Aujourd'hui nous allons discuter :

- L'algorithme d'Euclide pour calculer le pgcd
- L'algorithme d'Euclide-Bézout, 2 versions
- Le théorème de Bézout et des conséquences.

Division avec reste

Montré hier :

Théorème (Division-avec-reste)

Soit $m > 0$ *un nombre naturel non-zéro fixé.*

Pour chaque $n \in \mathbb{Z}$ *il existe deux uniques nombres entiers* q, r *tels que simultanément :*
(i) $n = qm + r$;
(ii) $0 \leq r < m$.

L'algorithme d'Euclide

Pour calculer le $\text{pgcd}(24871, 18480)$.
Divisions avec reste :

$$\begin{aligned}
\color{red}{24871} &= 1 \cdot 18480 + 6391 \\
\color{red}{18480} &= 2 \cdot 6391 + 5698 \\
6391 &= 1 \cdot 5698 + 693 \\
5698 &= 8 \cdot 693 + 154 \\
693 &= 4 \cdot 154 + \color{red}{77} \\
154 &= 2 \cdot 77 + 0
\end{aligned}$$

Conclusion : $\text{pgcd}(24871, 18480) = 77$.

L'algorithme d'Euclide-Bézout

Avec administration :

$$
\begin{aligned}
(1)24871 + (0)18480 &= 24871 \\
(0)24871 + (1)18480 &= 18480 \\
(1)24871 + (-1)18480 &= 6391 = 24871 - 18480 \\
(-2)24871 + (3)18480 &= 5698 = 18480 - 2 \cdot 6391 \\
(3)24871 + (-4)18480 &= 693 = 6391 - 5698 \\
(-26)24871 + (35)18480 &= 154 = 5698 - 8 \cdot 693 \\
(107)24871 + (-144)18480 &= 77 = 693 - 4 \cdot 154
\end{aligned}
$$

Donc

$$(107)24871 + (-144)18480 = 77.$$

Autre méthode. Début : La suite des divisons avec reste :

$$\begin{aligned} 24871 &= 1 \cdot 18480 + 6391 \\ 18480 &= 2 \cdot 6391 + 5698 \\ 6391 &= 1 \cdot 5698 + 693 \\ 5698 &= 8 \cdot 693 + 154 \\ 693 &= 4 \cdot 154 + 77 \\ 154 &= 2 \cdot 77 + 0 \end{aligned}$$

donne

$$\begin{aligned} 77 &= 693 - 4 \cdot 154 \\ 154 &= 5698 - 8 \cdot 693 \\ 693 &= 6391 - 5698 \\ 5698 &= 18480 - 2 \cdot 6391 \\ 6391 &= 24871 - 18480 \end{aligned}$$

$$\begin{aligned}
77 &= 693 - 4 \cdot 154 \\
154 &= 5698 - 8 \cdot 693 \\
693 &= 6391 - 5698 \\
5698 &= 18480 - 2 \cdot 6391 \\
6391 &= 24871 - 18480
\end{aligned}$$

Substituer, modifier, répéter :

$$\begin{aligned}
{\color{red}77} &= 693 - 4 \cdot {\color{red}154} \\
&= 693 - 4 \cdot (5698 - 8 \cdot 693) = (33){\color{red}693} - (4)5698 \\
&= (33)(6391 - 5698) - (4)5698 = (33)6391 - (37){\color{red}5698} \\
&= (33)6391 - (37)(18480 - 2 \cdot 6391) = (107){\color{red}6391} - (37)18480 \\
&= (107)(24871 - 18480) - (37)18480 \\
&{\color{red}= (107)24871 - (144)18480}
\end{aligned}$$

Euclide-Bézout : Méthode par substitutions

(i) Pour $1351, 1064$. On commence par la suite des restes :

$$\begin{aligned}
287 &= 1351 - 1 \cdot 1064 \\
203 &= 1064 - 3 \cdot 287 \\
84 &= 287 - 1 \cdot 203 \\
35 &= 203 - 2 \cdot 84 \\
14 &= 84 - 2 \cdot 35 \\
7 &= 35 - 2 \cdot 14 \\
0 &= 14 - 2 \cdot 7.
\end{aligned}$$

