

Exercice n°1

a) $123 = 3 \times 41$ donc les diviseurs de 123 sont : 1, 3, 41, 123.

b) $56 = 2^3 \times 7$ donc les diviseurs de 56 sont :
 — les facteurs premiers et 1 : 1, 2, 7 ;
 — les produits à deux facteurs premiers : $2 \times 2 = 4$, $2 \times 7 = 14$;
 — les produits à 3 facteurs premiers : $2^3 = 8$ et $2^2 \times 7 = 28$;
 — les produits à 4 facteurs premiers : $2^3 \times 7 = 56$.

L'ensemble des diviseurs de 56 est donc : $\{1; 2; 4; 7; 8; 14; 28; 56\}$.

c) $78 = 2 \times 3 \times 13$ donc les diviseurs de 78 sont :
 — les facteurs premiers et 1 : 1, 2, 3, 13 ;
 — les produits à deux facteurs premiers : $2 \times 3 = 6$, $2 \times 13 = 26$ et $3 \times 13 = 39$;
 — les produits à 3 facteurs premiers : $2 \times 3 \times 13 = 78$.

L'ensemble des diviseurs de 78 est donc : $\{1; 2; 3; 6; 13; 26; 39; 78\}$.

d) $1517 = 37 \times 41$ donc les diviseurs de 1517 sont 1, 37, 41 et 1517.

Exercice n°2

```
def liste_diviseurs(n):
    L = []
    for k in range(1, abs(n)+1):
        if n%k == 0:
            L.append(k)

    return L
```

Exercice n°3

1. $n + 7$ multiple de 5 signifie qu'il existe un entier k tel que $n + 7 = 5k$, soit $n = 5k - 7$.

Les entiers naturels n tels que $n + 7$ soit un multiple de 5 sont les entiers n s'écrivant $n = 5k - 7$, $k \geq 2$.

2. $51n = 17 \times 3n$ donc $51n$ est divisible par 17. Or, 7 n'est pas divisible par 17 donc $51n + 7$ n'est pas divisible par 17.

Exercice n°4

On sait que :

$$\begin{aligned} a|b &\iff \exists k \in \mathbb{Z}, b = ka \iff n + 13 = k(2n + 1) \\ &\iff (2k - 1)n = 13 - k. \end{aligned}$$

Cherchons à présent une combinaison linéaire de a et b indépendante de n . Notons-la $pa + qb$. Comme $a|a$ et $a|b$, $a|(pa + qb)$. Comme $pa + qb$ est indépendante de n , cela signifie que a est un diviseur de cette combinaison linéaire, et on pourra exploiter cela.

$$pa + qb = 2pn + p + qn + 13q = (2p + q)n + p + 13q.$$

$pa + qb$ indépendante de $n \iff 2p + q = 0 \iff q = -2p$.
 On peut alors prendre $p = 1$ et $q = -2$.

$$a - 2b = -25.$$

Par conséquent, $a|25$, donc $a \in \{-25; -5; -1; 1; 5; 25\}$.

- si $a = -25$, alors $2n + 1 = -25$ et $n = -13$;
- si $a = -5$, alors $2n + 1 = -5$ et $n = -3$;
- si $a = -1$, alors $2n + 1 = -1$ et $n = -1$;
- si $a = 1$, alors $2n + 1 = 1$ et $n = 0$;
- si $a = 5$, alors $2n + 1 = 5$ et $n = 2$;
- si $a = 25$, alors $2n + 1 = 25$ et $n = 12$.

On doit maintenant vérifier que pour toutes les valeurs de n trouvées, a divise b , ce qui se fait rapidement.

Les valeurs de n cherchées sont donc : $-13, -3, -1, 0, 2$ et 12 .

Exercice n°5

$a|b \iff a|(pa + qb)$, où p et q sont deux entiers relatifs.

$pa + qb = (p + 3q)n - (4p + 17q)$ est indépendante de n si $p + 3q = 0$, soit $p = -3q$.

Prenons alors $p = -3$ et $q = 1$:

$$pa + qb = -3a + b = -3(n - 4) + 3n - 17 = -5.$$

Ainsi, $a|5$, dans les cas suivants :

- $a = 1$, ce qui entraîne, $n - 4 = 1$, soit $n = 5$;
- $a = 5$, ce qui entraîne, $n - 4 = 5$, soit $n = 9$;
- $a = -1$, ce qui entraîne, $n - 4 = -1$, soit $n = 3$;
- $a = -5$, ce qui entraîne, $n - 4 = -5$, soit $n = -1$.

Si $n = 5$, $a = 1$ et $b = 2$ et a divise bien b .

Si $n = 9$, $a = 5$ et $b = 10$ et a divise bien b .

Si $n = 3$, $a = -1$ et $b = -8$ et a divise bien b .

Si $n = -1$, $a = -5$ et $b = -20$ et a divise bien b .

Ainsi, les valeurs de n telles que a divise b sont $-1, 3, 5$ et 9 .

Exercice n°6

Soit n un entier naturel non nul.

$$\begin{aligned} 1. \quad n^3 + n^2 + n + 1 &= \frac{n^4 - 1}{n - 1} \\ &= \frac{(n^2 - 1)(n^2 + 1)}{n - 1} \\ &= \frac{(n - 1)(n + 1)(n^2 + 1)}{n - 1} \\ &= (n + 1)(n^2 + 1). \end{aligned}$$

Donc $n^3 + n^2 + n + 1$ est bien divisible par $n + 1$.

2. $1\ 111 = 10^3 + 10^2 + 10 + 1$ est divisible par $10 + 1 = 11$.
De plus, d'après la question précédente, $10^2 + 1 = 101$ est aussi un diviseur de $1\ 111$.
Deux diviseurs non triviaux de $1\ 111$ sont donc 11 et 101 .

Exercice n°7

Soit n un entier naturel.

- Supposons que n soit pair. Alors, il existe un entier k tel que $n = 2k + 1$.
Ainsi, $n^2 - 1 = (2k + 1)^2 - 1 = (2k + 1 - 1)(2k + 1 + 1) = (2k)(2k + 2) = 4k(k + 1)$.
Par conséquent, 4 divise bien $n^2 - 1$.
- Supposons que 4 divise $n^2 - 1$. Alors, il existe un entier k tel que $n^2 - 1 = 4k$, soit $n^2 = 4k + 1$.
On se demande si n est nécessairement impair. Supposons donc qu'il ne le soit pas, et qu'il existe un entier p tel que $n = 2p$.
Alors,
 $n^2 = 4k + 1 \iff 4p^2 = 4k + 1 \iff 4(p^2 - k) = 1$, ce qui est impossible (car cela voudrait dire que 1 est divisible par 4).
Ainsi, la réciproque est vraie.

