

Nombres premiers

1 PGCD de deux nombres entiers

Propriété - Définition

Soient a et b deux entiers relatifs dont l'un au moins est non nul.

L'ensemble des diviseurs communs à a et à b admet un plus grand élément que l'on appelle le **plus grand diviseur commun** et que l'on note $\text{PGCD}(a; b)$.

Démonstration

L'ensemble des diviseurs de a et b est un ensemble non vide puisque 1 est un élément de cet ensemble.

De plus, il s'agit d'un ensemble fini.

Cet ensemble admet donc un plus grand élément.

Remarque

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

Exemple

D'après la décomposition en produit de facteurs premiers de 60 on a $60 = 2^2 \times 3 \times 5$.

D'après la décomposition en produit de facteurs premiers de 50 on a $50 = 2 \times 5^2$.

On a ainsi $\text{PGCD}(60; 50) = 2 \times 5 = 10$.

Propriétés

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

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

Propriété

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

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

Démonstration

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

Théorème

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

Exemple : Algorithme d'Euclide

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

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

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

2 Théorème de Bezout**Définition : nombres premiers entre eux**

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

Exemples

- Dans l'exemple précédent, 4 539 et 1 958 ne sont pas premiers entre eux.
- Les nombres 55 et 42 sont-ils premiers entre eux ? Vérifions à l'aide de l'algorithme d'Euclide.

$$55 = 42 \times 1 + 13$$

$$42 = 13 \times 3 + 3$$

$$13 = 3 \times 4 + 1$$
 Le dernier reste non nul vaut 1, qui est le PGCD de 55 et 42. Ils sont donc premiers entre eux.

Théorème : Identité de Bezout

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

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

Démonstration

Notons E l'ensemble des entiers naturels non nuls de la forme $ax + by$ où x et y sont des entiers relatifs. E est une partie non vide de \mathbb{N} . Elle admet donc un plus petit élément que l'on note n .

Par définition de E , il existe donc des entiers relatifs u et v tels que $n = au + bv$.

Or Le PGCD de a et b divise a et b donc $\text{PGCD}(a; b)$ divise n . Ainsi, $\text{PGCD}(a; b) \leq n$.

Posons la division euclidienne de a par n : $a = nq + r$ avec $0 \leq r < n$ et $q \in \mathbb{Z}$.

On a donc $r = a - nq = a - q(au + bv) = a(1 - qu) + b(-qv)$

Ainsi, r est de la forme $ax + by$ avec x et y des entiers relatifs. De plus, $r < n$, donc r n'est pas un élément de E .

On a donc nécessairement $r = 0$ ce qui signifie que n divise a .

De la même manière, on montre que n divise b .

Par définition du PGCD de a et b , $n \leq \text{PGCD}(a; b)$.

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

Théorème de Bezout

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

$$au + bv = 1$$

Démonstration

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

Réciproquement, supposons qu'il existe deux entiers u et v tels que $au + bv = 1$. $\text{PGCD}(a; b)$ divise a et $\text{PGCD}(a; b)$ divise b donc $\text{PGCD}(a; b)$ divise aussi $au + bv$ et donc $\text{PGCD}(a; b) = 1$.

Exemple

Soit n un entier naturel.

On souhaite montrer que $2n + 1$ et $3n + 2$ sont premiers entre eux.

Il faut trouver deux entiers u et v tels que $u(2n + 1) + v(3n + 2) = 1$.

En prenant $u = -3$ et $v = 2$ on obtient : $-3(2n + 1) + 2(3n + 2) = -6n - 3 + 6n + 4 = 1$.

Puisqu'il existe deux entiers u et v tels que $u(2n + 1) + v(3n + 2) = 1$ alors $2n + 1$ et $3n + 2$ sont premiers entre eux.

Méthode : Déterminer un couple d'entiers de Bézout

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

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

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

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

Le PGCD(59; 27) = 1 donc 59 et 27 sont premiers entre eux.

On remonte ensuite ces égalités :

$$1 = 5 - 2 \times 2 \quad \text{d'après (3)}$$

$$1 = 5 - 2 \times (27 - 5 \times 5) \quad \text{d'après (2)}$$

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

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

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

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

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

Propriété

Soit a un nombre entier.

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

Exemple : résoudre une équation du type $ax \equiv n \pmod{n}$

On souhaite résoudre l'équation $5x \equiv 7 \pmod{16}$ où x est un entier.

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

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

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

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

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

3 Théorème de Gauss

Théorème de Gauss

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

Démonstration

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

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

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

Exemple

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

7 divise $5(x - 1)$ et 7 et 5 sont premiers entre eux.

Alors d'après le théorème de Gauss, 7 divise $x - 1$. Il existe donc un entier relatif k tel que $7k = x - 1$ soit $x = 7k + 1$.

