

PGCD : exercices

Les solutions ne sont pas entièrement rédigées. ce ne sont que des indications, qui seraient insuffisantes sur une copie. Assurez-vous que vous comprenez bien toutes les étapes et que vous savez les détailler et les justifier en utilisant des théorèmes du cours (voir la deuxième section : théorème utilisés).

1. a, b sont des entiers naturel non nuls.

Démontrer que $\text{PGCD}(a^3, b^3) = (\text{PGCD}(a, b))^3$

Indications : utiliser la décomposition en facteurs premiers de a et b , appliquer à partir de là la méthode pour calculer le PGCD (facteurs premiers communs, plus petits exposants). Faire de même avec a^3 et b^3 et comparer les résultats.

2. Démontrer l'équivalence entre les deux propriétés P_1 et P_2 suivantes, pour a entier relatif :

P_1 : L'équation $ax \equiv 1 \pmod{6}$ n'a aucune solution x dans $\mathbb{Z}$

P_2 : a est divisible par 2 ou par 3.

Indications :

Par contraposée :

L'équation $ax \equiv 1 \pmod{6}$ a au moins une solution $\Leftrightarrow$

$\Leftrightarrow a$ est premier avec 6 (Bézout) à préciser

$\Leftrightarrow a$ n'est divisible ni par 2 ni par 3 (décomposition en facteurs premiers de 6).

3. m et n sont des entiers naturels non nuls.

Démontrer que, si m est premier avec n^2 , alors m est premier avec n

m n'a aucun facteur premier commun avec n^2 , les facteurs premiers de n^2 sont les mêmes que ceux de n , donc m n'a aucun facteur premier commun avec n

Ou bien : $am + bn^2 = 1 \Rightarrow am + kn = 1 \Rightarrow m$ et n premiers entre eux (Bézout).

4. a et n sont deux entiers naturels non nuls, et premiers entre eux.

Démontrer que l'équation $ax \equiv 2 \pmod{n}$ ne peut pas avoir plus d'une solution x dans $[0; n-1]$.

Par l'absurde : si $ax \equiv 2 \pmod{n}$ et $ay \equiv 2 \pmod{n}$ avec x et y dans $[0; n-1]$, alors

$a(x-y)$ est divisible par n , donc $x-y$ est divisible par n (Gauss).

Or $-(n-1) \leq x-y \leq n-1$. Donc la seule possibilité est $x-y=0$, soit $x=y$.

5. Déterminer tous les n entiers naturels tels que $\text{PGCD}(5n+2, 4n+3) = 7$.

Lemme d'Euclide : $\text{PGCD}(5n+2, 4n+3) = \dots = \text{PGCD}(n-1, 7)$

$\text{PGCD}(a, b) = b \Leftrightarrow b$ divise a .

Réponse = $n = 1 + 7k$ (avec $k \geq 0$).

6. Déterminer l'ensemble des n entiers naturels non nuls tels que la fraction $\frac{3n+2}{n+2}$ soit irréductible.

$3n+2 = 3(n+2) - 4$, donc (lemme d'Euclide) :

$\text{PGCD}(3n+2, n+2) = \text{PGCD}(n+2, -4) = \text{PGCD}(n+2, 4)$.

On cherche donc les n tels que $\text{PGCD}(n+2, 4) = 1$, c'est-à-dire différent de 2 et de 4 (diviseurs de 4).

$\text{PGCD}(n+2, 4) = 1 \Leftrightarrow$

$\Leftrightarrow n+2$ n'est divisible ni par 4 ni par 2

$\Leftrightarrow n+2$ est impair

$\Leftrightarrow n$ est impair.

7. Soient a et b deux entiers relatifs premiers entre eux, $A = 11a + 2b$ et $B = 18a + 5b$. Exprimer a et b en fonction de A et B et en déduire que tout diviseur commun à A et B est un diviseur commun à $19a$ et $19b$.

Calculer $\text{PGCD}(A, B)$.

$19a = 5A - 2B$ et $19b = -18A + 11B$.

Donc (combinaisons linéaires) $\text{PGCD}(A, B)$ divise $19a$ et $19b$.

Donc (théorème) il divise $\text{PGCD}(19a, 19b)$.

Or $\text{PGCD}(19a, 19b) = 19\text{PGCD}(a, b)$ (théorème).

Comme $\text{PGCD}(a, b) = 1$, $\text{PGCD}(19a, 19b) = 19$. Donc $\text{PGCD}(A, B) = 19$ ou 1.

C'est 19 si et seulement si A et B sont divisibles par 19, sinon c'est 1.

8. On considère l'équation $3x - 5y = 2$

Démontrer l'équivalence suivante : (a, b) est solution $\Leftrightarrow (a + 5k, b + 3k)$ est solution.

Trouver toutes les solutions avec $0 \leq y \leq 2$ et en déduire l'ensemble des solutions.

$3(a + 5k) - 5(b + 3k) = 3a - 5b$.

Donc : (a, b) est solution $\Leftrightarrow (a + 5k, b + 3k)$ est solution.

Puisque $y = b + 3k$ d'après ce qui précède, il suffit d'essayer les valeurs de y dans $\{0, 1, 2\}$. On trouve $(x = 4, y = 2)$.

