Arithmétique

exercices

Divisibilité et pgcd

101 Racines n-èmes de l'unité

Soit $(m,n) \in (\mathbb{N}^*)^2$. Montrer $\mathbb{U}_m \subset \mathbb{U}_n \iff m \mid n$.

102 Un classique

Soit $n \in \mathbb{N}$.

1. Montrer qu'il existe un unique couple $(a_n, b_n) \in \mathbb{N}^2$ tel que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$.
2. Calculer $a_n^2 - 2b_n^2$.
3. En déduire que a_n et b_n sont premiers entre eux.

Binôme de Newton

103 Un pgcd

Montrer que le pgcd de $2n+4$ et $3n+3$ ne peut être que 1, 2, 3 ou 6.

104 Sierpiński 1

Trouver tous les entiers $n \geqslant 1$ tels que n^2+1 est divisible par $n+1$.

105 Critère de divisibilité

Déterminer les entiers n tels que $n-3$ divise n^3-3.

106 Sierpiński 41

Soit $k \in \mathbb{N}$. *Les deux questions sont indépendantes.*

1. Montrer que $2k+1$ et $9k+4$ sont premiers entre eux.
2. Exprimer $\text{pgcd}(9k+4, 2k-1)$ en fonction de k.

107 Sierpiński 14

Montrer que pour tout $n \geqslant 1$, l'entier n^2 divise $(n+1)^n - 1$.

108 Somme et produit de nombres premiers entre eux

Soit a et b deux nombres premiers entre eux. Montrer que l'on a $a \wedge (a+b) = b \wedge (a+b) = 1$.
Sans preuve, dire ce que l'on peut en déduire sur $a+b$ et ab.

109 Type de $\sqrt{n}$

1. Soit $(a,b) \in \mathbb{N}^2$. Montrer $a \mid b \iff a^2 \mid b^2$.
2. Soit $n \in \mathbb{N}$. Montrer que $\sqrt{n}$ est entier ou irrationnel.

110 Division euclidienne sur $\mathbb{Z}$

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ un entier *relatif non nul*. En s'appuyant sur la division euclidienne du cours, montrer qu'il *existe* un couple $(q,r) \in \mathbb{Z}^2$ tel que $\begin{cases} a = bq + r \\ 0 \leqslant r < |b|. \end{cases}$

On peut montrer que ce couple est nécessairement unique.

Écrire les quatre divisions euclidiennes suivantes : de 17 par 5, puis par -5 ; de -17 par 5, puis par -5.

111 Nombre de Fermat et pgcd

Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$.

1. Montrer que $\forall n \in \mathbb{N}^*,\ F_n = 2 + \prod_{k=0}^{n-1} F_k$.
2. Montrer que, si $n \neq m$, alors F_n et F_m sont premiers entre eux.

112 Nombres de Mersenne

Soit $n \geqslant 2$.

1. On suppose que $2^n - 1$ est premier. Montrer que n est premier.
2. Que constate-t-on si l'on prend $n = 11$? Conclusion ?

Les nombres premiers de la forme $2^p - 1$ sont les *nombres de Mersenne*.

113 Nombres de Fermat premiers

Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit premier.
Montrer que m est une puissance de 2.

114 Pgcd en mode « vache qui rit »

1. Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. On note r le reste de la division euclidienne de a par b.
   Montrer que $2^r - 1$ est le reste de la division euclidienne de $2^a - 1$ par $2^b - 1$.
2. En déduire $\forall a, b \in \mathbb{N},\ (2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1$.