On remplace x par $7k + 1$ dans notre équation pour trouver $y = 7k$.

Les solutions de cette équation sont donc de la forme $x = 7k + 1$ et $y = 7k$ où $k \in \mathbb{Z}$.

Corollaire du théorème de Gauss

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

Démonstration

Puisque b et c divisent a alors il existe deux entiers k et k' tels que $a = kb$ et $a = k'c$.

Cela donne donc $kb = k'c$. Ce qui signifie que b divise $k'c$. Puisque b et c sont premiers entre eux, alors d'après le théorème de Gauss, b divise k' . Il existe donc un entier relatif k'' tel que $k' = k''b$.

On a alors $a = k'c = k''bc$ ce qui implique que bc divise a .

Définition : équation diophantienne

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

Exemple

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

- On cherche tout d'abord une solution particulière.
Ici, une solution évidente est le couple $(2; 1)$ puisque $17 \times 2 - 33 \times 1 = 1$;
- On va maintenant trouver toutes les solutions.
Soit $(x; y)$ une solution de l'équation. On a donc le système :

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

On soustrait ces deux lignes pour obtenir $17(x-2) - 33(y-1) = 0$ ce qui est équivalent à $17(x-2) = 33(y-1)$. Cela signifie que 33 divise $17(x-2)$ et puisque 17 et 33 sont premiers entre eux, d'après le théorème de Gauss, 33 divise $x-2$. Il existe donc un entier relatif k tel que $33k = x-2$ ou encore $x = 33k + 2$.

En remplaçant dans notre équation de départ, on obtient $y = 1 + 17k$.

Les solutions sont donc de la forme

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

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

4 Les nombres premiers**Définition**

Soit n un nombre entier naturel.

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

Exemple

Voici les premiers nombres premiers :

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

Remarques

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

Propriété

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

Démonstration

On va raisonner par l'absurde.

Supposons qu'il existe un nombre fini de nombres premiers : $p_1 < p_2 < \dots < p_n$.

On pose $N = p_1 \times p_2 \times \dots \times p_n + 1$.

- Si N est premier alors il existe un nombre premier plus grand que p_n puisque $p_1 \times p_2 \times \dots \times p_n + 1 > p_n$.
- Si N n'est pas premier, il admet au moins un diviseur premier p .

Supposons que p soit compris entre p_1 et p_n . Ainsi, p divise $p_1 \times p_2 \times \dots \times p_n$.

Puisque p divise aussi N , alors p divise 1, ce qui est contradictoire avec notre hypothèse. Cela signifie que $p > p_n$. Il existe donc un nombre premier p plus grand que p_n .

Propriété

Soit n un entier naturel supérieur ou égal à 2.

Si n n'est pas premier alors il admet un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

Démonstration

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

L'ensemble des diviseurs de n n'est donc pas vide et admet un plus petit élément p .

Si p n'était pas premier, il admettrait un diviseur d qui diviserait n . C'est impossible puisque p est le plus petit élément de l'ensemble des diviseurs de n . Donc p est premier.

n admet donc un diviseur premier p tel que $n = p \times q$ avec $p \leq q$.

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

Remarque

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

Exemple

Est-ce que 109 est un nombre premier ?

On a $10 < \sqrt{109} < 11$.

Or 109 n'est divisible ni par 2, ni par 3, ni par 5 ni par 7.

Cela signifie que 109 est un nombre premier.

Théorème fondamental de l'arithmétique

Soit n un entier naturel supérieur ou égal à 2.

Cet entier se décompose de façon unique (à l'ordre des facteurs près) sous la forme d'un produit de nombres premiers. On note

