Nombres premiers

1 PGCD de deux nombres entiers

Propriété - Définition

Soient a et b deux entiers relatifs dont l'un au moins est non nul.
L'ensemble des diviseurs communs à a et à b admet un plus grand élément que l'on appelle le **plus grand diviseur commun** et que l'on note $\text{PGCD}(a\,;\,b)$.

Démonstration

L'ensemble des diviseurs de a et b est un ensemble non vide puisque 1 est un élément de cet ensemble.
De plus, il s'agit d'un ensemble fini.
Cet ensemble admet donc un plus grand élément.

Remarque

On trouvera parfois la notation $a \wedge b$ dans les manuels ou dans les ressources en ligne. Elle remplace la notation $\text{PGCD}(a\,;\,b)$.

Exemple

D'après la décomposition en produit de facteurs premiers de 60 on a $60 = 2^2 \times 3 \times 5$.
D'après la décomposition en produit de facteurs premiers de 50 on a $50 = 2 \times 5^2$.
On a ainsi $\text{PGCD}(60\,;\,50) = 2 \times 5 = 10$.

Propriétés

Soient a et b deux entiers relatifs avec $a \neq 0$.

- $\text{PGCD}(a\,;\,b) = \text{PGCD}(|a|\,;\,|b|)$
- $\text{PGCD}(a\,;\,0) = a$
- $\text{PGCD}(a\,;\,1) = 1$
- Si b divise a alors $\text{PGCD}(a\,;\,b) = |b|$
- $\forall k \in \mathbb{Z}^*\,;\,\text{PGCD}(ka\,;\,kb) = k\text{PGCD}(a\,;\,b)$

Propriété

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

$$\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,r)$$

Démonstration

Notons q et r le quotient et le reste de la division euclidienne de a par b.
Si d est un diviseur de b et r alors d divise $a = bq + r$ et donc d est un diviseur de a et b.
Réciproquement, si d est un diviseur de a et b alors d divise $r = a - bq$ et donc d est un diviseur de b et r.
Finalement, l'ensemble des diviseurs commun de a et b est égal à l'ensemble des diviseurs communs de b et r. On a en particulier $\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,r)$.

Théorème

Soit a et b deux entiers naturels non nuls.
La suite des divisions euclidiennes du diviseur par le reste de la division euclidienne précédente est finie. Le dernier reste non nul est alors le PGCD de a et b.

Exemple : Algorithme d'Euclide

On souhaite déterminer le PGCD de 4 539 et 1 958.

$$\begin{aligned} 4\,539 &= 1\,958 \times 2 + 623 \\ 1\,958 &= 623 \times 3 + 89 \\ 623 &= 89 \times 7 + 0 \end{aligned}$$

Ainsi, $\text{PGCD}(4\,539\,;\,1\,958) = 89$.

2 Théorème de Bezout

Définition : nombres premiers entre eux

Soient a et b deux entiers naturels non nuls.
On dit que a et b sont **premiers entre eux** quand leur PGCD vaut 1.

Exemples

- Dans l'exemple précédent, 4 539 et 1 958 ne sont pas premiers entre eux.
- Les nombres 55 et 42 sont-ils premiers entre eux ? Vérifions à l'aide de l'algorithme d'Euclide.
  $55 = 42 \times 1 + 13$
  $42 = 13 \times 3 + 3$
  $13 = 3 \times 4 + 1$
  Le dernier reste non nul vaut 1, qui est le PGCD de 55 et 42. Ils sont donc premiers entre eux.

Théorème : Identité de Bezout

Soient a et b deux entiers relatifs non nuls. Il existe deux entiers relatifs u et v tels que

$$au + bv = \text{PGCD}(a\,;\,b)$$

Démonstration

Notons E l'ensemble des entiers naturels non nuls de la forme $ax + by$ où x et y sont des entiers relatifs. E est une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément que l'on note n.
Par définition de E, il existe donc des entiers relatifs u et v tels que $n = au + bv$.
Or Le PGCD de a et b divise a et b donc PGCD$(a\,;\,b)$ divise n. Ainsi, PGCD$(a\,;\,b) \leqslant n$.