115 Suite de Fibonacci

Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci, c'est-à-dire la suite définie par $\begin{cases} F_0 = 0 \\ F_1 = 1 \\ \forall n \in \mathbb{N},\ F_{n+2} = F_{n+1} + F_n \end{cases}$

1. Montrer $\forall n \in \mathbb{N}^*,\ F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.
2. En déduire $\forall n \in \mathbb{N},\ F_n \wedge F_{n+1} = 1$.
3. Montrer $\forall n \in \mathbb{N},\ \forall m \in \mathbb{N}^*,\ F_{m+n} = F_m F_{n+1} + F_{m-1}F_n$.
4. En déduire $\forall n, m \in \mathbb{N},\ F_n \wedge F_{m+n} = F_n \wedge F_m$. On aura sûrement besoin du lemme de Gauss.
5. En déduire $\forall a \in \mathbb{N},\ \forall b \in \mathbb{N}^*,\ F_a \wedge F_b = F_b \wedge F_r$ où r est le reste de la division euclidienne de a par b.
6. Montrer $\forall m, n \in \mathbb{N},\ F_m \wedge F_n = F_{m\wedge n}$.

Autour de Bézout

116 Preuve de Bézout et Gauss

1. Montrer le théorème de Bézout :

   Pour tout $a, b \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$.

   Commencer par le cas $b \in \mathbb{N}$ en considérant $\mathcal{H}_b$ la propriété « Pour tout $a \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = \text{pgcd}(a, b)$ ».
2. En déduire le lemme de Gauss :

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

   $$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c$$

117 Équation diophantienne

Dans cette exercice, on pourra (devra ?) faire appel à Bézout et Gauss.

1. Soit $a, b, d \in \mathbb{Z}$. Montrer l'équivalence

   $$\Big(\exists\, u, v \in \mathbb{Z},\ au + bv = d\Big) \iff \text{pgcd}(a, b) \mid d$$

2. Soit $a, b \in \mathbb{N}^*$ premiers entre eux.
   On souhaite résoudre l'équation $au + bv = 1$ d'inconnue $(u, v) \in \mathbb{Z}^2$.
   Justifier l'existence d'un couple solution (u_0, v_0).
   Montrer que toute solution est de la forme $(u_0 - kv, v_0 + ku)$ où $k \in \mathbb{Z}$, puis conclure.
3. Soit $a, b \in \mathbb{N}^*$ et $\delta = \text{pgcd}(a, b)$.
   Soit $d \in \mathbb{Z}$. On souhaite résoudre l'équation $au + bv = d$ d'inconnue $(u, v) \in \mathbb{Z}^2$.
   À l'aide des deux questions précédentes, résoudre cette équation.

Quelques équations avec pgcd et ppcm

118 Homogénéité du pgcd/ppcm

1. Soit $a, b \in \mathbb{N}^*$ et $c \in \mathbb{N}^*$. À l'aide de la DFP, prouver les formules

$$\text{pgcd}(ca, cb) = c\ \text{pgcd}(a, b) \qquad \text{et} \qquad \text{ppcm}(ca, cb) = c\ \text{ppcm}(a, b)$$

   Ce résultat est même vrai pour $a, b \in \mathbb{Z}$.

2. Retrouver le résultat suivant :

   Soit $a, b \in \mathbb{N}$ et $d = a \wedge b$.
   Alors il existe a', b' premiers entre eux tels que $a = da'$ et $b = db'$.
   Et on a l'égalité $a \vee b = da'b'$.

119 Système avec pgcd et ppcm

Résoudre dans $\mathbb{N}^2$ les systèmes suivants.

1. $\begin{cases} \text{pgcd}(x, y) &= 18 \\ \text{ppcm}(x, y) &= 540. \end{cases}$ 2. $\begin{cases} \text{pgcd}(x, y) &= 3 \\ x + y &= 21. \end{cases}$

120 Une équation

Résoudre dans $\mathbb{N}^2$ l'équation $\text{pgcd}(x, y) + \text{ppcm}(x, y) = x + y$.

On aura sûrement besoin d'exploiter l'exercice « Homogénéité du pgcd/ppcm ».

121 CNS

Soit $m, d \in \mathbb{N}^*$.

Déterminer une condition nécessaire et suffisante sur d et m pour que le système $\begin{cases} \text{pgcd}(x, y) &= d \\ \text{ppcm}(x, y) &= m \end{cases}$ possède une solution.

On aura sûrement besoin d'exploiter l'exercice « Homogénéité du pgcd/ppcm ».

Autres

122 Nombres premiers congrus à 3 modulo 4

Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 3$.