Exercice n°8

n divise n donc pour que n divise $n + p$, il est nécessaire que n divise p .

Exercice n°9

Posons n un entier relatif. Alors,
 $n + (n + 1) + (n + 2) + (n + 3) = 4n + 6 = 2(n + 3)$.
On constate alors que la somme des quatre entiers consécutifs est un multiple de 2 .

Exercice n°10

Avant tout, remarquons que :

$$n^2 = m^2 + 11 \iff n^2 - m^2 = 11 \iff (n + m)(n - m) = 11.$$

Ainsi, il est nécessaire que $n + m$ ou $n - m$ divise 11 . Or, 11 est un nombre premier donc,

$$\begin{cases} n + m = 11 \\ n - m = 1 \end{cases} \quad \text{ou} \quad \begin{cases} n - m = 11 \\ n + m = 1 \end{cases}.$$

Ou bien,

$$\begin{cases} n + m = -11 \\ n - m = -1 \end{cases} \quad \text{ou} \quad \begin{cases} n - m = -11 \\ n + m = -1 \end{cases}.$$

Autrement dit,

$$n = 6 \quad \text{et} \quad m = 5 \quad \text{ou} \quad m = -5.$$

Ou bien,

$$n = -6 \quad \text{et} \quad m = 5 \quad \text{ou} \quad m = -5.$$

Ainsi, les solutions de l'équation $n^2 = m^2 + 11$ sont les couples $(-6; 5)$ et $(-6; -5)$, $(6; -5)$ et $(6; 5)$.

Exercice n°11

On pose $A_n = 2n^2 + 11n + 32$ et $B_n = n + 3$ pour tout entier relatif n . On se demande pour quelles valeurs de n B_n divise A_n .

- $(n + 3)(2n + 5) + 17 = 2n^2 + 5n + 6n + 15 + 17$.
 $= 2n^2 + 11n + 32$
 $= A_n$
- B_n divise A_n si $\frac{A_n}{B_n} \in \mathbb{Z}$, pour $n \neq -3$. Or,

$$\begin{aligned} \frac{A_n}{B_n} &= \frac{(n + 3)(2n + 5) + 17}{n + 3} \\ &= \frac{(n + 3)(2n + 5)}{n + 3} + \frac{17}{n + 3} \\ &= 2n + 5 + \frac{17}{n + 3}. \end{aligned}$$

$$(2n + 5) \in \mathbb{Z} \text{ donc } \frac{A_n}{B_n} \in \mathbb{Z} \iff (n + 3) \mid 17.$$

17 étant un nombre premier, il n'est divisible que par 1 et 17 donc il faut que $n + 3 = \pm 1$ (i.e. $n = 1 - 3 = -2$ ou $n = -1 - 3 = -4$)
ou $n + 3 = \pm 17$ (i.e. $n = 17 - 3 = 14$ ou $n = -17 - 3 = -20$).

Exercice n°12

On souhaite démontrer que $5^n + 19$ est toujours divisible par 4 pour tout entier naturel n .

- On sait que $1 + q + q^2 + \dots + q^n = \frac{1 - q^{n+1}}{1 - q}$ pour $q \neq 1$.
Ainsi,
$$1 + 5 + 5^2 + \dots + 5^{n-1} = \frac{1 - 5^n}{1 - 5} = \frac{5^n - 1}{4}.$$
- La somme $1 + 5 + 5^2 + \dots + 5^{n-1}$ est entière donc $5^n - 1$ est divisible par 4 .
Ainsi, $5^n - 1 + 4k \in \mathbb{N}$ pour tout entier relatif k .
En prenant $k = 5$, on obtient $5^n - 1 + 4 \times 5 = 5^n + 19$, donc $5^n + 19$ est toujours divisible par 4 .

Exercice n°13

- Divisibilité par 2 . Deux cas se présentent :
— Si p est pair : $p = 2k$, $k \in \mathbb{Z}$. Dans ce cas, $p(p^2 - 1) = 2k(4k^2 - 1)$ est divisible par 2 .
— Si p est impair : $p = 2k + 1$, $k \in \mathbb{Z}$. Dans ce cas,

$$\begin{aligned} p(p^2 - 1) &= (2k + 1)[(2k + 1)^2 - 1] \\ &= (2k + 1)(4k^2 + 2k + 1 - 1) \\ &= (2k + 1)(4k^2 + 2k) \\ &= 2(2k + 1)(2k^2 + k) \end{aligned}$$

Ainsi, $p(p^2 - 1)$ est divisible par 2 .

Dans tous les cas, le résultat est démontré.

- Divisibilité par 3 . Trois cas se présentent :
— $p = 3k$, $k \in \mathbb{Z}$. Alors, $p(p^2 - 1) = 3k(9k^2 - 1)$ est divisible par 3 .

— $p = 3k + 1$. Alors,

$$\begin{aligned} p(p^2 - 1) &= (3k + 1)[(3k + 1)^2 - 1] \\ &= (3k + 1)(9k^2 + 6k) \\ &= 3k(3k + 2)(3k + 1). \end{aligned}$$

Donc $p(p^2 - 1)$ est divisible par 3.

— $p = 3k + 2$. Alors,

$$\begin{aligned} p(p^2 - 1) &= (3k + 2)[(3k + 2)^2 - 1] \\ &= (3k + 2)(9k^2 + 12k + 3) \\ &= 3(3k^2 + 4k + 1)(3k + 2). \end{aligned}$$

Donc $p(p^2 - 1)$ est divisible par 3.

Dans tous les cas, $p(p^2 - 1)$ est divisible par 3.

Exercice n°14

n est impair donc $n = 2k + 1$, $k \in \mathbb{N}$.

Ainsi,

$$\begin{aligned} n^2 - 1 &= (2k + 1)^2 - 1 \\ &= 4k^2 + 4k \\ &= 4k(k + 1). \end{aligned}$$

k et $k + 1$ sont deux entiers consécutifs donc l'un des deux est pair ; ainsi, leur produit est pair et s'écrit donc $k(k + 1) = 2q$, $q \in \mathbb{N}$.

On a donc : $n^2 - 1 = 4 \times 2q = 8q$, ce qui prouve que $n^2 - 1$ est divisible par 8.

