

7

Théorèmes de Bézout et de Gauss

HISTOIRE DES MATHS

L'arithmétique des entiers est présente chez les mathématiciens grecs. Ainsi, vers 300 avant notre ère, **Euclide** décrit, dans les *Éléments*, un algorithme du calcul du PGCD de deux nombres. **Diophante**, surnommé « le père de l'algèbre », résout des problèmes d'arithmétique.

En 1624, **Bachet de Méziriac** reprend l'algorithme d'Euclide dans son ouvrage *Problèmes plaisants et délectables qui se font par les nombres*. Il y caractérise deux nombres premiers entre eux.

En 1764, **Étienne Bézout** généralise le résultat de Bachet.

En 1801, **Carl Friedrich Gauss** énonce un autre théorème fondamental de l'arithmétique, connu sous le nom de Théorème de Gauss.



Bachet de Méziriac

Étienne Bézout

► **Claude-Gaspard Bachet de Méziriac** (1581-1638) est un mathématicien et poète français. Il consacre une grande partie de ses travaux à l'arithmétique. Expert en langues anciennes, il traduit en latin, en les commentant, les *Arithmétiques* de Diophante.

► **Étienne Bézout** (1730-1783) est un mathématicien, académicien et professeur du siècle des lumières. Il est l'auteur d'une *Théorie générale des équations algébriques* publiée en 1779. Les résultats qu'il obtient participent au développement de la géométrie algébrique.

1624

Bachet de Méziriac formalise une condition nécessaire et suffisante pour que deux nombres soient premiers entre eux.

1661
Colbert intendant au service de Louis XIV

1650

1764

Bézout présente à l'Académie dans l'un de ses mémoires l'identité reliant deux entiers et leur PGCD.

1715
Louis XV devient Roi de France

1700

1718
Premiers succès littéraires de Voltaire

1750

1801

Gauss publie son ouvrage *Disquisitiones Arithmeticae* où figurent de nombreux théorèmes fondamentaux.

1769
Watt met au point une machine à vapeur

1800

Dedekind, dernier élève de Gauss, a élargi le champ d'action de l'arithmétique.

1789
Début de la Révolution française

1850



Le QR code est l'un des codes à deux dimensions les plus utilisés.

Les premiers procédés de chiffrement datent de l'antiquité avec des hiéroglyphes chez les Égyptiens et le scytale chez les Spartiates. Aujourd'hui, ces techniques font intervenir des algorithmes très sophistiqués qui jouent un rôle crucial dans la sécurité des systèmes informatiques et des communications : guichet automatique, achat en ligne à l'aide d'un smartphone, ouverture d'un véhicule avec une clé électronique ...

Les contenus et capacités travaillés dans ce chapitre

	Savoir-faire	Exercices
• PGCD de deux entiers. Algorithme d'Euclide.	1 à 6, 24, 26	28 à 40
• Couples d'entiers premiers entre eux. Théorème de Bézout.	7 à 14, 16, 25, 27	41 à 74, 77 à 80
• Déterminer un inverse de a modulo n lorsque a et n sont premiers entre eux.	15, 17	75, 76, 105 à 116
• Théorème de Gauss	19, 21 à 23	81 à 91
• Résoudre des équations diophantiennes simples.	18, 20	92 à 104



Rappels utiles

• Divisibilité dans \mathbb{Z}

a et b désignent deux nombres entiers relatifs.
Dire que a divise b (ou que b est un multiple de a) signifie qu'il existe un nombre entier relatif k tel que :

$$b = k \times a.$$

• Propriétés de la divisibilité

a , b et c désignent des nombres entiers relatifs.
Si a divise b et c , alors pour tous nombres entiers relatifs u et v , a divise $bu + cv$.
En particulier, si a divise b et c , alors :

- a divise $b + c$;
- a divise $b - c$;

• Division euclidienne

a désigne un nombre entier relatif et b un nombre entier naturel non nul.
Il existe un unique couple de nombres entiers relatifs $(q; r)$ tel que :

$$a = bq + r \text{ et } 0 \leq r < b.$$

• Congruences dans \mathbb{Z}

a et b désignent deux nombres entiers relatifs et n un nombre entier naturel, $n \geq 2$.
Dire que a et b sont congrus modulo n signifie que a et b ont le même reste dans la division euclidienne par n .
On note $a \equiv b \pmod{n}$.

À l'oral

Questions-Tests

Pour chaque question, il y a une seule réponse exacte.

1 Le nombre $11^4 - 3^4$ est un multiple de :

(1) 11 (2) 3 (3) 112

2 Le nombre $17^5 - 13^5$ est divisible par :

(1) 4 (2) 7 (3) 10

3 La somme de deux nombres impairs consécutifs est toujours divisible par :

(1) 3 (2) 4 (3) 5

4 a et n désignent deux nombres entiers relatifs tels que a divise $2n+1$ et a divise $n+3$.
Alors a divise :

(1) 5 (2) 4 (3) 7

5 n est un nombre entier naturel tel que n divise $n+8$.
Alors, n est un diviseur de :

(1) 3 (2) 5 (3) 8

6 « n est un entier naturel tel que $n+2$ divise $n+3$. »
Alors cette affirmation est :

- (1) vraie pour tout entier naturel n ;
- (2) vraie pour un unique entier naturel n ;
- (3) fausse pour tout entier naturel n .

7 Le reste de la division euclidienne de -15 par 4 est égal à :

- (1) -3 (2) 3 (3) 1

8 On peut lire le quotient et le reste de la division euclidienne de 275 par 14 avec l'égalité :

- (1) $275 = 14 \times 18 + 23$
 (2) $275 = 14 \times 19 + 9$
 (3) $275 = 14 \times 20 - 5$

9 a désigne un nombre entier naturel.

Le reste de la division euclidienne de a par 144 est 67 .
Alors le reste de la division euclidienne de a par 36 est :

- (1) 4 (2) 31 (3) 67

10 La congruence vraie est :

- (1) $48 \equiv 21 [6]$ (2) $37 \equiv 9 [7]$ (3) $59 \equiv 26 [13]$

11 a désigne un entier relatif.

La congruence $a \equiv 30\,757 [10]$ peut aussi s'écrire :

- (1) $a \equiv 0 [10]$ (2) $a \equiv 3 [10]$ (3) $a \equiv 7 [10]$

12 a est un entier naturel tel que $a \equiv -32 [8]$.
Alors, a peut être égal à :

- (1) 37 (2) 88 (3) -47

1

PGCD de deux nombres entiers

Un fleuriste a reçu une commande de 126 iris et 210 roses. Il utilise toutes ses fleurs pour réaliser des bouquets contenant tous le même nombre d'iris et le même nombre de roses. Par exemple, il peut réaliser 21 bouquets contenant 6 iris et 10 roses.



- 1**
 - a) Quel est le plus grand nombre possible p de bouquets que le fleuriste peut réaliser ?
 - b) Quelle est alors la composition florale de chacun de ces bouquets ?

- 2**
 - a) Donner toutes les compositions florales possibles.
 - b) Que peut-on dire du nombre de bouquets de chacune de ces compositions par rapport au nombre p ?

On dit que le nombre p est le PGCD de 126 et 210, on le note $\text{PGCD}(126 ; 210)$.

2

Vers la résolution d'une équation diophantienne

a , b et n désignent des nombres entiers naturels non nuls.

Cécile dispose de deux sabliers, l'un mesure une durée entière de a minutes et l'autre une durée entière de b minutes.

Elle souhaite mesurer une durée de n minutes avec ses deux sabliers.

1 Un exemple

On suppose que $a = 11$ et $b = 5$.

a) Fred affirme :

« Il est possible de mesurer une durée de 2 minutes car $11 \times 2 - 5 \times 4 = 2$ ». Expliquer comment Cécile doit procéder.

b) Justifier que Cécile peut mesurer toute durée de n minutes, c'est-à-dire trouver un couple $(x ; y)$ de nombres entiers naturels solution de l'équation, dite diophantienne $11x - 5y = n$.

**HISTOIRE DES MATHS**

L'adjectif « diophantienne » qualifie les équations à coefficients entiers dont on cherche uniquement des solutions entières.

Le mathématicien grec Diophante (vers 250) a formulé de nombreux problèmes de ce type.

2 Plus généralement

On admet dans une situation particulière que Cécile peut mesurer une durée de n minutes avec ses deux sabliers.

Démontrer alors que le PGCD des nombres a et b divise n .

1

PGCD de deux nombres entiers

A Diviseurs communs à deux nombres entiers relatifs

Définition

a et b désignent deux nombres entiers relatifs non nuls.

Le plus grand commun diviseur à a et b est appelé le PGCD de a et de b ; on le note $\text{PGCD}(a; b)$ ou $\text{PGCD}(b; a)$.

Conséquence : $\text{PGCD}(a; b) = |b|$ si, et seulement si, b divise a .

En effet, si b divise a , alors $|b|$ est un diviseur commun à a et b ; or $|b|$ est le plus grand diviseur de b , donc $\text{PGCD}(a; b) = |b|$. Réciproquement, si $\text{PGCD}(a; b) = |b|$, alors b divise a .

Exemples

- Les diviseurs de 30 et de -30 sont : -30 ; -15 ; -10 ; -6 ; -5 ; -3 ; -2 ; -1 ; 1 ; 2 ; 3 ; 5 ; 6 ; 10 ; 15 ; 30.
- Ceux de 12 et -12 sont : -12 ; -6 ; -4 ; -3 ; -2 ; -1 ; 1 ; 2 ; 3 ; 4 ; 6 ; 12.
- Donc $\text{PGCD}(30; 12) = \text{PGCD}(30; -12) = \text{PGCD}(-30; 12) = \text{PGCD}(-30; -12) = 6$.

B PGCD et algorithme d'Euclide

LEMME D'EUCLIDE

a, b, q et r désignent des nombres entiers relatifs non nuls.

Si $a = bq + r$, alors $\text{PGCD}(a; b) = \text{PGCD}(b; r)$.

Démonstration

- Si d est un diviseur commun à a et b , il divise aussi a et bq , donc $a - bq$, c'est-à-dire r .
Donc d est un diviseur commun à b et r .
- Si d' est un diviseur commun à b et r , il divise aussi bq et r , donc $bq + r$, c'est-à-dire a .
Donc d' est un diviseur commun à a et b .

Conclusion : l'ensemble des diviseurs communs à a et b et l'ensemble des diviseurs communs à b et r ont les mêmes éléments et donc le même plus grand élément : $\text{PGCD}(a; b) = \text{PGCD}(b; r)$.

Algorithme d'Euclide : $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ avec $a > b$.

Pour déterminer $\text{PGCD}(a; b)$, on utilise l'algorithme d'Euclide : il consiste à remplacer $(a; b)$ par des couples de nombres de plus en plus petits qui ont le même ensemble de diviseurs communs.

Opération	Reste	Commentaire
On divise a par b	r_0	$0 < r_0 < b$ et $\text{PGCD}(a; b) = \text{PGCD}(b; r_0)$
On divise b par r_0	r_1	$0 < r_1 < r_0$ et $\text{PGCD}(b; r_0) = \text{PGCD}(r_0; r_1)$
On divise r_0 par r_1	r_2	$0 < r_2 < r_1$ et $\text{PGCD}(r_0; r_1) = \text{PGCD}(r_1; r_2)$
.	.	.
.	.	.
On divise r_{n-2} par r_{n-1}	r_n	$0 < r_n < r_{n-1}$ et $\text{PGCD}(r_{n-2}; r_{n-1}) = \text{PGCD}(r_{n-1}; r_n)$
On divise r_{n-1} par r_n	0	$\text{PGCD}(r_{n-1}; r_n) = r_n$

Après un nombre fini de divisions, on trouve un reste nul, car les restes sont des nombres positifs ($0 < r_n < r_{n-1} < \dots < r_2 < r_1 < r_0 < b$) qui vont en décroissant strictement. Ci-dessus, on note r_n le dernier reste non nul. Donc d'après le lemme d'Euclide, $\text{PGCD}(a; b) = \text{PGCD}(b; r_0) = \dots = \text{PGCD}(r_{n-1}; r_n) = r_n$. D'où :

Propriété

Lorsque b ne divise pas a , le PGCD des nombres entiers naturels non nuls a et b est égal au **dernier reste non nul** obtenu par l'algorithme d'Euclide.

EXERCICES RÉSOLUS

1 Calculer un PGCD avec l'algorithme d'Euclide

Calculer le PGCD de 1 636 et 1 128 avec l'algorithme d'Euclide.

Solution

Étape	a	b	Reste	Calculs
1	1 636	1 128	508	$1636 = 1128 \times 1 + 508$
2	1 128	508	112	$1128 = 508 \times 2 + 112$
3	508	112	60	$508 = 112 \times 4 + 60$
4	112	60	52	$112 = 60 \times 1 + 52$
5	60	52	8	$60 = 52 \times 1 + 8$
6	52	8	4	$52 = 8 \times 6 + 4$
7	8	4	0	$8 = 4 \times 2 + 0$

Avec la calculatrice :

• Casio : OPTN > F4 (NUMERIC) > F2 (GCD)

• TI : math ► (NBRE) 9 (pgcd())

• NumWorks : gcd(p, q) PGCD

GCD(1636, 1128)

4

Le dernier reste non nul est 4, donc $\text{PGCD}(1636 ; 1128) = 4$.

2 Démontrer l'égalité de deux PGCD

a) a et b désignent des nombres entiers naturels non nuls et λ est un nombre entier relatif non nul tel que $\lambda a + b \neq 0$. Démontrer que $\text{PGCD}(a ; b) = \text{PGCD}(a ; \lambda a + b)$.

b) n désigne un nombre entier naturel non nul.

