chA3 : pgcd dans N

Objectif : approfondir nos connaissances sur le pgcd de deux entiers naturels

I. PLUS GRAND DIVISEUR COMMUN

1. définition pgcd

a) pgcd d'entiers non nuls

a et b deux entiers positifs non nuls :
le plus grand des diviseurs communs à *a* et à b est appelé pgcd de *a* et de b, noté pgcd(*a*,b)

On notera ici {div (a,b)} = l'ensemble des diviseurs communs à a et b
exemple : les diviseurs positifs de 18 sont 1 ; 2 ; 3 ; 6 ; 9 ; 18 ; ceux de 30 sont 1 ; 2 ; 3 ; 5 ; 6 ; 10 ; 15 ; 30 donc {div(18;30)} = {1 ; 2 ; 3 ; 6} et pgcd(18,30) = 6

b) cas de 0

rq : on peut étendre la définition au cas où l'un d'eux est nul :

prop: pour $a \neq 0$, pgcd(*a*,*0*) = *a*

dem : tous les entiers sont diviseurs de 0 ; les diviseurs communs à *0* et à *a* sont les diviseurs de *a*, dont le plus grand est *a*

2. premières propriétés

* pgcd(*a*,*b*)= pgcd(*b*,*a*)
* si *a* divise b alors pgcd(*a*,*b*) = *a*

(rq ça marche pour *a* qui divise 0)

3. nombres premiers entre eux

def deux entiers *a* et b sont premiers entre eux lorsque pgcd(*a*,*b*) = 1.
exemple : pgcd(18;35) =1

II. ALGORITHMES D'EUCLIDE

1. algo par soustraction :

a) pgcd et soustraction

rappel PROP (chapitre I.): si c divise *a* et *b* alors c divise *ua+vb*,
Ÿ en particulier: si c divise *a* et b alors c divise *a+b*, *a-b*, (mais aussi *2a+3b*, *5a-4b* , ...)

prop : **pgcd(*a*,*b*) = pgcd(*a-b*,*b*)**
On doit ici démontrer l'égalité de deux ensembles :
l'ensemble des diviseurs communs à a et b = l'ensemble des diviseurs communs à a-b et b:
dans deux ensembles contenant les mêmes éléments, le plus grand élément est le même!
Le procédé général est de démontrer une « double inclusion » : chaque élément de l'un est contenu dans l'autre ; et réciproquement, chaque élément de l'autre est contenu dans l'un. Les deux ensembles sont alors bien identiquement les mêmes.

dem : si *d* divise *a* et *b* alors *d* divise aussi *a-b* Ÿ si *d* divise *a* et *b* alors *d* divise *b* et *a-b* ;
si *d* divise *b* et *a-b* alors *d* divise aussi *a* Ÿ si *d* divise *b* et a-b alors *d* divise *a* et *b*
Ÿ {div (*a*,*b*)} = {div(*a-b*;*b*) }Ÿ pgcd(*a*,*b*) = pgcd(*a-b*,*b*)

b) application au calcul du pgcd
exemple :
pgcd(145,15) = pgcd(130;15) = é = pgcd (10,15) = pgcd(10,5)=pgcd(5,5) = [= pgcd(5,0)] = 5

2. algo par division euclidienne:

a) pgcd et div euclidienne
prop : si $a=bq+r$ alors pgcd(a,b) = pgcd(b,r)
dem : si d divise a et b alors (PROP) d divise aussi $r = 1a-qb$ Ÿ si d divise a et b alors d divise b et r ;
si d divise b et r alors d divise aussi $a = qb+1r$Ÿ si d divise b et r alors d divise a et b
Ÿ {div (a,b)} = {div(b,r) }Ÿ pgcd(a,b) = pgcd(b,r)

remarque : cette propriété est valable si $a=bq+r$, même si la condition $0 \leq r \leq b-1$ n'est pas respectée (donc même si ce n'est pas une écriture de division euclidienne);
En particulier, en écrivant $a=1*b + (a-b)$, on retrouve la propriété « pgcd et soustraction »

b) application au calcul du pgcd
exemple : en appliquant successivement cette propriété, on peut écrire :
pgcd(145,15) = pgcd(15,10) = pgcd (10,5) = [= pgcd(5,0)] = 5
(NB : 5 est en fait le dernier reste non nul)
méthode on applique successivement la propriété liant le pgcd et la division euclidienne : la suite des restes est une suite d'entiers positifs, strictement décroissante (car r < b) donc cette suite aboutit nécessairement à 0:
pgcd(a;b) = pgcd (b;r_1) = pgcd (r_1;r_2) é =pgcd (r_n ; 0) = r_n dernier reste non nul.

III. PGCD ET DIVISIBILITÉ
prop pgcd et multiplication : pgcd(ka,kb) = k*pgcd (a,b)
dem : l'égalite $a=bq+r$ équivaut à $ka = kbq+kr$, donc pgcd(ka,kb) = pgcd (kb,kr)
Par conséquent la succession d'égalités de l'algorithme d'Euclide conduit à un dernier reste non nul égal à $k* r_n$

Ÿ conséquences

prop si d divise a et b alors d divise pgcd(a,b)
dem
si d divise a et b alors $a=da'$ et $b=db'$ donc pgcd(a,b) = d*pgcd(a',b') ce qui montre que d divise pgcd(a,b) (CF def « divise »)
la réciproque est évidente : si d divise le pgcd de a et de b, comme le pgcd de a et b est lui-même un diviseur de a (et de b), par transitivité d divise a (et b)

prop D = pgcd(a,b) si et ssi $a=Da'$ et $b=Db'$ avec pgcd(a',b')=1 (càd a' et b' premiers entre eux)
dem
* si D = pgcd(a,b) alors $a=Da'$ et $b=Db'$ et l'égalité pgcd(a,b) = D*pgcd(a',b') = D donne pgcd(a',b') = 1
* réciproquement, si $a=Da'$ et $b=Db'$ avec pgcd(a',b')=1 alors pgcd(a,b) = D*pgcd(a',b') = D*1 = D

exemple : pgcd(18,30) = 6 et on a bien 18=6*3 et 30=6*5 avec 3 et 5 premiers entre eux.