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

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

Propriété

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

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

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

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

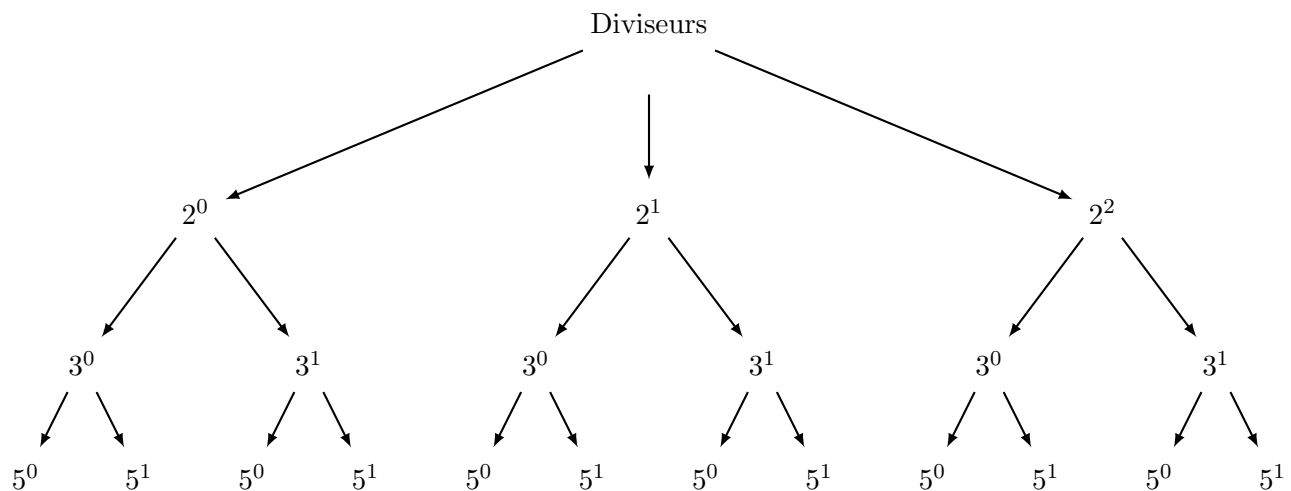
Exemple

On souhaite déterminer le nombre de diviseurs de 60 et la liste de ces diviseurs.

On a $60 = 2^2 \times 3^1 \times 5^1$.

Le nombre de diviseurs de 60 est donc $(2 + 1)(1 + 1)(1 + 1) = 12$. Le nombre 60 admet 12 diviseurs.

On peut ensuite utiliser un arbre pour faire la liste des diviseurs de 60 :



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

5 Le petit théorème de Fermat**Théorème**

Soit p un nombre premier et soit n un entier naturel qui ne soit pas un multiple de p .

$a^{p-1} - 1$ est divisible par p . On peut également noter :

$$a^{p-1} \equiv 1 \pmod{p}$$

Démonstration

On considère les $p - 1$ premiers multiples de a : $a, 2a, \dots, (p - 1)a$.

On considère leurs restes dans la division euclidienne par p : r_1, r_2, \dots, r_{p-1} .

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

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

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

- Ces restes sont donc tous différents et puisqu'il y a $p - 1$ multiples, on trouve tous les restes non nul possibles dans la division par p .
- On a alors $r_1 \times r_2 \times \dots \times r_{p-1} = 1 \times 2 \times \dots \times (p - 1) = (p - 1)!$.

- On a ensuite $a \times 2a \times \dots \times (p - 1)a \equiv (p - 1)! \pmod{p}$

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

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

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

Corollaire

Soit p un nombre premier et soit a un entier naturel.

Le nombre $a^p - a$ est divisible par p . On peut également noter :

$$a^p \equiv a \pmod{p}$$

Démonstration

Il suffit de multiplier l'égalité du précédent théorème par a .

L'égalité reste vraie si a est un multiple de p puisque l'on aura alors $a \equiv 0 \pmod{p}$.

Exemples

- $4^{12} \equiv 1 \pmod{13}$ car 13 est premier avec 4 et non multiple de 13.
- 7 est premier et 3 est non multiple de 7. D'après le petit théorème de Fermat, on a :

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

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

> Résoudre une congruence $ax \equiv b \pmod{n}$, déterminer un inverse**Exercice n°7**

Déterminer les entiers x tels que $3x \equiv 5 \pmod{4}$.

Exercice n°8

1. Pour tout entier naturel n , notons a le reste de la division euclidienne de $8n$ par 5. Compléter le tableau suivant :

n	0	1	2	3	4
a					

- Résoudre dans \mathbb{Z} l'équation $8n \equiv 4 \pmod{5}$.
- Résoudre dans \mathbb{Z} l'équation $5n \equiv 2 \pmod{6}$.
- Montrer que, dans \mathbb{Z} , l'équation $6n \equiv 5 \pmod{4}$ n'admet aucune solution.

Exercice n°9 On considère l'ensemble $A_7 = \{1; 2; 3; 4; 5; 6\}$.

1. Pour tout élément de A_7 , écrire l'unique élément y de A_7 tel que $ay \equiv 1 \pmod{7}$.

a	1	2	3	4	5	6
y						6

- Pour tout entier relatif x , montrer que l'équation $3x \equiv 5 \pmod{7}$ équivaut à $x \equiv 4 \pmod{7}$.
- Soit a un élément de A_7 . Montrer que les seuls entiers relatifs x solutions de $ax \equiv 0 \pmod{7}$ sont les multiples de 7.

> Résoudre des équations diophantienne

Exercice n°10 On considère l'équation $12x + 31y = 503$ où x et y sont des entiers relatifs.

