PGCD ET NOMBRES PREMIERS (SPÉCIALITÉ)

1. PGCD

DÉFINITION

Soient a et b deux entiers naturels tels que $a \neq 0$ ou $b \neq 0$.

Le PGCD de a et de b est le plus grand diviseur commun à a et à b.

EXEMPLE

On cherche le PGCD de 60 et de 45.

Les diviseurs de 60 sont : 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 10 ; 12 ; 15 ; 20 ; 30 et 60.

Les diviseurs de 45 sont : 1 ; 3 ; 5 ; 9 ; 15 et 45.

Les diviseurs communs à 60 et 45 sont : 1 ; 3 ; 5 et 15.

Donc le PGCD de 60 et 45 est 15.

REMARQUES

- Si b divise a, PGCD$(a;b) = b$. En effet, b divise alors a et b, et b est le plus grand diviseur de b. En particulier, PGCD$(a;1) = 1$ et PGCD$(0\,;\,b) = b$
- On prolonge la notion de PGCD à des entiers **relatifs** a et b par PGCD$(a;b)$=PGCD$(|a|;|b|)$.

THÉORÈME

Soient a et b deux entiers naturels non nuls et r le reste de la division euclidienne de a par b.

Alors : PGCD$(a;b)$ = PGCD$(b;r)$.

EXEMPLE

Le reste de la division euclidienne de 60 par 45 est 15. donc PGCD$(60\,;\,45)$ = PGCD$(45\,;\,15)$.

Si l'on réitère le processus, le reste de la division euclidienne de 45 par 15 est 0 donc PGCD$(45\,;\,15)$ = PGCD$(15\,;\,0) = 15$.

ALGORITHME D'EUCLIDE

- On effectue la division euclidienne de a par b et on note r_1 le reste de cette division.
- Puis si $r_1 \neq 0$, on effectue la division euclidienne de b par r_1 et on note r_2 le reste de cette division.
- Puis si $r_2 \neq 0$, on effectue la division euclidienne de r_1 par r_2, et ainsi de suite...

La suite $r_0 = b$, r_1, r_2, ... est strictement décroissante, et pour un certain rang n on aura $r_n = 0$.

Par conséquent :

$\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,r_0) = \text{PGCD}(r_0\,;\,r_1) = \ldots$

$= \text{PGCD}(r_{n-1}\,;\,r_n) = \text{PGCD}(r_{n-1}\,;\,0) = r_{n-1}$

Le PGCD de a et b est donc **le dernier reste non nul** dans cette suite.

EXEMPLE

On cherche à déterminer le PGCD de 2691 et de 1404.

- le reste de la division euclidienne de 2691 par 1404 est 1287,
- le reste de la division euclidienne de 1404 par 1287 est 117,
- le reste de la division euclidienne de 1287 par 117 est 0.

Par conséquent $\text{PGCD}(2691\,;\,1404) = 117$.

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls.

L'ensemble des diviseurs communs à a et à b est l'ensemble des diviseurs de leur PGCD.

DÉFINITION

On dit que deux entiers naturels non nuls sont **premiers entre eux** si leur PGCD est égal à 1.

REMARQUE

On peut généraliser cette notion à plus de deux entiers de deux façons différentes.

Si a, b et c sont trois entiers non nuls :

- on dit que a, b et c sont premiers entre eux **dans leur ensemble** lorsque le seul diviseur commun à a, b et c est 1 ;
- on dit que a, b et c sont premiers entre eux **deux à deux** lorsque $\text{PGCD}(a\,;\,b) = 1$, $\text{PGCD}(b\,;\,c) = 1$ et $\text{PGCD}(a\,;\,c) = 1$.

Par exemple 4 , 6 et 9 sont premiers entre eux dans leur ensemble (pas de diviseur commun à ces trois nombres autre que 1) mais ne sont pas premiers entre eux deux à deux puisque $\text{PGCD}(4\,;\,6) = 2$ et $\text{PGCD}(6\,;\,9) = 3$.

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls.

d est le PGCD de a et de b si et seulement si il esiste deux entiers a' et b' **premiers entre eux** tels que $a = a'd$ et $b = b'd$.

EXEMPLE

Le PGCD de 60 et de 45 est 15. On a :

$60 = 4\times15$ et $45 = 3\times15$ et 4 et 3 sont premiers entre eux.

THÉORÈME (DE BÉZOUT)

Deux entiers naturels a et b non nuls sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que :

$$au + bv = 1.$$

REMARQUE

Les valeurs de u et de v peuvent être obtenues à l'aide de l'algorithme d'Euclide (fiche méthode à venir...)

EXEMPLE

Pour tout entier naturel n, $2n+1$ et n sont premiers entre eux.

En effet $1 \times (2n+1) - 2 \times n = 1$. Donc d'après le théorème de Bézout (avec $u = 1$ et $v = -2$), n et $2n+1$ sont premiers entre eux.

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls et d leur PGCD.

Alors, il existe deux entiers relatifs u et v tels que :

$$au + bv = d.$$

REMARQUE

Attention, la réciproque est fausse.

Si $au+bv = d$ on peut seulement en déduire que le PGCD de a et de b divise d (d'après une propriété du chapitre précédent). Par exemple $3 \times 4 + 2 \times (-5) = 2$ mais le PGCD de 3 et de 2 est 1 (ils sont premiers entre eux) et non 2.

