⟵ r'
   u ⟵ u'
   v ⟵ v'
   r' ⟵ rs - q * r'
   u' ⟵ us - q * u'
   v' ⟵ vs - q * v'
Afficher "PGCD = ", r
Afficher " avec "
Afficher r, " = ", u, " * ", a, " + ",
     v, " * ", b
```

■ THÉORÈME : (Théorème de Bézout)

Soient a et b deux entiers non nuls. Alors

$$a \wedge b = 1$$

si et seulement s'il existe deux entiers u et v tels que $au + bv = 1$

Démonstration. Si $a \wedge b = 1$ alors d'après l'Identité de Bézout, il existe bien deux entiers u et v tels que

$$au + bv = a \wedge b = 1$$

Réciproquement : Supposons que les entiers naturels a, b, u, v vérifient $au + bv = 1$ et soit d un diviseur commun positif aux entiers a et b. Comme d divise a b, d divise la combinaison linéaire $au + bv$, donc d divise 1 et donc $d = 1$. Ainsi, le seul diviseur commun à a et b est 1, donc $a \wedge b = 1$. □

Exemple :

Deux entiers consécutifs sont toujours premiers entre eux. En effet, deux entiers consécutifs n et $(n+1)$ vérifient

$$1 \times (n+1) - 1 \times n = 1$$

donc $n \wedge (n+1) = 1$.

Attention

Si les entiers a, b, u et v vérifient $au + bv = c$, avec $c \neq 1$, cela n'implique pas que $c = a \wedge b$.
Par exemple, $4 \times 7 + 5 \times (-5) = 3$ et $3 \neq 4 \wedge 5$.
En effet, tout diviseur de 4 et de 5 est un diviseur de 3, mais la réciproque est fausse.

Remarque : Mais il faut retenir que : si les entiers a, b, u et v vérifient $au + bv = c$ et si c est un diviseur positif de a et de b, alors $c = a \wedge b$.
En effet : $(a \wedge b)|a$ et $(a \wedge b)|b$ donc par combinaison linéaire : $(a \wedge b)|c$. Si en plus $c|a$ et $c|b$ alors $c|(a \wedge b)$ (c'est le corollaire page 2). Ainsi $(a \wedge b)|c$ et $c|(a \wedge b)$ où $c > 0$, donc $c = a \wedge b$.

■ COROLLAIRE :

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

Exemple :

Montrer avec l'Identité de Bézout que si a, b et k sont des entiers non nuls, alors :

$$\text{pgcd}(ka\,;\,kb) = |k| \times \text{pgcd}(a\,;\,b)$$

Preuve : en exercice !

3. Théorème de Gauss

THÉORÈME : (Théorème de Gauss[2])

Soient a, b et c trois entiers non nuls.
Si $a \wedge b = 1$ et a divise $b \times c$, alors $a|c$.

Démonstration. a et b étant premiers entre eux, d'après l'Identité (ou le théorème) de Bézout, il existe deux entiers u et v tels que

$$au + bv = 1$$

Donc : $acu + bcv = c$. De plus, $a|bc$, donc il existe un entier k tel que $bc = ak$. D'où avec l'égalité précédente : $acu + akv = c$ et d'où : $a(cu + kv) = c$.
Comme $cu + kv$ est un entier, ceci montre que $a|c$. □

Exemples :

- Déterminer les entiers x et y tels que $7x = 15y$.
  On a $7 \wedge 15 = 1$ et $7|15y$, donc d'après le théorème de Gauss, $7|y$. Ainsi y est un multiple de 7.
  Ainsi il existe $k \in \mathbb{Z}$ tel que $y = 7k$. Donc
  $$7x = 15 \times 7k$$
  c'est-à-dire
  $$x = 15k$$
  Donc $\begin{cases} x = 15k \\ y = 7k \end{cases}$ où $k \in \mathbb{Z}$.
  Cela convient : $7 \times 15k = 15 \times 7k$.
- On veut déterminer tous les couples d'entiers $(x\,;\,y)$ tels que $7x + 15y = 39$.

  Montrer que $7x + 15y = 39$ est équivalente à $7(x+3) = 15(4-y)$.

  $$7(x+3) = 15(4-y) \iff 7x + 21 = 60 - 15y$$
  $$\iff 7x + 15y = 39$$

  Utiliser la question précédente pour exprimer x et y en fonction d'un entier k.