Exercice n°15

Chaque nombre à deux chiffres x peut s'écrire sous la forme $x = \overline{du} = 10d + u$. Ainsi,

- $x = 10d + u = (7d + 3d) + u = 7d + (3d + u)$.
 x est divisible par 7 équivaut à dire que $7d + (3d + u)$ l'est aussi, i.e. que $3d + u$ est divisible par 7 car $7d$ l'est toujours.
- On peut s'inspirer du raisonnement précédent en posant :

$$\begin{aligned} x &= 392 \\ &= 39 \times 10 + 2 \\ &= 39 \times (7 + 3) + 2 \\ &= 39 \times 7 + 3 \times 39 + 2 \end{aligned}$$

392 est divisible par 7 si et seulement si $3 \times 39 + 2$ l'est aussi.

$$3 \times 39 + 2 = 3 \times (40 - 1) + 2 = 120 - 3 + 2 = 119.$$

On recommence avec 119 :

$$119 = 11 \times 7 + 11 \times 3 + 9.$$

119 est divisible par 7 si et seulement si $11 \times 3 + 9$ l'est aussi.

$$11 \times 3 + 9 = 33 + 9 = 42 = 7 \times 6.$$

Ainsi, 119 est divisible par 7, donc 392 aussi.

- $611 \times 3 + 9 = 1833 + 9 = 1842$.

$$184 \times 3 + 2 = 552 + 2 = 554$$

$$55 \times 3 + 4 = 165 + 4 = 169$$

$$16 \times 3 + 9 = 48 + 9 = 57$$

57 n'est pas divisible par 7 donc 6119 non plus.

Exercice n°16

Soit a un entier naturel.

$$\begin{aligned} 1. \quad a^5 - a &= a(a^4 - 1) \\ &= a(a^2 - 1)(a^2 + 1) \\ &= a(a - 1)(a + 1)(a^2 + 1). \end{aligned}$$

Entre a et $a + 1$, il y a un nombre pair ; donc $a^5 - a$ est divisible par 2.

$a - 1$, a et $a + 1$ sont trois nombres consécutifs. Si l'un des deux est divisible par 5, alors $a^5 - 1$ l'est aussi et donc au final, il est divisible par 10.

Si aucun des nombres $a - 1$, a et $a + 1$ n'est divisible par 5, alors notons r le reste de la division euclidienne de a par 5 : $a = 5q + r$, $0 < r < 5$, $q \in \mathbb{N}$.

Si $a - 1$ n'est pas divisible par 5, alors $r \neq 1$;

si $a + 1$ n'est pas divisible par 5, alors $r \neq 4$.

Alors, $a^2 + 1 = (5q + r)^2 + 1 = 25q^2 + 10qr + r^2 + 1$, avec $r = 2$ ou $r = 3$.

— Si $r = 2$, $r^2 + 1 = 5$;

— Si $r = 3$, $r^2 + 1 = 10$.

Dans les deux cas, $a^2 + 1$ est divisible par 5.

Ainsi, $a^5 - a$ est divisible par 5 et par 2, donc par 10.

- $a^5 - b^5$ divisible par 10.

Or, on peut écrire :

$$a^5 - b^5 = a^5 - a + a - (b^5 - b) - b = (a^5 - a) - (b^5 - b) + (a - b).$$

$a^5 - a$ et $b^5 - b$ sont divisibles par 10 d'après la question précédente ; ainsi, si $a^5 - b^5$ est divisible par 10, $a - b$ doit l'être aussi.

Ainsi, $a - b = 10q$, $q \in \mathbb{N}$ et donc $a = 10q + b$. En ajoutant b dans les deux membres, on obtient $a + b = 10q + 2b = 2(5q + b)$, et donc $a + b$ est divisible par 2.

$a - b$ est divisible par 10 et $a + b$ est divisible par 2, donc $(a - b)(a + b) = a^2 - b^2$ est divisible par 20.

Exercice n°17

On remarque que :

$$1000! = (1 \times 2 \times 3 \times \cdots \times 10) \times (11 \times \cdots \times 20) \times \cdots \times (991 \times \cdots \times 1000).$$

Combien de multiples de 3 avons-nous ici ? Il y en a 333 ($999 \div 3$).

On peut donc factoriser ainsi :

$$\begin{aligned} 1000! &= 3^{333} (1 \times 2 \times \color{red}{1} \times 4 \times 5 \times \color{red}{2} \times 7 \times 8 \times \color{red}{3} \times 10) \times \cdots \\ &\quad \times (991 \times 992 \times \color{red}{331} \cdots \times \color{red}{333} \times 1000) \\ &= 3^{333} \times \color{red}{1} \times \color{red}{2} \times \cdots \times \color{red}{333} \times \underbrace{1 \times 2 \times 4 \times 5 \times \cdots \times 1000}_{\text{aucun multiples de 3}} \\ &= 3^{333} \times 333! \times N_1, \quad \text{avec } N_1 \text{ non multiple de 3.} \end{aligned}$$

De plus, dans $333!$, il y a 111 multiples de 3 donc, avec un même raisonnement, on a :

$$333! = 3^{111} \times 111! \times N_2, \quad \text{avec } N_2 \text{ non multiple de 3.}$$

On voit apparaître $111!$ dans lequel il y a 37 multiples de 3 (3, 6, 9, ..., 99, 102, 105, 108, 111). On peut donc écrire :

$$111! = 3^{37} \times 37! \times N_3, \quad \text{avec } N_3 \text{ non multiple de 3.}$$

De même, on voit $37!$ apparaître, où il y a 12 multiples de 3 donc on peut écrire :

$$37! = 3^{12} \times 12! \times N_4, \text{ avec } N_4 \text{ non multiple de 3.}$$

On voit $12!$ apparaître, où il y a 4 multiples de 3 donc on peut écrire :

$$12! = 3^4 \times 4! \times N_5, \text{ avec } N_5 \text{ non multiple de 3.}$$

On voit apparaître $4!$ où il y a 1 multiple de 3 et on peut écrire :

$$4! = 3^1(1 \times 2 \times 1 \times 4).$$

Finalement, dans $1000!$, on peut mettre en facteur $3^{333+111+37+12+4+1} = 3^{498}$.

Ainsi, le plus grand entier n tel que 3^n divise $1000!$ est $n = 498$.

Exercice n°18

On écrit $a = bq + r$ avec $a = 7n + 5$ et $b = 3n + 1$:

$$7n + 5 = 2(3n + 1) + n + 3, \quad 0 \leq n + 3 < 3n + 1.$$

La condition sur le reste $0 \leq n + 3 < 3n + 1$ équivaut à écrire que $n > 1$. Donc,

- si $n > 1$ le quotient est égal à 2 et le reste à $n + 3$;
- si $n = 0$, $a = bq + r \iff 5 = 5 \times 1 + 0$ donc dans ce cas, le quotient est égal à 5 et le reste à 0;
- si $n = 1$, $a = bq + r \iff 12 = 3 \times 4 + 0$ donc ici, le quotient est égal à 3 et le reste à 0.