Posons la division euclidienne de a par n : $a = nq + r$ avec $0 \leqslant r < n$ et $q \in \mathbb{Z}$.
On a donc $r = a - qn = a - q(au + bv) = a(1 - qu) + b(-qv)$
Ainsi, r est de la forme $ax + by$ avec x et y des entiers relatifs. De plus, $r < n$, donc r n'est pas un élément de E.
On a donc nécessairement $r = 0$ ce qui signifie que n divise a.

De la même manière, on montre que n divise b.
Par définition du PGCD de a et b, $n \leqslant$ PGCD$(a\,;\,b)$.
Ainsi : PGCD$(a\,;\,b) = n = au + bv$.

Théorème de Bezout

Deux entiers relatifs a et b sont premiers entre eux si et seulement si, il existe deux entiers relatifs u et v tels que

$$au + bv = 1$$

Démonstration

Si a et b sont premiers entre eux alors PGCD$(a\,;\,b) = 1$ et à l'aide de l'identité de Bezout, on montre qu'il existe deux entiers u et v tels que $au + bv = 1$.
Réciproquement, supposons qu'il existe deux entiers u et v tels que $au + bv = 1$. PGCD$(a\,;\,b)$ divise a et PGCD$(a\,;\,b)$ divise b donc PGCD$(a\,;\,b)$ divise aussi $au + bv$ et donc PGCD$(a\,;\,b) = 1$.

Exemple

Soit n un entier naturel.
On souhaite montrer que $2n + 1$ et $3n + 2$ sont premiers entre eux.
Il faut trouver deux entier u et v tels que $u(2n + 1) + v(3n + 2) = 1$.
En prenant $u = -3$ et $b = 2$ on obtient : $-3(2n + 1) + 2(3n + 2) = -6n - 3 + 6n + 4 = 1$.
Puisqu'il existe deux entiers u et v tels que $u(2n + 1) + v(3n + 2) = 1$ alors $2n + 1$ et $3n + 2$ sont premiers entre eux.

Méthode : Déterminer un couple d'entiers de Bézout

On souhaite déterminer deux entiers u et v tels que $59u + 27 = 1$.
Appliquons l'algorithme d'Euclide :

$59 = 27 \times 2 + 5 \quad (1)$

$27 = 5 \times 5 + 2 \quad (2)$

$5 = 2 \times 2 + 1 \quad (3)$

Le PGCD$(59\,;\,27) = 1$ donc 59 et 27 sont premiers entre eux.
On remontre ensuite ces égalités :

$1 = 5 - 2 \times 2$ d'après (3)

$1 = 5 - 2 \times (27 - 5 \times 5)$ d'après (2)

$1 = 5 - 2 \times 27 + 10 \times 5$

$1 = 59 - 2 \times 27 - 2 \times 27 + 10 \times (59 - 2 \times 27)$ d'après (1)

$1 = 59 - 2 \times 27 - 2 \times 27 + 10 \times 59 - 20 \times 27$

$1 = 59 \times 11 + 27 \times (-24)$

Les entiers u et v recherchés sont donc $u = 11$ et $v = -24$.

Propriété

Soit a un nombre entier.
a admet un inverse modulo n si a et n sont premiers entre eux.

Exemple : résoudre une équation du type $ax \equiv n\ (n)$

On souhaite résoudre l'équation $5x \equiv 7\ (16)$ où x est un entier.

Puisque 5 et 16 sont premiers entre eux, 5 admet un inverse modulo 16. Notons x cet inverse.
x est congru à 0 ou 1 ou 2 ou ... ou 15 modulo 16. On a donc :

x modulo 16	0	1	2	3	...
$5x$ modulo 16	0	5	10	15 ou -1	...

On s'arrête puisque si $5 \times 3 \equiv -1\ (16)$ alors $5 \times (-3) \equiv 1\ (16)$.
-3 est donc un inverse de 5 modulo 16.