  On pose $X = x+3$ et $Y = 4-y$. Alors l'équation $7(x+3) = 15(4-y)$ est équivalente à
  $$7X = 15Y$$
  D'après l'exemple précédent :
  $X = 15k$ et $Y = 7k$.
  On en conclut que $x + 3 = 15k$ et $4 - y = 7k$ et donc $x = 15k - 3$ et $y = -7k + 4$.

2. Carl Friedrich Gauß, mathématicien allemand (1777-1855)

Étude générale de l'équation diophantienne d'inconnue $(x\,;\,y) \in \mathbb{Z}^2$: $ax + by = c$ où $(a\,;\,b\,;\,c) \in \mathbb{Z}^3$:

1. Montrer que s'il existe deux entiers x_0 et y_0 tels que $ax_0 + by_0 = c$, alors : $a \wedge b | c$.
   On a $ax + by = c$. Posons $d = a \wedge b$. Alors $a = da'$ et $b = db'$ Donc $da'x_0 + db'y_0 = c$, ou encore $d(a'x + b'y) = c$, donc $d|c$ (condition nécessaire).
   Montrons qu'elle est suffisante. Si $d|c$, posons $c = dc'$, alors $a'x + b'y = c'$. On sait que a' et b' sont premiers entre eux, donc $a'x + b'y = 1$ a des solutions. Alors $a'x + b'y = c'$ a des solutions (ce sont les solutions de $a'x + b'y = 1$ multipliés par c').
   Ainsi, l'équation a des solutions si et seulement si c est un multiple de $a \wedge b$.
   On suppose donc dans la suite que $a \wedge b$ divise c.
2. L'algorithme d'Euclide étendu fournit une solution $(x_0\,;\,y_0)$ de l'équation $ax + by = a \wedge b$.
   En déduire une solution de l'équation $ax + by = c$.
   Montrer enfin que si $(x\,;\,y)$ est une solution quelconque de l'équation $ax + by = c$, alors :
   $$a'(x - x_0) = b'(y_0 - y) \text{ où : } a' = \frac{a}{a \wedge b} \text{ et } b' = \frac{b}{a \wedge b}$$
   En déduire enfin l'ensemble « potentielle » des solutions de l'équation $ax + by = c$.
   Si $ax_0 + by_0 = a \wedge b$ et $a \wedge b$ divise c, alors $c = k(a \wedge b)$ pour un certain entier k. Une solution particulière de $ax + by = c$ est $(kx_0\,;\,ky_0)$.
   Si $(x\,;\,y)$ est une solution quelconque, alors
   $$ax + by = c = akx_0 + bky_0$$
   Alors $a(x - kx_0) = b(ky_0 - y)$.
   En divisant par $a \wedge b$:
   $$a'(x - kx_0) = b'(ky_0 - y)$$
   où $a' = \frac{a}{a \wedge b}$ et $b' = \frac{b}{a \wedge b}$.
   Comme $a' \wedge b' = 1$ et $a'|b'(ky_0 - y)$, le théorème de Gauss donne $a'|(ky_0 - y)$.
   Donc $ky_0 - y = a't$ pour un certain entier t, d'où $y = ky_0 - a't$.
   Et $x - kx_0 = b't$, d'où $x = kx_0 + b't$.
   L'ensemble des solutions appartient à
   $$\mathcal{S} = \{kx_0 + b't\,;\,ky_0 - a't \mid t \in \mathbb{Z}\}$$

3. Démontrer réciproquement que les couples trouvés à la question 2 sont bien solutions de l'équation, puis conclure.

Vérifions

$$\begin{aligned} &a(kx_0 + b't) + b(ky_0 - a't) \\ &= akx_0 + ab't + bky_0 - ba't \\ &= k(ax_0 + by_0) \\ &= k(a \wedge b) = c \end{aligned}$$

Donc tous les couples de la forme $(kx_0 + b't, ky_0 - a't)$ sont bien des couples solution.

L'ensemble des solutions est exactement $\mathcal{S} = \{kx_0 + b't\,;\, ky_0 - a't \mid t \in \mathbb{Z}\}$

Exemples :

- Résoudre dans $\mathbb{Z}^2$ l'équation : $741x + 531y = 5$.