Selon la parité de n , déterminer $\text{PGCD}(n ; n + 2)$.

Solution

a) E est l'ensemble des diviseurs communs à a et b .

F est l'ensemble des diviseurs communs à a et $\lambda a + b$.

• Si $d \in E$, alors d divise a et b donc d divise $\lambda a + b$.

De d divise a et $\lambda a + b$, on déduit que $d \in F$.

• Si $d \in F$, alors d divise a et $\lambda a + b$ donc d divise $(\lambda a + b) - \lambda a$, c'est-à-dire d divise b .

De d divise a et b , on déduit que $d \in E$.

Conclusion : $E = F$ et donc $\text{PGCD}(a ; b) = \text{PGCD}(a ; \lambda a + b)$.

b) Avec $a = n$, $b = n + 2$ et $\lambda = -1$, on obtient : $\text{PGCD}(n ; n + 2) = \text{PGCD}(n ; 2)$ car $\lambda a + b = -n + n + 2 = 2$.

Ainsi : • si n est pair, $\text{PGCD}(n ; n + 2) = 2$; • si n est impair, $\text{PGCD}(n ; n + 2) = 1$.

Pour démontrer l'égalité de deux PGCD, on démontre, avec les notations ci-contre, que $E = F$ c'est-à-dire :

• si $d \in E$, alors $d \in F$

• si $d \in F$, alors $d \in E$

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 1

3 Dans chaque cas, déterminer à la main, le PGCD des deux nombres entiers relatifs.

a) 1 386 et 1 180 b) -6 292 et 5 852

Vérifier à l'aide de la calculatrice.

4 Éléna possède 256 timbres étrangers et 848 timbres français. Elle souhaite les répartir dans des pochettes identiques de même composition.

Comment l'aider ?

Sur le modèle de l'exercice résolu 2

5 n désigne un nombre entier naturel, $n \geq 2$. On pose $a = n - 1$ et $b = 3n + 2$.

a) Démontrer que $\text{PGCD}(a ; b) = \text{PGCD}(a ; 5)$.

b) Déterminer, selon les valeurs de l'entier n , le PGCD de a et b .

6 k désigne un nombre entier naturel.

Déterminer le PGCD des deux nombres suivants : $2k + 1$ et $9k + 4$.

2

Couples de nombres premiers entre eux

A Propriétés du PGCD

Propriété

Les diviseurs communs à deux nombres entiers relatifs non nuls a et b sont les diviseurs de $\text{PGCD}(a; b)$.

Démonstration

- Lorsque $a \in \mathbb{N}^*, b \in \mathbb{N}^*$ avec $a \geq b$ (si $a < b$, on échange a et b).
- Si $a = b$, alors $\text{PGCD}(a; b) = a = b$ et le résultat est immédiat.
- Si $a > b$, alors, avec l'algorithme d'Euclide (page 170), les diviseurs communs à a et b sont les diviseurs communs à b et r_0 , à r_0 et r_1 , à r_1 et r_2 , ..., à r_{n-1} et r_n .
Or r_n divise r_{n-1} donc les diviseurs communs à r_{n-1} et r_n sont ceux de r_n , c'est-à-dire de $\text{PGCD}(a; b)$.
- Lorsque $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$, la propriété est vraie car les diviseurs communs à a et b sont les diviseurs communs à $|a|$ et $|b|$ et $\text{PGCD}(a; b) = \text{PGCD}(|a|; |b|)$.

Propriété

a, b et k désignent des nombres entiers naturels non nuls,

$$\text{PGCD}(ka; kb) = k \text{PGCD}(a; b)$$

Démonstration

On suppose $a \geq b$ (si $a < b$, on échange a et b).

- Si $a = b$, le résultat est immédiat.
- Si $a > b$, $a = bq + r_0$ avec $0 \leq r_0 < b$, alors $ka = kbq + kr_0$ avec $0 \leq kr_0 < kb$ (car $k \in \mathbb{N}^*$).

Donc kr_0 est le reste de la division de ka par kb . Avec l'algorithme d'Euclide (page 170), en multipliant chaque membre des égalités par k , on obtient $\text{PGCD}(ka; kb) = \text{PGCD}(kb; kr_0) = \dots = kr_0 = k \text{PGCD}(a; b)$.

Remarque : lorsque $a \in \mathbb{Z}^*, b \in \mathbb{Z}^*$ et $k \in \mathbb{Z}^*$, $\text{PGCD}(ka; kb) = |k| \text{PGCD}(a; b)$

car $\text{PGCD}(ka; kb) = \text{PGCD}(|ka|; |kb|)$ et $\text{PGCD}(a; b) = \text{PGCD}(|a|; |b|)$.

Conséquence

Si k est un nombre entier naturel non nul, diviseur commun aux entiers naturels non nuls a et b , alors :

$$\text{PGCD}(a; b) = k \text{PGCD}\left(\frac{a}{k}; \frac{b}{k}\right)$$

Ceci découle de la propriété précédente en écrivant $a = k \times \frac{a}{k}$ et $b = k \times \frac{b}{k}$.

B Nombres premiers entre eux

Définition

Dire que deux nombres entiers relatifs non nuls **a et b sont premiers entre eux** signifie que $\text{PGCD}(a; b) = 1$.

Propriété

a et b désignent deux nombres entiers relatifs non nuls, on pose $d = \text{PGCD}(a; b)$.

Alors $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont premiers entre eux.

Démonstration

$d = \text{PGCD}(a; b)$, donc d divise a et il existe un entier relatif non nul a' tel que $a = da'$. De même, il existe un entier relatif non nul b' tel que $b = db'$. Donc $d = \text{PGCD}(a; b) = \text{PGCD}(da'; db') = |d| \text{PGCD}(a'; b')$.

Or $d \geq 1$, donc $|d| = d$ et $d \neq 0$, d'où $\text{PGCD}(a'; b') = 1$.

EXERCICES RÉSOLUS

7 Déterminer les diviseurs communs à deux nombres entiers **Tice**

Si l'on divise 4 373 et 826 par un même entier naturel n , on obtient respectivement 8 et 7 pour restes.

- Déterminer, à l'aide du tableur, une valeur possible de n .
- Justifier que la valeur trouvée est la seule qui convient.

Solution

a) La feuille de calcul ci-contre permet de dire que $n = 9$ convient.

b) Il existe $q \in \mathbb{N}$ et $q' \in \mathbb{N}$ tels que $4\ 373 = n \times q + 8$ avec $0 \leqslant 8 < n$ et $826 = n \times q' + 7$ avec $0 \leqslant 7 < n$. Ainsi, $4\ 365 = n \times q$ et $819 = n \times q'$ et $n > 8$. n est donc un diviseur commun de 4 365 et 819, donc un diviseur de $\text{PGCD}(4\ 365 ; 819)$ avec $n > 8$. À l'aide de la calculatrice, on obtient :

$$\text{PGCD}(4\ 365 ; 819) = 9.$$

n est un diviseur de 9 et $n > 8$, donc $n = 9$.

	A	B	C
1	n	Reste de 4 373 par n	Reste de 826 par n
2	2	1	0
3	3	2	1
4	4	1	2
5	5	3	1
6	6	5	4
7	7	5	0
8	8	5	2
9	9	8	7

En cellule B2, on saisit la formule
=MOD(4373;A2)
pour obtenir par recopie vers le bas la colonne B.

8 Reconnaître des nombres premiers entre eux

On donne $a = 3n + 4$ et $b = 2n + 3$ où n désigne un nombre entier naturel.

Démontrer que a et b sont premiers entre eux.

Solution

On remarque que $3b - 2a = 3(2n + 3) - 2(3n + 4) = 1$.

On note $d = \text{PGCD}(a ; b)$, d divise a et b donc d divise $3b - 2a$, c'est-à-dire d divise 1. Le seul diviseur positif de 1 est lui-même donc $d = 1$.

Ainsi, pour tout entier naturel n , a et b sont premiers entre eux.

Ici, pour démontrer que a et b sont premiers entre eux, on détermine une combinaison linéaire de a et b égale à 1.

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 7

9 **Tice** Si l'on divise 2 747 et 613 par un même nombre entier naturel n , on obtient respectivement 3 et 5 pour restes.

- Déterminer, à l'aide du tableur, une valeur de n possible.
- Justifier que la valeur trouvée est la seule qui convient.

10 Un photographe doit réaliser une exposition de ses œuvres sur des panneaux contenant chacun le même nombre de paysages et le même nombre de portraits. Il dispose de 288 portraits et de 224 paysages et souhaite présenter au moins 20 panneaux.

De quel arrangement dispose-t-il pour l'exposition ?

Sur le modèle de l'exercice résolu 8

11 On donne $a = 21n + 4$ et $b = 16n + 3$ où n désigne un nombre entier naturel.

Démontrer que a et b sont premiers entre eux.

12 (u_n) est la suite arithmétique de raison 3 et de premier terme $u_0 = 5$.

(v_n) est la suite définie par $v_0 = 7$ et pour nombre entier naturel n , $v_{n+1} = v_n + 4$.

Démontrer que, pour tout nombre entier naturel n ,

$$\text{PGCD}(u_n ; v_n) = 1.$$

13 Prouver que la fraction $\frac{n}{2n+1}$ est irréductible pour tout entier naturel non nul n .

3 Le théorème de Bézout

A Identité de Bézout

Identité de Bézout

a et b désignent deux nombres entiers relatifs non nuls.

Si $d = \text{PGCD}(a; b)$, alors il existe des entiers relatifs u et v tels que $au + bv = d$.

Démonstration

E désigne l'ensemble des nombres entiers naturels non nuls de la forme $au + bv$ avec $u \in \mathbb{Z}, v \in \mathbb{Z}$.

- $E \neq \emptyset$ car $|a|$ appartient à E . En effet, si $a > 0$, $|a| = a = 1a + 0b$ et si $a < 0$, $|a| = -a = -1a + 0b$, donc E admet un plus petit élément. On le note c . On note également $d = \text{PGCD}(a; b)$.
- On sait que d divise a et b , donc d divise toute combinaison linéaire de a et b , donc d divise c .
- En effectuant la division euclidienne de a par c , on obtient l'existence d'un unique couple $(q; r)$ de nombres entiers tel que $a = c \times q + r$ avec $0 \leq r < c$.

Comme $r = a - c \times q$, r est une combinaison linéaire de a et c . Or, c est une combinaison linéaire de a et b , donc r est combinaison linéaire de a et b .

On raisonne par l'absurde et on suppose que $r > 0$. Alors r serait une combinaison linéaire strictement positive de a et b telle que $r < c$, ce qui est absurde car c est le plus petit élément de E . On en déduit que $r = 0$ et ainsi c divise a .

On démontre de même que c divise b . Ainsi, c est un diviseur commun de a et b , donc c divise d .

Alors $c = d$ et $\text{PGCD}(a; b)$ peut s'écrire $au + bv$ avec u et v dans \mathbb{Z} .

Exemple

- On sait que $\text{PGCD}(55; 35) = 5$, donc d'après l'identité de Bézout, il existe des nombres entiers relatifs u et v tels que $55u + 35v = 5$.
- Par exemple, $u = 2$ et $v = -3$. En effet, $55 \times 2 + 35 \times (-3) = 5$.

Remarques :

- Le couple $(u; v)$ n'est pas unique. Si $a = 3$ et $b = 2$, $\text{PGCD}(a; b) = 1$ et $3 \times 1 + 2 \times (-1) = 1$, mais aussi $3 \times (-1) + 2 \times 2 = 1$.
- La réciproque de l'identité de Bézout est fausse.

Par exemple, $2 \times (-2) + 3 \times 2 = 2$ et pourtant 2 n'est pas le PGCD de 2 et 3.

B Théorème de Bézout

Théorème de Bézout

a et b désignent deux nombres entiers relatifs non nuls.

a et b sont premiers entre eux si, et seulement si, il existe des entiers relatifs u et v tels que $au + bv = 1$.

Démonstration

- Si a et b sont premiers entre eux, alors $\text{PGCD}(a; b) = 1$.

L'identité de Bézout permet alors de dire qu'il existe des nombres entiers relatifs u et v tels que $au + bv = 1$.

- Réciproquement, s'il existe des nombres entiers relatifs u et v tels que $au + bv = 1$, tout diviseur commun à a et b divise $au + bv$, donc divise 1. Ainsi $\text{PGCD}(a; b) = 1$ et donc a et b sont premiers entre eux.

Exemple

- Pour tout entier naturel n , $3 \times (5n + 7) - 5 \times (3n + 4) = 1$, donc d'après le théorème de Bézout, 5n + 7 et 3n + 4 sont premiers entre eux.

EXERCICES RÉSOLUS

14 Calculer les coefficients de Bézout

On donne $a = 145$ et $b = 55$.

a) Déterminer $\text{PGCD}(a; b)$ avec l'algorithme d'Euclide.

b) En exprimant de proche en proche chaque reste en fonction des restes précédents, déterminer un couple $(u; v)$ de nombres entiers relatifs tels que $au + bv = \text{PGCD}(a; b)$.

Solution

a)	a	b	q	r	Calculs
Étape 1	145	55	2	35	$145 = 55 \times 2 + 35$
Étape 2	55	35	1	20	$55 = 35 \times 1 + 20$
Étape 3	35	20	1	15	$35 = 20 \times 1 + 15$
Étape 4	20	15	1	5	$20 = 15 \times 1 + 5$
Étape 5	15	5	3	0	$15 = 5 \times 3$

On effectue de proche en proche des divisions euclidiennes pour déterminer $\text{PGCD}(a; b)$.

Le dernier reste non nul est 5 donc $\text{PGCD}(a; b) = 5$.

b) On remonte l'algorithme d'Euclide à partir de l'étape 4 en isolant les différents restes obtenus.