Exercice n°19

D'après l'énoncé, on a :

$$\begin{cases} n = 4q + 3 \\ n = 5q + 1 \end{cases}$$

donc $4q + 3 = 5q + 1 \iff q = 2$. Par conséquent, $n = 4q + 3 = 11$.

Exercice n°20

```
L = [ 2*q+1 for q in range(50) ]
P = [ 3*q+2 for q in range(33) ]
Q = [ 5*q+4 for q in range(20) ]
N = [ n for n in L if n in P and n in Q ]
print( N )
```

Exercice n°21

1. Le reste de la division euclidienne de n par 17 est égal à 7 :

$$n = 17q + 7.$$

Par conséquent,

$$\begin{aligned} n^2 &= (17q + 7)^2 \\ &= 17^2 q^2 + 17 \times 14q + 49 \\ &= 17(17q^2 + 14q) + 17 \times 2 + 15 \\ &= 17(17q^2 + 14q + 2) + 15. \end{aligned}$$

On s'est ici arrangé pour écrire n^2 sous la forme $17Q + r$, $0 \leq r < 17$, afin d'avoir une division euclidienne.

Ainsi, le reste de la division euclidienne de n^2 par 17 est 15.

2. Procédons de même avec n^3 :

$$\begin{aligned} n^3 &= (17q + 7)^3 \\ &= 17^3 q^3 + 3 \times 17^2 \times q^2 \times 7 + 3 \times 17q \times 7^2 + 7^3 \\ &= 17(17^2 q^3 + 3 \times 17 \times 7q^2 + 3q \times 7^2) + 20 \times 17 + 3 \\ &= 17(289q^3 + 357q^2 + 147q + 20) + 3. \end{aligned}$$

Ainsi, le reste de la division euclidienne de n^3 par 17 est 3.

Exercice n°22

1. $10^2 = 100 = 9 \times 11 + 1$

$$10^3 = 1000 = 90 \times 11 + 10$$

$$10^4 = 10000 = 909 \times 11 + 1$$

$$10^5 = 100000 = 9090 \times 11 + 10$$

On peut conjecturer que lorsque n est pair, le reste de la division euclidienne de 10^n par 11 est égal à 1 et lorsqu'il est impair, ce reste est égal à 10.

2. — Supposons que n soit un entier naturel pair. Alors, $n = 2k$, $k \in \mathbb{N}$ et

$$10^n = 10^{2k} = 100^k = (99 + 1)^k.$$

Or, $(a + b)^k = \sum_{p=0}^k c_p a^p b^{k-p}$, où les c_p sont des coefficients entiers.

Autrement dit, $(99 + 1)^k = 99^k + 99^{k-1}c_1 + 99^{k-2}c_2 + \dots + 99c_{p-1} + 1$.

Chaque terme de cette somme (sauf le dernier) étant un multiple de 99, le reste de la division euclidienne de 100^k par 11 est égale à 1 (le dernier terme de la somme).

Cela montre que si n est pair, alors le reste de la division euclidienne de 10^n par 11 est égal à 1.

- Supposons que n soit impair. Alors, $n = 2k + 1$, $k \in \mathbb{N}$ et $10^n = 10^{2k+1} = 10^{2k} \times 10$. D'après ce qui a été fait précédemment, on peut alors écrire :

$$10^{2k} \times 10 = 10 \times 99^k + 10 \times 99^{k-1}c_1 + 10 \times 99^{k-2}c_2 + \dots + 10 \times 99c_{p-1} + 10.$$

Ainsi, le reste de la division euclidienne de 10^{2k+1} par 11 est égal à 10.

La conjecture est alors démontrée.

Exercice n°23

Remarquons que :

$$73 \equiv 3 \pmod{5}$$

donc :

$$73^{37} \equiv 3^{37} \pmod{5}.$$

Regardons les premières puissances de 3 modulo 5 :

- $3^1 \equiv 3 \pmod{5}$
- $3^2 \equiv 9 \equiv 4 \pmod{5}$
- $3^3 \equiv 27 \equiv 2 \pmod{5}$
- $3^4 \equiv (3^2)^2 \equiv 4^2 \equiv 1 \pmod{5}$

Ce dernier reste est intéressant car il signifie que $(3^4)^k \equiv 1 \pmod{5}$ pour tout entier naturel k .

Or,

$$3^{37} = 3^{4 \times 9 + 1}$$

donc :

$$73^{37} \equiv 3^{4 \times 9 + 1} \pmod{5}$$

soit :

$$73^{37} \equiv (3^4)^9 \times 3^1 \pmod{5}$$

donc :

$$73^{37} \equiv 1 \times 3^1 \pmod{5}.$$

Finalement,

$$\boxed{73^{37} \equiv 3 \pmod{5}}.$$

Ainsi, le reste de la division euclidienne de 73^{37} par 5 est 3.

Exercice n°24

$13 \equiv -1 \pmod{14}$ donc $13^{1789} \equiv (-1)^{1789} \equiv -1 \equiv 13 \pmod{14}$.

Le reste de la division euclidienne de 13^{1789} par 14 est donc 13.

Exercice n°25

Nous savons que $32 = 4 \times 7 + 4$ donc $32 \equiv 4 \pmod{7}$.

Ainsi, $32^{45} \equiv 4^{45} \pmod{7}$.

Or, $4^2 = 16 \equiv 2 \pmod{7}$ et $4^3 = 64 \equiv 1 \pmod{7}$.

On peut donc écrire :

$$\begin{aligned} 32^{45} &\equiv 4^{3 \times 15} \pmod{7} \\ &\equiv (4^3)^{15} \pmod{7} \\ &\equiv 1^{15} \pmod{7} \\ &\equiv 1 \pmod{7}. \end{aligned}$$

Le reste de la division euclidienne de 32^{45} par 7 est donc 1.

Exercice n°26

Calculer le reste de la division euclidienne de 17^{548} par 7.

$17 \equiv 3 \pmod{7}$ car $17 = 2 \times 7 + 3$.

Ainsi, $17^2 \equiv 3^2 \equiv 2 \pmod{7}$, et donc $17^6 \equiv 2^3 \equiv 1 \pmod{7}$.

On écrit 548 sous la forme : $548 = 6 \times 91 + 2$ donc :

$$\begin{aligned} 17^{548} &= (17^6)^{91} \times 17^2 \\ &\equiv 1^{91} \times 2 \pmod{7} \\ &\equiv 2 \pmod{7} \end{aligned}$$

Ainsi, le reste de la division euclidienne de 17^{548} par 7 est égal à 2.