- Montrer que $(-2; 17)$ est un couple solution de cette équation.
- Déterminer tous les couples d'entiers relatifs $(x; y)$ tels que $12x + 31y = 503$.

Exercice n°11 On considère l'équation $51x - 26y = 1$ où x et y sont des entiers relatifs.

- Justifier que cette équation admet au moins un couple solution.
- Donner une solution particulière à cette équation.
- Déterminer l'ensemble des couples solutions de cette équation.

Exercice n°12 On considère l'équation $7x - 6y = 1$ où x et y sont des entiers relatifs.

- Donner une solution particulière de cette équation.
- Déterminer l'ensemble des couples solutions de cette équation.

Exercice n°13 On souhaite résoudre (E) : $4x + 7y = 10$ où x et y sont des entiers relatifs.

1. Justifier l'existence d'entiers relatifs u et v tels que $4u + 7v = 1$.
2. Déterminer un couple d'entiers relatifs $(u; v)$ solutions de $4u + 7v = 1$ en utilisant l'algorithme d'Euclide.
3. En déduire un couple d'entiers $(x_0; y_0)$ solution de (E).
4. Montrer que (E) $\Leftrightarrow 4(x - 20) = 7(-y - 10)$.
5. En déduire les solutions de (E).

> Exercices complets

Exercice n°14 Pondichéry 2015

Les nombres de la forme $2^n - 1$ où n est un entier naturel non nul sont appelés les nombres de Mersenne.

1. Soient a , b et c trois entiers naturels non nul tels que $\text{PGCD}(b; c) = 1$. Prouver, à l'aide du théorème de Gauss que si b divise a et c divise a alors le produit bc divise a .
2. On considère le nombre de Mersenne $2^{33} - 1$. A l'aide de sa calculatrice, un élève obtient :

$(2^{33} - 1) \div 3$	2863311530
$(2^{33} - 1) \div 4$	2147483648
$(2^{33} - 1) \div 12$	715827882,6

Il affirme que 3 divise $(2^{33} - 1)$ et 4 divise $(2^{33} - 1)$ et 12 ne divise pas $(2^{33} - 1)$.

- (a) En quoi cette affirmation contredit-elle le résultat démontré à la question 1 ?
 - (b) Justifier en réalité que 4 ne divise pas $(2^{33} - 1)$.
 - (c) En remarquant que $2 \equiv -1 \pmod{3}$, montrer que, en réalité, 3 ne divise pas $(2^{33} - 1)$.
 - (d) Calculer la somme $S = 1 + 2^3 + (2^3)^2 + \dots + ((2^3)^{10})$.
 - (e) En déduire que 7 divise $(2^{33} - 1)$.
3. On considère le nombre de Mersenne $2^7 - 1$. Est-il premier ?
 4. On donne le programme suivant où $N \% k$ donne le reste de la division euclidienne de N par k .

```

1 from math import*
2 n=int(input('valeur de n(supérieure ou égale à 3):'))
3 k=2
4 while ((2**n-1)%k!=0&k<=sqrt(2**n-1)):
5     k=k+1
6 print(k)
7 if k>sqrt(2**n-1):
8     print('CAS 1')
9 else:
10    print('CAS 2')
```

- (a) Qu'affiche cet algorithme si on saisit $n = 33$? Et si on saisit $n = 7$?
- (b) Que représente le CAS 2 pour le nombre de Mersenne étudié ? Que représente alors le nombre k affiché pour le nombre de Mersenne étudié ?
- (c) Que représente le CAS 1 pour le nombre de Mersenne étudié ?

Exercice n°15 Antilles Guyane 2015**Partie A**

Pour deux entiers naturels non nuls a et b , on note $a\%b$ le reste dans la division euclidienne de a par b .
On considère le programme suivant :

```

1 a=int(input('Saisir un entier naturel a non nul'))
2 a=int(input('Saisir un entier naturel b non nul'))
3 c=a%b
4 while c!=0:
5     a=b
6     b=c
7     c=a%b
8 print(b)

```

1. Faire fonctionner ce programme avec $a = 26$ et $b = 9$ en indiquant les valeurs de a , b et c à chaque étape.
2. Ce programme donne en sortie le PGCD de a et de b . Le modifier pour qu'il indique si les entiers saisis sont premiers entre eux ou non.

Partie B

A chaque lettre de l'alphabet, on associe un nombre entier entre 0 et 25 :

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 définit un procédé de la façon suivante :

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

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

Étape n° 3 On calcule l'entier x' tel que $x' \equiv px + q \pmod{26}$ et $0 \leq x' \leq 25$.