Considérer $N = 4n - 1$ avec n bien choisi.

123 Petit théorème de Fermat

Soit p un nombre premier.

1. Montrer que pour tout $k \in [\![1, p-1]\!]$, l'entier p divise $\binom{p}{k}$.
2. En déduire que pour tout $(x, y) \in \mathbb{N}^2$, l'entier p divise $(x + y)^p - (x^p + y^p)$.
3. En déduire que pour tout $a \in \mathbb{N}$, l'entier p divise $a^p - a$.
4. En déduire que si l'entier a n'est pas un multiple de p, le reste de la division euclidienne de a^{p-1} par p est 1.

124 Infinitude de l'ensembles des nombres premiers

Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un nombre premier compris entre $(n + 1)$ et $n! + 1$.
En déduire une nouvelle preuve de l'existence d'une infinité de nombre premiers.

125 Critère de divisibilité par 7

Soit $n \in \mathbb{N}$. On note d son nombre de dizaines et u son chiffre des unités, c'est-à-dire $n = 10d + u$.
Montrer que n est divisible par 7 si et seulement si $d - 2u$ est divisible par 7.
413 est-il divisible par 7 ? 123 456 est-il divisible par 7 ?

Des petits défis pour les curieux !

126 Des trous arbitrairement grands dans les nombres premiers

Montrer qu'il existe 2023 entiers naturels consécutifs parmi lesquels ne figure aucun nombre premier.

127 Multiples de 164

Combien de nombres à 6 chiffres sont multiples de 164 et se terminent par 164 ?

128 Sierpiński 47

Montrer que tout entier $n \geqslant 7$ est la somme de deux entiers $\geqslant 2$ premiers entre eux.

Indication. Disjonction de cas en fonction du reste de la division euclidienne de n par 4.

129 Sierpiński 75

Trouver tous les nombres premiers qui sont à la fois la somme et la différence de deux nombres premiers.

130 Produit de trois entiers consécutifs

Soit $n \geqslant 2$. Montrer que le produit de trois entiers $\geqslant 1$ consécutifs n'est jamais une puissance n-ième.

131 Sierpiński 44 et 46

1. Soit a et b deux entiers différents. Montrer qu'il existe une infinité de $n \geqslant 1$ tels que $a+n$ et $b+n$ soient premiers entre eux.
2. Trouver quatre entiers différents a, b, c et d tels que $a+n$, $b+n$, $c+n$ et $d+n$ ne soient deux à deux premiers entre eux pour aucun $n \geqslant 1$.

132 Pas d'anagrammes dans les puissances de 2

On dira que deux nombres sont des *anagrammes* si l'on peut passer de l'écriture décimale de l'un à celle de l'autre en permutant les chiffes significatifs. Par exemple, 169 et 196 sont deux carrés parfaits anagrammes l'un de l'autre.
Une puissance de 2 peut-elle être l'anagramme d'une autre puissance de 2 ?

133 $1+3^n+3^m$ n'est pas un carré parfait

Soit $n, m \in \mathbb{N}$. Montrer que $1+3^n+3^m$ n'est pas un carré parfait.

À quoi est congru un carré modulo 8 ?

134 Deux nombres premiers

Déterminer les couples (p, q) de nombres premiers tels que $p+q = (p-q)^3$.

Arithmétique

corrigés

101

Dans cet exercice, il faut plutôt utiliser la définition de $\mathbb{U}_n$ (à gauche ci-dessous) et sa caractérisation *faible* (à droite)

$$\mathbb{U}_n = \left\{z \in \mathbb{C} \mid z^n = 1\right\} \qquad \text{et} \qquad \mathbb{U}_n = \left\{\mathrm{e}^{\mathrm{i}\frac{2k\pi}{n}},\ k \in \mathbb{Z}\right\}$$

Disons qu'il ne faut pas *abuser* de sa caractérisation *forte* :

$$\mathbb{U}_n = \left\{\mathrm{e}^{\mathrm{i}\frac{2k\pi}{n}},\ k \in [\![0, n-1]\!]\right\}$$

