RUNSER Laure
03.02.2021

Maths 4 : Ampli 2 - Suite du Chapitre 1 : Arithmétique

I/ Algorithme d'Euclide (suite)

Ce lemme nous donne un algo pour calculer le PGCD → algorithme d'Euclide.

Algorithme d'Euclide : on suppose $a \geq b$ (sinon on les échange)

* Soit (q_1, r_1) la division euclidienne de a par b.
* Si $r_1 = 0$: $b \mid a \Rightarrow PGCD(a,b) = b$ ✱

  Sinon : par le lemme d'Euclide, $PGCD(a,b) = PGCD(b, r_1)$. On recommence.
* Le PGCD est le dernier reste $\neq 0$.

Exemple : $PGCD(21,15) = 3$ car $21 = 1 \times 15 + \overbrace{6}^{\neq 0}$ $\quad 15 = 2 \times 6 + \overbrace{3}^{\neq 0}$ $\quad 6 = 2 \times 3 + 0$ (3 : PGCD)

II/ Théorème de Bezout

Théorème : Soit $a, b \in \mathbb{Z}$. Alors $\exists u, v \in \mathbb{Z}$ tels que $PGCD(a,b) = ua + vb$

⚠ u et v ne sont PAS uniques.

Preuve constructive (Algorithme d'Euclide étendu)

idée : on applique l'algo d'Euclide, et on "remonte" à partir de la fin.

preuve : On suppose $a, b \geq 0$

On écrit $a = bq_1 + r_1$ (✱)

Si $r_1 = 0$ $\quad PGCD(a,b) = b = 0 \times a + 1 \times b$

Sinon $\quad b = r_1 q_2 + r_2$

Si $r_2 = 0$ $\quad PGCD(a,b) = r_1$ $\quad$ D'après (✱) $\quad r_1 = 1 \times a - q_1 b$

Sinon $\quad r_2 = r_1 q_3 + r_3$ (✱)

Si $r_3 = 0$ $\quad PGCD(a,b) = r_2$ D'après (✱) $r_2 = b - r_1 q_2$ D'après (✱) $r = b - (a - bq_1)q_2 = b - aq_2 + bq_1 q_2 = -q_2 a + (1 + q_1 q_2) b$

Sinon On continue de la même façon.

Exemple

$21 = 1 \times 15 + 6$
$15 = 2 \times 6 + 3$
~~$6 = 3 \times 2 + 0$~~

$PGCD(21,15) = 3 = 15 - 2 \times 6 = 15 - 2 \times (21 - 15) = 15 - 2 \times 21 + 2 \times 15 = (-2) \times 21 + 3 \times 15$ $\quad$ donc $(u,v) = (-2, 3)$

Prop : Soient $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si $\exists u, v \in \mathbb{Z}$ tq $ua + vb = 1$

Preuve :

$\Rightarrow$ a et b 1ers entre eux $\Rightarrow$ PGCD $(a,b) = 1 \Rightarrow$ par Bezout $\exists u, v \in \mathbb{Z}$ tq $ua + vb = 1$

$\Leftarrow$ Si u et v existent tq $ua + vb = 1$
Puisque PGCD (a,b) divise a et b, alors PGCD $(a,b) \mid ua + vb$
donc PGCD $(a,b) \mid 1$ donc PGCD $(a,b) = 1$ donc a et b 1ers entre eux.

Lemme : Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{Z}$ un diviseur commun de a et b.
Alors $c \mid$ PGCD (a,b)

Lemme : Soient $a, b, c \in \mathbb{Z}$
PGCD $(ca, cb) = |c| \times$ PGCD (a,b)

Lemme de Gauss : Soient $a, b \in \mathbb{Z}$ et $c \mid ab$
Si c est premier avec a, alors $c \mid b$.

Preuve : Puisque PGCD $(a,c) = 1$, d'après Bezout $\exists u, v \in \mathbb{Z}$ tq $au + cv = 1$

En multipliant par b : $abu + cbv = b$

Par hypothèse, $c \mid ab$ donc $c \mid abu$
Par ailleurs, $c \mid bcv$

Donc $c \mid abu + bcv = b$

Corollaire (Lemme d'Euclide) : Soient $a, b \in \mathbb{Z}$, et p un nombre premier.
Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Preuve : De 2 choses l'une :
* Soit $p \mid a$ $\rightarrow$ OK
* Sinon $\Rightarrow$ PGCD $(a,p) = 1$ Par le lemme de Gauss, $p \mid b$ $\rightarrow$ OK

Corollaire : Soient $a, b, c \in \mathbb{Z}$
Si $a \mid c$ et $b \mid c$ et PGCD $(a,b) = 1$, alors $ab \mid c$

Preuve : $a \mid c \Rightarrow \exists k \in \mathbb{Z}$ tq $c = ak$
PGCD $(a,b) = 1$ et $b \mid c$
Lemme de Gauss $\Rightarrow b \mid k \Rightarrow ab \mid ak \Rightarrow ab \mid c$

Lemme : Soient $a, b \in \mathbb{Z}$, alors PGCD $(a,b) \times$ PPCM $(a,b) = a, b$

Rq : a et b 1ers entre eux $\Rightarrow$ PPCM $(a,b) = ab$

Preuve : Soit $d =$ PGCD (a,b) et m un multiple commun
On pose $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$

$\exists k, l$ tq $m = ka = lb$. En divisant par d : $ka' = lb'$

Par le lemme de Gauss, $a' \mid l$ donc $\exists q \in \mathbb{Z}$ tq $l = a'q$

Ça nous dit que $m = qa'b'd$
$ab = \underbrace{a'd}_{\text{PPCM}}\underbrace{b'd}_{\text{PGCD}}$

Réciproquement : $\forall q \in \mathbb{Z}$, $q\,a'b'd$ multiple commun de ab.

Donc le plus petit, $q = 1$, $PPCM(a, b) = a'b'd = ab/PGCD(a, b)$