Exercice n°27

Remarquons que $24 \equiv 3 \pmod{7}$ car $24 = 3 \times 7 + 3$.

Ainsi, $24^1 \equiv 3^1 \equiv 3 \pmod{7}$

$$24^2 \equiv 3^2 \equiv 2 \pmod{7}$$

$$24^3 \equiv 3^3 \equiv 6 \pmod{7}$$

$$24^4 \equiv 3^4 \equiv 4 \pmod{7}$$

$$24^5 \equiv 3^5 \equiv 5 \pmod{7}$$

$$24^6 \equiv 3^6 \equiv 1 \pmod{7}$$

$$24^7 \equiv 3^7 \equiv 3 \pmod{7}$$

La boucle est bouclée pour 7 et on peut en conclure que $24^{6k+1} \equiv 3 \pmod{7}$, où $k \in \mathbb{N}$.

Ainsi, le reste de la division euclidienne de 24^n par 7 est égal à 3 pour $n \equiv 1 \pmod{6}$.

Exercice n°28

Il est assez aisé de voir :

$$\begin{aligned} x^2 &\equiv -11 \pmod{100} \iff x^2 \equiv 300 - 11 \pmod{100} \\ &\iff x^2 \equiv 289 \pmod{100} \\ &\iff x^2 \equiv 17^2 \pmod{100}. \end{aligned}$$

Ainsi, $x \equiv 17 [100]$ ou $x \equiv -17 [100]$.

Exercice n°29

1. — Initialisation : $4^0 = 1$ et $1 + 3 \times 0 = 1$ donc $4^n \equiv 1 + 3n \pmod{9}$ est vraie pour $n = 0$.

— Hérédité : supposons que pour un entier n fixé, $4^n \equiv 1 + 3n \pmod{9}$.

Alors, $4^{n+1} \equiv 4 \times (1 + 3n) \pmod{9}$, soit $4^{n+1} \equiv 4 + 12n \equiv 4 + 3n \equiv 1 + 3(n+1) \pmod{9}$.

L'hérédité est alors vérifiée.

Ainsi, pour tout entier naturel n , $4^n \equiv 1 + 3n \pmod{9}$.

$$\begin{aligned} 2. \quad 2^{2n} + 15n - 1 &\equiv 4^n + 15n - 1 \pmod{9} \\ &\equiv 1 + 3n + 15n - 1 \pmod{9} \\ &\equiv 18n \pmod{9} \\ &\equiv 0 \times n \pmod{9} \\ &\equiv 0 \pmod{9}. \end{aligned}$$

Exercice n°30

Posons :

$$\mathcal{P}_n : (n+1)(n+2) \cdots (2n-1) \times 2n \equiv 0 \pmod{2^n}.$$

Notons :

$$A_n = (n+1)(n+2) \cdots (2n-1) \times 2n.$$

Montrons par récurrence que $\mathcal{P}_n$ est vraie pour tout entier naturel n .

— Initialisation : $\mathcal{P}_0$ est vraie car $A_0 = 1$ et $2^0 = 1$.
On a donc bien $A_0 \equiv 0 \pmod{1}$.

— Supposons que pour un entier n fixé, $\mathcal{P}_n$ est vraie, donc que $A_n = 2^n B_n$.

$$A_{n+1} = 2A_n \times (2n+1)$$

$$= 2^n B_n \times 2(2n+1)$$

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

Ainsi, A_{n+1} est divisible par 2^{n+1} . L'hérédité est alors vérifiée.

Ainsi, $\mathcal{P}_n$ est vraie pour tout entier naturel n .

$$A_n = \frac{(2n)!}{n!}, \text{ donc}$$

$$\frac{A_n}{2^n} = \frac{(2n)!}{2^n(n!)} = 1 \times 3 \times 5 \times \cdots \times (2n-1).$$

Le quotient de A_n par 2^n est donc égal à $\prod_{k=0}^{n-1} (2k+1)$.

Exercice n°31

En notant :

$$x = \sum_{k=0}^n x_k \times 10^k$$

démontrer cette propriété.

Démontrer que le critère de divisibilité par 9 est semblable.

On sait que $10 \equiv 1 \pmod{3}$ donc :

$$\forall k \in \mathbb{N}, \quad 10^k \equiv 1 \pmod{3}$$

et donc :

$$\sum_{k=0}^n x_k \times 10^k \equiv \sum_{k=0}^n x_k \pmod{3}.$$

x est divisible par 3 $\iff x \equiv 0 \pmod{3}$

$$\iff \sum_{k=0}^n x_k \equiv 0 \pmod{3}$$

$\iff$ la somme des chiffres de x est divisible par 3.

$10 \equiv 1 \pmod{9}$ donc le critère de divisibilité par 9 est identique : un nombre est divisible par 9 si la somme de ses chiffres l'est aussi.

Exercice n°32

$$1. \quad 2070 = 4 \times 432 + 342 \quad 2. \quad 1065 = 4 \times 235 + 125$$

$$432 = 1 \times 342 + 90 \quad 235 = 1 \times 125 + 110$$

$$342 = 3 \times 90 + 72 \quad 125 = 1 \times 110 + 15$$

$$90 = 1 \times 72 + 18 \quad 110 = 7 \times 15 + 5$$

$$72 = 4 \times 18 + 0. \quad 15 = 3 \times 5 + 0.$$

Ainsi, $2070 \wedge 432 = 18$. Ainsi, $1065 \wedge 235 = 5$.

$$3. \quad 792 = 2 \times 363 + 66 \quad 4. \quad 910 = 1 \times 858 + 52$$

$$363 = 5 \times 66 + 33 \quad 858 = 16 \times 52 + 26$$

$$66 = 2 \times 33 + 0. \quad 52 = 2 \times 26 + 0.$$

Ainsi, $792 \wedge 363 = 33$. Ainsi, $910 \wedge 858 = 26$.