(ii) On commence en bas avec la combinaison $\mathbb{Z}$-linéaire :

$$7 = 35 - 2 \cdot 14;$$

on substitue $14 = 84 - 2 \cdot 35$ et on réécrit

$$7 = 35 - 2 \cdot (84 - 2 \cdot 35) = -2 \cdot 84 + 5 \cdot 35.$$

Puis on monte une ligne. On substitue $35 = 203 - 2 \cdot 84$ et on rééecrit :

$$7 = -2 \cdot 84 + 5 \cdot 35 = -2 \cdot 84 + 5 \cdot (203 - 2 \cdot 84) = 5 \cdot 203 + (-12) \cdot 84.$$

Puis on monte une ligne. On substitue $84 = 287 - 1 \cdot 203$ et on réécrit :

$$7 = 5 \cdot 203 + (-12) \cdot 84 = 5 \cdot 203 + (-12) \cdot (287 - 1 \cdot 203) = (-12) \cdot 287 + 17 \cdot 203.$$

On monte jusqu'en haut.

Le résultat :

$$\begin{aligned}
7 &= 35 - 2 \cdot 14 = 35 - 2 \cdot (84 - 2 \cdot 35) = \\
&= -2 \cdot 84 + 5 \cdot 35 = -2 \cdot 84 + 5 \cdot (203 - 2 \cdot 84) = \\
&= 5 \cdot 203 + (-12) \cdot 84 = 5 \cdot 203 + (-12) \cdot (287 - 203) = \\
&= (-12) \cdot 287 + 17 \cdot 203 = (-12) \cdot 287 + 17 \cdot (1064 - 3 \cdot 287) = \\
&= 17 \cdot 1064 + (-63) \cdot 287 = 17 \cdot 1064 + (-63)(1351 - 1064) = \\
&= (-63) \cdot 1351 + 80 \cdot 1064.
\end{aligned}$$

Pour être sûr qu'on n'a pas fait une erreur de calcul on vérifie la réponse. En effet

$$(-63) \cdot 1351 + 80 \cdot 1064 = -85113 + 85120 = 7$$

À cause de toutes les substitutions on risque facilement de faire une erreur de calcul.

Il y a une autre méthode, qui est un peu plus propre avec moins de risque d'erreur de calcul.
Cette méthode calcule le pgcd et la combinaison $\mathbb{Z}$-linéaire simultanément.

Moi, je prèfére cette méthode, que j'appele la méthode de Bézout.

Euclide-Bézout : Méthode de Bézout

Commence avec deux combinaisons $\mathbb{Z}$-linéaire triviales. Le début :

$$\begin{aligned} {\color{red}1} \cdot 1351 + {\color{red}0} \cdot 1064 &= 1351 \\ {\color{red}0} \cdot 1351 + {\color{red}1} \cdot 1064 &= 1064 \end{aligned}$$

Le premier reste est $287 = 1351 - 1064$. Donc aussi

$$287 = 1351 - 1064 = [1 \cdot 1351 + 0 \cdot 1064] - [0 \cdot 1351 + 1 \cdot 1064] =$$

$$= (1 - 0) \cdot 1351 + (0 - 1) \cdot 1064.$$

D'où une ligne de plus

$$\begin{aligned} 1 \cdot 1351 + 0 \cdot 1064 &= 1351 \\ 0 \cdot 1351 + 1 \cdot 1064 &= 1064 \\ {\color{red}1 \cdot 1351 + (-1) \cdot 1064} &{\color{red}=} {\color{red}287} \end{aligned}$$

Le deuxième reste est $203 = 1064 - 3 \cdot 287$ donc aussi

$$\begin{aligned}
203 &= 1064 - 3 \cdot 287 \\
&= [0 \cdot 1351 + 1 \cdot 1064] + (-3) \cdot [1 \cdot 1351 + (-1) \cdot 1064] \\
&= (0 - 3) \cdot 1351 + (1 + (-3)(-1)) \cdot 1064 \\
&= (-3) \cdot 1351 + (4) \cdot 1064
\end{aligned}$$

Et une autre ligne s'est ajoutée :

$$\begin{aligned}
1 \cdot 1351 + 0 \cdot 1064 &= 1351 \\
0 \cdot 1351 + 1 \cdot 1064 &= 1064 \\
1 \cdot 1351 + (-1) \cdot 1064 &= 287 \\
(-3) \cdot 1351 + (4) \cdot 1064 &= 203
\end{aligned}$$

Et on répète.