Étape 4	Étape 3	Étape 2	Étape 1
$5 = 20 - 15 \times 1$	$15 = 35 - 20 \times 1$	$20 = 55 - 35 \times 1$	$35 = 145 - 55 \times 2$
	$5 = 20 - (35 - 20 \times 1) \times 1$ $5 = -35 + (55 - 35 \times 1) \times 2$	$5 = -35 + (55 - 35 \times 1) \times 2$ $5 = 55 \times 2 - 35 \times 3$	$5 = 55 \times 2 - (145 - 55 \times 2) \times 3$ $5 = 55 \times 8 - 145 \times 3$

Donc $5 = 145 \times (-3) + 55 \times 8$, on en déduit que $5 = au + bv$ avec $u = -3$ et $v = 8$.

15 Déterminer un inverse de a modulo n lorsque a et n sont premiers entre eux

On dit qu'un nombre entier relatif a admet un inverse modulo n ($n \in \mathbb{N}$, $n \geq 2$) ou encore qu'il est inversible modulo n lorsqu'il existe un entier relatif b tel que $ab \equiv 1 [n]$.

a) Démontrer que 17 est inversible modulo 26.

b) Résoudre dans \mathbb{Z} l'équation $17x \equiv 15 [26]$.

Solution

a) De l'égalité $17 \times (-3) + 26 \times 2 = 1$, on déduit $17 \times (-3) \equiv 1 [26]$.

Ainsi 17 est inversible modulo 26.

b) Pour tout $x \in \mathbb{Z}$, $17x \equiv 15 [26]$ équivaut à $(-3) \times 17x \equiv (-3) \times 15 [26]$, c'est-à-dire $x \equiv -45 [26]$, soit $x \equiv 7 [26]$.

Les solutions de l'équation sont les nombres $x = 7 + 26k$ avec $k \in \mathbb{Z}$.

Les coefficients de Bézout u et v tels que $17u + 26v = 1$ peuvent être obtenus par la méthode décrite à l'exercice 14.

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 14

16 On donne $a = 559$ et $b = 325$.

a) Déterminer $\text{PGCD}(a; b)$ avec l'algorithme d'Euclide.

b) Déterminer un couple $(u; v)$ d'entiers relatifs tels que $au + bv = \text{PGCD}(a; b)$.

Sur le modèle de l'exercice résolu 15

17 a) Démontrer que 4 est inversible modulo 9.

b) Dans chaque cas, résoudre dans \mathbb{Z} l'équation.

$$\bullet 4x \equiv 3 [9]$$

$$\bullet 7x \equiv 5 [9]$$

4 Le théorème de Gauss

A Le théorème de Gauss

Théorème de Gauss

a, b et c désignent trois nombres entiers relatifs non nuls.

Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c .

Démonstration

a et b sont premiers entre eux, d'après le théorème de Bézout, il existe des nombres entiers relatifs u et v tels que $au + bv = 1$.

En multipliant chaque membre de l'égalité par c , on obtient $auc + bvc = c$.

a divise auc et par hypothèse, a divise bc donc bvc , alors a divise $auc + bvc$, c'est-à-dire a divise c .

Remarque : l'hypothèse a et b sont premiers entre eux est essentielle. En effet, a peut diviser bc sans diviser ni b , ni c . Par exemple 6 divise 300 sans diviser ni 15 ni 20.

Exemple

- Résolution de l'équation $7x = 11y$ avec $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$.
 - Si $7x = 11y$, alors 11 divise $7x$.
 - Or 7 et 11 sont premiers entre eux, donc d'après le théorème de Gauss, 11 divise x .
 - Par conséquent, il existe un entier relatif k tel que $x = 11k$.
 - Alors de $7x = 11y$, on déduit que $7 \times 11k = 11y$, soit $y = 7k$.
 - Réciproquement, tous les couples $(11k ; 7k)$ avec $k \in \mathbb{Z}$, sont solutions de l'équation $7x = 11y$.
 - En effet, $7 \times 11k = 11 \times 7k$.
 - Conclusion
 - Les solutions de l'équation $7x = 11y$ sont les couples $(11k ; 7k)$ avec $k \in \mathbb{Z}$.

B Conséquence

Propriété

a, b et c désignent des nombres entiers relatifs non nuls.

Si b et c sont premiers entre eux et divisent a , alors bc divise a .

Démonstration

- b divise a donc il existe un entier relatif k tel que $a = kb$.
- c divise a donc il existe un entier relatif k' tel que $a = k'c$.

Alors $kb = k'c$ et on en déduit que b divise $k'c$.

b et c étant premiers entre eux, d'après le théorème de Gauss, b divise k' donc il existe un entier relatif k'' tel que $k' = k''b$.

De $a = k'c$, on déduit alors $a = k''bc$ donc bc divise a .

Exemples

- Le nombre 1 573 875 est divisible par 5 (car le chiffre des unités est 5) et il est divisible par 9 (car la somme de ses chiffres est divisible par 9).
- Or 5 et 9 sont premiers entre eux, donc 1 573 875 est divisible par 5×9 , soit 45.
- Le produit $n(n+1)(n+2)$ de trois nombres entiers naturels consécutifs est divisible par 2 et par 3.
- Ce produit est donc divisible par 6 car 2 et 3 sont premiers entre eux.

EXERCICES RÉSOLUS

18 Résoudre une équation diophantienne

(E) est l'équation $7x - 11y = 3$ où x et y sont des nombres entiers relatifs.

a) Vérifier que le couple $(x_0 ; y_0) = (13 ; 8)$ est solution de l'équation (E).

b) Utiliser l'exemple du paragraphe A pour résoudre l'équation (E).

Solution

a) $7x_0 - 11y_0 = 7 \times 13 - 11 \times 8 = 3$, donc $(x_0 ; y_0)$ est une solution de (E).

b) Un couple $(x ; y)$ est solution de (E) si, et seulement si, $7x - 11y = 3$, ce qui équivaut à :

$$7x - 11y = 7x_0 - 11y_0, \text{ c'est-à-dire } 7(x - x_0) = 11(y - y_0).$$

On sait que les solutions de l'équation $7x = 11y$ sont les couples $(11k ; 7k)$ avec $k \in \mathbb{Z}$.

Donc les solutions de $7(x - x_0) = 11(y - y_0)$ sont les couples tels que $(x - x_0 ; y - y_0) = (11k ; 7k)$ avec $k \in \mathbb{Z}$.

Ainsi, les solutions de l'équation (E) sont les couples $(x ; y)$ tels que :

$$x = x_0 + 11k = 13 + 11k \text{ et } y = y_0 + 7k = 8 + 7k \text{ avec } k \in \mathbb{Z}.$$

19 Établir une divisibilité

n désigne un nombre entier naturel et on pose $a = n(2n+1)(7n+1)$.

Démontrer que a est divisible par 6.

Solution

• On démontre que a est divisible par 2.

On construit le tableau de congruences modulo 2 ci-contre.

Donc, pour tout n de \mathbb{N} , $a \equiv 0 [2]$, c'est-à-dire 2 divise a .

n	0	1
$2n+1$	1	1
$7n+1$	1	0
a	0	0

Pour démontrer qu'un nombre est divisible par 6, il suffit de démontrer qu'il est divisible par 2 et 3. En effet, $6 = 2 \times 3$ et 2 et 3 sont premier entre eux.

• On démontre que a est divisible par 3.

On construit le tableau de congruences modulo 3 ci-contre.

Donc, pour tout n de \mathbb{N} , $a \equiv 0 [3]$, c'est-à-dire 3 divise a .

n	0	1	2
$2n+1$	1	0	2
$7n+1$	1	2	0
a	0	0	0

2 et 3 sont premiers entre eux, donc d'après une conséquence du théorème de Gauss, le produit 2×3 , c'est-à-dire 6, divise a .

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 18

20 x et y désignent des nombres entiers relatifs.

(E) est l'équation $4x - 3y = 5$.

a) Déterminer un couple $(x_0 ; y_0)$ solution particulière de l'équation (E).

b) Démontrer qu'un couple $(x ; y)$ est solution de (E) si, et seulement si, $4(x - x_0) = 3(y - y_0)$.

c) Résoudre l'équation (E).

Sur le modèle de l'exercice résolu 19

21 n désigne un nombre entier naturel.

Démontrer que $a = n(5n^2 + 1)$ est divisible par 6.

22 n désigne un nombre entier naturel.

Démontrer que $a = 5(n^2 + n)^2$ est divisible par 20.

23 Démontrer que pour tout entier naturel n , $n^7 - n$ est un multiple de 21.

EXERCICES RÉSOLUS

24 Calculer un PGCD avec l'algorithme d'Euclide

Cours 1. B

- a) Compléter l'algorithme d'Euclide ci-contre où a et b sont des nombres entiers naturels avec $a > b > 0$.
- b) Coder cet algorithme en langage Python et tester le programme obtenu.

Solution

a) Pointillés rouges : b Pointillés verts : r .

b)

```

1 def Euclide(a,b):
2     while b!=0:
3         r=a%b
4         a=b
5         b=r
6     return a
    
```

```

>>> Euclide(756,98)
14
>>> Euclide(2020,663)
1
    
```

Tant que $b \neq 0$
 $r \leftarrow$ reste de la division de a par b
 $a \leftarrow \dots$
 $b \leftarrow \dots$

Fin Tant que

En langage Python :

- $b!=0$ signifie $b \neq 0$;
- $a\%b$ donne le reste de la division euclidienne de a par b .

25 Calcul d'un couple de coefficients de Bézout

Cours 3. A

Le programme ci-contre écrit en langage Python définit une fonction **CBezout** dont les paramètres sont des entiers naturels a et b avec $a > b > 0$.

1. a) Exécuter pas à pas ce programme pour les valeurs $a = 28$ et $b = 13$ des paramètres.
b) Expliquer le rôle de cette fonction. Que représentent les éléments de la liste qu'elle renvoie ?
2. Saisir et tester cette fonction avec différents couples $(a; b)$.

Solution

1. a) Voici ci-contre un tableau de suivi des variables.

Le résultat renvoyé est la liste $[-6, 13, 1]$.

b) De façon générale, cette fonction renvoie une liste $[u, v, d]$ où $d = \text{PGCD}(a; b)$ et u, v sont des entiers relatifs tels que $au + bv = d$.

2. Par exemple :

```
>>> CBezout(1221,621)
[59, -116, 3]
```

Ainsi $\text{PGCD}(1221; 621) = 3$ et $1221 \times 59 + 621 \times (-116) = 3$.

```

1 def CBezout(a,b):
2     La=[1,0,a]
3     Lb=[0,1,b]
4     Lr=[0,0,0]
5     r=b
6     while r!=0:
7         q=La[2]/r
8         for k in range(0,3):
9             Lr[k]=La[k]-q*Lb[k]
10            La[k]=Lb[k]
11            Lb[k]=Lr[k]
12        r=Lb[2]
13    return La
    
```

q		2	6	2
La	[1,0,28]	[0,1,13]	[1,-2,2]	[-6,13,1]
Lb	[0,1,13]	[1,-2,2]	[-6,13,1]	[13,-28,0]
Lr	[0,0,0]	[1,-2,2]	[-6,13,1]	[13,-28,0]
r	13	2	1	0

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 24

- 26 Le programme de l'exercice 24, fonctionne-t-il lorsque a et b sont des entiers naturels non nuls tels que $a \leq b$?
Expliquer.

Sur le modèle de l'exercice résolu 25

- 27 a, b désignent des entiers naturels avec $a > b > 0$. D est un multiple de $\text{PGCD}(a; b)$. Écrire en langage Python une fonction de paramètres a, b, d' qui renvoie un couple $(u; v)$ d'entiers relatifs tels que $au + bv = D$.

PGCD et algorithme d'Euclide

Cours 1

Questions flash

À l'oral

28 Dans chaque cas, déterminer mentalement le PGCD des nombres.

- a) 21 et 28 b) 13 et 56 c) 45 et 60

29 Déterminer mentalement $\text{PGCD}(18 ; 999)$.

30 Le PGCD de 56 et 70 est :

- (1) 1 (2) 7 (3) 14 (4) 28

31 Paul a effectué les divisions suivantes :

$$204 = 39 \times 5 + 9$$

$$39 = 9 \times 4 + 3$$

$$9 = 3 \times 3 + 0$$

Il en déduit que $\text{PGCD}(204 ; 39) = 3$. A-t-il raison ?

32 n est un nombre entier naturel non nul.

Lily affirme : « Si $\text{PGCD}(n ; 125) = 5$, alors n est un multiple de 5 ».

Son affirmation est-elle exacte ?

33 Dans chaque cas, utiliser l'algorithme d'Euclide pour déterminer le PGCD des deux nombres.

- a) 324 et 111 b) 4 135 et 272
c) 2 534 et 722 d) 2 481 et 276

34 Justifier avec l'algorithme d'Euclide les résultats obtenus à l'écran de calculatrice ci-dessous.

GCD(345, 90)	15
GCD(408, 120)	24
GCD(224, 210)	14

35 Dans le cadre d'un voyage humanitaire, Cloé a réuni 34 cahiers et 153 stylos.

Elle constitue des lots ayant le même nombre de cahiers et le même nombre de stylos qu'elle donnera aux enfants d'une école.

- a) Combien l'école compte-t-elle d'enfants ?
b) Combien y aura-t-il de cahiers et de stylos dans chaque lot ?

36 On cherche les entiers naturels non nuls n inférieurs à 100 tels que $\text{PGCD}(n ; 126) = 9$.

- a) Justifier que n est un multiple de 9.
b) Déterminer alors les entiers n cherchés.

