Propriétés du pgdc

07.11.23

Soit $a \in \mathbb{Z}$, $b \in \mathbb{Z}$

① $\operatorname{pgdc}(a, a) = a$

② $\operatorname{pgdc}(a, 0) = a$

③ $\operatorname{pgdc}(a, b) = \operatorname{pgdc}(a, a-b)$

④ Si $a = qb + r$ avec $0 \leq r < b$, alors

$\operatorname{pgdc}(a, b) = \operatorname{pgdc}(a, r) = \operatorname{pgdc}(a, a \bmod b)$

2.3.1 Appliquer l'algorithme d'Euclide (soustractions successives) à

a) 135 et 156 ;

b) 17017 et 19210 ;

c) 21331 et 43947.

b) $\text{pgdc}(19'210,\ 17'017) = \text{pgdc}(17'017,\ 2193) = \text{pgdc}(14\,824,\ 2193) = \text{pgdc}(12'631,\ 2193)$

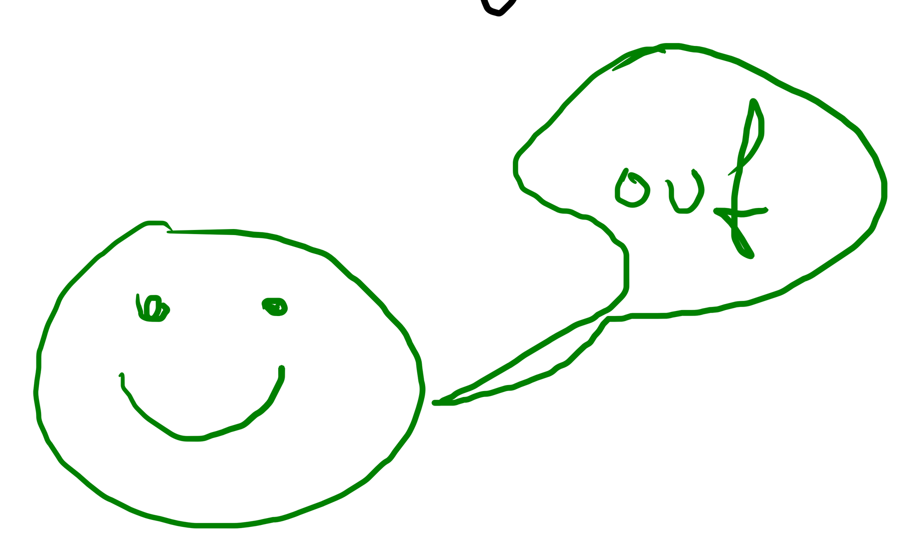
$= \text{pgdc}(10\,438,\ 2193) = \text{pgdc}(8245,\ 2193) = \text{pgdc}(6052,\ 2193) = \text{pgdc}(3859,\ 2193)$

$= \text{pgdc}(2193,\ 1666) = \text{pgdc}(1666,\ 527) = \text{pgdc}(1139,\ 527) = \text{pgdc}(612,\ 527)$

$= \text{pgdc}(527,\ 85) = \text{pgdc}(442,\ 85) = \text{pgdc}(357,\ 85) = \text{pgdc}(272,\ 85)$

$= \text{pgdc}(187,\ 85) = \text{pgdc}(102,\ 85) = \text{pgdc}(85,\ 17) = \text{pgdc}(68,\ 17)$

$= \text{pgd}(51,\ 17) = \text{pgdc}(34,\ 17) = \text{pgdc}(17,\ 17) = \text{pgd}(17,\ 0) = 17$



2.3.2 Appliquer l'algorithme d'Euclide (divisions avec reste) à

a) 121 et 365 ;

b) 89 et 144 ;

c) 295 et 595 ;

d) 1001 et 1309.

c)

Itération	a	b	a mod b	Commentaire
1	595	295	5	$595 = 2 \cdot 295 + 5$
2	295	5	0	$295 = 59 \cdot 5$