Exercice n°33

$$x \wedge y = 354 \iff \exists (x'; y') \in \mathbb{N}, x = 354x', y = 354y', x' \wedge y' = 1.$$

Ainsi,

$$x + y = 5664 \iff 354x' + 354y' = 5664 \iff x' + y' = 16.$$

On cherche donc deux entiers x' et y' premiers entre eux dont la somme vaut 16. On peut en faire la liste :

$$- (x'; y') = (1; 15)$$

$$- (x'; y') = (3; 13)$$

$$- (x'; y') = (5; 11)$$

$$- (x'; y') = (7; 9)$$

$$- (x'; y') = (9; 7)$$

$$- (x'; y') = (11; 5)$$

$$- (x'; y') = (13; 3)$$

$$- (x'; y') = (15; 1)$$

En multipliant ces valeurs par 354, on obtient tous les couples $(x; y)$:

$$- (x; y) = (354; 5310)$$

$$- (x; y) = (1062; 4602)$$

$$- (x; y) = (1770; 3894)$$

$$- (x; y) = (2478; 3186)$$

$$- (x; y) = (3186; 2478)$$

$$- (x; y) = (3894; 1770)$$

$$- (x; y) = (4602; 1062)$$

$$- (x; y) = (5310; 354)$$

Exercice n°34

1. $a \wedge b$ divise a et b , donc divise $a + b = 8n$, multiple de 8.

Par conséquent, $a \wedge b$ divise 8.

2. $n = 8k + 5$ donc :

$$- a = 3(8k + 5) + 1 = 24k + 16 = 8(3k + 2),$$

$$- b = 5(8k + 5) - 1 = 40k + 24 = 8(5k + 3).$$

Ainsi, 8 divise a et b , donc 8 divise $a \wedge b$.

Or, $a \wedge b$ divise 8 d'après la question précédente.

Par conséquent, $a \wedge b = 8$.

Exercice n°35

1. Pour $n = 0$, $3n + 7 = 7$ et $n + 2 = 2$ sont bien premiers entre eux.

Soit $n \in \mathbb{N}^*$. Nous allons chercher une combinaison linéaire de $3n + 7$ et $n + 2$ qui est égale à 1 : on regarde les termes en n et on s'aperçoit qu'en multipliant par 3 le deuxième nombre, on a :

$$(3n + 7) - 3(n + 2) = 1.$$

Il existe donc une combinaison linéaire de ces deux nombres qui est égale à 1 ; par conséquent, ils sont premiers entre eux d'après le théorème de Bézout.

2. De la même façon que dans la question précédente, on a :

$$-2(3n + 4) + 3(2n + 3) = 1.$$

Donc $3n + 4$ et $2n + 3$ sont premiers entre eux pour $n \in \mathbb{N}^*$.

Pour $n = 0$, 4 et 3 sont bien premiers entre eux.

Exercice n°36

On a :

$$n \times n - (n^2 - 1) = 1.$$

Donc il existe un couple $(u; v) = (n; -1)$ tel que $nu + (-1)(n^2 - 1) = 1$.

Ainsi, d'après le théorème de Bézout, n et $n^2 - 1$ sont premiers entre eux.

Exercice n°37

On a :

$$99 = 1 \times 56 + 43$$

$$56 = 1 \times 43 + 13$$

$$43 = 3 \times 13 + 4$$

$$13 = 3 \times 4 + 1$$

$$4 = 4 \times 1 + 0.$$

En « remontant », on a :

$$1 = 13 - 3 \times 4$$

$$= (56 - 43) - 3(43 - 3 \times 13)$$

$$= 56 - 4 \times 43 + 9 \times 13$$

$$= 56 - 4 \times (99 - 56) + 9(56 - 43)$$

$$= 14 \times 56 - 4 \times 99 - 9 \times 43$$

$$= 14 \times 56 - 4 \times 99 - 9(99 - 56)$$

$$= 23 \times 56 - 13 \times 99.$$

Il existe donc un couple $(u; v) = (-13; 23)$ tel que $99u + 56v = 1$.

Ainsi, d'après le théorème de Bézout, $99 \wedge 56 = 1$.

Exercice n°38

a est inversible modulo p

$$\iff \exists x \in \mathbb{N}^* \mid ax \equiv 1 \pmod{p}$$

$$\iff \exists (x, y) \in \mathbb{N}^* \times \mathbb{N} \mid ax = py + 1$$

$$\iff \exists (x, y) \in \mathbb{N}^* \times \mathbb{N} \mid ax - py = 1$$

$$\iff \exists (x, y) \in \mathbb{N}^* \times \mathbb{N} \mid ax + p(-y) = 1$$

$$\iff a \wedge p = 1 \text{ d'après le théorème de Bézout.}$$

Exercice n°39

1. En utilisant l'algorithme d'Euclide, on obtient :

$$693 = 1 \times 550 + 143$$

$$550 = 3 \times 143 + 121$$

$$143 = 1 \times 121 + 22$$

$$121 = 5 \times 22 + 11$$

$$22 = 2 \times 11 + 0.$$

Ainsi, $550 \wedge 693 = 11$.

2. D'après la question précédente, on obtient :

$$11 = 121 - 5 \times 22$$

$$= (550 - 3 \times 143) - 5 \times (143 - 121)$$

$$= 550 - 3 \times (693 - 550) - 5[(693 - 550)$$

$$- 550 + 3(693 - 550)]$$

$$= 550 - 3 \times 693 + 3 \times 550 - 5 \times 693 + 10 \times 550$$

$$- 15 \times 693 + 15 \times 550$$

$$= 29 \times 550 - 23 \times 693.$$

Un couple $(u; v)$ tel que $550u + 693v = 11$ est donc $(29; -23)$.

Exercice n°40

Notons $d = (bc - a) \wedge b$.

- D'après l'égalité de Bézout, il existe un couple d'entiers relatifs $(u; v)$ tel que $(bc - a)u + bv = d$.

$$(bc - a)u + bv = d \iff bcu - au + bv = d$$

$$\iff a(-u) + b(cu + v) = d$$

$-u \in \mathbb{Z}$ et $(cu + v) \in \mathbb{Z}$ donc il existe un couple d'entiers relatifs $(u'; v')$, avec $u' = -u$ et $v' = cu + v$, tel que $au' + bv' = d$.

Donc $a \wedge b$ divise d .

- De plus, $d = (bc - a) \wedge b \Rightarrow d \mid b$ et $d \mid (bc - a) \Rightarrow d \mid a$ car si $d \mid b$, alors $d \mid (bc)$ donc si $d \mid (bc - a)$, alors nécessairement, $d \mid a$.

Ainsi, $d \mid a$ et $d \mid b$ donc $d \mid a \wedge b$

Finalement, $a \wedge b \mid d$ et $d \mid a \wedge b$ donc $d = a \wedge b$.

