Exercices calculs et automatismes

29 PGCD

Déterminer de tête et à l'aide des règles de divisibilité :

a) PGCD(12 , 42) **b)** PGCD(45 , 105)
c) PGCD(92 , 69) **d)** PGCD(72 , 108)

30 Résoudre un problème

1. Sur un vélodrome, deux cyclistes partent en même temps d'un point M et roulent à vitesse constante. Le coureur A boucle le tour en 35 secondes et le coureur B en 42 secondes.
Au bout de combien de secondes le coureur A aura-t-il un tour d'avance sur le coureur B ?

a 7 b 175
c 210 d 420

2. On veut découper un rectangle de 24 cm sur 40 cm en carrés sans perte. Quel peut être le côté du carré ?

a 6 cm b 8 cm
c 10 cm d 120 cm

31 Propriétés du PGCD

Sachant que PGCD(426 , 144) = 6, déterminer de tête :

a) PGCD(852 , 288) **b)** PGCD(142 , 48)
c) PGCD(426 , 6) **d)** PGCD(– 144 , 426)

32 Algorithme d'Euclide

Méthode Comment faire pour déterminer les PGCD suivants en utilisant l'algorithme d'Euclide ?

a) PGCD(78 , 108) **b)** PGCD(202 , 138)

33 Quotients et algorithme d'Euclide

L'affirmation suivante est-elle vraie ou fausse ? Justifier.	V	F
Les quotients successifs (comprenant la dernière division de reste nul) de l'algorithme d'Euclide appliqué aux entiers 644 et 345 sont : 1, 1, 5, 2.	☐	☐

34 Nombres premiers entre eux (1)

Les affirmations suivantes sont-elles vraies ou fausses ? Justifier.	V	F
a) PGCD (144, 840) = 12.	☐	☐
b) 441 et 277 sont premiers entre eux.	☐	☐

35 Nombre premiers entre eux (2)

1. Méthode Comment faire pour montrer que, pour tout entier n non nul, les entiers $4n + 1$ et n sont premiers entre eux ?

2. En est-il de même avec $4n$ et $n + 1$?

36 Identité et théorème de Bézout

Les affirmations suivantes sont-elles vraies ou fausses ? Justifier.	V	F
a) Si a et b sont premiers entre eux, alors il existe un couple d'entiers relatifs $(u ; v)$ tel que : $au + bv = 2$.	☐	☐
b) S'il existe une combinaison linéaire de a et de b telle que $au + bv = 2$, alors PGCD $(a, b) = 2$.	☐	☐

37 Divisibilité

Choisir la(les) bonne(s) réponse(s).

Un entier est divisible par 6 et 35. Son plus grand diviseur est :

a 35 b 42
c 70 d 210

Un entier est divisible par 6 et 15. Son plus grand diviseur est :

a 30 b 45
c 60 d 90

38 Théorème de Gauss

En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs $(x ; y)$ qui vérifient les équations suivantes.

1. $5(x + 3) = 4y$ **2.** $41x + 9y = 0$

39 Équation à solution entière

1. Trouver un couple d'entier relatif $(x ; y)$ qui vérifie l'équation : $7x + 5y = 1$.

2. Méthode Comment à partir de ce couple solution en trouver un deuxième ?

40 Existence de solution

Les affirmations suivantes sont-elles vraies ou fausses ? Justifier.	V	F
a) L'équation : $37x + 25y = 1$ admet des solutions entières.	☐	☐
b) L'équation : $51x + 39y = 1$ n'admet pas de solution entière.	☐	☐
c) L'équation $51x + 39y = 2\,016$ n'admet pas de solution entière.	☐	☐

41 Théorèmes de Bézout et Gauss

Choisir la(les) bonnes réponse(s).

Soit a et b deux entiers naturels non nuls.

a Si a divise bc et si a ne divise pas b alors a divise c.
b Si b et c divise a alors bc divise a.
c Les nombres a et $2a + 1$ sont premiers entre eux.
d Les nombre $3b$ et $2b + 1$ sont premiers entre eux.

Exercices d'application

Utiliser le PGCD

Méthode 1 Méthode 2 p. 109

42 Déterminer les couples d'entiers naturels $(a\,;\,b)$ tels que :

$$\text{PGCD}(a\,,\,b) = 18 \text{ et } a + b = 360.$$

43 Trouver les entiers naturels a et b avec $a < b$ tels que :

$$ab = 7\,776 \text{ et } \text{PGCD}(a\,,\,b) = 18.$$

44 En un point donné du ciel, un astre A apparaît tous les 28 jours et un astre B tous les 77 jours. Sachant que les deux astres sont déjà apparu simultanément en ce point, avec quelle périodicité les verra-t-on dans cette configuration ?

45 Une boîte parallélépipédique rectangle de dimensions intérieures 31,2 cm, 13 cm et 7,8 cm est entièrement remplie par des cubes à jouer dont l'arête est un nombre entier de millimètres.
Quel est le nombre minimal de cubes que peut contenir cette boîte ?

46 Algo

a et b sont deux entiers naturels non nuls tels que $a > b$.

1. Démontrer que $\text{PGCD}(a\,,\,b) = \text{PGCD}(a - b\,,\,b)$.

2. Calculer les PGCD des entiers suivants par cette méthode, répétée autant de fois que nécessaire.

a) 308 et 165 **b)** 735 et 210

3. Compléter cette fonction en **Python** permettant de déterminer $\text{PGCD}(a\,,\,b)$ par cette méthode, les nombres a et b n'étant pas ordonnés.

```
def pgcd(a,b):
while ...:
...
...
...
return ...
```

47 Soit n un naturel non nul.
On pose $a = 5n + 1$ et $b = 2n - 1$.
On note $D = \text{PGCD}(a\,,\,b)$.

1. Démontrer que les valeurs possibles de D sont 1 ou 7.

2. Déterminer les entiers n tels que :

$$a \equiv 0\ (7) \text{ et } b \equiv 0\ (7).$$

3. En déduire, suivant les valeurs de n, la valeur de D.

48 Soit n un naturel non nul.
On pose : $a = 3n + 1$ et $b = 5n - 1$.

1. Montrer que $\text{PGCD}(a\,,\,b)$ est un diviseur de 8.

2. Pour quelles valeurs de n, $\text{PGCD}(a\,,\,b) = 8$?

Appliquer l'algorithme d'Euclide

Méthode 3 p. 111

49 Utiliser l'algorithme d'Euclide pour trouver :
a) PGCD(4 935 , 517)
b) PGCD(2 012 , 7 545)
c) PGCD(18 480 , 8 745)

50 Les entiers suivants sont-ils premiers entre eux ?
a) 4 847 et 5 633
b) 5 617 et 813

51 Soit a et b deux entiers naturels non nuls tels que :

$$\text{PGCD}\,(a\,,\,b) = 7.$$

La dernière division de reste nul étant écrite, les quotients successifs de l'algorithme d'Euclide sont : 3 ; 1 ; 1 ; 3.
Quelles sont les valeurs de a et b ?