  Calculons d'abord pgcd$(741, 531)$:

$$\begin{aligned} 741 &= 531 \times 1 + 210 \\ 531 &= 210 \times 2 + 111 \\ 210 &= 111 \times 1 + 99 \\ 111 &= 99 \times 1 + 12 \\ 99 &= 12 \times 8 + 3 \\ 12 &= 3 \times 4 + 0 \end{aligned}$$

  Donc pgcd$(741\,;\,531) = 3$. Comme $3 \nmid 5$, l'équation $741x + 531y = 5$ n'a pas de solution dans $\mathbb{Z}^2$.

- Résoudre dans $\mathbb{Z}^2$ l'équation : $741x + 531y = 21$.

  pgcd$(741\,;\,531) = 3$ et $3|21$, donc l'équation admet des solutions.

  Remontons l'algorithme d'Euclide pour trouver une relation de Bézout :

$$\begin{aligned} 3 &= 99 - 12 \times 8 \\ &= 99 - (111 - 99) \times 8 = 9 \times 99 - 8 \times 111 \\ &= 9(210 - 111) - 8 \times 111 \\ &= 9 \times 210 - 17 \times 111 \\ &= 9 \times 210 - 17(531 - 210 \times 2) \\ &= 43 \times 210 - 17 \times 531 \\ &= 43(741 - 531) - 17 \times 531 \\ &= 43 \times 741 - 60 \times 531 \end{aligned}$$

  Donc $741 \times 43 + 531 \times (-60) = 3$.

  Pour obtenir $21 = 7 \times 3$, on multiplie par 7 : $741 \times 301 + 531 \times (-420) = 21$

  Une solution particulière est

$$(x_0\,;\,y_0) = (301\,;\,-420)$$

Soit $(x\,;\,y)$ une solution de l'équation. Alors

$$\begin{aligned} 741x + 531y &= 21 \\ 741 \times 301 + 531 \times (-420) &= 21 \end{aligned}$$

Par différence,

$$741x - 741 \times 301 + 531y - 531\,(-420) = 21 - 21$$

i.e. $741\,(x - 301) + 531\,(y + 420) = 0$

i.e. $741\,(x - 301) = -531\,(y + 420)$

Ainsi 741 divise $-531\,(y + 420)$ et 741 ne divise pas -531, donc d'après le théorème de Gauss, 741 divise $y+420$. Donc il existe $k \in \mathbb{Z}$ tel que $y+420 = 741k$.

On remplace dans l'équation précédente

$$\begin{aligned} &741\,(x - 301) = 531\,(y + 420) \\ \iff &741\,(x - 301) = 531 \times 741k \\ \iff &x - 301 = 531k \end{aligned}$$

Donc $\begin{cases} x = 531k + 301 \\ y = -741k - 420 \end{cases}$

On vérifie :

$$\begin{aligned} &741\,(531k + 301) + 531\,(-741k - 420) \\ &= 741 \times 531k + 741 \times 301 - 531 \times 741k - 531 \times 420 \\ &= 741 \times 301 - 531 \times 420 \\ &= 21 \end{aligned}$$

COROLLAIRE :

Soient a, b et c trois entiers non nuls.

i. Si a et b divisent c et $a \wedge b = 1$, alors $ab|c$

ii. Si p est premier et $p|ab$, alors ($p|a$ ou $p|b$)

Démonstration. i. $a|c$ donc il existe un entier k tel que $c = ak$. $b|c$ donc il existe un entier k' tel que $c = bk'$. Donc $ak = bk'$. Donc $a|bk'$. Or, $a \wedge b = 1$ donc d'après le théorème de Gauss : $a|k'$. Donc il existe un entier k'' tel que $k' = ak''$ et donc $c = bk' = abk''$. Ceci montre que $ab|c$.

ii. Si $p|a$ alors $p|ab$ et donc la propriété est évidente. Si p ne divise pas a : comme p est premier, il admet exactement deux diviseurs positifs qui sont 1 et p. Comme $p \wedge a$ est un diviseur de p alors $p \wedge a = 1$ ou $p \wedge a = p$. Or, si $p \wedge a = p$ alors $p|a$, ce qui est exclu par hypothèse. Donc $p \wedge a = 1$ et comme par hypothèse aussi, $p|ab$, on en déduit par le théorème de Gauss que $p|b$. La propriété est démontrée. □

4. PPCM de deux entiers

■ THÉORÈME :

Soient a et b deux entiers naturels non nuls. L'ensemble des multiples strictement positifs communs à a et b admet un plus petit élément, appelé **Plus Petit Commun Multiple** de a et b et noté $a \vee b$ ou $\text{ppcm}(a\,;\,b)$.

