2025/2026

Nombres premiers et PGCD

Les plus anciennes traces des nombres premiers remontent à 20 000 ans avant notre ère, sur un os appelé los dIshango retrouvé au Congo, près du Lac Edward. On y trouve des entailles marquant les nombres 11, 13, 17 et 19.
Cest Euclide (vers 300 avant J.C.) qui, dans le livre VII de ses Éléments posa une définition du nombre premier : « Le nombre premier est celui qui est mesuré par la seule unité ».

I PGCD de deux entiers

Définition

Soit a et b deux entiers relatifs tels que $(a, b) \neq (0; 0)$, on appelle **plus grand diviseur commun** de a et b, le plus grand des diviseurs communs de a et b et on le note $\text{PGCD}(a, b)$.

Remarque

Soit a et b deux entiers relatifs, $\text{PGCD}(a, b) \geq 1$, donc le PGCD est un entier naturel non nul. D'autre part $\text{PGCD}(a, b) = \text{PGCD}(|a|, |b|)$.

Exemple

Les diviseurs de 60 dans $\mathbb{N}$ sont $\{1; 2; 3; 4; 5; 6; 10; 12; 15; 20; 30; 60\}$ et les diviseurs de 100 dans $\mathbb{N}$ sont $\{1; 2; 4; 5; 10; 20; 25; 50; 100\}$.
Quel est le PGCD de 100 et 60 ?

Théorème

Algorithme d'Euclide : Soit a, b et r trois entiers relatifs avec $b > 0$. Si r est le reste de la division euclidienne de a par b, alors

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

Démonstration

soit q et r le quotient et le reste de la division euclidienne de a par b. On a alors $a = bq + r$. Soit D un diviseur de b et de r. Donc D est aussi un diviseur de a.
Réciproquement, si D est un diviseur de a et de b, alors D divise $a - bq = r$, donc D divise r.
Donc l'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs communs à b et r. Donc plus particulièrement, $\text{PGCD}(a, b) = \text{PGCD}(b, r)$.

Exemple

Déterminer le PGCD de 252 et 360.

Théorème

Soit a, b et Δ trois entiers relatifs avec $(a, b) \neq (0; 0)$.

- Pour tout $d \in \mathbb{Z}$, $(d|a$ et $d|b)$ ssi $(d|\text{PGCD}(a, b))$;
- Pour tout $k \in \mathbb{Z}^*$, $\text{PGCD}(ka, kb) = |k|\text{PGCD}(a, b)$;
- $(\Delta = \text{PGCD}(a, b))$ ssi $(\exists a',\ b' \in \mathbb{Z} : a = \Delta a'$ et $b = \Delta b'$ et $\text{PGCD}(a', b') = 1)$.

Remarque

La première proposition de ce théorème affirme que les diviseurs communs à a et b sont les diviseurs de leur PGCD et réciproquement.

Démonstration

- On a démontré précédemment que l'ensemble de diviseurs communs à a et b, est également l'ensemble des diviseurs communs à b et r.
  On poursuit alors le raisonnement et on crée une suite (r_n) strictement décroissante :
  - $a = bq + r_0$
  - $b = r_0q' + r_1$
  - $r_0 = r_1q'' + r_2$

    .
    .
    .

  Or il n'existe qu'un nombre fini d'entiers entre r_0 et 0, il existe donc un rang k tel que r_k soit différent de 0 et $r_{k+1} = 0$.
  Ainsi l'ensemble des diviseurs communs de a et b est égal à l'ensemble des diviseurs communs de r_k et 0.
  On en déduit que l'ensemble des diviseurs communs de a et b est égal à l'ensemble des diviseurs de r_k.
- En appliquant l'algorithme d'Euclide, on obtient successivement :
  $k \in \mathbb{Z}^*$, $\text{PGCD}(ka, kb) = \text{PGCD}(kb, kr) = \text{PGCD}(kr, kr_1) = ... = \text{PGCD}(kr_k, 0) = |k|r_k = |k|\text{PGCD}(a, b)$.
- Sens direct :
  Si Δ est le PGCD de a et de b alors il existe a' et b' entiers relatifs tel que $a = a'\Delta$ et $b = b'\Delta$ car Δ est diviseur commun à a et b.
  Raisonnons par l'absurde en supposant alors que le PGCD de a' et b' est un certain $\delta > 1$.
  Donc il existe a'' et b'' entiers relatifs tel que $a' = a''\delta$ et $b' = b''\delta$.
  Donc $a = a'\Delta = a''\delta\Delta$ et $b = b'\Delta = b''\delta\Delta$.
  C'est absurde, car cela voudrait dire qu'il existe un diviseur commun à a et b, plus grand que Δ.
  Donc $\text{PGCD}(a', b') = 1$.
  La réciproque est évidente :
  $\text{PGCD}(a, b) = \text{PGCD}(\Delta a', \Delta b') = \Delta\text{PGCD}(a', b') = \Delta$.