52 Soit a et b deux entiers naturels non nuls tels que :

$$\text{PGCD}\,(a\,,\,b) = 15.$$

La dernière division de reste nul étant écrite, les quotients successifs de l'algorithme d'Euclide sont : 2 ; 4 ; 1 ; 3 ; 2.
Quelles sont les valeurs de a et b ?

53 Si on divise 4 294 et 3 521 par un même entier positif, on obtient respectivement comme reste 10 et 11.
Quel est ce diviseur ?

Déterminer un couple d'entiers de Bézout

Méthode 4 p. 113

54 Montrer que 17 et 40 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x\,;\,y)$ tel que :

$$17x - 40y = 1.$$

55 Montrer que 23 et 26 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x\,;\,y)$ tel que :

$$23x - 26y = 1.$$

56 Montrer que 221 et 331 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x\,;\,y)$ tel que :

$$221x - 331y = 1.$$

57 **1.** Déterminer PGCD(58, 24) à l'aide de l'algorithme d'Euclide.

2. En déduire un couple d'entiers relatifs $(x\,;\,y)$ tel que :

$$58x - 24y = 2.$$

58 La proposition suivante est-elle vraie ou fausse ? Justifier.
« S'il existe deux entiers relatifs u et v tels que $au + bv = 5$ alors $\text{PGCD}(a\,,\,b) = 5$. »

59 Démontrer que, pour tout relatif k, $(7k + 3)$ et $(2k + 1)$ sont premiers entre eux.

60 Démontrer que, pour tout entier naturel n, $(7n + 4)$ et $(5n + 3)$ sont premiers entre eux.

61 Démontrer que pour tout entier relatif n, les entiers $(14n + 3)$ et $(5n + 1)$ sont premiers entre eux. En déduire : PGCD(87 ; 31).

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

63 Prouver que la fraction $\frac{2n+1}{n(n+1)}$ est irréductible pour tout entier naturel n.

64 Déterminer a et b tels que :
$$n^2 - 3 + (an + b)(n - 2) = 1.$$
Que peut-on déduire pour la fraction $\frac{n^2-3}{n-2}$?

65 Prouver que la fraction $\frac{n^3+n}{2n+1}$ est irréductible pour tout entier naturel n.

Démo

66 Démontrer le corollaire du théorème de Bézout : « l'équation $ax + by = c$ admet des solutions entières si, et seulement si, c est un multiple PGCD(a , b) ».
On raisonnera par double implication.

67 L'équation $6x + 3y = 1$ admet-elle des solutions ? Et l'équation $7x + 5y = 1$?

Appliquer le théorème de Gauss

Méthode 5 Méthode 6 p. 115

68 **1.** Déterminer les couples d'entiers relatifs $(a ; b)$ tels que : $29a - 13b = 0$.
2. Vérifier que le couple (11 ; 24) est solution de l'équation (E) : $29x - 13y = 7$.
En déduire les couples $(x ; y)$ solutions de (E).

69 On considère dans un repère, les points A(7 ; 2) et B(–3 ; –4).
1. Montrer qu'un point M$(x ; y)$ appartient à la droite (AB) si $3(x - 7) = 5(y - 2)$.
2. En déduire l'ensemble des points à coordonnées entières appartenant à la droite (AB).

70 Un joueur a totalisé 200 points en lançant sur une cible 25 fléchettes.
La cible possède 3 zones qui rapportent respectivement 0 ; 5 et 12 points.
1. Montrer que le nombre de fléchettes qui ont atteint la zone à 12 points est divisible par 5.
2. En déduire la répartition des fléchettes dans les différentes zones.

Résoudre une équation diophantienne

Méthode 7 p. 116

71 Soit l'équation (E) : $3x - 4y = 6$.
1. Déterminer une solution particulière à (E).
2. Déterminer l'ensemble des solutions entières.

72 Soit l'équation (E) : $13x - 23y = 1$.
1. Déterminer une solution particulière à (E) en utilisant l'algorithme d'Euclide.
2. Déterminer l'ensemble des solutions entières.

73 **1.** Déterminer l'ensemble des couples d'entiers relatifs (x , y), solutions de l'équation (E) : $8x - 5y = 3$.
2. Soit m un nombre entier relatifs tel qu'il existe un couple $(p ; q)$ de nombres entiers vérifiant : $m = 8p + 1$ et $m = 5q + 4$.
Montrer que le couple $(p ; q)$ est solution de l'équation (E).
3. Déterminer le plus petit de ces nombres entiers m supérieurs à 2 000.

74 **1.** On considère l'équation (E) à résoudre dans $\mathbb{Z}^2$:
$$7x - 5y = 1.$$
a) Vérifier que (3 ; 4) est solution de (E).
b) Déterminer les couples solutions de (E).
2. Une boîte contient 25 jetons, des rouges, des verts et des blancs. Sur les 25 jetons il y a x jetons rouges et y jetons verts. Sachant que $7x - 5y = 1$, quels peuvent être les nombres de jetons rouges, verts et blancs ?

75 **1.** Lisa veut mesurer une durée de 2 minutes avec deux sabliers, l'un mesurant une durée de 11 minutes et l'autre une durée de 5 minutes.
Expliquer comment Lisa doit procéder.

2. Est-il possible pour Lisa de mesurer toute durée entière de d minutes avec ces deux sabliers ?

76 On veut résoudre le système suivant dans $\mathbb{Z}$.
$$(S) : \begin{cases} x \equiv 1\ (11) \\ x \equiv 3\ (4) \end{cases}$$
1. Montrer que résoudre ce système revient à résoudre l'équation
$$(E) : 11u - 4v = 2$$
où u et v sont des entiers relatifs.
2. Résoudre l'équation (E).
3. En déduire les solutions de (S).

Exercices d'entraînement

Systèmes : équation – PGCD

77 Trouver les entiers naturels a et b tels que :
$ab - b^2 = 2\,028$ et PGCD$(a\,;b) = 13$.

78 **1.** Déterminer l'ensemble des entiers naturels n tels que PGCD$(2n+3\,;n) = 3$.
2. En déduire l'ensemble des entiers naturels n tels que PGCD$(2n+3\,;n) = 1$.