37 Algo python

A et B désignent des nombres entiers relatifs non nuls tels que $A > B$.

a) Démontrer que $\text{PGCD}(A ; B) = \text{PGCD}(B ; A - B)$.

b) Voici un programme écrit en langage Python.

```
1 from math import *
2
3 def Diff(a,b):
4     A=max(a,b)
5     B=min(a,b)
6     D=A-B
7     while D!=0:
8         A=max(B,D)
9         B=min(B,D)
10        D=A-B
11    return A
```

Reproduire et compléter le tableau ci-dessous avec $a = 236$ et $b = 172$ en exécutant pas à pas ce programme.

A	B	D
236	172	64
172	64	...
...

c) Expliquer le rôle de ce programme.

38 n désigne un nombre entier naturel non nul.

- a) Montrer que $\text{PGCD}(n ; 2n + 5) = \text{PGCD}(n ; 5)$.
b) Déterminer $\text{PGCD}(n ; 2n + 5)$ lorsque n est un multiple de 5.

39 a et b désignent des nombres entiers naturels non nuls. On donne :

$$m = 3a + 4b \text{ et } n = 2a + 3b.$$

a) Justifier qu'un diviseur commun à a et b est aussi un diviseur commun à m et n .

b) Calculer $3m - 4n$ et $3n - 2m$.

En déduire qu'un diviseur commun à m et n est aussi un diviseur commun à a et b .

c) Que peut-on dire de $\text{PGCD}(a ; b)$ et $\text{PGCD}(m ; n)$?

40 On donne $a = 5n^2 + 7$ et $b = n^2 + 2$ avec n nombre entier naturel.

- a) Déterminer une combinaison linéaire de a et b éliminant n^2 .
b) Démontrer que $\text{PGCD}(a ; b)$ est un diviseur de 3.
c) Montrer que, si le reste de la division euclidienne de n par 3 est 2, alors $\text{PGCD}(a ; b) = 3$.
d) Justifier par exemple que :

$$\text{PGCD}\left(5 \times 101^2 + 7 ; 101^2 + 2\right) = 3.$$

Couples de nombres premiers entre eux

Cours 2

Questions flash

À l'oral

41 Les nombres 25 et 54 sont-ils premiers entre eux ? Justifier.

42 Stann affirme : « Pour tout entier naturel n , $n+4$ et $2n+1$ sont premiers entre eux ». A-t-il raison ?

43 Louise affirme : « Deux nombres entiers relatifs non nuls et consécutifs sont premiers entre eux ». A-t-elle raison ?

44 Algo python

Élise a exécuté le programme suivant écrit en langage Python :

```
1 from sympy import *
2
3 c=0
4 for k in range(0,1000):
5     if gcd(3*k+1,5*k+2)==1:
6         c=c+1
7 print(c)
```

Elle obtient 1 000. Que peut-elle en déduire ?

45 Déterminer mentalement PGCD(500 ; 700).

46 Jules affirme : « $90 = 18 \times 5$ et $126 = 18 \times 7$ » donc PGCD(90 ; 126) = 18. A-t-il raison ?

Pour les exercices **47 à 50**, déterminer les diviseurs communs positifs à a et b , puis indiquer si a et b sont premiers entre eux.

47 $a = 1286$ et $b = 1070$

48 $a = 1237$ et $b = -120$

49 $a = -2197$ et $b = 2140$

50 $a = -1236$ et $b = -567$

51 n désigne un nombre entier naturel tel que $n \geq 2$. On pose :

$$a = n^2 + 2n - 3 \text{ et } b = n^2 + 4n + 3.$$

a) Factoriser a et b .

b) Déterminer PGCD($n-1$; $n+1$) en distinguant les cas n pair et n impair.

c) Exprimer alors PGCD(a ; b) en fonction de n .

52 a et b désignent des nombres entiers naturels non nuls tels que :

$$(S) \begin{cases} a+b=216 \\ \text{PGCD}(a;b)=27 \end{cases}$$

a) On pose $a' = \frac{a}{27}$ et $b' = \frac{b}{27}$.

Que peut-on dire des entiers naturels a' et b' ?

b) Justifier que résoudre le système (S) revient à résoudre le système :

$$(S') \begin{cases} a'+b'=8 \\ \text{PGCD}(a';b')=1 \end{cases}$$

c) Résoudre alors le système (S') puis donner les couples solutions du système (S).

Pour les exercices **53 à 55**, déterminer les couples (a ; b) d'entiers naturels non nuls solutions du système.

$$\begin{array}{l} \text{53} \quad (S) \begin{cases} a-b=84 \\ \text{PGCD}(a;b)=12 \end{cases} \\ \text{54} \quad (S) \begin{cases} ab=10\,830 \\ \text{PGCD}(a;b)=19 \end{cases} \end{array}$$

$$\begin{array}{l} \text{55} \quad (S) \begin{cases} a^2-b^2=5\,440 \\ \text{PGCD}(a;b)=8 \end{cases} \end{array}$$

56 Déterminer PGCD(a ; b) sans utiliser ni la calculatrice ni l'algorithme d'Euclide.

a) $a = 656$ et $b = 312$

b) $a = 72$ et $b = 171$

c) $a = 630$ et $b = 360$

57 n désigne un nombre entier naturel.

On note $a = 13n+3$ et $b = 8n+2$.

La feuille de calcul ci-dessous donne PGCD(a ; b) pour les premières valeurs de n .

A	B	C	D	E	F	G	H	I	J	K	L
1	n	0	1	2	3	4	5	6	7	8	9
2	a	3	16	29	42	55	68	81	94	107	120
3	b	2	10	18	26	34	42	50	58	66	74
4	PGCD(a,b)	1	2	1	2	1	2	1	2	1	2

a) Conjecturer une condition sur n pour que a et b soient premiers entre eux.

b) Démontrer la conjecture émise au **a)**.

c) En déduire les valeurs de n pour lesquelles la fraction $\frac{13n+3}{8n+2}$ est irréductible.

58 n désigne un nombre entier naturel supérieur ou égal à 2.

a) Déterminer le PGCD des entiers naturels $n(n+1)$ et $(n-1)(n+2)$.

b) Que peut-on conclure pour les nombres :

$$a = \frac{n(n+1)}{2} \text{ et } b = \frac{(n-1)(n+2)}{2},$$

Le théorème de Bézout

Cours 3

Questions flash

À l'oral

- 59** Justifier mentalement qu'il existe des nombres entiers relatifs u et v tels que :

$$15u + 39v = 3.$$

- 60** De l'égalité $85 \times 26 - 23 \times 96 = 2$, un élève affirme que $\text{PGCD}(85; 23) = 2$.

A-t-il raison ? Expliquer oralement.

- 61** Existe-t-il des entiers relatifs x et y tels que :

$$2x + 4y = 3 ?$$

- 62** Déterminer un couple d'entiers relatifs solution de l'équation $7x + 5y = 1$.

- 63** Dire mentalement si les couples $(1+4k; 1+6k)$ avec $k \in \mathbb{Z}$ sont solutions de l'équation $3x - 2y = 1$.

Pour les exercices **64** et **65**, écrire l'algorithme d'Euclide pour déterminer $\text{PGCD}(a; b)$, puis en déduire des nombres entiers relatifs u et v tels que :

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

- 64** a) $a = 1050 ; b = 735$ b) $a = 564 ; b = 235$

- 65** a) $a = 364 ; b = 119$ b) $a = 956 ; b = 231$

- 66** a) Déterminer $\text{PGCD}(438; 128)$ et obtenir des nombres entiers relatifs u et v tels que $438u + 128v = 2$.

- b) En déduire des nombres entiers relatifs u' et v' tels que $438u' + 128v' = 6$.

67 Algo python

- a) Au début de cet algorithme, on affecte 3 à la variable i . Quel est le rôle de cet algorithme ?

```
Tant que  $i \leqslant 100$ 
|    $d \leftarrow \text{PGCD}(4i - 7; -3i + 6)$ 
|   Afficher  $d$ 
|    $i \leftarrow i + 1$ 
Fin Tant que
```

- b) Coder cet algorithme en langage Python et l'exécuter afin d'émettre une conjecture, puis la démontrer.

- c) Déterminer des nombres entiers relatifs u et v tels que, pour tout entier naturel $n \geqslant 3$, $(4n - 7)u + (-3n + 6)v = 3$.

- 68** a) Calculer $83 \times 167 - 84 \times 165$.

- b) Que peut-on en déduire pour les nombres 83 et 165 ?

- c) Peut-on dire également que les nombres 167 et -165 sont premiers entre eux ?

- 69** a) Démontrer que, pour tout entier relatif n , $14n + 3$ et $5n + 1$ sont premiers entre eux.

- b) En déduire que $\text{PGCD}(87; 31) = 1$.

- c) À l'aide des résultats précédents, déterminer une solution particulière $(u; v)$ de l'équation : $87u + 31v = 1$.

- 70** Démontrer par l'absurde qu'il n'existe pas d'entiers relatifs n tels que $\frac{n-3}{12}$ et $\frac{n-2}{15}$ soient tous les deux des entiers.

- 71** n désigne un nombre entier naturel non nul.

- a) Factoriser $n(2n + 1) - 1$.

- b) Trouver le PGCD de $n + 1$ et $2n + 1$ à l'aide du théorème de Bézout.

- 72** n désigne un nombre entier naturel non nul.

Dans chaque cas, utiliser le théorème de Bézout pour démontrer que a et b sont premiers entre eux.

- a) $a = 7n + 2$ et $b = 11n + 3$

- b) $a = 4n + 5$ et $b = 5n + 6$

- c) $a = n^2 + 1$ et $b = n$

- d) $a = (n+1)^2$ et $b = n+2$

- 73** On considère l'équation $89x + 37y = 1$ où x et y sont des nombres entiers relatifs.

- a) Utiliser l'algorithme d'Euclide pour déterminer un couple $(x; y)$ d'entiers relatifs solution de l'équation.

- b) Ce couple est-il unique ?

- 74** Dans chacun des cas ci-dessous, utiliser l'algorithme d'Euclide pour trouver un couple de nombres entiers relatifs solution de l'équation proposée.

- a) $135x + 29y = 1$

- b) $27x + 11y = 1$

- c) $48x + 21y = 3$

- d) $135x + 75y = 15$

- 75** a) Démontrer que 4 est inversible modulo 17.

- b) Résoudre l'équation $4x \equiv 11 [17]$.

- 76** a) Démontrer que 7 est inversible modulo 12.

- b) Résoudre l'équation $7x \equiv 10 [12]$.

- 77** m et n désignent des nombres entiers naturels non nuls. Démontrer que si m et n^2 sont premiers entre eux, alors m et n sont premiers entre eux.

78 n désigne un nombre entier naturel, $n \geq 2$.

La fraction $\frac{n^2 - 1}{n}$ est-elle irréductible, c'est-à-dire $n^2 - 1$ et n sont-ils premiers entre eux ?

79 n désigne un nombre entier naturel non nul.

Dans chaque cas, dire si la fraction est irréductible.

a) $\frac{n}{n^2 + 1}$ b) $\frac{5n + 2}{7n + 3}$ c) $\frac{2n + 1}{8n + 5}$

80 On considère la suite (u_n) définie pour tout

nombre entier naturel $n \geq 1$ par $u_n = \frac{3^n - 1}{2}$.

a) Justifier que pour tout n de \mathbb{N}^* , u_n est un entier.

b) À partir de la feuille de calcul ci-dessous, conjecturer le PGCD de u_n et u_{n+1} .

	A	B	C	D
	u_n	u_{n+1}	PGCD($u_n; u_{n+1}$)	
1	n			
2	1	4	1	
3	2	13	1	
4	3	40	1	
5	4	121	1	
6	5	364	1	

c) Vérifier que pour tout n de \mathbb{N}^* ,

$$u_{n+1} = 3u_n + 1.$$

d) En déduire que pour tout n de \mathbb{N}^* , u_n et u_{n+1} sont premiers entre eux.

Le théorème de Gauss

Cours 4

Questions Flash

À l'oral

81 5 divise $7m$ avec $m \in \mathbb{N}^*$.

Peut-on affirmer que m est un multiple de 5 ?

82 $11m = 12n$ avec $m \in \mathbb{Z}$, $n \in \mathbb{Z}$.

Paul affirme : « n est donc un multiple de 11 ».

Louis énonce : « m est donc un multiple de 12 ».

Les deux amis ont-ils raison ?

83 a est un nombre entier naturel divisible par 4 et 6. Marie affirme : « a est nécessairement divisible par 24 ». A-t-elle raison ?

84 3, 5 et 7 divisent un même nombre entier naturel n . Alors, n est-il divisible par $3 \times 5 \times 7$?

85 n désigne un nombre entier relatif.

L'implication : « Si $7x \equiv 0 [5]$, alors $x \equiv 0 [5]$ » est-elle vraie ? Justifier oralement.

86 n désigne un nombre entier naturel.

On donne $a = n(n^2 + 5)$.

a) Reproduire et compléter les tableaux de congruence.

$n \equiv \dots [2]$	0	1
$n^2 + 5 \equiv \dots [2]$		
$a \equiv \dots [2]$		

$n \equiv \dots [3]$	0	1	2
$n^2 + 5 \equiv \dots [3]$			
$a \equiv \dots [3]$			

b) En déduire que a est divisible par 6.

87 Montrer que si $n \equiv 0 [5]$ et $n \equiv 0 [8]$, alors $n \equiv 0 [40]$.

88 n désigne un nombre entier naturel. Démontrer que le produit $(n^2 - n)(2n - 1)$ est divisible par 6.