THÉORÈME (DE GAUSS)

Soient a, b et c trois entiers naturels non nuls.

- Si a divise le produit bc
- et si a est premier avec b,

alors, a divise c.

EXEMPLE

On cherche tous les couples d'entiers naturels $(m;n)$ tels que $5m = 3n$.

L'égalité $5m = 3n$ signifie que 5 divise $3n$. Comme 5 et 3 sont premiers entre eux, d'après le théorème de Gauss 5 divise n. Donc il existe un entier naturel k tel que $n = 5k$. On a alors $5m = 3n = 15k$ soit $m = 3k$.

Réciproquement, on vérifie aisément que tout couple de la forme $(3k;5k)$ (où $k \in \mathbb{N}$) est solution de l'équation proposée.

PROPRIÉTÉ

Si a et b divisent c et sont premiers entre eux, alors le produit ab divise c.

EXEMPLES

D'après cette propriété :

- n est divisible par 6 si et seulement si il est divisible par 2 et par 3 (car 2 et 3 sont premiers entre eux).
- n est divisible par 15 si et seulement si il est divisible par 3 et par 5 (car 3 et 5 sont premiers entre eux).

REMARQUE

L'hypothèse « a et b sont premiers entre eux » est essentielle. Par exemple 90 est divisible par 6 et par 10 mais n'est pas divisible par $6\times10 = 60$.

2. NOMBRES PREMIERS

DÉFINITION

Un entier naturel est premier s'il admet exactement deux diviseurs (dans $\mathbb{N}$) : 1 et lui-même.

REMARQUE

1 n'est pas un nombre premier (il possède un seul diviseur).

PROPRIÉTÉS

- Tout entier naturel $n > 1$ admet au moins un diviseur premier.
- Tout entier naturel $n > 1$ **non premier** admet au moins un diviseur premier inférieur ou égal à $\sqrt{n}$.

REMARQUE

La seconde propriété est souvent utilisée pour démontrer (par l'absurde) qu'un entier naturel n est premier. Il suffit, en effet, de montrer que n n'est divisible par aucun nombre premier p inférieur ou égal à $\sqrt{n}$. On peut donc arrêter la recherche de diviseurs premiers p dès que $p^2 > n$.

EXEMPLE

41 est-il premier ?

- 41 n'est pas divisible par 2 (dernier chiffre impair),
- 41 n'est pas divisible par 3 (somme des chiffres 4+1=5),
- 41 n'est pas divisible par 5 (dernier chiffre différent de 0 et de 5),
- 7^2=49 > 41 (donc $7 > \sqrt{41}$) : inutile de chercher plus loin...

Conclusion : 41 est un nombre premier.

PROPRIÉTÉ

Il existe une infinité de nombres premiers.

DÉMONSTRATION

On raisonne par l'absurde en supposant que l'ensemble des nombres premiers n'est pas infini. Il existe alors un plus grand nombre premier p.

On pose $N = 2 \times 3 \times 5 \times \cdots \times p$ (produit de tous les nombres premiers).

Comme tout entier naturel supérieur à 1 admet au moins un diviseur premier, $N+1$ admet un diviseur premier d.

Or d divise aussi le nombre N puisque N est le produit de **tous** les nombres premiers.

d divise $N+1$ et N, donc il divise leur différence 1, ce qui est impossible.

PROPRIÉTÉ

Si p est un nombre premier et a un entier naturel non nul non divisible par p, alors p et a sont premier entre eux.

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls.

Si un nombre premier p divise le produit ab, alors p divise a ou b.

REMARQUE

Cette propriété résulte immédiatement de la propriété précédente et du théorème de Gauss.

THÉORÈME (THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE)

Tout entier naturel $n > 1$ se décompose en produit de nombres premiers.

Cette décomposition peut s'écrire :

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

où les p_i sont des nombres premiers distincts et les a_i des entiers naturels non nuls.

Cette décomposition est unique à l'ordre près des facteurs.

EXEMPLE

Cherchons la décomposition de 60 en facteurs premiers.

- 60 est divisible par 2 et le quotient de cette division est 30.
- 30 est divisible par 2 et le quotient est 15.
- 15 est divisible par 3 et le quotient est 5.
- Enfin, 5 est premier.

Donc $60 = 2^2 \times 3 \times 5$.

PROPRIÉTÉ

Soit n un entier naturel supérieur à 1 dont la décomposition en facteurs premiers s'écrit $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

Alors, les diviseurs de n sont les entiers de la forme :

$$n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

avec $0 \leqslant b_i \leqslant a_i$ pour tout $0 \leqslant i \leqslant k$.

EXEMPLE

$60 = 2^2 \times 3 \times 5$ admet comme diviseurs les nombres de la forme $2^{b_1} \times 3^{b_2} \times 5^{b_3}$ avec $0 \leqslant b_1 \leqslant 2$, $0 \leqslant b_2 \leqslant 1$ et $0 \leqslant b_3 \leqslant 1$.

Il y a trois valeurs possibles pour b_1 et deux valeurs possibles pour b_2 et pour b_3. Au total, 60 possède donc $3 \times 2 \times 2 = 12$ diviseurs (en comptant 1 et lui-même).