79 Résoudre les systèmes suivants, $x, y \in \mathbb{N}$.

a) $\begin{cases} xy = 1512 \\ \text{PGCD}(x\,;y) = 6 \end{cases}$ **b)** $\begin{cases} xy = 300 \\ \text{PGCD}(x\,;y) = 5 \end{cases}$

On donnera la réponse sous forme de tableau.

Recherche de PGCD

80 Soit n un entier naturel.
On pose $a = 9n+4$ et $b = 2n+1$.
Montrer que a et b sont premiers entre eux.

81 Soit n un entier naturel.
On pose $a = n+4$ et $b = 3n+7$.
Déterminer PGCD$(a\,;b)$ suivant les valeurs de n.

82 Soit a et b deux entiers premiers entre eux. La fonction **bezout** programmée en **Python** permet de trouver les entiers u et v tels que :
$au + bv = 1$. Algo

```
1 def bezout(a,b):
2     r=0
3     u=0
4     while r!=1:
5           u=u+1
6           r=a*u%b
7     v=int((1-a*u)/b)
8     return u,v
```

PYTHON
Programme
lienmini.fr/maths-e04-06

1. a) Expliquer la condition de la ligne 4.
b) Pourquoi le calcul de la ligne 6 suppose que b soit positif ?
2. Que fait la fonction **int()** à la ligne 7 ?
3. Modifier cet algorithme pour qu'il puisse calculer les entiers u et v lorsque le signe de b est quelconque.
4. Faire fonctionner cet algorithme pour les couples $(a\,;b)$ suivants.
a) $(37\,;15)$ **b)** $(11\,;-24)$

83 Soit n un entier relatif.
$A = n-1$ et $B = n^2 - 3n + 6$.
1. Démontrer que le PGCD de A et de B est égal au PGCD de A et de 4.
2. Déterminer, selon les valeurs de l'entier n, le PGCD de A et de B.
3. Pour quelles valeurs de l'entier relatif n, $n \neq 1$ a-t-on :
$$\frac{n^2 - 3n + 6}{n-1} \in \mathbb{Z} \text{ ?}$$

Théorème de Gauss

84 Soit a et b deux rationnels non nuls tels que $a+b$ et ab sont des entiers.
On pose alors $a = \frac{p_1}{q_1}$ et $b = \frac{p_2}{q_2}$ fractions irréductibles avec $q_1 > 0$ et $q_2 > 0$.
1. Montrer que q_1 divise q_2.
2. En déduire que $q_1 = q_2$.
3. Prouver alors que a et b sont des entiers.

85 Cinq entiers naturels a, b, c, d, e sont cinq termes consécutifs non nuls d'une suite géométrique de raison $q > 1$ et telle que q est premier avec a. On sait de plus que $6a^2 = e - b$.
1. Montrer que : $6a = q(q^3 - 1)$.
2. Montrer que q divise 6 puis déterminer les valeurs possibles pour q.
3. En déduire les valeurs de a, b, c, d et e.

Montrer la rationalité d'un nombre

Méthode 8 p. 117

86 Soit $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux.
Soit f le polynôme : $f(x) = 2x^3 + 5x^2 + 5x + 3$.
1. Montrer que si $\frac{p}{q}$ est une racine de f alors p divise 3 et q divise 2.
2. Déduire que f admet deux solutions rationnelles.

87 Soit f le polynôme :
$f(x) = x^4 - 4x^3 - 8x^2 + 13x + 10$.
1. Montrer que si $f(x) = 0$ admet une solution rationnelle α alors α est un entier.
2. Montrer que si α est une solution entière de $f(x) = 0$ alors α divise 10.
3. Trouver les racines entières éventuelle de $f(x) = 10$.

Travailler l'oral

88 En montagne, un randonneur a effectué des réservation dans deux types d'hébergement :
l'hébergement A et l'hébergement B.
Une nuit en hébergement A coûte 24 € et une nuit en hébergement B coûte 45 €.
Il se rappelle que le coût total de sa réservation est de 438 €.
On souhaite retrouver les nombres x et y de nuitées passées respectivement en hébergement A et en hébergement B.
Proposer une solution algorithmique et une solution arithmétique.

89 Bézout et Gauss. Vrai ou faux ?

Pour chacune des trois propositions, indiquer si elle est vraie ou fausse et donner une démonstration de la réponse choisie.

a) Proposition 1 Pour tout $n \in \mathbb{N}^*$, $3n$ et $2n + 1$ sont premiers entre eux.

b) Soit S l'ensemble des couples $(x\,;\,y)$ d'entiers relatifs solutions de l'équation $3x - 5y = 2$.

Proposition 2 L'ensemble S est l'ensemble des couples $(5k - 1\,;\,3k - 1)$ où k est un entier relatif.

c) Soit a et b deux entiers naturels.

Proposition 3 S'il existe deux entiers relatifs u et v tels que $au + bv = 2$ alors le PGCD de a et b est égal à 2.

90 Comètes

A ▶ Ensemble S

On appelle S l'ensemble des entiers relatifs n vérifiant le système :

$$\begin{cases} n \equiv 13\ (19) \\ n \equiv 6\ (12) \end{cases}$$

1. Recherche d'un élément de S.

On désigne par $(u\,;\,v)$ un couple d'entiers relatifs tel que

$$19u + 12v = 1.$$

a) Justifier l'existence d'un tel couple $(u\,;\,v)$.

b) On pose $n_0 = 6 \times 19u + 13 \times 12v$.

Démontrer que n_0 appartient à S.

c) Donner un entier n_0 appartenant à S.

2. Caractérisation des éléments de S.

a) Soit n un entier relatif appartenant à S.

Démontrer que $n - n_0 \equiv 0\ (228)$.

b) En déduire qu'un entier relatif n appartient à S si et seulement si n peut s'écrire sous 1a forme $n = -6 + 228k$ où k est un entier relatif.

B ▶ Application

La comète A passe tous les 19 ans et apparaîtra la prochaine fois dans 13 ans.

La comète B passe tous les 12 ans et apparaîtra la prochaine fois dans 6 ans.

Dans combien d'années pourra-t-on observer les deux comètes la même année ?

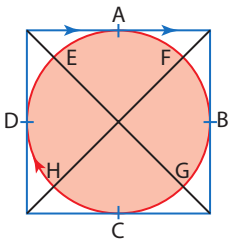
91 Pompon et manège

1. On considère l'équation (E) : $17x - 24y = 9$ où $(x\,,\,y)$ est un couple d'entiers relatifs.

a) Vérifier que le couple $(9\,;\,6)$ est solution de l'équation (E).

b) Résoudre l'équation (E).