$\text{pgdc}(595, 295) = 5$

d)

Itération	a	b	a mod b	Commentaire
1	1309	1001	308	$1309 = 1 \cdot 1001 + 308$
2	1001	308	77	$1001 = 3 \cdot 308 + 77$
3	308	77	0	$308 = 4 \cdot 77 + 0$

$\text{pgdc}(1309, 1001) = 77$

2.3.3 En utilisant l'algorithme d'Euclide (divisions avec reste), trouver le plus grand diviseur commun de

a) 17017 et 18900 ;

b) 21063 et 43137 ;

c) 92263 et 159037 ;

d) 112345 et 112354.

A faire à la maison !

Calcul du pgdc avec la factorisation en facteurs premiers

$$\text{pgdc}(120, 84) = 12$$

120	2
60	2
30	2
15	3
5	5
1	1

84	2
42	2
21	3
7	7
1	1

$$120 = 2^3 \cdot 3 \cdot 5 \qquad 84 = 2^2 \cdot 3 \cdot 7$$

$$\text{pgdc}(120, 84) = 2^2 \cdot 3 = 4 \cdot 3 = 12$$

Théorème du pgdc

Soit a, b deux nombres entiers. Il existe deux nombres entiers x et y tels que $a \cdot x + b \cdot y = \text{pgdc}(a,b)$

On ne va pas démontrer ce théorème avec une preuve directe.

On va créer un algorithme qui donne x et y à partir de a et b.

Cet algorithme s'appelle l'algorithme d'Euclide étendu.

On commence par écrire

$$a = 1 \cdot a + 0 \cdot b$$
$$b = 0 \cdot a + 1 \cdot b$$
$$r = 1 \cdot a + (-q \cdot b) \qquad a = q \cdot b + r$$

On réitère les deux dernières lignes

Prenons un exemble : $a = 2322$ et $b = 654$

Ligne	reste	$\cdot a$	$\cdot b$	commentaire	q	Calcul de q
1	2322	1	0			
2	654	0	1			
3	360	1	−3	La 1ère ligne moins 3 fois la 2ème ligne	3	$2322 = 3 \cdot 654 + 360$
4	294	−1	4	La 2ème ligne moins 1 fois la 3ème ligne	1	$654 = 1 \cdot 360 + 294$
5	66	2	−7	La 3ème ligne moins 1 fois la 4ème ligne	1	$360 = 1 \cdot 294 + 66$
6	30	−9	32	La 4ème ligne moins 4 fois la 5ème ligne	4	$294 = 4 \cdot 66 + 30$
7	6	20	−71	La 5ème ligne moins 2 fois la 6ème ligne	2	$66 = 2 \cdot 30 + 6$
8	0			L'algorithme est fini	5	$30 = 5 \cdot 6$

$$\boxed{20 \cdot 2322 + (-71) \cdot 654 = 6}$$

2.3.7 Calculer les nombres s et t tels que $s \cdot a + t \cdot b = \text{pgcd}(a, b)$, avec les nombres a et b suivants :

a) $a = 72$, $b = 39$;

b) $a = 1008$, $b = 25$;

Ligne	reste	$\cdot a$	$\cdot b$	Commentaire	q	Calcul de q
1	72	1	0			
2	39	0	1		1	$72 = 1 \cdot 39 + 33$
3	33	1	−1	La 1ère ligne moins 1 fois la 2ème ligne	1	$39 = 1 \cdot 33 + 6$
4	6	−1	2	La 2ème ligne moins 1 fois la 3ème ligne	5	$33 = 5 \cdot 6 + 3$
5	3	6	−11	La 3ème ligne moins 5 fois la 4ème ligne		$6 = 2 \cdot 3 + 0$
6	0			L'algorithme est fini		

$$6 \cdot 72 - 11 \cdot 39 = 3$$