89 n désigne un nombre entier naturel.

a) Démontrer que le produit $n(n^6 - 1)$ est divisible par 7 et 6 pour tout entier naturel n .

b) En déduire que le produit $n(n^6 - 1)$ est divisible par 42 pour tout entier naturel n .

c) Déterminer les entiers naturels n pour lesquels le produit $n(n^6 - 1)$ est divisible par 4.

d) En déduire les entiers naturels n tels que le produit $n(n^6 - 1)$ soit divisible par 84.

90 n désigne un nombre entier naturel strictement supérieur à 2 et $a = n(n^2 - 1)(n^2 - 4)$.

1. a) Écrire a sous forme d'un produit de cinq entiers consécutifs.

b) Démontrer que a est divisible par 3 et que a est divisible par 5.

2. Démontrer que a est divisible par 8.

3. En déduire que a est divisible par 120.

91 a, b, c et d sont des nombres entiers naturels non nuls, termes consécutifs d'une suite géométrique dont la raison q est un nombre entier premier avec a .

De plus $10a^2 = d - b$.

a) Démontrer que $q(q + 1)(q - 1) = 10a$.

b) Déterminer les valeurs possibles de q .

c) Pour chaque valeur de q , donner les valeurs a, b, c et d correspondantes.

92 On considère l'équation (E) : $2x = 3y$ où x et y sont des nombres entiers relatifs.

a) Justifier que si $(x ; y)$ est un couple solution de (E), alors il existe $k \in \mathbb{Z}$ tel que $x = 3k$ et $y = 2k$.

b) Vérifier réciproquement que les couples $(3k ; 2k)$ avec $k \in \mathbb{Z}$ sont solutions de (E).

c) En déduire l'ensemble des couples $(x ; y)$ d'entiers relatifs solutions de (E).

Pour les exercices 93 et 94, résoudre dans \mathbb{Z}^2 l'équation proposée.

93 a) $7x = 5y$ b) $22x = 26y$

94 a) $5(x-4) = 3(y+1)$ b) $55(x-2) = 10(y-3)$

\mathbb{Z}^2 désigne l'ensemble de tous les couples $(x; y)$ avec $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$.

95 Chacune des équations suivantes a-t-elle des solutions dans \mathbb{Z}^2 ? Justifier.

a) $3x - 2y = 7$ b) $4x + 7y = 5$

96 On résout dans \mathbb{Z}^2 l'équation diophantienne (E) : $17x - 11y = 5$.

a) À l'aide de l'algorithme d'Euclide, déterminer un couple $(u; v)$ d'entiers relatifs tels que :

$$17u - 11v = 1.$$

b) En déduire un couple $(x_0; y_0)$ solution de (E).

c) On note $(x; y)$ un couple solution de l'équation (E).

Démontrer que $17(x - x_0) = 11(y - y_0)$.

d) En déduire qu'un couple solution de (E) est la forme $(10 + 11k; 15 + 17k)$ avec $k \in \mathbb{Z}$.

e) Vérifier réciproquement que les couples $(10 + 11k; 15 + 17k)$ avec $k \in \mathbb{Z}$ sont solutions de (E), puis conclure.

97 x et y désignent des nombres entiers relatifs.

On résout l'équation diophantienne (E) : $4x - 3y = 5$.

a) Déterminer un couple $(x_0; y_0)$ solution particulière de l'équation (E).

b) Démontrer qu'un couple $(x; y)$ est solution de (E) si, et seulement si, $4(x - x_0) = 3(y - y_0)$.

c) En déduire les couples de \mathbb{Z}^2 solutions de (E).

98 a et b désignent des entiers relatifs non nuls.

Dans le langage Python, `gcdex(a,b)` renvoie un couple solution dans \mathbb{Z}^2 de l'équation $ax + by = \text{PGCD}(a; b)$ ainsi que $\text{PGCD}(a; b)$.

Utiliser la copie d'écran ci-dessous pour répondre aux questions.

```
>>> from sympy import *
>>> gcdex(17, -11)
(2, 3, 1)
```

1. a) Quelle équation résout-on dans \mathbb{Z}^2 ?

b) Donner une solution particulière de cette équation.

c) Résoudre cette équation.

2. Déterminer les solutions dans \mathbb{Z}^2 de l'équation :

$$17x + 11y = 2.$$

99 n désigne un nombre entier naturel. On donne : $a = 2n - 1$, $b = 9n + 4$ et $d = \text{PGCD}(a; b)$.

a) Déterminer les valeurs possibles de d .

b) Montrer que $d = \text{PGCD}(a; 17)$.

c) Résoudre dans \mathbb{Z}^2 l'équation $2x - 17y = 1$.

d) En déduire les valeurs de n pour lesquelles $d = 17$.

100 n désigne un nombre entier naturel. On donne : $a = 11n + 3$ et $b = 13n - 1$.

a) Démontrer que tout diviseur de a et b est un diviseur de 50.

b) Déterminer les couples $(x; y)$ d'entiers relatifs solutions de l'équation $50x - 11y = 3$.

c) En déduire les valeurs de n pour lesquelles a et b ont 50 pour plus grand commun diviseur.

101 a) Déterminer les couples $(x; y)$ de \mathbb{Z}^2 solutions de l'équation (E) : $3x - 7y = 2$.

b) m désigne un nombre entier naturel tel que $m = 3 + 7p$ et $m = 1 + 3q$ avec $(p; q)$ dans \mathbb{N}^2 .

Montrer que le couple $(q; p)$ est solution de (E).

c) Déterminer le plus petit entier naturel m supérieur à 2020.

102 Algo python

On se propose de résoudre dans \mathbb{N}^2 l'équation (E) : $8x + 15y = 146$.

1. $(x; y)$ désigne un couple solution de (E). Montrer que les nombres entiers naturels x et y vérifient respectivement $x \leqslant 18$ et $y \leqslant 9$.

2. Voici un algorithme incomplet permettant d'obtenir les couples $(x; y)$ d'entiers naturels solutions de (E).

Pour x allant de 0 à ...

 Pour y allant de 0 à ...

 Si ... Alors

 Afficher x et y

 Fin Si

 Fin Pour

Fin Pour

a) Recopier et compléter l'algorithme.

b) Coder cet algorithme en langage Python. Saisir le programme et l'exécuter afin d'obtenir tous les couples solutions de (E).

103 n désigne un nombre entier naturel compris entre 1 et 100 dont le reste dans la division par 9 est 7 et dont le reste dans la division par 7 est 1.

a) Résoudre dans \mathbb{N}^2 l'équation $7u - 9v = 6$.

b) En déduire la valeur de n .

- 104** Pour réassortir sa vitrine, un bijoutier achète des pendentifs et des bracelets. Il paie chaque pendentif 35 € et chaque bracelet 37 €.



Il a payé 10 € de plus pour tous les pendentifs que pour tous les bracelets et la vitrine ne peut contenir que 100 bijoux.

x désigne le nombre de pendentifs et y le nombre de bracelets.

a) Montrer que $35x - 37y = 10$.

b) Résoudre l'équation précédente dans \mathbb{N}^2 .

c) En déduire le nombre de pendentifs et de bracelets dans la vitrine.

- 105** n désigne un nombre entier naturel, $n \geq 2$.

a) Démontrer qu'un nombre entier relatif non nul a est inversible modulo n si, et seulement si, a et n sont premiers entre eux.

b) Démontrer que si a est inversible modulo n , alors il existe un unique nombre entier naturel r compris entre 1 et $n-1$ tel que $ar \equiv 1 [n]$.

On dit que r est l'inverse de a modulo n .

c) Les entiers 4 et 17 sont-ils inversibles modulo 29 ?

Si oui, déterminer leur inverse.

- 106** a) Justifier que 25 est inversible modulo 97.

b) Déterminer son inverse modulo 97.

c) Résoudre dans \mathbb{Z} l'équation $25x \equiv 2 [97]$.

Pour les exercices 107 à 109, x désigne un nombre entier relatif. Résoudre les équations proposées.

107 a) $11x \equiv 7 [26]$ b) $17x \equiv 8 [34]$

108 a) $7x \equiv 9 [31]$ b) $8x \equiv 11 [17]$

109 a) $3x \equiv 2 [14]$ b) $8x \equiv 16 [14]$

110 b désigne un nombre entier naturel non nul. x désigne un nombre entier naturel et on considère l'équation (E) : $12x \equiv b [18]$.

1. a) Démontrer que (E) a des solutions si, et seulement si, 6 divise b .

b) Lorsque 6 divise b , montrer que l'équation (E) a six solutions comprises entre 0 et 17.

2. Dans chaque cas, dire si l'équation possède des solutions. Si oui, déterminer les 6 solutions comprises entre 0 et 17.

a) $12x \equiv 6 [18]$ b) $12x \equiv 7 [18]$

- 111** On associe à chaque lettre de l'alphabet, un nombre entier naturel compris entre 0 et 25.

La lettre A est associée à 0, la lettre B à 1, ... la lettre Z à 25.

On définit un chiffrement affine de la façon suivante : à l'entier x associé à la lettre à chiffrer, on fait correspondre l'entier y compris entre 0 et 25, tel que :

$$y \equiv 11x + 8 [26].$$

La lettre chiffrée est alors celle associée à l'entier y .

1. a) Justifier que la lettre M est codée par la lettre K.

b) Coder le mot MATHS.

2. Démontrer que deux lettres distinctes sont codées par deux lettres distinctes.

3. a) Déterminer l'inverse de 11 modulo 26, c'est-à-dire trouver l'entier r compris entre 0 et 25 tel que $11r \equiv 1 [26]$.

b) Démontrer que :

$$y \equiv 11x + 8 [26] \text{ équivaut à}$$

$$x \equiv 19y + 4 [26].$$

c) Décoder TAXGUAJSAVVA.

- 112** On crypte un message avec un chiffrement affine défini par $y \equiv ax + b [26]$ où a , b , x et y désignent des nombres entiers naturels compris entre 0 et 25.

Dans chaque cas, déterminer les nombres entiers c et d compris entre 0 et 25 tels que $x \equiv cy + d [26]$.

a) $a = 3$ et $b = 6$

b) $a = 17$ et $b = 5$

- 113** Dans un chiffrement affine, la lettre E est codée W et la lettre P est codée D.

1. x et y désignent des entiers compris entre 0 et 25.

a) Démontrer que ce chiffrement est défini par :

$$y \equiv 3x + 10 [26].$$

b) Démontrer que le déchiffrement est défini par :

$$x \equiv 9y + 14 [26].$$

2. Décoder NJKVA.

Pour les exercices 114 à 116, on crypte un message avec un chiffrement affine défini par $y \equiv ax + b [26]$, où a , b , x , y sont des entiers naturels compris entre 0 et 25.

Déterminer a et b si possible.

- 114** E est codé par M et P est codé par P.

- 115** E est codé par U et S est codé par O.

- 116** E est codé par Q et S est codé par S.

117 QCM Dans chaque cas, donner la réponse exacte sans justifier.

	A	B	C	D
1 PGCD(168;108) est égal à ...	2	3	6	12
2 $a = 2n+7, b = n+3$ avec $n \in \mathbb{N}$. PGCD($a; b$) est égal à ...	1	2	7	3
3 Une solution particulière de l'équation $5x - 3y = 2$ dans \mathbb{Z}^2 est ...	(2;4)	(2;-4)	(-2;4)	(-2;-4)
4 L'équation $3x + 2y = 1$ possède dans \mathbb{Z}^2 ...	une seule solution	deux solutions	une infinité de solutions	au plus une solution
5 Un nombre entier naturel n non nul est divisible par 2 ; 3 ; 4 et 6. Alors on peut affirmer que n est divisible par ...	8	12	18	24

118 QCM Dans chaque cas, donner la (ou les) réponse(s) exacte(s) sans justifier.

	A	B	C	D
1 $a = 4n+10, b = 2n+1$ avec $n \in \mathbb{N}$. PGCD($a; b$) est égal à ...	1	2	4	8
2 Si $3x = 2y$ avec x et y dans \mathbb{Z} , alors ...	x est un multiple de 2	y est divisible par 3	y est pair	$x \equiv 0[2]$
3 Les solutions de l'équation $7x + 3y = 1$ dans \mathbb{Z}^2 sont les couples ...	$(1-3k; -2+7k)$ avec $k \in \mathbb{Z}$	$(1+3k; -2-7k)$ avec $k \in \mathbb{Z}$	$(-2-3k; 5+7k)$ avec $k \in \mathbb{Z}$	$(1-6k; -2+14k)$ avec $k \in \mathbb{Z}$
4 a, b et c sont de nombres entiers naturels non nuls. S'il existe des nombres entiers relatifs u et v tels que $au + bv = c$ alors ...	$c = \text{PGCD}(a; b)$	c divise a et b	tout diviseur commun à a et b divise c	tout diviseur commun à u et v divise c

119 Vrai/Faux Dans chaque cas, dire si l'affirmation est vraie ou fausse en justifiant.

On considère les équations diophantiennes suivantes :

$$(E) 368x + 117y = 1 \text{ et } (F) 368x + 117y = 2.$$

- 1 **Affirmation :** 368 et 117 sont premiers entre eux.
- 2 **Affirmation :** l'équation (E) n'a pas de solution.
- 3 **Affirmation :** si $(x_0; y_0)$ est une solution de (E), alors $368(x - x_0) = 117(y - y_0)$.
- 4 **Affirmation :** le couple $(-55; 173)$ est une solution particulière de (E).
- 5 **Affirmation :** les couples solutions de (F) sont $(-110 + 234k; 346 - 736k)$ avec $k \in \mathbb{Z}$.

Vérifiez vos réponses : p. 293

120 Démontrer l'égalité de deux PGCD

a, b, α, β sont des nombres entiers relatifs non nuls tels que $\begin{cases} \alpha = 4a + 3b \\ \beta = 5a + 4b \end{cases}$.