2. Dans une fête foraine, Pablo s'installe dans un manège circulaire représenté par le schéma ci-dessous.



Il peut s'installer sur l'un des huit points indiqués sur le cercle. Le manège comporte un jeu qui consiste à attraper un pompon qui se déplace sur un câble formant un carré dans lequel est inscrit le cercle. Le manège tourne dans le sens des aiguilles d'une montre, à vitesse constante. Il fait un tour en 24 secondes. Le pompon se déplace dans le même sens à vitesse constante. Il fait un tour en 17 secondes. Pour gagner, Pablo doit attraper le pompon, et il ne peut le faire qu'aux points de contact qui sont notés A, B, C et D sur le dessin. À l'instant $t = 0$, Pablo part du point H en même temps que le pompon part du point A.

a) On suppose qu'à un certain instant t Pablo attrape le pompon en A. Il a déjà pu passer un certain nombre de fois en A sans y trouver le pompon. À l'instant t, on note y le nombre de tours effectués depuis son premier passage en A et x le nombre de tours effectués par le pompon. Montrer que $(x\,;\,y)$ est solution de l'équation (E) de la question **1.**

b) Pablo a payé pour 2 minutes ; aura-t-il le temps d'attraper le pompon ?

c) Montrer qu'en fait il n'est possible d'attraper le pompon qu'au point A.

Coup de pouce On pourra montrer que si l'on attrape le pompon respectivement au point B, C et D, le couple $(x\,;\,y)$ doit vérifier respectivement les équations : $68x - 96y = 43$, $34x - 48y = 25$, $68x - 96y = -39$.

d) Pablo part maintenant du point E. Aura-t-il le temps d'attraper le pompon en A avant les deux minutes ?

Exercices bilan

92 Suite

Soit (u_n) la suite définie pour $n \in \mathbb{N}$ par :

$$u_0 = 0 \text{ et } u_{n+1} = 4u_n + 1.$$

1. a) Calculer u_1, u_2 et u_3.
b) Montrer que pour $n \in \mathbb{N}$, u_{n+1} et u_n sont premiers entre eux.
2. On pose pour $n \in \mathbb{N}$:

$$v_n = u_n + \frac{1}{3}.$$

a) Montrer que (v_n) est une suite géométrique.
b) En déduire l'expression de v_n puis celle de u_n en fonction de n.
3. Calculer PGCD$(4^{n+1} - 1 , 4^n - 1)$.

93 Codage

À chaque lettre de l'alphabet on associe, d'après le tableau suivant, un nombre entier compris entre 0 et 25.

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8
J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z	
18	19	20	21	22	23	24	25	

On définit un procédé de codage de la façon suivante.

Étape 1
On choisit deux entiers naturels p et q compris entre 0 et 25.

Étape 2
À la lettre que l'on veut coder, on associe l'entier x correspondant dans le tableau ci-dessus.

Étape 3
On calcule l'entier y défini par les relations :

$$y \equiv px + q0 \ (26) \text{ et } 0 \leqslant y \leqslant 25.$$

Étape 4
À l'entier y, on associe la lettre correspondante dans le tableau.

1. On choisit $p = 9$ et $q = 2$.
a) Démontrer que la lettre V est codée par la lettre J.
b) Citer le théorème qui permet d'affirmer l'existence de deux entiers relatifs u et v tels que : $9u + 26v = 1$.
Donner sans justifier un couple $(u ; v)$ qui convient.
c) Démontrer que :

$$y \equiv 9x + 2 \ (26) \Leftrightarrow x \equiv 3y + 20 \ (26).$$

d) Décoder la lettre R.
2. On choisit $q = 2$ et p est inconnu.
On sait que J est codé par D. Déterminer la valeur de p (on admettra que p est unique).
3. On choisit $p = 13$ et $q = 2$.
Coder les lettres B et D.
Que peut-on dire de ce codage ?

D'après Bac Antilles-Guyane 2015

94 Casser un code

À chaque lettre de l'alphabet, on associe un entier n comme à l'exercice précédent. On choisit 2 entiers a et b compris entre 0 et 25. Tout entier n compris entre 0 et 25 est codé par le reste de la division de $an + b$ par 26.
Le tableau suivant donne les fréquences f en pourcentage des lettres utilisées dans un texte écrit en français.

A	B	C	D	E	F	G	H	I
9,42	1,02	2,64	3,38	15,87	0,94	1,04	0,77	8,41
J	K	L	M	N	O	P	Q	R
0,89	0,00	5,33	3,23	7,14	5,13	2,86	1,06	6,46
S	T	U	V	W	X	Y	Z	
7,90	7,36	6,24	2,15	0,00	0,30	0,24	0,32	

A ▶ Un texte écrit en français et suffisamment long a été codé selon ce procédé. L'analyse fréquentielle du texte codé a montré qu'il contient 15,9 % de O et 9,4 % de E.
On souhaite déterminer les nombres a et b qui ont permis le codage.
1. Quelles lettres ont été codées par O et E ?
2. Montrer que les entiers a et b sont solutions du système

$$\begin{cases} 4a + b \equiv 13 \ (26) \\ b \equiv 4 \ (26) \end{cases}$$

3. Déterminer tous les couples d'entiers $(a ; b)$ ayant pu permettre le codage de ce texte.
B ▶ 1. On choisit $a = 22$ et $b = 4$.
Coder les lettres K et X. Ce codage est-il envisageable ?
2. On choisit $a = 9$ et $b = 4$.
a) Montrer que pour tous $n, m \in \mathbb{N}$, on a :

$$m \equiv 9n + 4 \ (26) \Leftrightarrow n \equiv 3m + 14 \ (26).$$

b) Décoder le mot NBELLA.

D'après Bac Polynésie 2017

95 Théorème des restes chinois

On se propose de déterminer l'ensemble S des entiers relatifs n vérifiant le 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 $(u ; v)$.
b) On pose $n_0 = 3 \times 17u + 9 \times 5v$.
Démontrer que n_0 appartient à S.
c) Donner un entier n_0 appartenant à S.
2. a) Soit n un entier relatif appartenant à S.
Démontrer que $n - n_0 \equiv 0 \ (85)$.
b) En déduire qu'un entier relatif n appartient à S si, et seulement si, n peut s'écrire sous la forme $n = 43 + 85k$ où k est un entier relatif.
3. Application : Assa 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 ?

PGCD

Soit $a, b \in \mathbb{Z}^*$.

L'ensemble des diviseurs communs à a et b admet un plus grand élément d, appelé **p**lus **g**rand **c**ommun **d**iviseur noté PGCD(a , b).