On a les équivalences suivantes :

$$\begin{aligned}
\mathbb{U}_m \subset \mathbb{U}_n &\iff \forall\, z \in \mathbb{U}_m,\ z^n = 1 \\
&\iff \forall\, k \in \mathbb{Z},\ \left(\mathrm{e}^{\mathrm{i}\frac{2k\pi}{m}}\right)^n = 1 \\
&\iff \forall\, k \in \mathbb{Z},\ 2k\pi\tfrac{n}{m} \equiv 0\ [2\pi] \qquad \text{congruence réelle} \\
&\iff \forall\, k \in \mathbb{Z},\ kn \equiv 0\ [m] \qquad \text{congruence entière} \\
&\iff \forall\, k \in \mathbb{Z},\ m \mid kn \\
&\overset{\text{WHY}}{\iff} m \mid n
\end{aligned}$$

103

Soit $d \in \mathcal{D}(2n+4, 3n+3)$.
Alors d divise $3(2n+4) - 2(3n+3) = 6$.
Ainsi, $\mathcal{D}(2n+4, 3n+3) \subset \{\pm 1, \pm 2, \pm 3, \pm 6\}$.
On conclut en remarquant que le pgcd appartient à $\mathcal{D}(2n+4, 3n+3) \cap \mathbb{N}$.

104

Soit $n \geqslant 1$. On a

$$n^2 + 1 = (n+1)(n-1) + 2,$$

On a donc les équivalences suivantes

$$n+1 \mid n^2+1 \iff n+1 \mid 2$$

Comme $n+1 \geqslant 2$, on a $n+1 \mid 2 \iff n+1 = 2 \iff n = 1$.
Bilan : $\{n \geqslant 1 \text{ tel que } n+1 \mid n^2+1\} = \{1\}$.

105

Soit $n \geqslant 3$. On a

$$n^3 - 3 = (n-3)(n^2+3n+9) + 24$$

d'où l'équivalence

$$n-3 \mid n^3-3 \iff n-3 \mid 24 \iff n \in (\mathcal{D}(24)+3) \cap \mathbb{N} = \{0,2,4,6,7,9,11,15,27\}$$

106

1. Appliquons l'algorithme d'Euclide :

$$\begin{aligned} 9k+4 &= 4\times(2k+1)+k \\ 2k+1 &= 2\times k+1, \end{aligned}$$

donc $9k+4$ et $2k+1$ sont premiers entre eux.
Autre preuve (très similaire). Soit $d \in \mathcal{D}(9k+4)\cap\mathcal{D}(2k+1)$.
Alors d divise toute combinaison $\mathbb{Z}$-linéaire de ces deux nombres, par exemple :

$$d \mid (9k+4)-4(2k+1) = k$$

Donc $d \mid 2k$. Or $d \mid 2k+1$. Donc $d \mid 1$.

2. Calculons $\operatorname{pgcd}(9k+4, 2k-1)$.
Ecrivons des égalités du type $a = bq+r$ (qui ne sont pas nécessairement des divisions euclidiennes, car on ne contrôle pas le reste) :

$$\begin{aligned} 9k+4 &= 4\times(2k-1)+k+8 \\ 2k-1 &= 2\times(k+8)-17, \end{aligned}$$

donc

$$\operatorname{pgcd}(9k+4,2k-1) = \operatorname{pgcd}(2k-1,k+8) = \operatorname{pgcd}(k+8,-17) = \begin{cases} 17 & \text{si } 17 \mid k+8 \\ 1 & \text{sinon} \end{cases}$$

Pour info, la condition $17 \mid k+8$ s'écrit $k \in \{17q-8, q \geqslant 1\}$.

107

Fixons $n \geqslant 1$. On a

$$\begin{aligned}(n+1)^n - 1 &= \sum_{k=0}^{n} \binom{n}{k} n^k - 1 \\ &= \binom{n}{1} \times n + \sum_{k=2}^{n} \binom{n}{k} n^k \\ &= n^2 + \sum_{k=2}^{n} \binom{n}{k} n^k \\ &= n^2 + n^2 \sum_{k=2}^{n} \binom{n}{k} n^{k-2} \\ &= n^2 \left(1 + \sum_{j=0}^{n-2} \binom{n}{j+2} n^j\right)\end{aligned}$$

Donc n^2 divise $(n+1)^n - 1$.