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

1. Dans cette question, $p = 9$ et $q = 2$.
 - (a) Montrer que la lettre V est codée par la lettre J.
 - (b) Quel théorème permet d'affirmer qu'il existe deux entiers u et v tels que $9u + 26v = 1$? Donner un couple $(u; v)$ qui convient.
 - (c) Démontrer que $x' \equiv 9x + 2 \pmod{26}$ équivaut à $x \equiv 3x' + 20 \pmod{26}$.
 - (d) Décoder la lettre R.
2. Dans cette question, on prend $q = 2$ et p est inconnue. On sait que J est codée par la lettre D. Déterminer la valeur de p (on admettra que p est unique).
3. Dans cette question, $p = 13$ et $q = 2$. Coder les lettres B et D. Que peut-on dire de ce codage?

Correction des exercices sur les nombres premiers

> Déterminer les diviseurs d'un entier, le PGCD de deux entiers

Exercice n°1

- D'après l'algorithme d'Euclide, on a $525 = 390 \times 1 + 135$
 $390 = 135 \times 2 + 120$
 $135 = 120 \times 1 + 15$
 $120 = 15 \times 8$.
 Le PGCD est le dernier reste non nul, c'est à dire $d = 15$.

L'ensemble des diviseurs communs à 390 et 525 est l'ensemble des diviseurs du PGCD.
 il s'agit donc de l'ensemble $\{-15; -5; -3; -1; 1; 3; 5; 15\}$.

- D'après la propriété caractéristique du PGCD, les nombres $\frac{390}{15} = 26$ et $\frac{525}{15} = 35$ sont premiers entre eux.
- $\text{PGCD}(n; m) = 2 \times 3 \times 11 = 66$. Donc $\text{PGCD}\left(\frac{n}{66}; \frac{m}{66}\right) = 1$.

Exercice n°2

- On utilise l'algorithme d'Euclide : $360 = 252 \times 1 + 108$
 $252 = 108 \times 2 + 36$
 $108 = 36 \times 3$
 Le PGCD est le dernier reste non nul, c'est à dire 36.

2. $315 = 3^2 \times 5 \times 7$ et $825 = 3 \times 5^2 \times 11$.

- Le PGCD de ces deux nombres est 3×5 c'est à dire 15. Les diviseurs communs à 315 et 825 sont donc les diviseurs de 15 soit l'ensemble $\{-15; -5; -3; -1; 1; 3; 5; 15\}$.

Exercice n°3

$$\begin{aligned} 350 &= 1 \times 200 + 150 \\ 200 &= 1 \times 150 + 50 \\ 150 &= 3 \times 50 \\ \text{Le PGCD vaut } &50. \end{aligned}$$

$$\begin{aligned} 7\,000 &= 3 \times 1\,800 + 1\,600 \\ 1\,800 &= 1 \times 1\,600 + 200 \\ 1\,600 &= 8 \times 200 \\ \text{Le PGCD vaut } &200 \end{aligned}$$

$$\begin{aligned} 2\,002 &= 1 \times 1\,892 + 108 \\ 1\,892 &= 17 \times 108 + 56 \\ 108 &= 1 \times 56 + 52 \\ 56 &= 1 \times 52 + 4 \\ 52 &= 13 \times 4 \end{aligned}$$

Exercice n°4

L'ensemble des diviseurs de 18 est $\{-1; 1; -2; 2; -3; 3; -6; 6; -9; 9; -18; 18\}$.

L'ensemble des diviseurs de 24 est $\{-1; 1; -2; 2; -3; 3; -6; 6; -8; 8; -12; 12; -24; 24\}$?

Exercice n°5

$$n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1).$$

Si n est pair, il s'écrit sous la forme $n = 2k$ où k est un entier naturel.

Donc $n^3 - n = (2k + 1)2k(2k + 2)$ qui est divisible par 2.

Si n est impair, il s'écrit sous la forme $n = 2k + 1$ où k est un entier naturel.

Donc $n^3 - n = (2k + 1)2k(2k + 2)$ qui est divisible par 2.

n s'écrit sous la forme $3k$, $3k + 1$ ou $3k + 2$.

On a soit $n^3 - n = 3k(3k - 1)(3k + 1)$ qui est divisible par 3.

Ou bien $n^3 - n = (3k + 1)3k(3k + 2)$ qui est divisible par 3.

Ou bien $n^3 - n = (3k + 2)(3k + 1)(3k + 3) = (3k + 1)(3k + 2)3(k + 1)$ qui est divisible par 3.

Exercice n°6

1. $u_2 = 5u_1 - 4u_0 = 5$.

De la même façon, on trouve $u_3 = 21$ et $u_4 = 85$.

2. Montrons cela par récurrence.

Initialisation

$4u_0 + 1 = 1$ et $u_1 = 1$. La propriété est donc vraie au rang 0.

Hérédité

Supposons que pour un entier naturel n supérieur ou égal à 0, la propriété soit vraie. On a donc $u_{n+1} = 4u_n + 1$.