Propriétés

- PGCD(ka , kb) = kPGCD(a , b)
- Si b divise a alors PGCD(a , b) = $|b|$
- a et b sont **premiers entre eux** si, et seulement si, PGCD(a , b) = 1

Théorème de Bézout

- **Identité de Bézout**

Soit D = PGCD(a , b) alors il existe un couple d'entiers relatifs (u ; v) tel que : $\boldsymbol{au + bv = D}$.

- **Conséquence**

Tout diviseur commun à a et b divise D.

- **Théorème de Bézout**

a et b premiers entre eux si, et seulement si, il existe un couple d'entiers relatifs (u , v) tel que :

$$\boldsymbol{au + bv = 1}.$$

- **Corollaire de Bézout**

L'équation $ax + by = c$ admet des solutions entières si, et seulement si, c est un multiple de PGCD(a , b)

Algorithme d'Euclide

Soit $a, b \in \mathbb{N}$ et b ne divise pas a.

$a = bq + r$ alors PGCD(a , b) = PGCD(b , r)

Les divisions successives des diviseurs par le reste des divisions précédentes finissent par s'arrêter.

Le dernier reste non nul est alors PGCD(a , b).

C'est le principe de la **descente infinie** dans $\mathbb{N}$.

Théorème de Gauss

- **Théorème de Gauss**

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

- **Corollaire de Gauss**

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

Chiffrement affine

Soit une fonction de codage affine, par exemple : $f(x) = 11x + 8$.

- À une lettre du message, on associe un entier x entre 0 et 25 suivant l'ordre alphabétique.
- On calcule $f(x) = 11x + 8$ et l'on détermine le reste y de la division euclidienne de $f(x)$ par 26.
- On traduit y par une lettre suivant l'ordre alphabétique

Équation diophantienne du premier degré

Ce sont les équations de la forme : $ax + by = c$.

Cette équation admet des solutions si $c = k$ PGCD(a , b).

Pour résoudre cette équation :

- on divise l'équation par PGCD(a, b),
- on cherche une solution particulière,
- puis une solution générale en soustrayant termes à termes la solution particulière et la solution générale.

On applique le théorème de Gauss et on conclut sur l'ensemble des couples solutions.

Préparer le BAC — Je me teste

Je dois être capable de…		Parcours d'exercices
▶ Utiliser la définition et les propriétés du PGCD	Méthode 1, Méthode 2	1, 2, 3, 4, 42, 43
▶ Utiliser l'algorithme d'Euclide	Méthode 3	5, 6, 49, 50
▶ Déterminer un couple d'entiers de Bézout	Méthode 4	11, 12, 54, 67
▶ Appliquer le théorème de Gauss	Méthode 5, Méthode 6	17, 18, 19, 20, 68, 69
▶ Résoudre une équation diophantienne	Méthode 7	21, 22, 71, 72

EXOS
QCM interactifs
lienmini.fr/maths-e04-07

QCM

Pour les exercices suivants, choisir la (les) bonnes réponse(s).

	A	B	C	D
96 PGCD(2 517 , 4 272) =3. Dans l'algorithme d'Euclide, combien de divisions au minimum sont-elles nécessaires jusqu'à obtenir un reste nul ?	7	8	9	10
97 PGCD(a , b) = 7; $a \in \mathbb{N}$, $b \in \mathbb{N}$. Dans l'algorithme d'Euclide, les quotients successifs sont 3, 1, 1, 2 (comprenant la dernière division de reste nul). On a alors :	(a , b) = (35 , 63)	(a , b) = (35 , 126)	(a , b) = (25 , 126)	(a , b) = (14 , 35)
98 Combien de couples d'entiers naturels (a ; b) verifient PGCD(a , b) = 42 et $a + 2b = 336$?	5	3	2	1
99 Soit un entier relatif n. On pose : $a = 2n - 5$ et $b = 3n - 7$.	a et b sont premiers entre eux.	PGCD(a , b) = 11	Tout diviseur commun à a et b divise 11.	a et b ne sont pas premiers entre eux
100 Quelle fraction est irréductible pour tout $n \in \mathbb{N}^*$?	$\frac{3n}{2n+1}$	$\frac{n+8}{2n+5}$	$\frac{3n^2}{2n^2+n}$	$\frac{n}{(2n+1)(3n+1)}$
101 L'équation $5x - 8y = 1$ admet comme solution des couples d'entiers relatifs qui sont :	toujours premiers entre eux.	parfois premiers entre eux.	jamais premiers entre eux.	on ne peut répondre.
102 Un nombre est divisible par 15 et 24, alors ce nombre est divisible par :	360	120	90	72
103 Soit k un entier relatif. L'équation $5(x - 2) = 7k$ d'inconnue x a pour solution :	$x \equiv 2$ (5)	$x \equiv 5$ (7)	$x \equiv 2$ (7)	$x \equiv 0$ (7)
104 Soit l'équation (E) : $27x + 25y = 1$. Soit $(x_0 ; y_0)$ une solution de (E).	(−25 ; 27) est solution de (E)	x_0 et y_0 sont de parité différente	On peut avoir $x_0 + y_0 = 5$	(E) n'admet pas de solution.
105 Soit l'équation diophantienne (E) : $17x - 13y = 2$. Les solutions de (E) sont :	(E) n'admet pas de solution	$\begin{cases} x = -6 + 13k \\ y = -8 + 17k' \end{cases}$ $k \in \mathbb{Z}$	$\begin{cases} x = 7 + 26k \\ y = 9 + 34k' \end{cases}$ $k \in \mathbb{Z}$	$\begin{cases} x = 7 + 13k \\ y = 9 - 17k' \end{cases}$ $k \in \mathbb{Z}$

106 Des diviseurs

Si l'on divise 1 809 et 2 527 par un même entier b, les restes respectifs sont 9 et 7.
Quelles sont les valeurs possibles pour b ?

Méthode 1 p. 109

107 Un diviseur

Si l'on divise 1 545 et 3 375 par un même entier b, les restes respectifs sont 9 et 10.
Quel ce diviseur b ?

Méthode 2 p. 109

108 Algorithme d'Euclide

À l'aide de l'algorithme d'Euclide, déterminer :
a) PGCD(901 , 1 505)
b) PGCD(2 012 , 7 545)

Méthode 3 p. 111

109 Algorithme Algo

Soit l'algorithme ci-contre où A, B $\in \mathbb{N}$.
1. On rentre A = 12 et B = 14. Donner les valeurs successives que prennent A, B et D ainsi que la valeur affichée par l'algorithme
2. Que calcule cet algorithme ? Vérifier la validité mathématique de cet algorithme.

```
Lire A, B
D ← |B − A|
Tant que D ≠ 0
D ← A
A ← D
D ← |B − A|
Fin tant que
Afficher A
```

Méthode 4 p. 113

110 Théorème de Bézout (1)

Soit n un entier relatif.
1. On pose : $a = 7n + 3$ et $b = 2n + 1$.
Montrer que a et b sont premiers entre eux.
2. Même question avec :
$a = 4n + 5$ et $b = 7n + 9$.