108

Soit d divisant a et $a+b$.
Alors d divise $(a+b)-a=b$.
Comme $a \wedge b = 1$, on en déduit que $d \mid 1$.
Bilan $a \wedge (a+b) = 1$.

De la même façon, on a $b \wedge (a+b) = 1$.

L'entier $a+b$ est premier avec a et avec b, donc il est premier avec leur produit ab :

$$(a+b) \wedge ab = 1$$

109

1. C'est fait dans le cours.
   Pour le sens difficile utiliser la décomposition en facteurs premiers.
2. On rappelle qu'un réel est ou bien rationnel, ou bien irrationnel.
   Pour prouver que $\sqrt{n}$ est entier ou irrationnel, il suffit donc de le supposer rationnel et de montrer qu'il est en fait un entier.
   Supposons donc que $\sqrt{n} \in \mathbb{Q}$. Alors il existe $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $\sqrt{n} = \frac{p}{q}$.
   En élevant au carré, et en chassant le dénominateur, on a $q^2 n = p^2$.
   Ainsi, $q^2 \mid p^2$. D'après la question précédente, on obtient $q \mid p$, donc $\sqrt{n}$ est un entier (WHY ?).

110

La division de -17 par 5 donne $-17 = 5 \times (-4) + 3$, soit un quotient de -4 et un reste de 3.
La division de 17 par -5 donne $17 = (-5) \times (-3) + 2$, soit un quotient de -3 et un reste de 2.
La division de -17 par -5 donne $-17 = (-5) \times 4 + 3$, soit un quotient de 4 et un reste de 3.

111

1. On démontre le résultat par récurrence sur n.

   Initialisation. On a $F_1 = 5 = 2 + F_0$.

   Hérédité. Soit $n \in \mathbb{N}^*$ tel que $F_n = 2 + \prod_{k=0}^{n-1} F_k$.

   On calcule, en observant que $F_{n+1} = 2^{2^{n+1}} + 1 = \left(2^{2^n}\right)^2 + 1 = (F_n - 1)^2 + 1$:

   $$\begin{aligned} 2 + \prod_{k=0}^{n} F_k &= 2 + (F_n - 2)F_n && \text{(hypothèse de récurrence)} \\ &= 2 + F_n^2 - 2F_n \\ &= 1 + (F_n - 1)^2 \\ &= F_{n+1}. \end{aligned}$$

2. Sans perte de généralités, on peut supposer $m < n$.
   Soit d un diviseur commun à F_n et F_m.
   D'une part, d divise F_n.
   D'autre part, d divise F_m, donc divise le produit $F_0F_1 \cdots F_{n-1}$.
   Donc d divise la différence $F_n - F_0F_1 \cdots F_{n-1}$, qui vaut 2, d'après la question précédente.
   D'une part, d divise $F_n = 2^{2^n} + 1$ et d'autre part, d divise 2 donc 2^{2^n}, donc d divise la différence à savoir 1.
   Bilan : $F_n \wedge F_m = 1$.

   Autre fin de preuve. Reprenons à $d \mid 2$.
   Alors $d = \pm 1$ ou $d = \pm 2$.
   N'oublions pas que d divise F_n qui est un nombre impair.
   Donc d ne peut pas être égal à ± 2.
   Donc $d = \pm 1$, ce qui montre que $F_n \wedge F_m = 1$.

Remarque pour la culture. Chaque F_n admet (au moins) un diviseur premier p_n. Comme les F_n sont premiers entre eux, les p_n sont deux à deux distincts. Cela prouve (une nouvelle fois) le caractère infini de l'ensemble des nombres premiers.