$u_{n+2} = 5u_{n+1} - 4u_n = 5u_{n+1} - (u_{n+1} - 1)$ par hypothèse de récurrence.

Donc $u_{n+2} = 4u_{n+1} + 1$. La proposition est héréditaire.

Conclusion

La propriété est vraie pour $n = 0$ et héréditaire à partir de ce rang. Elle est donc vraie pour tout entier naturel n .

3. Montrons cela par récurrence.

Initialisation

$u_0 = 0$. La propriété est donc vraie au rang 0.

Hérédité

Supposons que pour un entier naturel n supérieur ou égal à 0, u_n soit un nombre entier.

$4u_n + 1$ est aussi un entier. Ce qui veut dire que u_{n+1} est un entier.

La proposition est donc héréditaire.

Conclusion

La propriété est vraie pour $n = 0$ et héréditaire à partir de ce rang. Elle est donc vraie pour tout entier naturel n .

4. Pour tout entier naturel n , u_n est un entier et $u_{n+1} - 4u_n = 1$. Les entiers u_n et u_{n+1} sont donc premiers entre eux.

$$5. v_{n+1} = u_{n+1} + \frac{1}{3} = 4u_n + 1 + \frac{1}{3} = 4u_n + \frac{4}{3} = 4\left(v_n - \frac{1}{3}\right) + \frac{4}{3} = 4v_n.$$

C'est donc une suite géométrique de raison 4 et de premier terme $v_0 = u_0 + \frac{1}{3} = \frac{1}{3}$.

$$6. v_n = v_0 \times 4^n = \frac{1}{3} \times 4^n \text{ donc } u_n = v_n - \frac{1}{3} = \frac{1}{3}(4^n - 1).$$

$$7. \text{PGCD}(4^n - 1; 4^{n+1} - 1) = \text{PGCD}(3u_n; 3u_{n+1}) = 3\text{PGCD}(u_n; u_{n+1}) = 3.$$

> Résoudre une congruence $ax \equiv b \pmod{n}$, déterminer un inverse

Exercice n°7

$$3x \equiv 5 \pmod{4} \Leftrightarrow 3x \equiv 1 \pmod{4}.$$

On s'aide d'un tableau pour réaliser une disjonction de cas :

$x \text{ modulo } 4$	0	1	2	3
$3x \text{ modulo } 4$	0	3	2	1

Donc $3 \times 3 \equiv 1 \pmod{4}$. On en déduit que $x \equiv 3 \pmod{4}$.

Les entiers x solutions sont donc tous les entiers de la forme $3 + 4k$ où k est un entier relatif.

Exercice n°8

$$1. 8 \times 0 \equiv 0 \pmod{5}$$

$$8 \times 1 \equiv 3 \pmod{5}$$

$$8 \times 2 \equiv 1 \pmod{5}$$

$$8 \times 3 \equiv 4 \pmod{5}$$

$$8 \times 4 \equiv 2 \pmod{5}$$

Ce qui donne le tableau suivant :

n	0	1	2	3	4
a	0	3	1	4	2

2. Notons r_n le reste de la division euclidienne de n par 5, on a :

$$8n = 4 \text{ donc } 8r_n \equiv 4 \pmod{5}.$$

Puisque r_n est un entier naturel inférieur ou égal à 4, on en déduit, d'après le tableau de la question précédente que $r_n = 3$.

Ainsi, les solutions de l'équation $8n \equiv 4 \pmod{5}$ sont tous les entiers de la forme $3 + 5k$ où $k \in \mathbb{Z}$.

3. On applique la même méthode qu'à la question précédente :

n	0	1	2	3	4	5
a	0	5	4	3	2	1

Notons r_n le reste de la division euclidienne de n par 6, on a $5n \equiv 2 \pmod{6} \Leftrightarrow 5r_n \equiv 2 \pmod{6}$.

D'après le tableau précédent, que les entiers solutions sont de la forme $4 + 6k$ où $k \in \mathbb{Z}$.

4. On applique la même méthode qu'à la question précédente :

n	0	1	2	3
a	0	2	0	2

On a l'équivalence $6n \equiv 5 \pmod{4} \Leftrightarrow a \equiv 1 \pmod{4}$.

D'après le tableau précédent, il n'y a pas de solution.