On a

$$\begin{array}{rcl}
1 \cdot 1351 + 0 \cdot 1064 & = & 1351 \\
0 \cdot 1351 + 1 \cdot 1064 & = & 1064 \\
1 \cdot 1351 + (-1) \cdot 1064 & = & 287 \\
(-3) \cdot 1351 + (4) \cdot 1064 & = & 203 \\
(4) \cdot 1351 + (-5) \cdot 1064 & = & 84 \\
(-11) \cdot 1351 + (14) \cdot 1064 & = & 35 \\
(26) \cdot 1351 + (-33) \cdot 1064 & = & 14 \\
(-63) \cdot 1351 + (80) \cdot 1064 & = & 7
\end{array}$$

La dernière ligne donne nos deux réponses, le pgcd et la combinaison $\mathbb{Z}$-linéaire.

Je vois cet algorithme (appelé *l'algorithme de Bézout*) comme l'algorithme d'Euclide renforcé par de l'administration.

La partie à la droite du $=$ est la suite des restes, pour calculer le pgcd(n, m) avec l'algorithme d'Euclide.

La partie à la gauche du $=$ commence par deux combinaisons triviales $\mathbb{Z}$-linéaire de n et m. Puis , ce qu'on fait à droit pour obtenir le prochain reste, on fait aussi à gauche pour maintenir l'administration.

Cet algorithme de Bézout/Euclide donne une preuve constructive du théorème de Bézout :

Théorème (Bézout)

Soient n, m deux entiers avec $d = \operatorname{pgcd}(n, m)$.
Alors il existe deux entiers s, t tel que $sn + tm = d$.

Démonstration.

Si $m = 0$, alors $1 \cdot n + 0 \cdot m = d$, si $n \geq 0$ et $-1 \cdot n + 0 \cdot m = d$, si $n < 0$. Et le résultat est vrai.
Sans perte de généralité on peut supposer que n et m sont des nombres naturels et $m > 0$. Puis l'algorithme de Bézout fonctionne pour calculer tels s et t.
On peut aussi utiliser l'induction pour montrer ce théorème. $\square$

Une variation.

Théorème

Soient a, b, c *trois entiers. Posons* $d = \mathrm{pgcd}(a, b)$*.*
Considérons l'équation

$$ax + by = c.$$

Il est possible de résoudre cette équation avec des entiers (c.-à-d. de trouver deux entiers x *et* y *tel que l'équation est satisfaite) si et seulement si* $d|c$*.*

Et il y a un algorithme !

Démonstration.

Supposons des entiers x, y existent tels que $ax + by = c$. On a $d|a$ et $d|b$ donc aussi $d|(ax + by)$ et nécessairement $d|c$.

Par contre si $d|c$, il existe $n \in \mathbb{Z}$ tel que $c = dn$. Par le théorème de Bézout ils existent s, t tels que $d = as + bt$ donc $c = dn = a(sn) + b(tn)$. Et on voit que le pair $x = sn$ et $y = tn$ forme une solution de l'équation. $\square$

Par exemple :
L'équation $1351x + 1064y = 29$ n'a pas de solution entière, car $\mathrm{pgcd}(1064, 1351) = 7$ ne divise pas 29.

L'équation $1351x + 1064y = 21$ a une solution entière, car $\mathrm{pgcd}(1064, 1351) = 7$ divise 21.

Trouver une solution.

L'équation $1351x + 1064y = 21$ a une solution entière, car $\mathrm{pgcd}(1064, 1351) = 7$ divise 21.
Heureusement nous savons déjà obtenu :

$$(-63) \cdot 1351 + 80 \cdot 1064 = 7,$$

donc

$$(-63 \cdot 3) \cdot 1351 + (80 \cdot 3) \cdot 1064 = 7 \cdot 3 = 21,$$

et

$$1351 \cdot (-189) + 1064 \cdot 240 = 21$$

Donc la couple $x = -189$ et $y = 240$ est une solution.

Autres solutions existent ? Oui.

Le théorème de Bézout a des corollaires utiles.

Théorème

(i) Soient a, b, c *trois entiers tels que* $a|bc$ *et* $\mathrm{pgcd}(a, b) = 1$*. Alors* $a|c$*.*
(ii) Soit p *un nombre premier tel que* $p|bc$*. Alors* $p|b$ *ou* $p|c$*.*

Mais $6|(2 \cdot 3)$ et $6 \not| 2$ et $6 \not| 3$ (6 n'est pas premier).

Corollaire

Si p est un nombre premier tel que $p|(n_1 n_2 \dots n_s)$. Alors il existe un i tel que $p|n_i$.

(Par induction sur s)

Démonstration.