Démonstration. L'ensemble des multiples strictement positifs communs à a et b est une partie de $\mathbb{N}^*$ non vide, puisqu'elle contient $a \times b$, donc elle admet d'après l'axiome du plus petit élément, un plus petit élément. □

■ PROPRIÉTÉ :

Soient a et b deux entiers naturels non nuls.

$$a \vee b = \frac{a \times b}{a \wedge b}$$

Démonstration. On sait que $a \wedge b$ divise a et b, d'où

$$\frac{ab}{a \wedge b} = a' \times b' \text{ où } a' = \frac{a}{a \wedge b} \text{ et } b' = \frac{b}{a \wedge b}$$

Ceci montre que l'entier $\dfrac{a \times b}{a \wedge b}$ est bien un multiple de a et de b.

On va maintenant montrer que si m est un multiple quelconque strictement positif commun à a et b, alors c'est un multiple de $\dfrac{a \times b}{a \wedge b}$ et donc que ce dernier est le plus petit de ces multiples :
m étant un multiple commun strictement positif à a et b, il existe deux entiers n et n' tels que $m = an$ et $m = bn'$, donc : $an = bn'$, puis avec les notations précédentes, en divisant par $a \wedge b$, on obtient $a'n = b'n'$ où $a' \wedge b' = 1$: Or, cette égalité implique que $a' | b'n'$ et donc, d'après le théorème de Gauss, on obtient : $a' | n'$. Donc il existe un entier $k > 0$ tel que $n' = ka'$.

Comme $m = bn'$, on obtient alors :

$$\begin{aligned} m &= b \times k \times a' \\ &= k \frac{a \times b}{a \wedge b} \end{aligned}$$

c'est-à-dire que le multiple quelconque strictement positif commun à a et b est un multiple de $\dfrac{a \times b}{a \wedge b}$, qui est donc le plus petit d'entre eux. □

On a de plus montré :

■ COROLLAIRE :

Tout multiple strictement positif commun à deux entiers naturels a et b est un multiple de $a \vee b$.

Exemples :

- Déterminer $1\,958 \vee 4\,539$.
  On a déjà calculé $1\,958 \wedge 4\,539 = 89$.
  Donc
  $$\begin{aligned} 1\,958 \vee 4\,539 &= \frac{1\,958 \times 4\,539}{89} \\ &= \frac{8\,887\,682}{89} \\ &= 99\,854 \end{aligned}$$

- Déterminer tous les couples d'entiers strictement positifs $(a\,;\,b)$ tels que : $a \wedge b + a \vee b = a + b$.
  Soit $d = a \wedge b$. Alors $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$.
  On a $a \vee b = \dfrac{ab}{a \wedge b} = \dfrac{da' \times db'}{d} = da'b'$.
  L'équation devient : $d + da'b' = da' + db'$
  En divisant par d : $1 + a'b' = a' + b'$
  Donc $a'b' - a' - b' + 1 = 0$, i.e. $(a'-1)(b'-1) = 0$.
  Donc $a' = 1$ ou $b' = 1$.
  - Si $a' = 1$, alors $a = d$ et $b = db'$.

    L'équation devient $d + db' = d + db'$, ce qui est vrai.
  - De même si $b' = 1$.

  Donc les solutions sont tous les couples (d, db') et (da', d) où $d \geqslant 1$ et a' et b' sont supérieurs ou égaux à 1.

5. Le petit théorème de Fermat

THÉORÈME : Petit théorème de Fermat

Si p est un nombre premier et a un entier tel que p ne divise pas a, alors $a^{p-1} \equiv 1\,[p]$

Exemples :

$2^{96} \equiv 1\,[97]$. Écrire d'autres congruences de ce type.

Autres exemples de congruences utilisant le petit théorème de Fermat :

- $3^{10} \equiv 1\,[11]$ (car 11 est premier et $11 \nmid 3$)
- $5^{12} \equiv 1\,[13]$ (car 13 est premier et $13 \nmid 5$)
- $7^{16} \equiv 1\,[17]$ (car 17 est premier et $17 \nmid 7$)
- $2^{22} \equiv 1\,[23]$ (car 23 est premier et $23 \nmid 2$)

Démonstration. On considère un nombre premier p et un entier a tel que p ne divise pas a.