Exercice n°9

1. Tableau complété :

a	1	2	3	4	5	6
y	1	4	5	2	3	6

2. On a $3x \equiv 5 \pmod{7}$

$$5 \times 3x \equiv 5 \times 5 \pmod{7}$$

$$15x \equiv 25 \pmod{7}$$

$$x \equiv 4 \pmod{7}$$

3. Soit a un élément de A_7 .

D'après la première question, pour a élément de A_7 , il existe un unique b de A_7 tel que $ab \equiv 1 \pmod{7}$.

$$ax \equiv 0 \pmod{7}$$

$$b(ax) \equiv b \times 0 \pmod{7}$$

$$(ba)x \equiv 0 \pmod{7}$$

$$x \equiv 0 \pmod{7}$$

Les solutions sont donc tous les multiples de 7.

> Résoudre des équations diophantiennes

Exercice n°10

1. $12 \times (-2) + 31 \times 17 = -24 + 527 = 503$.

2. Soit $(x; y)$ un couple solution.

D'après la question 1, on a $12x + 31y = 12 \times (-2) + 31 \times 17$

$$\text{Soit } 12(x + 2) = 31(17 - y).$$

12 est donc un diviseur de $31(17 - y)$. Or 31 et 17 sont premiers entre eux donc d'après le théorème de Gauss, 12 divise $17 - y$.

Il existe donc un entier k tel que $17 - y = 12k$. Ce qui revient à $y = 17 - 12k$.

Puisque $12x + 31y = 503$ cela donne $x = -2 + 31k$.

L'ensemble des solutions sont donc les couples de la forme $(-2 + 31k; 17 - 12k)$ où $k \in \mathbb{Z}$.

On vérifie ensuite que ce couple solution fonctionne en remplaçant x et y par ces valeurs.

Exercice n°11

1. Les entiers 51 et 26 sont premiers entre eux.

D'après le théorème de Bezout, il existe deux entiers relatifs u et v tels que $51u - 26v = 1$.

2. $51 \times (-1) - 26 \times (-2) = 1$. Le couple $(-1; -2)$ est donc solution.

3. Soit $(x; y)$ un couple solution.

On a alors $51x - 26y = 51 \times (-1) - 26 \times (-2)$ ce qui équivaut à $51(x + 1) = 26(y + 2)$.

26 divise donc $51(x + 1)$. Or 26 et 51 sont premiers entre eux donc d'après le théorème de Gauss, 26 divise $x + 1$.

Il existe donc un entier relatif k tel que $x + 1 = 26k$ ce qui revient à $x = 26k - 1$.

En remplaçant dans $51x - 26y = 1$ on trouve $y = 51k - 2$.

L'ensemble des solutions sont donc les couples de la forme $(26k - 1; 51 - 2k)$ où $k \in \mathbb{Z}$.

On vérifie ensuite que ce couple solution fonctionne en remplaçant x et y par ces valeurs.

Exercice n°12

1. $7 \times 1 - 6 \times 1 = 1$. Le couple $(1; 1)$ est donc bien une solution particulière.

2. Soit $(x; y)$ un couple solution.

On a alors $7x - 6y = 7 \times 1 - 6 \times 1$ ce qui est équivalent à $7(x - 1) = 6(y - 1)$.

7 est donc un diviseur de $6(y - 1)$. Or 6 et 7 sont premiers entre eux donc d'après le théorème de Gauss, 7 divise $y - 1$.

Il existe donc un entier relatif k tel que $y - 1 = 7k$ ce qui revient à $y = 7k + 1$.

En remplaçant dans $7x - 6y = 1$ on trouve $x = 6k + 1$.

L'ensemble des solutions sont donc les couples de la forme $(6k + 1; 7k + 1)$ où $k \in \mathbb{Z}$.

On vérifie ensuite que ce couple solution fonctionne en remplaçant x et y par ces valeurs.

Exercice n°13

1. C'est possible puisque 7 et 4 sont premiers entre eux et d'après le théorème de Bezout.

2. $7 = 4 \times 1 + 3$ et $4 = 3 \times 1 + 1$

On a donc $1 = 4 - 3 = 4 - (7 - 4) = 4 \times 2 + 7 \times (-1)$.

$(2; -1)$ est donc un couple solution.

3. En multipliant par 10, on obtient comme couple solution de (E) $(20; -10)$.

4. $4x + 7y = 10 \Leftrightarrow 4x + 7y = 4 \times 20 + 7 \times (-10) \Leftrightarrow 4(x - 20) = 7(-y - 10)$.

5. 4 divise $7(-y - 10)$ et 4 est premier avec 7 donc d'après le théorème de Gauss, 4 divise $-y - 10$.

Il existe donc un entier naturel k tel que $-y - 10 = 4k$ ce qui revient à $y = -10 - 4k$.

En remplaçant dans (E), on trouve $x = 20 + 7k$.

L'ensemble des solutions sont donc les couples de la forme $(7k + 20; -4k - 10)$ où $k \in \mathbb{Z}$.

On vérifie ensuite que ce couple solution fonctionne en remplaçant x et y par ces valeurs.