On note $d = \text{PGCD}(a; b)$, $d' = \text{PGCD}(\alpha; \beta)$ et on se propose d'établir que $d = d'$.

Rédiger la démonstration en suivant le guide ci-dessous.

(1) Utiliser la méthode énoncée à l'exercice résolu **2** :

E est l'ensemble des diviseurs communs à a et

F est l'ensemble des diviseurs communs à et

(2) Démontrer que E est inclus dans F : on suppose que $d \in E$, alors $d \dots a$ et b .

Or, d divise toute combinaison linéaire de a et b ; donc en particulier $4a + 3b$ et

Donc d divise et Ainsi, $d \in \dots$

(3) Exprimer a et b en fonction de α et β :

$$-5\alpha + 4\beta = -5(4a + 3b) + 4(\dots) = \dots$$

$$4\alpha - 3\beta = \dots$$

(4) Démontrer que F est inclus dans E : on suppose que $d' \in F$, alors d' divise ... et ..., donc d' divise $-5\alpha + 4\beta$ et ..., c'est-à-dire ... et Donc $d' \in \dots$

(5) Conclusion : conclure alors le raisonnement.



JAI
COMPRIS.COM

Toutes les démonstrations au programme en vidéo

Liste des démonstrations :

- Écriture du PGCD de a et b sous la forme $ax + by$, $(x; y) \in \mathbb{Z}^2$.
- Théorème de Gauss.

121 Résoudre une équation diophantienne

On résout dans \mathbb{Z}^2 l'équation (E) : $57x + 13y = 2$.

• Étape 1

Déterminer une solution particulière $(x_0; y_0)$ de l'équation (E).

• Étape 2

a) Démontrer que l'équation (E) est équivalente à l'équation :

$$(E') : 57(x - x_0) = -13(y - y_0).$$

b) Démontrer que, si $(x; y)$ est un couple de \mathbb{Z}^2 solution de (E'), alors il existe un entier relatif k tel que $x = x_0 + 13k$ et $y = y_0 - 57k$.

• Étape 3

Réiproquement, vérifier que tout couple $(x_0 + 13k; y_0 - 57k)$ avec $k \in \mathbb{Z}$ est solution de (E).

• Conclusion

Conclure la résolution de l'équation (E).

Conseil

Cette solution particulière peut être obtenue à l'aide de l'algorithme d'Euclide ou d'une fonction programmée (voir exercice **25**).

Conseil

La réciproque est indispensable pour donner l'ensemble des solutions de l'équation (E).

122 Caractériser les solutions d'une équation

On note (E) l'équation $a^2 = b^3$ où a et b sont des nombres entiers strictement positifs.

1. Donner des exemples de couples $(a; b)$ solutions de (E).

2. On suppose que a et b sont respectivement le cube et le carré d'un même nombre entier naturel $n \geq 1$. Démontrer alors que $(a; b)$ est un couple solution de (E).

3. Réiproquement, on suppose que $(a; b)$ est un couple solution de (E) et on note $d = \text{PGCD}(a; b)$.

a) Démontrer qu'il existe des entiers u et v premiers entre eux tels que $u^2 = dv^3$.

b) Démontrer que v divise u , puis que $v = 1$.

c) Terminer cette réciproque.

Conseil

On applique le théorème de Gauss.

UTILISER LE PGCD ET L'ALGORITHME D'EUCLIDE

123 n désigne un nombre entier naturel.

On donne, $a = n + 1$ et $b = 2n + 4$.

a) Démontrer que $\text{PGCD}(a ; b) = \text{PGCD}(a ; 2)$.

b) Déterminer $\text{PGCD}(a ; b)$ selon la parité de n .

Pour les exercices 124 et 125, déterminer $\text{PGCD}(a ; b)$ selon les valeurs du nombre entier naturel.

124 $a = 3n + 5$ et $b = 2n + 1$

125 $a = 2n + 2$ et $b = 5n + 3$

126 Démontrer que pour tout entier naturel n , $\text{PGCD}(n^2 + 2n ; n + 3)$ est égal à 3 si $n \equiv 0 \pmod{3}$ et est égal à 1 sinon.

127 a désigne un nombre entier relatif non nul.

Démontrer que $\text{PGCD}(a ; 20) = 1$ si, et seulement si, a n'est divisible ni par 2, ni par 5.

128 On désigne par p un nombre entier naturel.

On considère, pour tout entier naturel non nul n , le nombre $A_n = 2^n + p$.

On note d_n le PGCD de A_n et A_{n+1} .

a) Montrer que d_n divise 2^n .

b) Déterminer la parité de A_n selon la parité de p .

Justifier.

c) Déterminer la parité de d_n selon la parité de p .

d) En déduire le PGCD de $2^{2020} + 2020$ et $2^{2021} + 2020$.

129 (a_n) et (b_n) sont les suites définies par :

• $a_1 = 3$ et pour tout entier naturel $n \geq 1$:

$$a_{n+1} = a_n + 2.$$

• $b_1 = 2$ et pour tout entier naturel $n \geq 1$:

$$b_{n+1} = b_n + a_n.$$

1. Pour tout $n \geq 1$, exprimer a_n en fonction de n .

2. a) Démontrer que pour tout entier naturel $n \geq 2$,

$$b_n = 2 + \sum_{i=1}^{n-1} a_i.$$

b) En déduire b_n en fonction de n .

3. a) Démontrer que pour tout entier naturel $n \geq 1$, un diviseur commun à a_n et b_n est un diviseur de 5.

b) En déduire que $\text{PGCD}(a_n ; b_n) = 5$ si, et seulement si, $n \equiv 2 \pmod{5}$.

c) Que peut-on dire de a_n et b_n pour les autres valeurs de n ?

130 a et b désignent des nombres entiers naturels non nuls tels que $a > b$ et b ne divise pas a .

a) Montrer que si r est le reste de la division euclidienne de a par b , alors il existe un nombre entier naturel non nul q , tel que :

$$2^a - 1 = [(2^b)^q - 1] \times 2^r + 2^r - 1.$$

b) Vérifier que :

$$(2^b)^q - 1 = (2^b - 1)(2^{b(q-1)} + 2^{b(q-2)} + \dots + 1).$$

c) En déduire que :

$$\text{PGCD}(2^a - 1 ; 2^b - 1) = \text{PGCD}(2^b - 1 ; 2^r - 1).$$

d) Justifier, en utilisant l'algorithme d'Euclide, que $\text{PGCD}(2^a - 1 ; 2^b - 1) = 2^d - 1$ où $d = \text{PGCD}(a ; b)$.

e) Déterminer le PGCD de 2020 et 1996.

En déduire $\text{PGCD}(2^{2020} - 1 ; 2^{1996} - 1)$.

131 n désigne un nombre entier naturel non nul.

a) Vérifier que :

$$2n^2 + 12n + 13 = (2n + 2)(n + 5) + 3.$$

b) On pose $d = \text{PGCD}(2n^2 + 12n + 13 ; n + 5)$.

Pourquoi a-t-on $d = \text{PGCD}(n + 5 ; 3)$?

c) Justifier que $d = 3$ ou $d = 1$.

d) Pour quels entiers naturels $n \geq 1$, $2n^2 + 12n + 13$ et $n + 5$ sont-ils des nombres entiers premiers entre eux ?

132 n désigne un nombre entier naturel non nul.

On pose $S_n = 1 + 2 + \dots + n$.

a) Exprimer S_n en fonction de n sans utiliser de pointillés.

b) On note $d_n = \text{PGCD}(S_n ; S_{n+1})$.

En distinguant les cas n pair et n impair, exprimer d_n en fonction de n .

c) S_n et S_{n+1} sont-ils premiers entre eux ?

133 Les nombres de Fermat sont les termes de la suite (u_n) définie sur \mathbb{N} par :

$$u_n = 2^{2^n} + 1.$$

1. a) Démontrer que pour tout entier naturel,

$$u_{n+1} = (u_n - 1)^2 + 1.$$

b) Démontrer par récurrence que pour tout entier naturel $n \geq 1$,

$$u_n - 2 = u_0 \times u_1 \times \dots \times u_{n-1}.$$

2. a) m et n désignent deux nombres entiers naturels non nuls tels que $m < n$.

Montrer qu'il existe un entier naturel q tel que :

$$u_n = q u_m + 2.$$

b) Justifier que $\text{PGCD}(u_m ; u_n) = \text{PGCD}(u_m ; 2)$.

Conseil : Utiliser la méthode de l'exercice 2.

c) En déduire que $\text{PGCD}(u_m ; u_n) = 1$.

UTILISER LES THÉORÈMES DE BÉZOUT ET DE GAUSS

134 1. Montrer que pour tout entier relatif n , $7n+3$ et $5n+2$ sont premiers entre eux.

2. On considère l'équation (E) : $73x+52y=2$ où x et y sont des nombres entiers relatifs.

a) Justifier, avec 1., que 73 et 52 sont premiers entre eux.

b) Déterminer un couple $(u; v)$ d'entiers relatifs tel que $73u+52v=1$, puis un couple $(x_0; y_0)$ solution de (E).

c) Résoudre l'équation (E).

3. Dans un repère orthonormé, D est la droite d'équation réduite $y = -\frac{73}{52}x + \frac{1}{26}$.

Déterminer les points de D dont les deux coordonnées sont des nombres entiers relatifs compris entre $-1\ 000$ et $1\ 000$.

135 Algo python

On considère l'équation diophantienne de type Pell-Fermat, d'inconnue un couple $(x; y)$ de nombres entiers naturels (F) : $x^2 - 2y^2 = 1$.

1. On note $(a; b)$ un couple solution de (F).

a) Montrer que a est impair.

b) En déduire que b est pair.

c) Montrer que a et b sont premiers entre eux.

d) Vérifier que le couple $(3a+4b; 2a+3b)$ est aussi solution de (F).

2. a) Vérifier que (F) admet pour solution le couple $(1; 0)$.

b) Déduire quatre autres couples solutions de (F).

3. Voici une fonction écrite en langage Python, qui permet d'obtenir le n -ième couple solution de (F) obtenu à partir de la solution $(1; 0)$.

```
1 def Pell(n):
2     a=1
3     b=0
4     for k in range(1,n+1):
5         u=a
6         a=3*u+4*b
7         b=2*u+3*b
8     return a,b
```

a) Saisir et exécuter cette fonction pour $n = 10$.

b) Quel couple solution de (F) obtient-on ?

HISTOIRE DES MATHS

L'histoire des équations de Pell-Fermat est très ancienne. Diophante, le mathématicien indien Bhaskara au 12^e siècle, puis en Europe Fermat, Wallis, Pell et d'autres... ont contribué à leur résolution.

136 a et b désignent deux nombres entiers naturels non nuls premiers entre eux.

a) Démontrer que a et b^2 sont premiers entre eux.

b) Démontrer que pour tout entier naturel $n \geq 1$, a et b^n sont premiers entre eux.

c) Démontrer que quels que soient les entiers naturels non nuls n et p , a^p et b^n sont premiers entre eux.

137 On se propose de déterminer l'ensemble S des nombres entiers relatifs solutions du système :

$$\begin{cases} n \equiv 9 [17] \\ n \equiv 3 [5] \end{cases}.$$

1. On désigne par $(u; v)$ un couple d'entiers relatifs tel que $17u+5v=1$.

a) Justifier l'existence d'un tel couple.

b) On pose $n_0 = 3 \times 17u + 9 \times 5v$.

Démontrer que n_0 appartient à S .

c) Donner un exemple d'entier n_0 appartenant à S .

2. a) n désigne un nombre entier relatif appartenant à S .
Démontrer que $n - n_0 \equiv 0 [85]$.

b) En déduire qu'un nombre entier relatif n appartient à S si, et seulement si, il existe un entier relatif k tel que $n = 43 + 85k$.

3. Zoé sait qu'elle a entre 300 et 400 jetons.
Si elle fait des tas de 17 jetons, il lui en reste 9.

Si elle fait des tas de 5 jetons, il lui en reste 3.



Combien a-t-elle de jetons ?

138 x et y désignent deux nombres entiers naturels non nuls premiers entre eux.

On pose $S = x + y$ et $P = xy$.

1. a) Démontrer que x et S sont premiers entre eux, de même que y et S .

b) En déduire que S et P sont premiers entre eux.

c) Démontrer que S et P ont des parités différentes.

2. Déterminer les diviseurs positifs de 84.

3. Trouver les nombres premiers entre eux x et y de \mathbb{N}^* tels que $SP = 84$.

4. Déterminer les deux nombres entiers naturels non nuls a et b vérifiant les conditions suivantes :

$$\begin{cases} a+b=84 \\ ab=d^3 \end{cases} \text{ avec } d = \text{PGCD}(a; b).$$

Conseil : poser $a = dx$ et $b = dy$ avec x et y premiers entre eux.

139 Dans le plan complexe muni d'un repère orthonormé direct, A et B sont les points d'affixes $z_A = -1 + i$ et $z_B = 3 + 2i$.

À tout point M d'affixe z , on associe le point M' d'affixe z' tel que $z' = (1+i)\bar{z} - 1 + 3i$.

a) On note $z = x + iy$ (x, y nombres réels) l'affixe du point M.

Démontrer que \overrightarrow{AB} et $\overrightarrow{AM'}$ sont orthogonaux si, et seulement si, $5x + 3y = -2$.

b) Déterminer les points M dont les coordonnées entières appartiennent à l'intervalle $[-20; 20]$ et tels que \overrightarrow{AB} et $\overrightarrow{AM'}$ sont orthogonaux.

140 a et b désignent des nombres entiers relatifs.

a) Montrer que, si $ab \equiv 0 [19]$, alors :

$$a \equiv 0 [19] \text{ ou } b \equiv 0 [19].$$

b) En déduire que, si $a^2 \equiv 1 [19]$, alors :

$$a \equiv 1 [19] \text{ ou } a \equiv -1 [19].$$

141 a et b désignent des entiers naturels non nuls.