(i) Hypothèse $\operatorname{pgcd}(a, b) = 1$: il existe entiers s, t tels que $sa + tb = 1$ par Bézout, et donc

$$sac + tbc = c$$

Hypothèse $a|bc$: il existe u tel que $au = bc$. Donc

$$c = sac + tau = (sc + tu)a$$

ou

$$a|c$$

(ii) Si le nombre premier p ne divise pas b alors $pgcd(p, b) = 1$. Donc l'hypothése de (i) est satisfaite et on peut conclure. $\square$

Factorization première

Déjà montré :

Théorème

Pour chaque nombre naturel $n > 1$ il existe un entier $s \geq 1$ et des nombres premiers $p_1,\ p_2, \ldots, p_s$ tels que

$$n = p_1 p_2 \ldots p_s,$$

et $p_1 \leq p_2 \leq \ldots \leq p_s$.

On dit : "Une décomposition première existe".

On a unicité aussi :

Théorème

Soit $n > 1$ un nombre naturel. Si

$$\begin{aligned} n &= p_1 p_2 \dots p_s \\ &= q_1 q_2 \dots q_t \end{aligned}$$

où $p_1 \leq p_2 \leq \ldots \leq p_s$ et $q_1 \leq q_2 \leq \ldots \leq q_t$ des nombres premiers.

Alors $s = t$ et $p_1 = q_1$, $p_2 = q_2, \ldots, p_s = q_s$.

Démonstration.

Par induction sur n (seulement l'unicité).

Préparation : On a $p_i | (p_1 p_2 \dots p_s)$. Et si p est premier, la seule factorisation première est : $p = p$.
La fonction propositionnelle $P(n) :=$ "n a une unique factorization première". À montrer :

$$\forall n \geq 2 \ P(n)$$

Le début. Pour $n = 2$ il n'y a qu'une seule factorisation (car 2 est premier.)
Étape d'induction : Soit $n \geq 2$ et supposons pour chaque $2 \leq m \leq n$ la factorisation première pour m est unique. □

(suite).

Si $n+1$ est premier, il y a une seule factorisation, comme déjà remarqué.

Supposons $n+1$ est composé et $n+1 = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$ sont deux factorisations ordonnées. Les p_i et q_j sont tous des nombres premiers qui divisent $n+1$.

Soit $p \geq 2$ le plus petit nombre premier qui divise $n+1$. Alors $p | p_1 p_2 \dots p_s$ implique $p = p_i$ pour un i. Par minimalité nécessairement $p = p_1$. Et de même façon $p = q_1$. Donc au moins

$$p_1 = q_1.$$

$\square$

(suite).

Posons $m = p_2 \dots p_s = q_2 \dots q_t$, alors $2 \leq m \leq n$ (car $n+1$ est composé).

Par l'hypothèse d'induction, m a une seule factorization.
C'est à dire $s-1 = t-1$ et $p_2 = q_2$, $p_3 = q_3 \dots$. Donc aussi les deux factorisations de $n+1$ coïncident.

Conclusion : Par induction généreuse on conclut que l'unicité de la factorisation première est vraie. $\square$

Soit $n > 1$ alors on peut aussi écrire uniquement

$$n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s},$$

où $p_1 < p_2 < \dots < p_s$ sont des nombres premiers et les a_i des nombres naturels.

On a
$r = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ divise n

si et seulement si $e_1 \leq a_1,\ e_2 \leq a_2,\ \dots, e_s \leq a_s$.

Dans ce cas, posons $s = p_1^{a_1 - e_1} p_2^{a_2 - e_2} \dots p_s^{a_s - e_s}$, alors

$$rs = n.$$

Il y a une conséquence bien connue :

En général, trouver une factorisation première est très laborieux. Mais si on a déjà factorisé n et m on peut facilement calculer $\mathrm{pgcd}(n, m)$.

Théorème

Supposons

$$n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s},$$

et

$$m = p_1^{b_1} p_2^{b_2} \ldots p_s^{b_s},$$

où $p_1 < p_2 < \ldots < p_s$*, les* $a_i \geq 0$ *et les* $b_i \geq 0$*.*
Alors

$$\operatorname{pgcd}(n, m) = p_1^{c_1} p_2^{c_2} \ldots p_s^{c_s},$$

et

$$\operatorname{ppcm}(n, m) = p_1^{d_1} p_2^{d_2} \ldots p_s^{d_s},$$

où c_i *est le minimum de* $\{a_i, b_i\}$ *et* d_i *est le maximum de* $\{a_i, b_i\}$*.*