Méthode 4 p. 113

111 Théorème de Bézout (2)

Pour chacune des propositions suivantes indiquer si elle est vraie ou fausse et justifier.
a) Soit. $a, b, u, v \in \mathbb{Z}$
Proposition 1
Si $au + bv = 3$ alors PGCD(a , b) = 3.
b) Proposition 2
L'équation $51x + 9y = 2$ admet des solutions entières.
c) Proposition 3
Soit $k \in \mathbb{Z}$, les nombres a et b tels que $a = 14n + 3$ et $b = 5n + 1$ sont premiers entre eux.

Méthode 3 p. 111

112 Nombres de Bézout

Soit l'équation (E) : $221x + 338y = 26$.
1. L'équation (E) admet-elle des solutions entières ?
2. Déterminer une solution particulière de l'équation (E).

Méthode 3 p. 111

113 Théorème de Gauss

1. Déterminer les couples d'entiers relatifs (a ; b) tels que :
$$21a - 5b = 0.$$
2. Soit n un entier relatif. Montrer que si 5 et 11 divise (n – 9) alors $n \equiv 9$ (55).

Méthode 5 p. 115

114 Système d'équations

Soit le système (S) : $\begin{cases} n \equiv 1\,(5) \\ n \equiv 3\,(4) \end{cases}$
1. Montrer que si n est solution de (S) alors (n – 11) est divisible par 4 et par 5.
2. En déduire l'ensemble des solutions n du système.

Méthode 2 p. 109

115 Égalité de deux PGCD Démo

Soit n un entier relatf.
1. On pose : $a = n - 2$ et $b = n^2 + n + 3$.
Montrer que PGCD(a , b) =PGCD(a , 9).
2. Déterminer les valeurs n pour lesquelles :
$$\frac{n^2 + n + 3}{n - 2} \in \mathbb{Z}.$$

↪ Apprendre à démontrer p. 118

116 Équation diophantienne (1)

Soit l'équation (E) : $25x + 7y = 1$.
1. Pourquoi l'équation (E) admet-elle des solutions entières ?
2. Déterminer une solution particulière de l'équation (E).
3. Déterminer toutes les solutions entières de l'équation (E).

Méthode 6 p. 115

117 Équation diophantienne (2)

Soit l'équation (E) : $2x - 3y = 5$.
a) Déterminer une solution particulière de l'équation (E).
b) En déduire toutes les solutions entières de l'équation (E).

Méthode 7 p. 116

118 Rationalité

Soit $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux.
Soit f le polynôme :
$$f(x) = 3x^3 + 4x^2 + 2x - 4.$$
1. Montrer que si $\frac{p}{q}$ est une racine de f alors p divise 4 et q divise 3.
2. Déduire que f n'admet qu'une seule solution rationnelle.

Méthode 8 p. 117

Exercices vers le supérieur

119 PPCM

Soit deux entiers relatifs a et b. On appelle PPCM(a , b) le plus petit multiple strictement positif de a et de b.

1. Calculer PPCM(18 , 12) et PPCM(24 , 40).

2. Calculer $\frac{7}{6}+\frac{11}{15}$. Que représente PPCM(6 , 15) ?

120 PGCD et PPCM

Démo

Soit D = PGCD(a , b) et M = PPCM(a , b).

1. Montrer que : $\begin{cases} a = Da' \\ b = Db' \end{cases} \Rightarrow M = Da'b'$ et PGCD(a ,b) = 1.

2. En déduire que : $DM = ab$.

121 Encore un PPCM

Soit a et b deux naturels tels que $a < b$.

Déterminer a et b tels que :

PGCD(a , b) = 6 et PPCM(a , b) = 102.

122 Vrai-Faux

Soit l'équation (E) : $x^2 - 52x + 480 = 0$, où x est un entier naturel. La phrase suivante est-elle vraie ou fausse ? Justifier.

« Il existe deux entiers naturels non nuls dont le PGCD et le PPCM sont solutions de l'équation (E). »

123 Propriété du PGCD

Soit un entier naturel n non nul.

On pose : $a = 5n^2 + 7$ et $b = n^2 + 2$

1. Montrer que PGCD(a , b) vaut 1 ou 3.

2. Déterminer les valeurs de n pour lequel PGCD(a , b) = 3.

124 Recherche du PGCD

Pour tout entier naturel n supérieur ou égal à 5, on considère les nombres : $a = n^3 - n^2 - 12n$ et $b = 2n^2 - 7n - 4$.

1. Démontrer, après factorisation, que a et b sont des entiers naturels divisible par $(n - 4)$.

2. On pose $\alpha = 2n + 1$ et $\beta = n + 3$. On note d le PGCD(α , β).

a) Trouver une relation entre α et β indépendante de n.

b) Démontrer que d est un diviseur de 5.

c) Démontrer que les nombres α et β sont multiples de 5 si, et seulement si, $(n - 2)$ est multiple de 5.

3. Démontrer que $(2n + 1)$ et n sont premiers entre eux.

4. a) Déterminer, suivant les valeurs de n et en fonction de n, le PGCD(a , b).

b) Vérifier les résultats obtenus dans les cas particuliers $n = 11$ et $n = 12$.

125 Algorithme d'Euclide

À l'aide de l'algorithme d'Euclide, déterminer :

a) PGCD(99 099 , 43 928)

b) PGCD(153 527 , 245 479)

126 Calcul de PGCD

Soit $n \in \mathbb{Z}$. On pose $a = n^3 + 3n^2 - 5$ et $b = n + 2$.

Calculer PGCD(a , b).

127 Suite et PGCD

Soit la suite (u_n) définie sur $\mathbb{N}$ par :

$u_0 = 0$, $u_1 = 1$ et $u_{n+2} = 3u_{n+1} - 2u_n$.

1. On pose $v_n = 3u_{n+1} - 2u_n$.

Montrer que la suite (v_n) est une suite géométrique dont on déterminera la raison et le premier terme.

2. a) En déduire que pour tout entier n, u_n est un entier naturel et que $u_{n+1} = 2u_n + 1$.

b) En déduire que deux termes consécutifs de la suite (u_n) sont premiers entre eux.