On considère l'équation (E) : $a^2 - 3ab + b^2 = 0$.

a) Montrer que, si le couple $(a; b)$ est solution de (E), alors il existe un couple $(a'; b')$ d'entiers naturels non nuls premiers entre eux tel que :

$$a'^2 - 3a'b' + b'^2 = 0.$$

b) Montrer alors que a' divise b'^2 , puis que a' divise b' .

c) Établir que b' est solution de l'équation :

$$b'^2 - 3b' + 1 = 0.$$

d) Résoudre l'équation (E).

142 On note (F_n) la suite de Fibonacci définie par

$F_0 = F_1 = 1$ et pour tout entier naturel $n \geq 1$,

$$F_{n+2} = F_{n+1} + F_n.$$

a et b désignent des nombres entiers naturels non nuls et on considère l'équation (E) : $(a^2 + ab - b^2)^2 = 1$.

1. a) Vérifier que les couples $(F_i; F_{i+1})$ pour $0 \leq i \leq 5$ sont solutions de (E).

b) Déterminer $\text{PGCD}(F_i; F_{i+1})$ pour $0 \leq i \leq 5$.

2. Démontrer que si $(a; b)$ est un couple solution de (E), alors $a^2 - b^2 \leq 0$.

3. Démontrer que si $(x; y)$ est un couple solution de (E), alors le couple $(y; y+x)$ est aussi solution de (E).

4. a) Justifier qu'il existe des entiers relatifs u et v tels que $(a^2 + ab - b^2)^2 = au + bv$.

b) En déduire que si $(a; b)$ est solution de (E), alors a et b sont premiers entre eux.

5. a) Démontrer par récurrence que le couple $(F_n; F_{n+1})$ est solution de (E).

b) En déduire que F_n et F_{n+1} sont premiers entre eux.

143 1. On considère l'équation (E) :

$$6x + 7y = 55$$

où x et y sont des nombres entiers relatifs.

a) Déterminer un couple solution de (E).

b) Résoudre l'équation (E).

L'espace est muni d'un repère orthonormé, on note \mathcal{P} le plan d'équation $6x + 7y + 8z = 55$.

2. Déterminer les points de \mathcal{P} dont les coordonnées sont des nombres entiers naturels et qui appartiennent au plan $(O; \vec{i}, \vec{j})$.

3. M est un point de \mathcal{P} dont les coordonnées x, y et z sont des entiers naturels.

a) Montrer que y est impair.

b) On pose $y = 2p + 1$ avec $p \in \mathbb{N}$.

Montrer que $z + p$ est divisible par 3.

c) On pose $z + p = 3q$ avec $q \in \mathbb{N}$.

Démontrer que $x + p + 4q = 8$.

En déduire les valeurs prises par q.

4. Déterminer les points de \mathcal{P} dont les coordonnées sont des entiers naturels.

S'ENTRAÎNER À LA LOGIQUE → p. 290

144 Quantificateurs universel, existentiel

Pour chacune des affirmations ci-dessous, dire si elle est vraie ou fausse. Justifier

a) a et b désignent deux nombres entiers relatifs premiers entre eux.

Il existe un couple $(u; v)$ de nombres entiers relatifs tels que $au + bv = 2$.

b) Pour tout entier naturel n, les nombres $2n^2 + 4n + 1$ et $n + 2$ sont premiers entre eux.

c) a et b désignent deux nombres entiers relatifs non nuls. S'il existe un couple $(u; v)$ de nombres entiers relatifs tels que $au + bv = d$, alors $\text{PGCD}(a; b) = d$.

d) Pour tout entier naturel n non nul, la fraction $\frac{n^2 + 2n}{n^2 + 1}$ est irréductible.

145 Vrai ou faux

x est un nombre entier relatif tel que :

$$x \equiv 2 [3] \text{ et } x \equiv 2 [6].$$

Pour chaque proposition, dire si elle est vraie ou fausse. Justifier.

a) $x \equiv 2 [18]$

b) Il existe $(u; v) \in \mathbb{Z}^2$ tel que $xu + 3v = 1$.

146 Déterminer une condition nécessaire et suffisante

Raisonner Calculer

n est un nombre entier naturel non nul.

1. Justifier que si n est un carré parfait alors \sqrt{n} appartient à \mathbb{Q} .

2. On suppose que \sqrt{n} appartient à \mathbb{Q} , c'est-à-dire qu'il existe deux entiers naturels non nuls p et q premiers entre eux tels que $\sqrt{n} = \frac{p}{q}$.

a) Justifier que $nq^2 = p^2$.

b) En déduire que q divise p , puis que $n = p^2$.

3. Donner une condition nécessaire et suffisante pour que \sqrt{n} appartienne à \mathbb{Q} .

4. a) Énoncer la contraposée de cette condition nécessaire et suffisante.

b) Montrer que $\sqrt{2}$ est irrationnel.

147 Étudier un PGCD

Raisonner Calculer

a et b désignent deux nombres entiers naturels non nuls premiers entre eux.

a) Démontrer que $a+b$ et b sont premiers entre eux, puis qu'il en est de même de $a+b$ et a .

b) Que peut-on alors en déduire pour $a+b$ et ab ?

c) Développer $(a+b)^2 - 3ab$.

d) On pose $d = \text{PGCD}(a^2 - ab + b^2; a+b)$.

Démontrer que d divise $3ab$.

e) En déduire que $d = 1$ ou $d = 3$.

148 Démontrer le théorème de Lucas

Raisonner Calculer

La suite de Fibonacci est la suite définie par $F_0 = 1$, $F_1 = 1$ et pour tout entier naturel n , $F_{n+2} = F_{n+1} + F_n$.

On admet que pour tout entier naturel $m \geq 1$ et tout entier naturel $n \geq 0$:

$$F_{n+m} = F_m F_{n+1} + F_{m-1} F_n \text{ et } \text{PGCD}(F_n; F_{n+1}) = 1.$$

a) d désigne un nombre entier naturel non nul.

Montrer que d divise F_n et F_m équivaut à d divise F_n et F_{n+m} .

b) Montrer que pour tout entier naturel non nul k , d divise F_n et F_m équivaut à d divise F_n et F_{n+km} .

c) On suppose que $m > n > 0$.

Montrer que si r est le reste de la division euclidienne de m par n , alors :

$$\text{PGCD}(F_m; F_n) = \text{PGCD}(F_r; F_n).$$

d) En utilisant l'algorithme d'Euclide, démontrer le théorème de Lucas :

$$\text{PGCD}(F_m; F_n) = F_{\text{PGCD}(m; n)}.$$

149 Résoudre un système de congruences

Raisonner Calculer

n désigne un nombre entier relatif.

On considère le système (**S**) suivant :

$$\begin{cases} n \equiv 1 [7] \\ n \equiv 5 [11] \end{cases}.$$

1. Vérifier que 71 est une solution de (**S**).

2. On suppose que n est un entier relatif solution de (**S**).

a) Démontrer qu'il existe des entiers relatifs u et v tels que :

$$\begin{cases} n = 1 + 7u \\ 7u - 11v = 4 \end{cases}.$$

b) Résoudre dans \mathbb{Z}^2 l'équation $7u - 11v = 4$.

c) En déduire que $n \equiv 71 [77]$.

3. Démontrer que pour tout entier relatif,

$$n \equiv 71 [77]$$

équivaut à :

$$\begin{cases} n \equiv 1 [7] \\ n \equiv 5 [11] \end{cases}.$$

150 Prendre des initiatives

Raisonner Calculer

On définit la suite (u_n) sur \mathbb{N} par :

$$u_n = 1 + 6^{(2^n)}.$$

a) Vérifier que pour tous entiers naturels n et $k \geq 1$,

$$u_{n+k} - 1 = (u_n - 1)^{(2^k)}.$$

b) En déduire que pour tous entiers naturels n et $k \geq 1$,

$$u_{n+k} - 2 \text{ est divisible par } u_n.$$

c) Démontrer que deux termes distincts de la suite (u_n) sont premiers entre eux.

151 Démontrer que des fractions sont irréductibles

Chercher Raisonner Calculer

On pose $u = 2 + \sqrt{3}$.

On se propose d'étudier u^n pour $n \in \mathbb{N}^*$.

a) Exprimer u^2 sous la forme $a + b\sqrt{3}$ où a et b sont des nombres entiers naturels non nuls.

b) Démontrer par récurrence que pour tout entier naturel $n \geq 1$,

$$u^n = a_n + b_n \sqrt{3}$$

où a_n et b_n sont des nombres entiers naturels non nuls.

c) Exprimer a_{n+1} et b_{n+1} en fonction de a_n et b_n .

d) (α_n) est la suite définie sur \mathbb{N}^* par :

$$\alpha_n = a_n b_{n+1} - a_{n+1} b_n.$$

Démontrer que la suite (α_n) est constante.

e) En déduire que pour tout entier naturel $n \geq 1$, les fractions $\frac{a_n}{b_n}$, $\frac{a_{n+1}}{a_n}$ et $\frac{b_{n+1}}{b_n}$ sont irréductibles.

152 Chercher des solutions d'une équation diophantienne

Raisonner **Calculer**

On considère l'équation diophantienne (E) :

$$2x^2 + 2y^2 = 5z^2$$

où x, y et z sont des nombres entiers relatifs.

- a) Vérifier que le triplet $(1; 3; 2)$ est solution de (E).
- b) Démontrer que, si $(x; y; z)$ est solution de (E), alors z est divisible par 2 et $x^2 + y^2$ est divisible par 10.
- c) On suppose que $y = 3$. Montrer que, si $(x; 3; z)$ est solution de (E), alors $x^2 \equiv 1 [10]$.
- d) Déterminer quatre triplets $(x; 3; z)$ distincts de $(1; 3; 2)$ solutions de (E).

153 Formaliser un problème



Chercher **Représenter** **Raisonner**

Rédiger les différentes étapes de la recherche, sans omettre les fausses pistes et les changements de méthode.

Problème

Un phare émet un signal jaune toutes les 15 secondes et un signal rouge toutes les 28 secondes. On aperçoit le signal jaune 2 secondes après minuit et le rouge 8 secondes après minuit.

À quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?

154 Solve diophantine equations



Raisonner **Calculer** **Communiquer**

For each of the following diophantine equations :

- decide whether or not the solution exists,
- if a solution exists, find the general solution,
- find the solution in which x takes the smallest possible positive integer value.

a) $15x + 28y = 5$ b) $18x + 27y = 7$ c) $12x + 2y = 8$

155 Étudier des ensembles de nombres complexes

Chercher **Raisonner**

m et n sont deux nombres entiers naturels non nuls.

On note \mathbb{U}_n l'ensemble des nombres complexes z tels que $z^n = 1$.

- a) Montrer que si m divise n , alors tout élément de \mathbb{U}_m est un élément de \mathbb{U}_n .
- b) On note $d = \text{PGCD}(m; n)$. Montrer que \mathbb{U}_d est exactement l'intersection de \mathbb{U}_m et \mathbb{U}_n .

156 Décoder un message par chiffrement affine

Raisonner **Calculer**

On numérote les 26 lettres de l'alphabet de 0 pour A à 25 pour Z. On choisit deux nombres entiers naturels a et b avec $a \neq 0$.

Le couple $(a; b)$ s'appelle la clé de chiffrement.

On dit qu'elle est satisfaisante lorsque deux lettres différentes sont codées par deux lettres différentes.

Pour coder la lettre numéro x , on calcule le reste y dans la division euclidienne de $ax + b$ par 26.

Puis y est remplacé par la lettre correspondante.

- 1. Max choisit pour clé de chiffrement $(2; 8)$.

a) Vérifier que la lettre O est codée K.

b) La clé est-elle satisfaisante ?

2. a) Montrer que, si a et 26 sont premiers entre eux, alors la clé $(a; b)$ est satisfaisante.

b) Montrer que si la clé $(a; b)$ est satisfaisante avec a et 26 premiers entre eux, alors il existe un entier relatif u tel que $au \equiv 1 [26]$.

c) Déterminer alors une fonction de décodage.

d) Décoder le mot HDEPU obtenu avec la clé $(3; 4)$.

157 Imaginer une stratégie

Chercher **Raisonner**

Un soir dans une auberge s'arrêtent plusieurs diligences. Des hommes et des femmes, moins nombreuses, s'attablent.



Chaque homme doit payer 19 sous et chaque femme 13 sous. À la fin du repas, l'aubergiste a récolté exactement 1 000 sous.

Retrouver combien d'hommes et de femmes ont mangé à l'auberge ce jour-là.

158 Compter des solutions



Chercher **Raisonner**

m est un nombre entier naturel non nul.

On note (\mathbf{E}_m) l'équation :

$$11x + 13y = m$$

où x et y sont des nombres entiers naturels.

- a) On suppose $m < 143$.

Démontrer que l'équation (\mathbf{E}_m) a au plus une solution.

- b) On suppose $m \geq 143$.

Démontrer que l'équation (\mathbf{E}_m) a au moins une solution.

• 159 Le chiffrement de Vigenère

Voici un procédé pour coder le message « CECI EST MON PREMIER ESSAI ».

- À chaque lettre de l'alphabet français, on fait correspondre son rang x compris entre 0 et 25 (A : 0; B : 1; ...; Z : 25).
 - On regroupe les lettres du texte par blocs de longueur 5 sauf peut-être le dernier bloc. On obtient « CECIE STMON PREMI ERESS AI ».
 - On choisit une clé constituée de cinq nombres de 0 à 25.
Par exemple la clé (12; 0; 19; 7; 18) qui correspond au mot MATHS.
 - Pour chaque lettre d'un bloc, on calcule le reste y de la division euclidienne par 26 de $x + z$ (où x est le code de la lettre et z le nombre de la clé de même position que la lettre).