Exemple

a. Chercher les diviseurs communs de 2730 et 5610.
b. Chercher le PGCD de 420 et 540

II Nombres premiers entre eux

Définition

Deux entiers relatifs a et b sont premiers entre eux si leurs seuls diviseurs communs sont 1 et (-1). Autrement dit a et b sont premiers entre eux si $\mathrm{PGCD}(a,b)=1$.

Théorème

Identité de Bézout Soit a et b deux entiers relatifs avec $(a,b)\neq(0;0)$, alors il existe un couple d'entiers relatifs (u,v) tel que :

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

De plus, u et v sont premiers entre eux.

Démonstration

On note $\Delta=\mathrm{PGCD}(a,b)$ et ε l'ensemble des entiers naturels non nuls de la forme $ax+by$ avec x et y des entiers relatifs.
ε est une partie non vide de $\mathbb{N}$: si $a>0$ alors $a\times1+b\times0$ est dans ε.
$a<0$ alors $a\times(-1)+b\times0$ est dans ε.
Si $a=0$, il suffit d'utiliser le même raisonnement avec b.
ε admet donc un plus petit élément que l'on notera n, tel que $n=au+bv$ avec u et v entiers relatifs.
Or $\Delta|a$, $\Delta|b$ donc $\Delta|n$. Donc $\Delta\leq n$.
Soit q et r respectivement le quotient et le reste dans la division Euclidienne de a par n.
$a=nq+r=(au+bv)q+r$ donc $r=a\times(1-uq)+bq\times(-1)$ donc $r\in\varepsilon$.
Or $0\leq r<n$ ce qui n'est donc possible que dans le cas où $r=0$ car n est le plus petit élément de ε (cela signifie également que $r\notin\varepsilon$).
Donc $n|a$, $n|b$ (en utilisant le même raisonnement qu'avec a) et donc $n|\Delta$.
Or $\Delta|n$ également, donc $\Delta=n$.

Montrons que u et v sont alors premiers entre eux :
$\Delta|a$ donc $\exists a'\in\mathbb{Z}\mid a=\Delta a'$
$\Delta|b$ donc $\exists b'\in\mathbb{Z}\mid b=\Delta b'$
On a donc

$$au+bv=\Delta$$

$$\text{ssi}\quad \Delta a'u+\Delta b'v=\Delta$$

$$\text{ssi}\quad a'u+b'v=1$$

Or si u et v n'était pas premier entre eux, alors il existerait un $d\in\mathbb{Z}$ tel que $d|a'u+b'v$ et donc $d|1$. D'où $d=1$ ou $d=-1$, donc u et v sont premiers entre eux.

Théorème

Théorème de Bézout Soit a et b deux entiers relatifs avec $(a, b) \neq (0; 0)$, a et b sont premiers entre eux si, et seulement si, il existe un couple d'entiers relatifs (u, v) tel que :

$$au + bv = 1$$

Démonstration

- D'après l'égalité de Bézout, si a et b sont premiers entre eux, alors il existe u et v entiers relatifs tel que $au + bv = 1$.
- Supposons qu'il existe u et v entiers relatifs tel que $au + bv = 1$. Soit $\Delta = \text{PGCD}$.
  Donc $\Delta|au + bv$ donc $\Delta|1$ donc $\Delta = 1$.
  a et b sont donc premier entre eux.

Exemple

Démontrer que pour tout entier naturel n, $2n + 3$ et $5n + 7$ sont premiers entre eux

Propriété

Un entier a admet un inverse modulo n, si a et n sont premiers entre eux.

Exemple

a. Déterminer un inverse de 5 modulo 16.
b. En déduire les solutions de léquation $5x \equiv 7[16]$.

Théorème

Théorème de Gauss : soit a, b et c trois entiers relatifs avec $(a, b) \neq (0; 0)$. Si $a|bc$ et si a et b sont premiers entre eux, alors $a|c$.