112

1. Soit d un diviseur positif de n.
   Alors il existe $p \in \mathbb{N}^*$ tel que $n = dp$ et :
   $$2^{pd} - 1 = (2^d)^p - 1^p = (2^d - 1)(1 + 2^d + 2^{2d} + \cdots + 2^{(p-1)d}).$$
   L'entier $2^d - 1$ divise $2^n - 1$.
   Comme $2^n - 1$ est supposé premier, on en déduit $2^d - 1 \in \{1,\, 2^n - 1\}$.
   D'où $d = 1$ ou $d = n$.
2. On s'aperçoit que $2^{11} - 1 = 2047 = 23 \times 89$ n'est pas un nombre premier.
   La réciproque de la question précédente est donc fausse.

113

Écrivons m sous la forme $m = 2^a q$ avec $a \in \mathbb{N}$ et $q \in \mathbb{N}$ impair.
Posons $d = 2^a$ de sorte que $m = dq$. Montrons que $m = d$.
Comme q est impair, 1 s'écrit $-(-1)^q$. D'après la formule de Bernoulli, on a donc :

$$2^m + 1 \;=\; (2^d)^q - (-1)^q \;=\; (2^d + 1)(2^{d(q-1)} - 2^{d(q-2)} + \cdots + 1)$$

Or $2^d + 1 \geqslant 2$. Comme $2^m + 1$ est premier par hypothèse, on en déduit $2^m + 1 = 2^d + 1$.
D'où $m = d$.

Un nombre de la forme $F_n = 2^n + 1$ est appelé un nombre de Fermat. Actuellement (2023), les seuls nombres de Fermat premiers qui sont connus sont $3, 5, 17, 257$ et 65537 (ils correspondent à $F_0, \ldots, F_4$).
Le $5^{\text{ème}}$ nombre de Fermat est $F_5 = 4294967297$ et se factorise 641×6700417.

1. Par définition, on a $a = bq + r$ avec $r \in [\![0, b[\![$.
   Contemplons l'égalité merveilleuse suivante :
   $$2^a - 1 \;=\; (2^{bq} - 1)2^r \;+\; (2^r - 1)$$
   que l'on peut obtenir en disant
   $$2^a - 1 \;=\; 2^{bq}2^r - 1 \;=\; {\scriptstyle \text{(il n'y a plus le choix)}} \;+\; (2^r - 1)$$
   et du coup
   $${\scriptstyle \text{(il n'y a plus le choix)}} \quad \text{vaut} \quad (2^{bq}2^r - 1) - (2^r - 1) \qquad \text{c'est-à-dire } 2^r(2^{bq} - 1)$$
   Bref, revenons à l'égalité merveilleuse. D'après la formule de Bernoulli, il existe un entier c (que l'on peut déterminer explicitement) tel que
   $$2^{bq} - 1 = (2^b - 1)c$$
   Pour information, mais cela ne sera pas utilisé, on a $c = \sum_{k=0}^{q-1} (2^b)^k$.
   On a donc
   $$2^a - 1 \;=\; (2^b - 1)\, c\, 2^r \;+\; (2^r - 1)$$
   qui est du type $2^a - 1 = (2^b - 1) \times \text{truc} + (2^r - 1)$.
   Pour conclure, il reste à montrer que $2^r - 1 \in [\![0,\, 2^b - 1[\![$. À vous.
2. Montrons $\forall\, a, b \in \mathbb{N},\ (2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1$.
   Faisons une preuve par récurrence sur b.
   Pour tout $b \in \mathbb{N}$, notons $\mathcal{H}_b$ l'assertion
   $$\mathcal{H}_b : \quad \text{« } \forall\, a \in \mathbb{N},\ (2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1 \text{ »}$$
   Initialisation. Montrons $\mathcal{H}_0$. Pour cela, fixons $a \in \mathbb{N}$.
   Le membre gauche vaut $(2^a - 1) \wedge (2^0 - 1) = (2^a - 1) \wedge 0 = 0$.
   Le membre droit vaut $2^{a \wedge 0} - 1 = 2^0 - 1 = 0$.
   D'où $\mathcal{H}_0$.
   Hérédité.
   Soit $b \in \mathbb{N}^*$ tel que $\mathcal{H}_0, \ldots, \mathcal{H}_{b-1}$.
   Montrons $\mathcal{H}_b$.
   • Comme $b \neq 0$, on peut effectuer la division euclidienne de a par b :
   $$a = bq + r \quad \text{avec } 0 \leqslant r < b$$
   D'après le lemme de la PCSI (qui n'utilise pas la condition sur r), on a $\boxed{a \wedge b = b \wedge r}$.
   • D'autre part, la question 1 montre que l'on a l'égalité (j'oublie la condition sur le reste, car on ne l'utilise pas dans le lemme de la PCSI)
   $$2^a - 1 \;=\; (2^b - 1) \times \text{truc} \;+\; (2^r - 1)$$
   D'après le lemme de la PCSI (appliqué à quels entiers au fait ?), on a
   $$\boxed{(2^a - 1) \wedge (2^b - 1) \;=\; (2^b - 1) \wedge (2^r - 1)}$$
   • Utilisons à présent l'hypothèse de récurrence. Comme $r \in [\![0, b - 1[\![$, on sait que $\mathcal{H}_r$ est vraie. Ainsi (en particularisant, dans la $\forall$-assertion, à b) :
   $$\boxed{(2^b - 1) \wedge (2^r - 1) = 2^{b \wedge r} - 1}$$
   Maintenant, il suffit « d'agiter » les trois encadrés. Plus précisément, partons du dernier encadré, et utilisons les deux précédents. On obtient :
   $$(2^a - 1) \wedge (2^b - 1) \;=\; 2^{a \wedge b} - 1$$
   D'où $\mathcal{H}_b$.