Exercice n°41

$a \wedge b = 1$ donc il existe un couple d'entiers relatifs $(u; v)$ tel que :

$$au + bv = 1.$$

Nous allons montrer qu'il existe un couple d'entiers relatifs $(u'; v')$ tel que :

$$(3a + 5b)u' + (a + 2b)v' = 1.$$

$$\begin{aligned}(3a + 5b)u' + (a + 2b)v' &= 3au' + 5bu' + av' + 2bv' \\ &= a(3u' + v') + b(5u' + 2v').\end{aligned}$$

Pouvons-nous choisir u' et v' de sorte que
$$\begin{cases} 3u' + v' = u & (L_1) \\ 5u' + 2v' = v & (L_2) \end{cases} ?$$

Pour répondre à cette question, cherchons à résoudre ce dernier système.

En faisant $2(L_1) - (L_2)$, on obtient :

$$u' = 2u - v$$

et en faisant $-5(L_1) + 3(L_2)$, on obtient :

$$v' = -5u + 3v.$$

En prenant ces valeurs de u' et v' , on a $(3a + 5b)u' + (a + 2b)v' = au + bv = 1$.

Ainsi, d'après le théorème de Bézout, $3a + 5b \wedge a + 2b = 1$.

Exercice n°42

1. $31 = 1 \times 28 + 3$
 $28 = 9 \times 3 + 1$
 $3 = 3 \times 1 + 0$
Donc $31 \wedge 28 = 1$.

De l'algorithme précédent, on peut écrire :

$$\begin{aligned}1 &= 28 - 9 \times 3 \\ &= 28 - 9 \times (31 - 28) \\ &= 10 \times 28 - 9 \times 31\end{aligned}$$

Ainsi, si $x = -9$ et $y = -10$, $31x - 28y = 1$.

2. On a :

$$\begin{array}{rclcl} 31 \times & (-9) & - 28 \times & (-10) & = 1 \\ 31 \times & x & - 28 \times & y & = 1 \\ \hline 31 \times & (-9 - x) & - 28 \times & (-10 - y) & = 0 \end{array}$$

Ainsi :

$$31(-9 - x) = 28(-10 - y).$$

Or, $31 \wedge 28 = 1$ donc d'après le théorème de Gauss, 31 divise $(-10 - y)$ et 28 divise $(-9 - x)$:

$$\begin{cases} -9 - x &= 28k \\ -10 - y &= 31k \end{cases}, \quad k \in \mathbb{Z}$$

soit :

$$\begin{cases} x &= -9 - 28k \\ y &= -10 - 31k \end{cases}, \quad k \in \mathbb{Z}$$

Exercice n°43

— En utilisant l'algorithme d'Euclide, on obtient :

$$108 = 1 \times 55 + 53$$

$$55 = 1 \times 53 + 2$$

$$53 = 26 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

Donc, $PGCM(108; 55) = 1$.

De l'algorithme précédent, on peut écrire :

$$\begin{aligned}1 &= 53 - 26 \times 2 \\ &= (108 - 55) - 26 \times (55 - 53) \\ &= 108 - 55 - 26 \times 55 + 26 \times 53 \\ &= 108 - 27 \times 55 + 26(108 - 55) \\ &= 27 \times 108 - 53 \times 55\end{aligned}$$

Ainsi, $x_0 = 27$ et $y_0 = -53$ sont deux solutions particulières de l'équation diophantienne $108x + 55y = 1$.

— On a :

$$\begin{cases} 108 \times 27 + 55 \times (-53) &= 1 \\ 108 \times x + 55 \times y &= 1 \end{cases}$$

Donc, $108 \times (27 - x) + 55 \times (-53 - y) = 0$.

Ainsi,

$$108(27 - x) = 55(53 + y).$$

Or, $PGCD(108; 55) = 1$ donc d'après le théorème de Gauss, 108 divise $(53 + y)$ et 55 divise $(27 - x)$:

$$\begin{cases} 27 - x &= 55k \\ 53 + y &= 108k \end{cases}, \quad k \in \mathbb{Z}$$

soit,

$$\begin{cases} x &= 27 - 55k \\ y &= -53 + 108k \end{cases}, \quad k \in \mathbb{Z}.$$

Exercice n°44

Rappelons que si p est un nombre premier, alors il n'admet aucun diviseurs inférieurs à $\sqrt{p}$.

Or, $\sqrt{1789} \approx 42,3$.

Les nombres premiers inférieurs à 42 sont :

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

On vérifie que aucun d'entre eux ne divisent 1789. Par conséquent, 1789 est un nombre premier.

Exercice n°45

- La liste des nombres premiers inférieurs à 50 est :
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

- $\sqrt{1517} \approx 38,95$.

On teste sous python, si les nombres premiers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 divisent 1517.

```
>>> L = [2,3,5,7,11,13,17,19,23,29,31,37]
>>> for i in L:
    if 1517%i == 0: print(i)
37
```

On trouve que 37 divise 1517 donc 1517 n'est pas premier.

- $a^2 = b^2 + 1517$

$$\iff a^2 - b^2 = 1517$$

$$\iff (a - b)(a + b) = 37 \times 41$$

$$\iff \begin{cases} a - b = 37 \\ a + b = 41 \end{cases} \quad \text{ou} \quad \begin{cases} a - b = 1 \\ a + b = 1517 \end{cases}$$

$$\iff a = 39 \text{ et } b = 2 \text{ ou } a = 759 \text{ et } b = 758.$$

Ainsi, les deux couples $(a; b) \in \mathbb{N}^2$ tel que $a^2 = b^2 + 1517$ sont $(39; 2)$ et $(759; 758)$.

Exercice n°46

On a :

$$n^3 - 27 = n^3 - 3^3 = (n - 3)(n^2 + 3n + 9).$$

Ainsi,

$$n^3 - 27 \in \mathbb{P} \iff n - 3 = 1 \text{ ou } n^2 + 3n + 9 = 1.$$

Or, $n^2 + 3n + 9 \neq 1$. Donc, $n = 4$.

Exercice n°47

- Rappelons que a et b sont distincts modulo 3 si et seulement si $(a - b)$ n'est pas un multiple de 3.
 $n - (n + 2) = -2$ n'est pas un multiple de 3, donc n n'est pas congru à $n + 2$ modulo 3.
 $n - (n + 10) = -10$ et donc on aboutit à la même conclusion.

$(n + 2) - (n + 10) = -8$ et donc on aboutit à la même conclusion.

Ainsi, n , $n + 2$ et $n + 10$ sont distincts modulo 3.

- Notons $n \equiv r_1 \pmod{3}$, $n + 2 \equiv r_2 \pmod{3}$ et $n + 10 \equiv r_3 \pmod{3}$.

D'après la question précédente, r_1 , r_2 et r_3 sont deux à deux distincts. Or, il n'existe que 3 restes possibles dans la division euclidienne par 3 : 0, 1 ou 2.