$5x \equiv 7\ (16) \Leftrightarrow 5 \times (-3)x \equiv 7 \times (-3)\ (16) \Leftrightarrow 1x \equiv -21\ (16) \Leftrightarrow x \equiv 11\ (16)$.

Les entiers solutions sont donc les x de la forme $11 + 16k$ où k est un entier relatif.

3 Théorème de Gauss

Théorème de Gauss

Soient a, b et c des entiers relatifs non nuls.
Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration

Puisque a divise bc, il existe un entier relatif k tel que $bc = ka$.
Puisque a et b sont premiers entre eux, il existe, d'après le théorème de Bezout, deux entiers relatifs u et v tels que $au + bv = 1$.
Si on multiplie par c cette égalité, on obtient
Autrement dit :

$$c = acu + bvc = acu + kav = a(cu + kv)$$

Posons $m = cu + ku$, qui est un entier. On a alors $c = am$ donc c est un multiple de a ou encore, a divise c.

Exemple

On souhaite résoudre l'équation $5(x-1) = 7y$ où x et y sont des entiers relatifs.

7 divise $5(x-1)$ et 7 et 5 sont premiers entre eux.
Alors d'après le théorème de Gauss, 7 divise $x-1$. Il existe donc un entier relatif k tel que $7k = x-1$ soit $x = 7k+1$.
On remplace x par $7k+1$ dans notre équation pour trouver $y = 7k$.
Les solutions de cette équation sont donc de la forme $x = 7k+1$ et $y = 7k$ où $k \in \mathbb{Z}$.

Corollaire du théorème de Gauss

Soient a, b et c trois entiers naturels non nuls.
Si b et c sont premiers entre eux, si b divise a et c divise a alors ab divise a.

Démonstration

Puisque b et c divisent a alors il existe deux entiers k et k' tels que $a = kb$ et $a = k'c$.
Cela donne donc $kb = k'c$. Ce qui signifie que b divise $k'c$. Puisque b et c sont premier entre eux, alors d'après le théorème de Gauss, b divise k'. Il existe donc un entier relatif k'' tel que $k' = k''b$.
On a alors $a = k'c = k''bc$ ce qui implique que bc divise a.

Définition : équation diophantienne

On appelle **équation diophantienne** une équation de la forme $ax + by = c$ où les coefficients a, b et et c sont des entiers et où les solutions x et y sont aussi des nombres entiers.

Exemple

On souhaite résoudre l'équation $17x - 33y = 1$.

- On cherche tout d'abord une solution particulière.
  Ici, une solution évidente est le couple $(2\,;\,1)$ puisque $17 \times 2 - 33 \times 1 = 1$;

- On va maintenant trouver toutes les solutions.
  Soit $(x\,;\,y)$ une solution de l'équation. On a donc le système :

$$\begin{cases} 17x - 33y &= 1 \\ 17 \times 2 - 33 \times 1 &= 1 \end{cases}$$

  On soustrait ces deux lignes pour obtenir $17(x-2)-33(y-1) = 0$ ce qui est équivalent à $17(x-2) = 33(y-1)$.
  Cela signifie que 33 divise $17(x-2)$ et puisque 17 et 33 sont premiers entre eux, d'après le théorème de Gausse, 33 divise $x-2$. Il existe donc un entier relatif k tel que $33k = x-2$ ou encore $x = 33k+2$.
  En remplaçant dans notre équation de départ, on obtient $y = 1+17k$.
  Les solutions sont donc de la forme

$$\begin{cases} x &= 33k+2 \\ y &= 17k+1 \end{cases} \text{ où } k \in \mathbb{Z}$$

- On vérifie : $17(2+33k) - 33(1+17k) = 34 + 561k - 33 - 561k = 1$.

4 Les nombres premiers

Définition

Soit n un nombre entier naturel.
On dit que n est un **nombre premier** s'il admet exactement deux diviseurs distincts : 1 et lui-même.