Démonstration

Supposons donc que $a|bc$ et que a et b sont premiers entre eux.
Il existe donc $k \in \mathbb{Z}$, tel que $bc = ka$.
D'autre part, a et b étant premiers entre eux, il existe, d'après le théorème de Bézout, deux entiers relatifs u et v tel que $au + bv = 1$ donc $auc + bcv = c$ donc $a(uc + kv) = c$.
Or $cu + kv \in \mathbb{Z}$, donc $a|c$.

Propriété

Soit a, b et c trois entiers relatifs avec $(a, b) \neq (0; 0)$. Si $a|c$, $b|c$ et si a et b sont premiers entre eux, alors $ab|c$.

Supposons donc que $a|c$ et $b|c$. Supposons de plus que a et b sont premiers entre eux.
Il existe donc k et k' entiers relatifs tel que $c = ak$ et $c = bk'$ donc $ak = bk'$.
Or a et b sont premiers entre eux donc d'après le théorème de Gauss $a|k'$. Donc il existe k'' entier relatif tel que $k' = ak''$.
Donc $c = bk' = bak''$ et finalement, $ab|c$.

Démonstration

Exemple

a. Soit un entier naturel n. On suppose que $5n$ est un multiple de 3. Quelles sont les valeurs possibles pour n ?
b. Soit un entier naturel n multiple de 7 et de 11. Quelles sont les valeurs possibles pour n ?

Exemple

a. Déterminer les entiers relatifs x et y tels que $5x + 7y = 1$.
b. Déterminer les entiers relatifs x et y tels que $5x + 7y = 12$.

III Nombres premiers

Un nombre premier est un entier naturel supérieur ou égal à 2 qui n'admet pas d'autres diviseurs positifs que 1 et lui-même. Dans le cas contraire, il est dit composé.

Définition

Tout entier naturel $n > 1$ et non premier admet un diviseur premier p tel que $p \leq \sqrt{n}$.

Propriété

Soit n un entier naturel strictement supérieur à 1 et non premier.
On note alors E l'ensemble des diviseurs de n différent de 1 et lui même.
Cet ensemble est non vide car n n'est pas premier. Donc E admet un plus petit élément que l'on note p.
Si p admet un diviseur p' autre que 1 ou lui-même, alors p' est aussi un diviseur de n plus petit que p. Ce n'est pas possible car p est le plus petit élément de E.
On en déduit donc que p est un nombre premier.
Il existe donc $q \geq p$ (car p est le plus petit élément de E), tel que $n = pq \geq p^2$ donc $p \leq \sqrt{n}$.

Démonstration

Exemple

391 est-il premier ?

Théorème

L'ensemble des nombres premiers est infini.

Démonstration

Soit un nombre premier n quelconque. Nous allons démontrer quil existe un nombre premier plus grand que n.
Nous utiliserons un raisonnement par l'absurde en supposant qu'il existe un nombre fini de nombres premiers.
Soit $E = \{p_1, p_2, ..., p_m\}$ l'ensemble des nombres premiers avec $m \in \mathbb{N}$.
E est une partie non vide et finie de $\mathbb{N}$ de plus grand élément p_m.
On pose alors $n = p_1 \times p_2 \times ... \times p_m + 1$.
$n \notin E$ car $n > p_m$, donc n est composé et admet donc un diviseur premier inférieur ou égal à $\sqrt{n}$.
Il existe donc $k \in \mathbb{N}$, tel que $n \equiv 0\ [p_k]$.
Or $p_1 \times ... \times p_k \times ... \times p_m \equiv 0\ [p_k]$ donc $p_1 \times ... \times p_k \times ... \times p_m + 1 \equiv 1\ [p_k]$ donc $n \equiv 1\ [p_k]$ ce qui est contradictoire.
D'où n est un nombre premier. CQFD.

Théorème

Théorème fondamental de l'arithmétique : Soit n un entier naturel, $n \geq 2$. Il existe alors des nombres premiers $p_1, ..., p_r$ et des entiers naturels non nuls $\alpha_1, ..., \alpha_r$ tels que :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$$

Existence :
Soit n un entier naturel non nul.
Si n est premier, le résultat est immédiat, sinon, il existe un nombre premier p_1, plus petit diviseur de n strictement supérieur à 1. Donc il existe $k \in \mathbb{N}$ tel que $n = p_1 \times k$.
Si k est lui même premier, alors l'existence est établie, sinon on réitère le processus pour obtenir une suite (k_n) décroissante et finie d'entiers naturels. Ainsi, n se décompose en un produit de facteurs premiers du type : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$.