128 PGCD

Démo

Soit a et b deux entiers premiers entre eux tels que $a \geqslant b \geqslant 1$.

1. Montrer que PGCD($a + b$, $a - b$) vaut 1 ou 2.

2. Montrer que PGCD($a + b$, ab) = 1.

3. Montrer que PGCD($a + b$, $a^2 + b^2$) vaut 1 ou 2.

129 PGCD et congruence

Soit les entiers relatifs n vérifiant le système (S) suivant :

$$(S) : \begin{cases} n \equiv 1\,(5) \\ n \equiv 5\,(7) \end{cases}$$

1. a) Montrer que si n vérifie (S) alors n vérifie le système :

$$\begin{cases} 4n + 1 \equiv 0\,(5) \\ 4n + 1 \equiv 0\,(7) \end{cases}$$

b) En déduire alors que $4n \equiv -1\,(35)$

2. Déterminer les solutions de (S).

130 Racines rationnelles

Soit le polynôme f défini par :

$f(x) = x^4 - 4x^3 - 8x^2 + 13x + 10$.

1. Montrer que si f admet une racine rationnelle alors cette racine est entière.

2. a) Montrer que si f admet une racine entière α alors α est un diviseur de 10.

b) Quelles sont les racines entières éventuelles de f ?

3. a) Après avoir déterminé ces racines, factoriser $f(x)$.

b) Déterminer les autres racines de f.

131 Solutions entières

Soit l'équation

(E) : $2x + 5y = s$ avec $s \in \mathbb{N}$.

On veut montrer que si $s \geqslant 4$ l'équation (E) admet au moins une solution dans $\mathbb{N}^2$.

1. Soit $0 \leqslant s \leqslant 4$, déterminer les valeurs de s pour lesquelles (E) admet des solutions dans $\mathbb{N}^2$.

2. Montrer par récurrence que si $s \geqslant 4$, l'équation (E) admet au moins une solution dans $\mathbb{N}^2$.

132 Égalité de deux PGCD (1)

Démo

Soit $n, a, b \in \mathbb{Z}^*$

Montrer que si a et b sont premiers entre eux alors :

PGCD(ab , n) = PGCD(b , n).

133 Égalité de deux PGCD (2)

Démo

Soit $n \in \mathbb{Z}$, on pose
$a = n^4 + 3n^2 - n + 2$ et $b = n^2 + n + 1$.
Montrer que :

$$\text{PGCD}(a\,,\,b) = \text{PGCD}(n - 2\,,\,7).$$

134 Équation diophantienne

Déterminer l'ensemble des couples $(x\,;\,y)$ d'entiers relatifs tels que :

$$955x + 183y = 1.$$

On pourra remonter l'algorithme d'Euclide pour trouver une solution particulière.

135 Somme et PPCM

Soit a et b deux entiers naturels non nuls.
On pose $d = \text{PGCD}(a\,;\,b)$ et $m = \text{PPCM}(a\,,\,b)$.
On rappelle que :

$$m = da'b' \text{ avec } a = da' \text{ et } b = db.$$

1. On cherche les couples $(a\,,\,b)$ d'entiers naturels tels que :

$$a + b = 56 \text{ et } m = 180.$$

a) Montrer que les valeurs possibles pour d sont 1, 2 ou 4.
b) Analyser chaque cas puis déterminer les couples $(a\,;\,b)$ qui conviennent.
2. En procédant comme à la question **1**, déterminer les couples $(a\,;\,b)$ d'entiers naturels tels que :

$$a + b = 276 \text{ et } m = 1\,440.$$

136 Système PGCD-PPCM

Déterminer les couples $(a\,,\,b) \in \mathbb{N}^2$ tels que :

$$\begin{cases} \text{PGCD}(a\,,\,b) = 42 \\ \text{PPCM}(a\,,\,b) = 1680 \end{cases}$$

137 PGCD et suite de Fibonacci

Soit la suite définie sur $\mathbb{N}$ par :

$$u_0 = 0,\ u_1 = 1, \text{ et } u_{n+2} = u_{n+1} + u_n.$$

1. Calculer u_2, u_3, u_4, u_5 et u_6.
2. Montrer par récurrence que :

$$\text{pour tout } n \in \mathbb{N}^*,\ u_{n+1} \times u_{n-1} - (u_n)^2 = (-1)^n.$$

En déduire que les termes u_n et u_{n+1} sont premiers entre eux.
3. Démontrer que :
pour tout $n \in \mathbb{N}$, pour tout $p \geqslant 1$,

$$u_{n+p} = u_n \times u_{p-1} + u_{n+1} \times u_p.$$

4. a) Démontrer que :

$$\text{PGCD}(u_{n+p}\,,\,u_n) = \text{PGCD}(u_p\,,\,u_n).$$

b) En déduire que si r est le reste de la division de m par n alors :

$$\text{PGCD}(u_m\,,\,u_n) = \text{PGCD}(u_r\,,\,u_n)$$
$$\text{PGCD}(u_m\,,\,u_n) = u_{\text{PGCD}(m\,,\,n)} \qquad (1)$$

5. Application : calculer u_{12}, u_{18}.
Vérifier alors la relation (1) de la question **4. b)**

138 Repas gastronomique

28 personnes participent à un repas gastronomique. Le prix normal est de 26 € sauf pour les étudiants et les enfants qui paient respectivement 17 € et 13 €. La somme totale recueillie est de 613 €.
Calculer le nombre d'étudiants et d'enfants ayant participé au repas. Proposer deux méthodes pour résoudre ce problème.

139 Cryptage

Pour transmettre un message, on utilise le système suivant.
1re étape À chaque lettre du message en clair, on associe son numéro d'ordre dans l'alphabet :
A ↦ 01 ; B ↦ 01 ; C ↦ 03 ; … ; Y ↦ 25 ; Z ↦ 26.
On obtient ainsi une suite de nombres.
2e étape On considère la suite d'entiers naturels (x_n) définie par :

$$\begin{cases} x_1 = 1 \\ x_{n+1} \equiv 5x_n + 2\ (33) \end{cases}$$

3e étape On ajoute terme à terme les suites obtenues dans la 1re et la 2e étape : on a alors le message crypté.
1. Déterminer les 25 premiers termes de la suite (x_n).
2. Coder le message suivant :

DEBARQUEMENTLEHUITJUIN

3. Décoder le message suivant :
5, 12, 24, 37, 34, 21, 10, 19, 27, 34, 13, 8, 26, 27, 16, 23, 22, 25, 41

140 Théorème des restes chinois

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur.