Exemple

La 1^{re} lettre C est associée à 2 ; le 1^{er} nombre de la clé est 12. Ainsi $y \equiv 2 + 12 [26]$, soit $y = 14$ et C est codée par O.

- a) Vérifier que le bloc CECIE est codé O EVPW.

b) Voici une fonction **Vigenere** écrite en langage Python qui permet de coder un message avec la clé précédente.

Saisir et appliquer cette fonction à la suite du message.

Par exemple, dans la console, **Vigenere("CECIE")** donne '**O EVPW**'.

c) Modifier le programme pour décoder le mot NRTCG.

```
1 def Vigenere(message):
2     mc=[]
3     cle=[12,0,19,7,18]
4     i=0
5     for lettre in message:
6         n=ord(lettre)-65
7         nc=(n+cle[i])%26
8         lc=chr(nc+65)
9         i=(i+1)%5
10        mc.append(lc)
11    mc="".join(mc)
12    return(mc)
```

• 160 Le chiffrement de Hill

Voici un procédé pour coder un mot de deux lettres.

- À chaque lettre de l'alphabet français, on fait correspondre son rang x compris entre 0 et 25 (A:0;B:1;...;Z:25).

On obtient ainsi un couple $(x_1; x_2)$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

- $(x_1; x_2)$ est alors transformé en $(y_1; y_2)$ tel que $(S_1) \begin{cases} y_1 \equiv 11x_1 + 3x_2 [26] \\ y_2 \equiv 7x_1 + 4x_2 [26] \end{cases}$ avec $0 \leq y_1 \leq 25$ et $0 \leq y_2 \leq 25$.
 - $(y_1; y_2)$ est enfin transformé en un mot de deux lettres en utilisant la correspondance précédente.

Exemple $\underbrace{\text{TE}}_{\text{mot en clair}} \rightarrow (19; 4) \rightarrow (13; 19) \rightarrow \underbrace{\text{NT}}_{\text{mot codé}}$

- ## 1. Coder le mot ST.

2. On veut maintenant déterminer la procédure de décodage.

- a)** Montrer qu'un couple $(x_1; x_2)$ qui vérifie le système (S_1) vérifie le système (S_2) $\begin{cases} 23x_1 \equiv 4y_1 + 23y_2 [26] \\ 23x_2 \equiv 19y_1 + 11y_2 [26] \end{cases}$

b) Déterminer l'inverse de 23 modulo 26.

c) Montrer qu'un couple $(x_1; x_2)$ qui vérifie le système (S_2) vérifie le système (S_3) $\begin{cases} x_1 \equiv 16y_1 + y_2 [26] \\ x_2 \equiv 11y_1 + 5y_2 [26] \end{cases}$

d) Montrer, réciproquement, qu'un couple $(x_1; x_2)$ qui vérifie le système (S_3) vérifie le système (S_1) .

e) Décoder le mot YJ.

161 Une équation de Pell-Fermat

On considère l'équation (E) : $x^2 - 3y^2 = 1$ où les inconnues x et y sont des nombres entiers naturels non nuls.

1. On suppose dans cette question qu'il existe un couple $(a; b)$ solution de (E).

a) Justifier que $a > b$.

b) Montrer que a et b sont premiers entre eux.

c) Démontrer que a est inversible modulo 3, puis que $a \equiv 1 [3]$ ou $a \equiv 2 [3]$.

2. Donner le couple $(a_1; b_1)$ solution de (E) tel que b_1 soit le plus petit possible.

3. a) Démontrer par récurrence, que pour entier naturel $n \geq 1$, il existe un couple $(a_n; b_n)$ d'entiers naturels non nuls premiers entre eux tel que $(2 + \sqrt{3})^n = a_n + b_n\sqrt{3}$ et $(a_n; b_n)$ solution de (E).

b) En déduire que (E) admet une infinité de couples solutions.

4. a) Pour tout entier naturel $n \geq 1$ donner les expressions de a_{n+1} et b_{n+1} en fonction de a_n et b_n .

b) Compléter le programme ci-contre, écrit en langage Python, permettant d'obtenir n couples solutions de l'équation (E) à partir du couple $(a_1; b_1)$.

c) Saisir et tester le programme avec $n = 10$.

```

1 def CPell(n):
2     a=2
3     b=1
4     for k in range(1,n+1):
5         u=a
6         a= ...
7         b= ...
8         print("(",a,",",b,")")
9     return

```

162 Le lemme chinois

m et n sont deux nombres entiers naturels premiers entre eux avec $m \geq 2$ et $n \geq 2$.

a et b sont deux nombres entiers relatifs et on considère le système :

$$(S) \begin{cases} x \equiv a [m] \\ x \equiv b [n] \end{cases} \text{ où } x \text{ désigne un nombre entier relatif.}$$

1. a) Justifier qu'il existe des entiers relatifs u et v tels que $mu + nv = 1$.

b) Vérifier que $x_0 = anv + bmu$ est une solution particulière du système (S).

c) Démontrer que tout entier $x = x_0 + kmn$ avec $k \in \mathbb{Z}$ est solution du système (S).

2. a) Justifier que (S) est équivalent au système $\begin{cases} x \equiv x_0 [m] \\ x \equiv x_0 [n] \end{cases}$.

b) Donner alors l'ensemble des solutions du système (S).

3. Application

Voici un problème trouvé dans un livre du mathématicien chinois Sun Zi entre les 3^e et 5^e siècles :

« Combien l'armée de Han Xing compte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et rangés par 7 colonnes, il reste deux soldats ? ».

On note n le nombre de soldats de l'armée.

a) Justifier que n est solution du système (S) $\begin{cases} x \equiv 2 [3] \\ x \equiv 3 [5] \end{cases}$ où $x \in \mathbb{Z}$.

b) Résoudre le système $\begin{cases} x \equiv 2 [3] \\ x \equiv 3 [5] \end{cases}$

c) Démontrer que x est solution du système (S) si, et seulement si, $x \equiv 23 [105]$.

d) Le nombre n de soldats est compris entre 7 000 et 7 100. Déterminer la valeur de n .

163 Le critère d'Eisenstein

1. x désigne un nombre réel. On considère l'équation :

$$-x^3 + 3x^2 - 3x + 2 = 0.$$

a) Montrer que, si m est un nombre entier relatif solution de l'équation, alors m divise 2.

b) L'équation admet-elle une solution entière ?

2. x désigne un nombre réel. On considère l'équation (E) :

$$ax^3 + bx^2 + cx + d = 0$$

où a, b, c et d sont des nombres entiers relatifs avec $a \neq 0$.

On suppose que (E) admet une solution rationnelle non nulle, c'est-à-dire de la forme $\frac{p}{q}$ avec $p \in \mathbb{Z}^*$, $q \in \mathbb{N}^*$ et $\text{PGCD}(p; q) = 1$.

Démontrer que p divise d et q divise a .

Ce résultat est appelé le **critère d'Eisenstein**.

3. a) Justifier que l'équation suivante admet trois solutions réelles :

$$15x^3 - 43x^2 - 7x + 3 = 0.$$

b) Déterminer ces trois solutions en utilisant le critère d'Eisenstein.

164 Les triplets pythagoriciens

On appelle triplet pythagoricien tout triplet $(a; b; c)$ d'entiers naturels non nuls vérifiant la relation de Pythagore $a^2 + b^2 = c^2$.

1. a) Donner un exemple $(a_0; b_0; c_0)$ de triplet pythagoricien.

b) Justifier que tout triplet $(ka_0; kb_0; kc_0)$ avec $k \in \mathbb{N}^*$ est également un triplet pythagoricien.

2. $(a; b; c)$ est un triplet pythagoricien. Montrer que pour tout diviseur d (avec $d > 0$) commun à a, b et c , le triplet $\left(\frac{a}{d}; \frac{b}{d}; \frac{c}{d}\right)$ est aussi un triplet pythagoricien.

Dans la suite, on suppose que $(a; b; c)$ est un triplet pythagoricien dont les termes ont pour seul diviseur positif commun 1.

3. a) Montrer que a, b, c sont deux à deux premiers entre eux.

b) Montrer que a et b ne peuvent pas être de même parité.

On suppose dans la suite a impair et b pair

c) Démontrer que c est impair.

d) Justifier que $c + a$ et $c - a$ sont des nombres pairs.

4. a) Démontrer que :

$$\left(\frac{b}{2}\right)^2 = \left(\frac{c-a}{2}\right)\left(\frac{c+a}{2}\right).$$

b) On admet qu'il existe deux entiers naturels u, v avec $v > u > 0$ tels que :

$$c - a = 2u^2 \text{ et } c + a = 2v^2.$$

Exprimer a, b, c en fonction de u et v .

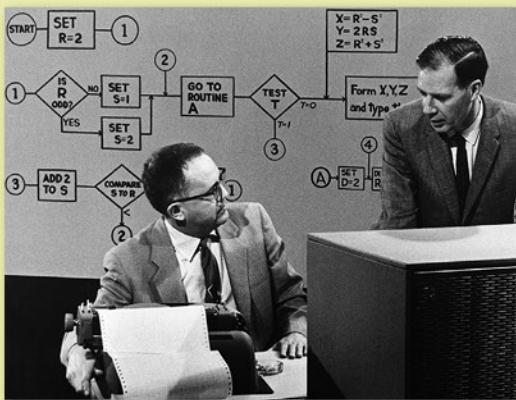
5. Réciproquement, on suppose que u et v sont deux entiers naturels tels que $v > u > 0$.

On pose $a = v^2 - u^2$, $b = 2uv$ et $c = u^2 + v^2$.

Démontrer que $(a; b; c)$ est un triplet pythagoricien.

165 Exemple de code correcteur**MATHS
& INFORMATIQUE**

Au milieu des années 1940, Richard Hamming travaille sur un modèle de calculateur à carte perforée peu fiable.



Durant la semaine, les ingénieurs peuvent corriger les erreurs, mais en fin de semaine, les machines s'arrêtent sur des bugs. C'est alors que Richard Hamming (1915-1998) met au point le premier code correcteur vraiment efficace.

À cette période Claude Shannon formalise la théorie de l'information comme une branche des mathématiques. Hamming développe, lui, la théorie des codes.

L'une des méthodes de fabrication d'un code correcteur porte son nom.

On considère les nombres de 10 chiffres $\underline{a_1 a_2 \dots a_{10}}$ où les a_i peuvent prendre les valeurs 0, 1, ..., 9.

On rajoute une clé constituée de deux chiffres a_{11} et a_{12} où a_{11} et a_{12} peuvent prendre les valeurs 0, 1, ..., 9 et aussi la valeur X représentant le nombre 10.

Le calcul de la clé se fait ainsi :

(1) a_{11} est le reste de la division euclidienne par 11 de $a_1 + a_2 + \dots + a_{10}$.

(2) a_{12} est le reste de la division euclidienne par 11 de $1a_1 + 2a_2 + \dots + 10a_{10}$.

1. Calculer la clé pour le numéro 0491413940.

2. On part d'un numéro muni de sa clé $\underline{a_1 a_2 \dots a_{12}}$.

On se propose de démontrer que, si en communiquant ce numéro on fait une erreur sur un seul des chiffres on peut détecter et corriger l'erreur.

a) Démontrer que si l'erreur est commise sur un a_i avec $1 \leq i \leq 10$, alors aucune des relations (1) et (2) n'est vérifiée.

b) Démontrer que si l'erreur est commise sur a_{11} , alors (1) n'est pas vérifiée mais (2) l'est.

c) Démontrer que si l'erreur est commise sur a_{12} , alors (1) est vérifiée mais (2) ne l'est pas.

d) 049132900000 est incorrect.

Réparer l'erreur commise.

166 Équation diophantienne de degré 2

On considère l'équation (E) : $x^2 + xy + y^2 = z^2$ d'inconnue un triplet (x, y, z) de nombres entiers naturels.

1. Vérifier que l'équation (E) est équivalente à l'équation (F) : $3xy = (x - y + z)(y - x + z)$.

Dans la suite, $(x ; y)$ est un couple solution de (E) avec $xy \neq 0$, x et y premiers entre eux.

2. On fait l'hypothèse que 3 divise $x - y + z$ et $y - x + z$.

a) Montrer alors que 3 divise x ou 3 divise y .

b) En déduire que 3 divise x et y .

c) Conclure que si 3 divise l'un des facteurs $x - y + z$ ou $y - x + z$, alors il ne divise pas l'autre.

Dans la suite, on suppose que 3 divise $x - y + z$.

3. Justifier que les entiers $x - y + z$ et $y - x + z$ sont positifs.

4. On note $(p ; q)$ le couple d'entiers naturels premiers entre eux vérifiant l'égalité :

$$\frac{p}{q} = \frac{x - y + z}{3y}.$$

a) Vérifier que $(3p + 2q)py = (2p + q)qx$.

b) Montrer qu'il existe un entier naturel n vérifiant :

$$(3p + 2q)p = nx, (2p + q)q = ny$$

$$\text{et } nz = (3m + 1)ny - nx = 3p^2 + 3pq + q^2.$$

c) Justifier que q n'est pas un multiple de 3.

d) En remarquant que :

$$n = \text{PGCD}((3p + 2q)p ; (2p + q)q),$$

démontrer que $n = 1$.

5. En déduire les solutions de (E).

**167 Payer en euros**

a et b désignent deux nombres entiers naturels premiers entre eux. On dispose d'un nombre non limité de pièces de a euros et d'un nombre non limité de pièces de b euros.

Quelle est la plus grande somme que l'on ne peut pas payer avec ces pièces ?