Exemple

Voici les premiers nombres premiers :

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 21 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43

Remarques

- 1 n'est pas un nombre premier puisqu'il n'a qu'un seul diviseur.
- Le seul nombre premier pair est 2.
- 42 n'est pas un nombre premier puisqu'il admet d'autres diviseurs que 1 et 42 $(2\,;\,6\,;\,7\,;\,21\,;\,...)$.

Propriété

L'ensemble des nombres premiers est infini : il existe une infinité de nombres premiers.

Démonstration

On va raisonner par l'absurde.
Supposons qu'il existe un nombre fini de nombres premiers : $p_1 < p_2 < ... < p_n$.
On pose $N = p_1 \times p_2 \times ... \times p_n + 1$.

- Si N est premier alors iil existe un nombre premier plus grand que p_n puisque $p_1 \times p_2 \times ... \times p_n + 1 > p_n$.
- Si N n'est pas premier, il admet au moins un diviseur premier p.
  Supposons que p soit compris entre p_1 et p_n. Ainsi, p divise $p_1 \times p_2 \times ... \times p_n$.
  Puisque p divise aussi N, alors p divise 1, ce qui est contradictoire avec notre hypothèse. Cela signifie que $p > n$. Il existe donc un nombre premier p plus grand que p_n.

Propriété

Soit n un entier naturel supérieur ou égal à 2.
Si n n'est pas premier alors il admet un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$.

Démonstration

Supposons que n soit un entier supérieur ou égal à 2 et non premier.

L'ensemble des diviseurs de n n'est donc pas vide et admet un plus petit élément p.
Si p n'était pas premier, il admettrait un diviseur d qui diviserait n. C'est impossible puisque p est le plus petit élément de l'ensemble des diviseurs de n. Donc p est premier.
n admet donc un diviseur premier p tel que $n = p \times q$ avec $p \leqslant q$.

En multipliant par p on obtient $p^2 \leqslant pq \Leftrightarrow p^2 \leqslant n$ soit $p \leqslant \sqrt{n}$.

Remarque

Cette propriété permet de montrer qu'un nombre est premier.

Exemple

Est-ce que 109 est un nombre premier ?
On a $10 < \sqrt{109} < 11$.
Or 109 n'est divisible ni par 2, ni par 3, ni par 5 ni par 7.
Cela signifie que 109 est un nombre premier.

Théorème fondamental de l'arithmétique

Soit n un entier naturel supérieur ou égal à 2.
Cet entier se décompose de façon unique (à l'ordre des facteurs près) sous la forme d'un produit de nombres premiers. On note

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_m^{\alpha_m}$$

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

Propriété

Soit n un entier naturel supérieur ou égal à 2 et sa décomposition en produit de facteurs premiers $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_m^{\alpha_m}$.

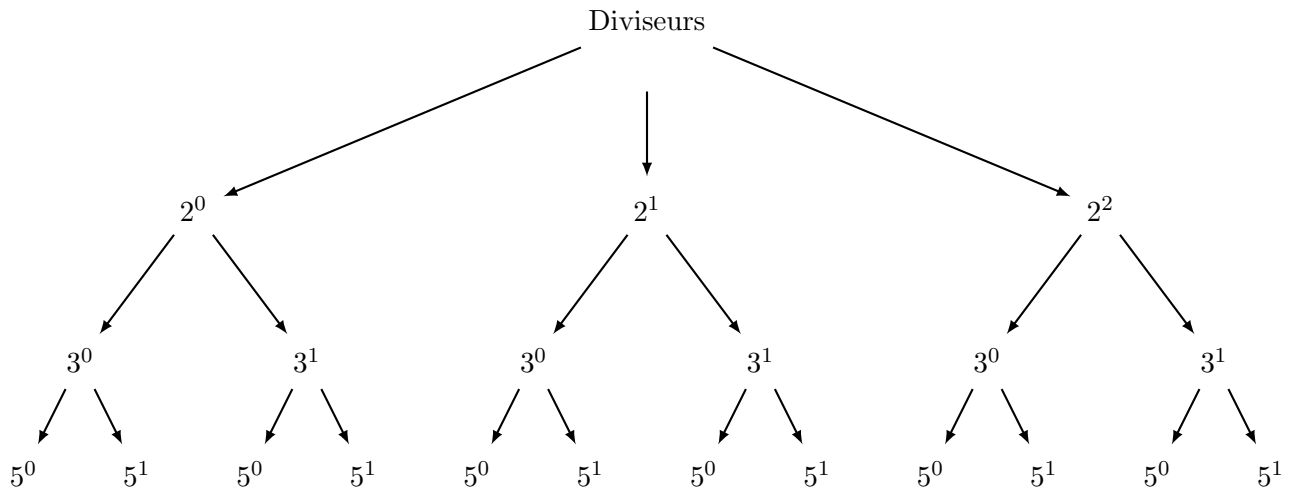
- Le nombre de diviseur de n est $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_m + 1)$.
- Tout diviseur d de n admet pour décomposition