Ils projettent de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier.
Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Travaux pratiques

TICE Algo Histoire des Maths 30 min Chercher Raisonner

1 Équation de Pell-Fermat

On étudie dans cet exercice les équations du type $x^2 - ny^2 = 1$ où n un entier naturel non carré.

A ▸ Une première équation $(E_1) : x^2 - 2y^2 = 1$

1. Soit $(a\,;b)$ une solution de (E_1).
a) Quelle est la parité de a et de b ?
b) Déterminer PGCD$(a\,,b)$.
c) Montrer que (A ; B) tel que $A = 3a + 4b$ et $B = 2a + 3b$ est aussi une solution de (E_1).
2. a) Déterminer une solution de (E_1).
b) Déduire de la question **1. c)** une solution avec des entiers supérieurs à 100.
3. Déterminer, à l'aide d'une boucle conditionnelle, un algorithme, écrit en langage naturel puis en **Python**, qui donne un couple solution de (E_1) d'entiers supérieurs à 1 000.

B ▸ Une deuxième équation $(E_2) : x^2 - 3y^2 = 1$

1. Déterminer la plus petite solution non triviale c'est-à-dire différente de (1 ; 0). Cette solution est appelée solution fondamentale et on la note $(x_0\,;y_0)$.
2. a) Vérifier l'identité de Brahmagupta pour tout entiers relatifs a_1, a_2, b_1, b_2 et n :
$(a_1^{\,2} - nb_1^{\,2})(a_2^{\,2} - nb_2^{\,2}) = (a_1a_2 + nb_1b_2)^2 - n(a_1b_2 + b_1a_2)^2$
b) En déduire à partir de cette relation, en prenant $n = 3$, une autre solution $(x_1\,;y_1)$ de (E_2) connaissant $(x_0\,;y_0)$.
c) Soit $(x_n\,;y_n)$ une solution générale de l'équation (E_2), montrer la relation de récurrence donnant la solution suivante $(x_{n+1}\,;y_{n+1})$ en fonction de $(x_n\,;y_n)$:

$$\begin{cases} x_{n+1} = 2x_n + 3y_n \\ y_{n+1} = x_n + 2y_n \end{cases}$$

d) Déterminer les 10 premières solutions de l'équation (E_2), à l'aide d'un algortihme, écrit en **Python**.

C ▸ Équation de Brahmagupta $(E_3) : x^2 - 92y^2 = 1$

1. a) Déterminer un algorithme en **Python** permettant de trouver la solution fondamentale, autre que la solution (1 ; 0) à l'équation (E_3).
b) Rentrer cet algorithme et donner cette solution.
c) Peut-on en déterminer une autre ?
Si oui comment est-elle déterminée.

L'équation $x^2 - ny^2 = 1$ porte le nom du mathématicien anglais John Pell, mais c'est une erreur due à Euler qui lui attribua faussement son étude.
En fait, le premier à avoir décrit l'ensemble des solutions de cette équation est le mathématicien indien Brahmagupta, qui vivait au VII^{e} siècle après J-C, soit près de 1 000 ans avant Pell. Ses résultats étaient totalement inconnus des mathématiciens européens du XVII^{e} siècle et c'est Fermat qui remit cette équation au goût du jour, conjecturant qu'elle avait toujours une infinité de solutions.
Enfin Lagrange, un siècle plus tard, donne une preuve totalement rigoureuse de l'infinité des solutions.

TICE Algo 55 min Modéliser, Calculer

2 Chiffrement de Hill

Le chiffrement de Hill a été publié en 1929. C'est un chiffre non polygraphique, c'est-à-dire qu'on ne chiffre pas les lettres les unes après les autres, mais par « paquets ». On présente ici un exemple *bigraphique*, c'est à dire que les lettres sont regroupées deux à deux.

Étape 1 On regroupe les lettres par 2. Chaque lettre est remplacée par un entier en utilisant le tableau ci-dessous.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient des couples d'entiers $(x_1 ; x_2)$ où x_1 correspond à la première lettre et x_2 correspond à la deuxième lettre.

Étape 2 Chaque couple $(x_1 ; x_2)$ est transformé en $(y_1 ; y_2)$ tel que :

$$(S_1) : \begin{cases} y_1 \equiv 11x_1 + 3x_2 \ (26) \\ y_2 \equiv 7x_1 + 4x_2 \ (26) \end{cases} \text{ avec } 0 \leqslant y_1 \leqslant 25 \text{ et } 0 \leqslant y_2 \leqslant 25.$$

Étape 3 Chaque couple $(y_1 ; y_2)$ est transformé en un couple de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1. On regroupe ensuite les lettres

Exemple : TE $\rightarrow (19 , 4) \rightarrow \begin{cases} 11 \times 19 + 3 \times 4 \equiv 13 \ (26) \\ 7 \times 19 + 4 \times 4 \equiv 19 \ (26) \end{cases} \rightarrow$ NT

1. Coder le mot ST.

2. a) Compléter l'algorithme en **Python** permettant de coder un groupe de deux lettres :

```
def hill(lettre1 , lettre2) :
    alphabet=["A","B","C","D","E","F","G","H","I","J","K",
    "L","M","N","O","P","Q","R","S","T","U","V","W","X","Y","Z"]
    x1=alphabet.index(lettre1)
    x2=alphabet.index(lettre2)
    y1=...
    y2=...
return ...,...
```

PYTHON Programme
lienmini.fr/maths-e04-08

b) À l'aide de cet algorithme coder les mets PALACE et RAPACE.

c) Que constatez-vous ?

3. On veut maintenant déterminer la procédure de déchiffrement.

a) Montrer que pour tout couple $(x_1 ; x_2)$ vérifiant le système (S_1), vérifie le système suivant.

$$(S_2) : \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \ (26) \\ 23x_2 \equiv 19y + 11y_2 \ (26) \end{cases}$$

b) Montrer que pour tout entiers relatifs a et b : $23a \equiv b \ (26) \Leftrightarrow a \equiv 17b \ (26)$.

c) En déduire alors que tout couple $(x_1 ; x_2)$ vérifiant (S_2), vérifie le système suivant.

$$(S_3) : \begin{cases} x_1 \equiv 16y_1 + y_2 \ (26) \\ x_2 \equiv 11y_1 + 5y_2 \ (26) \end{cases}$$

d) Écrire une fonction en **Python** sur le même principe que la fonction **`hill`** de chiffrage pour déchiffrer un mot.

e) Décoder le mot : PFXXKNU. Ce mot étant de 7 lettres, ajouter la lettre W à la fin du mot pour avoir des paquets de deux lettres. Le décodage terminé, supprimer la dernière lettre.