Unicité :
On effectue une démonstration à l'aide d'une récurrence forte :
Soit pour tout $n \geq 2$ entier naturel la proposition $P(n)$ suivante : « La décomposition en produit de facteurs premiers de n est unique ».

Initialisation :
rang $n = 2$.
2 est lui même un nombre premier donc P(2) est vraie.

Hérédité :
Supposons $P(k)$ vraie pour tous les $k \in [2; n-1]$ avec un certain $n \geq 3$ et montrons que cela implique $P(n)$ vrai.

- Supposons qu'il existe deux décompositions pour n tel que $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ et $n = q_1^{\beta_1} \times q_2^{\beta_2} \times ... \times q_r^{\beta_r}$
- On a donc p_1 qui divise $q_1^{\beta_1} \times q_2^{\beta_2} \times ... \times q_r^{\beta_r}$.
  Donc il existe q_k avec $k \in \mathbb{Z}$ tel que p_1 et q_k ne soit pas premier entre eux. Or p_1 et q_k sont deux nombres premiers donc $p_1 = q_k$.
  On pose $n' = \dfrac{n}{p_1}$. On a donc $n' < n$, admettant deux décompositions distinctes. C'est impossible d'après l'hypothèse de récurrence.
  Donc $P(n+1)$ est vraie

Conclusion :
La propriété est donc héréditaire à partir du rang $n = 2$.
D'après le principe de récurrence : $\forall n \geq 2,\ P(n)$ est vraie.
La propriété est ainsi démontrée.

Démonstration

Cette écriture, unique à l'ordre des facteurs près, s'appelle décomposition primaire de n.

Remarque

Exemple

a. Décomposer 17 640 et 411 600 en produits de facteurs premiers.
b. En déduire le PGCD et le PPCM de ces deux nombres.
c. Déterminer tous les diviseurs de 132.

Théorème

Petit théorème de Fermat : soit p un nombre premier et n un entier naturel. Alors :

- $n^p \equiv n\ [p]$
- si p ne divise pas n, $n^{p-1} \equiv 1\ [p]$.

Démonstration

Résultat préliminaire : Soit $k \in [[1, p-1]]$ et $n \in \mathbb{N}$.

$$k\binom{p}{k} = \frac{p!}{(k-1)!(p-k)!} = p\frac{(p-1)!}{(k-1)!(p-1-(k-1))!} = p\binom{p-1}{k-1}$$

Donc $p|k\binom{p}{k}$ or $k < p$ donc d'après le théorème de Gauss, $p|\binom{p}{k}$ donc $\binom{p}{k} \equiv 0\ [p]$

Pour tout entier naturel n, on considère la proposition $P(n)$ suivante : $n^p \equiv n\ [p]$ avec p premier.

Initialisation :

rang $n = 0$
$0^p \equiv 0\ [p]$ donc $P(0)$ est vraie.

Hérédité :

Supposons $P(n)$ vraie pour un certain rang $n \geq 0$ et montrons que cela implique $P(n+1)$ vrai.
$P(n)$ vraie $\iff n^p \equiv n\ [p]$
Or $(n+1)^p = \displaystyle\sum_{k=0}^{p}\binom{p}{k}n^k$
D'après le résultat préliminaire, pour $k \in [[1, p-1]]$, $\binom{p}{k} \equiv 0\ [p]$
donc $\displaystyle\sum_{k=0}^{p}\binom{p}{k}n^k \equiv 1 + n^p[p]$ or d'après l'hypothèse de récurrence $n^p \equiv n\ [p]$, donc $\displaystyle\sum_{k=0}^{p}\binom{p}{k}n^k \equiv 1 + n\ [p]$ donc $(n+1)^p \equiv n+1\ [p]$

Conclusion :

$P(n)$ vraie $\Longrightarrow P(n+1)$ vraie. La propriété est donc héréditaire à partir du rang $n = 0$.
D'après le principe de récurrence, $P(n)$ est vraie pour tout entier naturel $n \geq 0$.
La propriété est ainsi démontrée.

$n^p \equiv n\ [p]$ ssi $n(n^{p-1}-1) \equiv 0[p]$ donc $p|n(n^{p-1}-1)$. Or si p ne divise pas n alors ils sont premiers entre eux car p est premier, donc $p|n^{p-1}-1$ donc $n^{p-1} \equiv 1\ [p]$.

Exemple

Démontrer que pour tout entier naturel n, 7 divise $3^{6n} - 1$.