1. Par récurrence **simple** sur $n \in \mathbb{N}^*$.
   Lors de l'hérédité, on fixe $n \in \mathbb{N}^*$ tel que $\mathcal{H}_n$. On a
   $$\begin{aligned} F_{n+2}F_n - F_{n+1}^2 &= (F_{n+1}+F_n)F_n - (F_n+F_{n-1})^2 \\ &= F_n^2 - F_{n+1}F_{n-1} \\ &= -(-1)^n \quad \text{d'après } \mathcal{H}_n \\ &= (-1)^{n+1} \end{aligned}$$

2. Soit $n \in \mathbb{N}$. Montrons que $F_n \wedge F_{n+1} = 1$.
   Soit $d \in \mathcal{D}(F_n) \cap \mathcal{D}(F_{n+1})$.
   Alors d divise toute combinaison $\mathbb{Z}$-linéaire de F_n et F_{n+1}, donc divise $(-1)^n$ d'après la question précédente.
   Or $(-1)^n \mid 1$, donc $d \mid 1$.
   Donc $F_n \wedge F_{n+1} = 1$.

3. **Remarque.** (from François Sarcos, 2022-2023). En posant $m = m' + 1$, on peut symétriser la formule en
   $$\forall\, n \in \mathbb{N},\ \forall\, m' \in \mathbb{N},\ F_{m'+n+1} = F_{m'+1}F_{n+1} + F_{m'}F_n$$
   Ainsi, faire une récurrence sur n ou m, c'est kif-kif. □.
   Par récurrence sur $m \in \mathbb{N}^*$ avec l'assertion $\mathcal{H}_m$: « $\forall\, n \in \mathbb{N},\ F_{m+n} = F_mF_{n+1} + F_{m-1}F_n$ »
   Hérédité. Soit $m \in \mathbb{N}^*$ tel que $\mathcal{H}_m$.
   Montrons $\mathcal{H}_{m+1}$.
   Fixons $n \in \mathbb{N}$.
   On a
   $$\begin{aligned} F_{(m+1)+n} &= F_{m+(n+1)} \\ &= F_mF_{n+2} + F_{m-1}F_{n+1} \quad \text{d'après } \mathcal{H}_m \text{ appliquée à } n+1 \\ &= F_m(F_{n+1}+F_n) + F_{m-1}F_{n+1} \quad \text{définition de la suite } F \text{ avec l'indice } n \\ &= F_mF_{n+1} + F_{m-1}F_{n+1} + F_mF_n \quad \text{réorganisation} \\ &= (F_m + F_{m-1})F_{n+1} + F_mF_n \quad \text{définition de la suite } F \text{ avec l'indice } m \\ &= F_{m+1}F_{n+1} + F_mF_n \end{aligned}$$
   D'où $\mathcal{H}_{m+1}$.