Par conséquent, l'un des restes est nul et donc, l'un des nombres n , $n + 2$ et $n + 10$ est divisible par 3. Ce nombre n'est donc pas premier car il ne peut pas être égal à 3 (par hypothèse : $n > 3$).

Exercice n°48

On rappelle que la factorielle de n est le nombre :

$$n! = 2 \times 3 \times 4 \times \dots \times n.$$

- Entre 2^k et 2^{k+1} (non compris), il y a $2^{k+1} - 2^k - 2 = 2^k(2 - 1) - 2$ nombres. Le nombre avant 2^{k+1} étant nécessairement pair, on peut alors dire qu'il y a :

$$\frac{2^k - 2}{2} = 2^{k-1} - 1$$

nombres pairs, pour $k \in \mathbb{N}^*$.

- $(2^4)! = 2^1 \times 3 \times 2^2 \times 5 \times 6 \times 7 \times 2^3 \times \dots \times 2^4$.

Dans cette décomposition, il y a d'une part toutes les puissances de 2, mais aussi les nombres pairs entre ces puissances, nombres qui peuvent s'écrire sous la forme $q \times 2^p$, $p \geq 1$.

— Entre 2^2 et 2^3 , il y a 1 multiple de 2 : $6 = 2 \times 3$.

— Entre 2^3 et 2^4 , il y a 3 multiples de 2 : $10 = 2 \times 5$, $12 = 2^2 \times 3$ et $14 = 2 \times 7$.

Finalement, l'exposant de 2 dans la décomposition de $(2^4)!$ le plus grand est :

$$(1 + 2 + 3 + 4) + 1 + 1 + 2 + 1 = 15.$$

- Voici un programme possible :

```
def fact(n):
    f = 1
    for i in range(1, n+1):
        f = f * i

    return f
```

```
def maxpow(n):
    N = fact(2**n)
    p = 0
    while N%2 == 0:
        p = p+1
        N = N//2
```

```
    return p
```

Ces fonctions ont tout de même leur limite (surtout $n!$). En effet, à partir de $n = 15$, cette dernière fonction est longue pour renvoyer le résultat. On peut tout de même contrôler que 2^{65535} est la plus grande puissance de 2 qui divise $(2^{16})!$.

Exercice n°49

Soit p un nombre premier différent de 3.

Pour tout entier naturel n ,

$$3^{n+p} - 3^{n+1} \text{ est divisible par } p$$

$$\iff 3^{n+p} - 3^{n+1} \equiv 0 \pmod{p}$$

$$\iff 3^{n+p} \equiv 3^{n+1} \pmod{p}$$

$$\iff 3^n \times 3^p \equiv 3^n \times 3 \pmod{p}$$

$$\iff 3^p \equiv 3 \pmod{p} \quad \text{car } p \neq 3.$$

Cette dernière congruence est vraie d'après le petit théorème de Fermat (car p est premier et p ne divise pas 3).
Par conséquent, pour tout entier naturel n , $3^{n+p} - 3^{n+1}$ est divisible par p .

Exercice n°50

Soient p un nombre premier, n un entier naturel et a non divisible par p .

- Montrons ce résultat par l'absurde. Supposons qu'il existe deux restes égaux r et r' et notons pour $k \in \llbracket 0; p-1 \rrbracket$ et $k' \in \llbracket 0; p-1 \rrbracket$ différent de k :

$$\begin{aligned} ka &= pq + r & q \in \mathbb{Z}, 0 \leq r < p \\ k'a &= pq' + r & q' \in \mathbb{Z}, 0 \leq r < p \end{aligned}$$

Ainsi, par différence :

$$(k - k')a = (q - q')p.$$

p divise donc $(k - k')a$.

Or, $(k - k') < p$ donc p ne peut pas diviser $(k - k')$ et donc p divise a , ce qui est contradictoire avec nos hypothèses.

Par conséquent, il ne peut pas exister deux restes égaux dans la division euclidienne par p de $a, 2a, \dots, (p-1)a$.

- D'après ce qui précède :

$$\begin{aligned} a &\equiv r_1 \pmod{p} \\ 2a &\equiv r_2 \pmod{p} \\ &\vdots \\ (p-1)a &\equiv r_{p-1} \pmod{p} \end{aligned}$$

D'où, par produit :

$$(p-1)!a^{p-1} \equiv r_1 r_2 \cdots r_{p-1} \pmod{p}.$$

Comme les r_i sont tous distincts, $r_1 r_2 \cdots r_{p-1} = (p-1)!$ et comme $\text{PGCD}(p; (p-1)!) = 1$, on peut diviser chacun des membres de la congruence par $(p-1)!$, ce qui donne :

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

- Pour tout entier a tel que $\text{PGCD}(a; 561) = 1$, il existe un couple d'entiers relatifs $(u; v)$ tel que $au + 561v = 1$, soit tel que $au \equiv 1 \pmod{561}$.

On utilise 3 fois le petit théorème de Fermat :

$$\begin{cases} u^2 \equiv 1 \pmod{3} \iff u^{560} \equiv 1 \pmod{3} \\ u^{10} \equiv 1 \pmod{11} \iff u^{560} \equiv 1 \pmod{11} \\ u^{16} \equiv 1 \pmod{17} \iff u^{560} \equiv 1 \pmod{17} \end{cases}$$

D'où :

$$u^{560} \equiv r \pmod{561} \quad \text{avec} \quad r \equiv 1 \pmod{3}, r \equiv 1 \pmod{11}, r \equiv 1 \pmod{17}.$$

On a alors :

$$r = 3k + 1 = 11k' + 1 = 17k'' + 1,$$

soit :

$$3k = 11k' = 17k''.$$

Ainsi, 11 divise k et 17 divise k' , soit $k = 11m$ et $k' = 17m'$.

Alors,

$$r = 3 \times 11m + 1 = 11 \times 17m' + 1$$

soit :

$$3 \times 11m = 11 \times 17m'$$

et donc $3m = 17m'$. Ainsi, 17 divise m et on peut écrire $m = 17\lambda$.

On arrive ainsi à : $r = 3 \times 11 \times 17\lambda + 1$, soit $r \equiv 1 \pmod{561}$ et donc $u^{560} \equiv 1 \pmod{561}$.

Or, nous avons vu que $au \equiv 1 \pmod{561}$ donc $(au)^{560} \equiv 1 \pmod{561}$.

Comme $u^{560} \equiv 1 \pmod{561}$, cela nous donne : $a^{560} \equiv 1 \pmod{561}$, où 561 n'est pas un nombre premier.

Ceci prouve que la réciproque du petit théorème de Fermat est fausse.