Corollaire

Soit n et m deux nombres naturels positifs. Alors

$$nm = \mathrm{pgcd}(n, m) \cdot \mathrm{ppcm}(n, m)$$

Par exemple : On a

$$
\begin{aligned}
1064 &= 2^3 \cdot 7^1 \cdot 19^1 \cdot 193^0, \\
1351 &= 2^0 \cdot 7^1 \cdot 19^0 \cdot 193^1, \\
\mathrm{pgcd}(1064, 1351) &= 2^0 \cdot 7^1 \cdot 19^0 \cdot 193^0 = 7, \\
\mathrm{ppcm}(1064, 1351) &= 2^3 \cdot 7^1 \cdot 19^1 \cdot 193^1 = 205352, \\
205352 \cdot 7 &= 1437464 = 1064 \cdot 1351.
\end{aligned}
$$

Solutions générales entières

Cherchons toutes les solutions en entiers pour X et Y de l'équation

$$aX + bY = c,$$

où a, b, c sont trois entiers.

Déjà : Des solutions existent si et seulement si $\mathrm{pgcd}(a, b) | c$.

Posons $d := \text{pgcd}(a, b)$ et supposons que $d|c$.

Par l'algorithme d'Euclide-Bézout nous pouvons calculer des entiers m, n tels que $am + bn = d$.

On a $d|c$, donc il existe un entier q tel que $dq = c$.

Alors

$$a(mq) + b(nq) = dq = c,$$

et le couple $X = mq$ et $Y = nq$ est une solution particulière.

Par exemple, l'équation $1351X + 1064Y = 21$ a une solution entière, car $\text{pgcd}(1064, 1351) = 7$ divise 21.
Déjà obtenu :

$$(-63) \cdot 1351 + 80 \cdot 1064 = 7,$$

donc aussi

$$(-63 \cdot 3) \cdot 1351 + (80 \cdot 3) \cdot 1064 = 7 \cdot 3 = 21,$$

et

$$1351 \cdot (-189) + 1064 \cdot 240 = 21$$

Donc la couple $X = -189$ et $Y = 240$ est une solution.

Il y a d'autres solutions ?

On a $1351 = 7 \cdot 193$ et $1064 = 7 \cdot 152$, donc

$$152 \cdot 1351 = 152 \cdot 7 \cdot 193 = 1064 \cdot 193$$

Pour chaque entier $h \in \mathbb{Z}$ le couple $x = -189 + h \cdot 152$ et $y = 240 - h \cdot 193$ est aussi une solution :

$$(-189 + h \cdot 152) \cdot 1351 + (240 - h \cdot 193) \cdot 1064 =$$

$$= (-189) \cdot 1351 + (240) \cdot 1064 = 21,$$

Par exemple, $h = 1$ donne : $x = -37$ et $y = 47$, et en effet

$$1351 \cdot (-37) + 1064 \cdot 47 = -49987 + 50008 = 21.$$

Cette méthode fonctionne généralement pour trouver les autres solutions de $aX + bY = c$.

Posons encore $d = \mathrm{pgcd}(a, b)$ et $d|c$.
Pour certains entiers a' et b' on a $a = a'd,\ b = b'd$. Alors $a'b = a'b'd = ab'$.
Supposons le couple $(x, y) \in \mathbb{Z}^2$ est une solution particulière de l'équation $aX + bY = c$.
Alors pour chaque entier $n \in \mathbb{Z}$ on a

$$a(x + nb') + b(y - na') = ax + by + anb' - bna' = c.$$

Donc $(x + nb', y - na')$ est aussi une solution pour chaque n. C'est la solution générale.

Il n'y a pas d'autre solution

Preuve : Supposons (x, y) et (x', y') sont deux solutions entières de $aX + bY = c$: $ax + by = c = ax' + by'$.

Comme avant $d := \text{pgcd}(a, b)$, $a = a'd$, $b = b'd$, $c = c'd$.
Et donc $a'x + b'y = c' = a'x' + b'y'$, d'où $a'(x' - x) = b'(y - y')$ et $b'|(a'(x' - x))$.

Exercice : $\text{pgcd}(a', b') = 1$.

Donc le théorème montré ce matin donne : $b'|(x' - x)$, c.-à-d., il existe un $n \in \mathbb{Z}$ tel que $x' - x = nb'$ ou $x' = x + nb'$.

Et $b'(y - y') = a'(x' - x) = a'nb'$, donc $y - y' = a'n$ et $y' = y - na'$.

Donc (x', y') est une solution "générale". $\square$