L'ensemble des solutions est $\{(4 + 5k, 2 + 3k); k \in \mathbb{Z}\}$

9. Déterminer l'ensemble des couples (x, y) d'entiers relatifs tels que $37x + 22y = 2$

On trouve une solution particulière de $37x + 22y = 1$ (possible car 37 et 22 sont premiers entre eux) : $(25, -42)$ (par exemple en remontant l'algorithme d'Euclide ou bien en affichant le tableau des valeurs de $\frac{1-37x}{22}$, ce qui permet de conjecturer une solution et de la vérifier).

On multiplie par 2 : $(50, -84)$.

On applique ensuite la méthode habituelle (voir cours) en utilisant le théorème de Gauss et en n'oubliant pas la réciproque : $(x, y) = (50 - 22k, -84 + 37k)$

10. Avec la liste des nombres premiers de 2 à 59, combien faut-il faire de divisions euclidiennes pour vérifier que 2011 est premier ? On admettra que 2011 est premier. Démontrer qu'il existe un multiple de 2011 qui ne s'écrit qu'avec des chiffres 9 (utiliser le petit théorème de Fermat avec les puissances de 10).

On essaye toutes les divisions par les nombres premiers inférieurs ou égaux à $\sqrt{2011} \approx 44,84$. Les nombres premiers inférieurs à 44 sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43. Il y en a 14.

D'après le petit théorème de Fermat : puisque 10 est premier avec 2011, on a $10^{2010} \equiv 1 \pmod{2011}$. Donc $10^{2010} - 1$ est divisible par 2011.

Ce nombre est solution, puisqu'il s'écrit uniquement avec des chiffres 9 (2010 chiffres 9), puisque $10^{2010} - 1 = 9(1 + 10 + 10^2 + \dots + 10^{2009})$ (somme des termes d'une suite géométrique).

11. Démontrer que, si a est premier avec b et c , alors il est premier avec bc .

Il existe u et v tels que $au + bv = 1$ (Bézout). De même $au' + cv' = 1$. On multiplie les deux égalités entre elles. On obtient $ax + bcy = 1$, donc a est premier avec bc (Bézout).

Ou bien : a n'a aucun facteur premier commun avec b ni avec c , donc il ne peut pas en avoir avec bc , puisque bc n'a pas d'autres facteurs premiers que ceux de b et ceux de c .

12. m et n sont deux entiers naturels non nuls. calculer $\text{PGCD}(mn, n(2m+1))$

$\text{PGCD}(mn, n(2m+1)) = n\text{PGCD}(m, 2m+1)$ (théorème)

Or $\text{PGCD}(m, 2m+1) = 1$ puisque m et $2m+1$ sont premiers entre eux (Bézout : $(2m+1) - m = 1$).

Donc $\text{PGCD}(mn, n(2m+1)) = n$

- Théorème de Gauss.

Attention, dans ce théorème, ne pas oublier l'hypothèse fondamentale : a et b sont premiers entre eux.

D'autre part, ne pas oublier que ce théorème n'est qu'une implication et pas une équivalence.

- Lemme d'Euclide

Ne pas le généraliser inconsidérément. Dans ce théorème, un des deux nombres doit être conservé. Ne pas changer les deux nombres à la fois.

- Quels sont tous les multiples de n qui sont compris entre $-(n-1)$ et $n-1$?
- $\text{PGCD}(a, b) = b \Leftrightarrow \boxed{\dots?}$.
C'est une équivalence, on peut s'en servir dans les deux sens.
- Attention : dire que $\text{PGCD}(a, kp) = p$ n'est pas équivalent à dire que p divise a (même si p est premier).
- Qu'est-ce qu'une fraction irréductible ?
- Si un nombre divise a et b , alors il divise $\boxed{\dots?}$ (et la réciproque est vraie aussi).
- $\text{PGCD}(ka, kb) = \boxed{\dots?}$ (piège si $k < 0$).
- Lorsque p est un nombre premier, dire que $\text{PGCD}(a, b) = p$ équivaut à $\boxed{\dots?}$.
Attention à bien obtenir une équivalence, et pas seulement : $\text{PGCD}(a, b)$ est un multiple de p .
- Savoir comment on trouve une solution particulière (x, y) de $ax + by = 1$ en remontant l'algorithme d'Euclide, puis comment on en déduit ensuite toutes les solutions (en faisant attention d'obtenir une équivalence).
- Equation $ax + by = c$ lorsque $c = \text{PGCD}(a, b)$.
Savoir se ramener à $a'x + b'y = 1$
- Attention à l'équation $ax + by = c$ lorsque c n'est pas le PGCD de a et b .
Les solutions ne se déduisent pas directement de celles de $ax + by = \text{PGCD}(a, b)$
- Petit théorème de Fermat.
Ne pas oublier l'hypothèse fondamentale : a est premier avec p (et p est premier).
Donc ne pas pas appliquer le théorème dans des situations non adaptées.

Théorèmes utilisés (à retrouver)

- Comment calcule-t-on le PGCD à partir des décompositions en nombres premiers ?
- Théorème de Bézout. C'est une équivalence, et il peut servir dans les deux sens
- Comment exprimer que a et b sont premiers entre eux en utilisant leurs décompositions en facteurs premiers ?