> Exercices complets

Exercice n°14

1. Les nombres b et c sont premiers entre eux.

Il existe donc un entier naturel b' tel que $a = bb'$ et un entier naturel c' tel que $a = cc'$.

On a donc $bb' = cc'$.

Puisque b et c sont premiers entre eux, d'après le théorème de Gauss, b divise c' .

Il existe donc un entier naturel q tel que $c' = bq$.

Donc $a = cbq$ et donc bc divise a .

2. (a) 3 et 4 sont premiers entre eux et divisent tous les deux $2^{33} - 1$ d'après les résultats de la calculatrice de l'élève.
 $12 = 3 \times 4$ devrait donc aussi diviser $2^{33} - 1$.

(b) $33 > 2$ donc 4 divise 2^{33} .

Si 4 divise $2^{33} - 1$ alors 4 divise 1 ce qui est impossible.

Donc 4 ne divise pas $2^{33} - 1$.

(c) $2 \equiv -1 \pmod{3}$ donc $2^{33} \equiv -1 \pmod{3}$ donc $2^{33} - 1 \equiv -2 \pmod{3}$.

Ainsi, 3 ne divise pas $2^{33} - 1$.

(d) S est la somme de termes d'une suite géométrique de raison 2^3 . Ainsi :

$$S = \frac{1 - (2^3)^{11}}{1 - 2^3} = \frac{2^{33} - 1}{7}$$

(e) S est nécessairement un nombre entier. Par conséquent, $\frac{2^{33} - 1}{7}$ aussi et donc 7 divise $2^{33} - 1$.

3. $2^7 - 1 = 127$ et $\sqrt{127} \approx 11,3$.

Or 127 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7, ni par 11.

127 est donc bien un nombre premier.

4. (a) Avec $n = 33$, le programme nous renvoie CAS 2.

Avec $n = 7$, le programme nous renvoie CAS 1.

(b) Le CAS 2 signifie que le nombre de Mersenne n'est pas premier. Le nombre k affichée est le plus petit diviseur de $2^n - 1$ strictement supérieur à 1.

(c) Le CAS 1 signifie que le nombre de Mersenne est un nombre premier.

Exercice n°15**Partie A**

1. On a :

a	26	9	8
b	9	8	1
c	8	1	0

L'algorithme va donc afficher 1.

2. Voici le programme :

```

1 a=int(input('Saisir un entier naturel a non nul'))
2 a=int(input('Saisir un entier naturel b non nul'))
3 c=a%b
4 while c!=0:
5     a=b
6     b=c
7     c=a%b
8 if b==1:
9     print('a et b sont premiers entre eux.')
10 else:
11     print('a et b ne sont pas premiers entre eux.')
```

Partie B

1. (a) Étape 1 : $p = 9$ et $q = 2$

Étape 2 : On choisit V donc $x = 21$.

Étape 3 : $px + q = 191 \equiv 9 \pmod{26}$

Étape 4 : La lettre associée à 9 est J.

(b) Les nombres 9 et 26 sont premiers entre eux alors d'après le théorème de Bezout il existe un couple $(u; v)$ tel que $9u + 26v = 1$.

$9 \times 3 + 26 \times (-1) = 1$. Le couple $(3; -1)$ convient donc.

(c) $x' \equiv 9x + 2 \pmod{26} \Leftrightarrow 3x' \equiv 27x + 6 \pmod{26} \Leftrightarrow 3x' \equiv x + 6 \pmod{26} \Leftrightarrow 3x' - 6 \equiv x \pmod{26} \Leftrightarrow 3x' + 20 \equiv x \pmod{26}$.

(d) Si on obtient la lettre R alors $x' = 17$. Puis $3 \times 17 + 20 = 71 \equiv 19 \pmod{26}$.

La lettre initiale était donc T.

2. J est codée par D. Cela veut dire que si $x = 9$ alors $x' = 3$.

Avec $x' = px + 2 \pmod{26}$ ce qui donne $3 \equiv 9p + 2 \pmod{26}$ et donc $9p \equiv 1 \pmod{26}$.

Or $9 \times 3 = 27 \equiv 1 \pmod{26}$.

Donc $p = 3$.

3. $p = 13$ et $q = 2$.

Si on choisit la lettre B alors $x = 1$.

Puis $13 \times 1 + 2 = 15 \equiv 15 \pmod{26}$. Donc $x' = 15$ ce qui correspond à la lettre P.

Si on choisit la lettre D alors $x = 3$.

Puis $13 \times 3 + 2 = 41 \equiv 15 \pmod{26}$. Donc $x' = 15$ ce qui correspond à la lettre P.

Ce codage n'est donc pas optimale puisque deux lettres différentes sont codées par la même lettre.