1. Montrer que p ne divise aucun des entiers a, $2a$, $3a$, …, $(p-1)a$.
   Supposons par l'absurde qu'il existe $k \in \{1\,;\,2\,;\,\ldots\,;\,p-1\}$ tel que $p|ka$.
   Comme p est premier et $p \nmid a$ (par hypothèse), et comme $p|ka$, le corollaire du théorème de Gauss donne $p|k$.
   Mais $1 \leqslant k \leqslant p-1$, donc $k < p$, ce qui contredit $p|k$ (car les seuls multiples positifs de p sont $p, 2p, 3p\ldots$).
   Donc p ne divise aucun des $a, 2a, 3a, \ldots, (p-1)a$.
2. Montrer que pour $1 \leqslant i \leqslant p-1$ et $1 \leqslant j \leqslant p-1$ avec i et j entiers distincts, les restes de la division de ia et ja par p sont distincts.
   Supposons par l'absurde que $ia \equiv ja\,[p]$ avec $i \neq j$.
   Alors $p|(ia - ja) = (i-j)a$.
   Comme p est premier et $p \nmid a$, le corollaire du théorème de Gauss donne p divise $i-j$.
   Mais $(i\,;\,j) \in [\![1\,;\,p-1]\!]^2$ avec $i \neq j$, donc $|i-j| < p$, ce qui contredit le fait que p divise $i-j$.
   Donc les restes sont tous distincts.
3. Déduire des questions précédentes que les restes des divisions par p des entiers a, $2a$, $3a$, …, $(p-1)a$ sont les entiers : $1, 2, 3, \ldots, (p-1)$.
   D'après la question 1, aucun des entiers $a, 2a, \ldots, (p-1)a$ n'est divisible par p, donc leurs restes sont tous non nuls, c'est-à-dire dans $\{1, 2, \ldots, p-1\}$.
   D'après la question 2, ces $p-1$ restes sont tous distincts.
   Comme il y a exactement $p-1$ entiers dans $\{1, 2, \ldots, p-1\}$ et $p-1$ restes distincts, ces restes sont donc exactement $\{1, 2, \ldots, p-1\}$.
4. On considère maintenant les $p-1$ divisions euclidiennes suivantes :

$$\begin{aligned} a &= pq_1 + r_1 \text{ où } 0 < r_1 < p \\ 2a &= pq_2 + r_2 \text{ où } 0 < r_2 < p \\ &\vdots \\ ia &= pq_i + r_i \text{ où } 0 < r_i < p \\ &\vdots \\ (p-1)a &= pq_{p-1} + r_{p-1} \text{ où } 0 < r_{p-1} < p \end{aligned}$$

   Déduire de ces égalités et de la question précédente que : $1\times2\times\cdots\times(p-1)\times a^{p-1} \equiv 1\times2\times\cdots\times(p-1)\,[p]$ puis que $a^{p-1} \equiv 1\,[p]$.
   En multipliant toutes les congruences $ia \equiv r_i\,[p]$ pour $i = 1, 2, \ldots, p-1$:
   $(1\times a)(2\times a)\cdots((p-1)\times a) \equiv r_1 \times r_2 \cdots r_{p-1}\,[p]$

   Soit : $(1\times2\times\cdots\times(p-1))\times a^{p-1} \equiv r_1\times r_2\cdots r_{p-1}\,[p]$

   D'après la question précédente,

$$\{r_1, r_2, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}$$

   Donc $r_1 \times r_2 \cdots r_{p-1} = 1 \times 2 \times \cdots \times (p-1)$.

   Par conséquent :

   $(1\times2\times\cdots\times(p-1))\times a^{p-1} \equiv 1\times2\times\cdots\times(p-1)\,[p]$

   Comme p ne divise aucun des $1, 2, \ldots, p-1$, leur produit n'est pas divisible par p non plus.

   On peut donc simplifier par $(1 \times 2 \times \cdots \times (p-1))$ et obtenir : $a^{p-1} \equiv 1\,[p]$.

□

COROLLAIRE :

Soit p un nombre premier et a un un entier tel que p ne divise pas a. Alors

$$a^p \equiv a\,[p]$$

Remarque : La réciproque est fausse, on donnera un contre-exemple en exercice.