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_m^{\beta_m}$$

où les β_i sont tels que $0 \leqslant \beta_i \leqslant \alpha_i$ avec i un entier compris entre 1 et m.

Exemple

On souhaite déterminer le nombre de diviseurs de 60 et la liste de ces diviseurs.
On a $60 = 2^2 \times 3^1 \times 5^1$.
Le nombre de diviseurs de 60 est donc $(2+1)(1+1)(1+1) = 12$. Le nombre 60 admet 12 diviseurs.
On peut ensuite utiliser un arbre pour faire la liste des diviseurs de 60 :



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

5 Le petit théorème de Fermat

Théorème

Soit p un nombre premier et soit n un entier naturel qui ne soit pas un multiple de p.
$a^{p-1} - 1$ est divisible par p. On peut également noter :

$$a^{p-1} \equiv 1 \ (p)$$

Démonstration

On considère les $p-1$ premiers multiples de a : a, $2a$, ..., $(p-1)a$.
On considère leurs restes dans la division euclidienne par p : r_1, r_2, ..., r_{p-1}.

- Supposons qu'il existe deux restes identiques $r_i = r_j$ avec $i > j$. On a alors :

$$ia - ja \equiv r_i - r_j \ (p) \Leftrightarrow a(i-j) \equiv 0 \ (p)$$

  Cela veut dire que p divise $a(i-j)$ et d'après le théorème de Gauss, p divise a ou p divise $i-j$.
  Or a n'est pas un multiple de p et $i-j < p$. Ces restes sont donc tous différents.

- Ces restes sont donc tous différents et puisqu'il y a $p-1$ multiples, on trouve tous les restes non nul possibles dans la division par p.

- On a alors $r_1 \times r_2 \times ... \times r_{p-1} = 1 \times 2 \times ... \times (p-1) = (p-1)!$.

- On a ensuite $a \times 2a \times ... \times (p-1)a \equiv (p-1)! \ (p)$

  $\Leftrightarrow \quad (p-1)!a^{p-1} \equiv (p-1)! \ (p)$

  $\Leftrightarrow \quad (p-1)!(a^{p-1}-1) \equiv 0 \ (p)$

$(p-1)!$ est premier avec p puisque tous les facteurs de $(p-1)!$ sont inférieurs à p. D'après le théorème de Gauss, $a^{p-1}-1$ est donc un multiple de p.

Corollaire

Soit p un nombre premier et soit a un entier naturel.
Le nombre $a^p - a$ est divisible par p. On peut également noter :

$$a^p \equiv a \ (p)$$

Démonstration

Il suffit de multiplier l'égalité du précédent théorème par a.
L'égalité reste vraie si a est un multiple de p puisque l'on aura alors $a \equiv 0 \ (p)$.

Exemples

- $4^{12} \equiv 1 \ (13)$ car 13 est premier avec 4 et non multiple de 13.

- 7 est premier et 3 est non multiple de 7. D'après le petit théorème de Fermat, on a :

$$3^6 \equiv 1 \ (7) \Rightarrow 3^{6n} \equiv 1^n \equiv 1 \ (7) \Rightarrow 3^{6n} - 1 \equiv 0 \ (7)$$

  Le nombre $3^{6n} - 1$ est donc divisible par 7.