4. Remarquons que la formule est symétrique en m et n.
   Cas $m = 0$. Les deux membres sont égaux (WHY ?).
   Cas $m \in \mathbb{N}^*$. Le fait que m soit dans $\mathbb{N}^*$ va nous permettre d'utiliser 3.
   Soit $n \in \mathbb{N}$.
   Montrons que $\mathcal{D}(F_n) \cap \mathcal{D}(F_{m+n}) = \mathcal{D}(F_n) \cap \mathcal{D}(F_m)$, ce qui suffira à conclure quant à l'égalité des pgcd.
   $\boxed{\subset}$ Soit $d \in \mathcal{D}(F_n) \cap \mathcal{D}(F_{m+n})$.
   Alors d'après la relation 3, d divise toute combinaison $\mathbb{Z}$-linéaire de F_n et F_{m+n}, en particulier
   $$d \mid -F_{m-1}F_n + F_{m+n}$$
   Donc $d \mid F_mF_{n+1}$ d'après la relation 3.
   Or $d \mid F_n$ et $F_n \wedge F_{n+1} = 1$.
   On en déduit (WHY ?) que $d \wedge F_{n+1} = 1$.
   Reprenons $d \mid F_mF_{n+1}$ et utilisons $d \wedge F_{n+1} = 1$.
   D'après le lemme de Gauss, on en déduit $d \mid F_m$.
   Bilan $d \in \mathcal{D}(F_n) \cap \mathcal{D}(F_m)$.

   $\boxed{\supset}$ Soit $d \in \mathcal{D}(F_n) \cap \mathcal{D}(F_m)$.
   On a :
   — $d \in \mathcal{D}(F_n)$
   — $d \in \mathcal{D}(F_{m+n})$, car d'après 3, l'entier F_{m+n} est combinaison $\mathbb{Z}$-linéaire de F_m et F_n

Bilan $d \in \mathcal{D}(F_n) \cap \mathcal{D}(F_{m+n})$.

5. Avant de commencer la preuve de cette question, faisons des remarques concernant la relation de la question 4, où $n, m \in \mathbb{N}$.
   Si on lit la formule 4 de gauche à droite $F_n \wedge F_{m+n} = F_n \wedge F_m$, elle dit que l'on peut retirer n au deuxième indice.
   Si on la lit de droite à gauche, elle dit que l'on peut ajouter n au deuxième indice.
   Par récurrence immédiate, on prouve donc que l'on peut ajouter un multiple de n au deuxième indice en partant de $F_n \wedge F_m$, ainsi

$$\forall\, q \in \mathbb{N}, \quad F_n \wedge F_m = F_n \wedge F_{m+nq}$$

   Fixons désormais les intervenants de la question 5, à savoir $a \in \mathbb{N}$, $b \in \mathbb{N}^*$ et posons la division euclidienne $a = bq + r$.
   Alors le quotient est dans $\mathbb{N}$. On peut alors utiliser (♡), et on a

$$F_b \wedge F_{bq+r} \;=\; F_b \wedge F_r$$

   ce qu'il fallait démontrer.

6. Montrons $\forall\, m, n \in \mathbb{N},\ F_m \wedge F_n = F_{m\wedge n}$.
   Faisons une preuve par récurrence sur n.
   Pour tout $n \in \mathbb{N}$, notons $\mathcal{H}_n$ l'assertion

$$\mathcal{H}_n : \quad \text{« } \forall\, m \in \mathbb{N},\ F_m \wedge F_n = F_{m\wedge n} \text{ »}$$

   Initialisation. Montrons $\mathcal{H}_0$. Pour cela, fixons $m \in \mathbb{N}$.

   ....

   D'où $\mathcal{H}_0$.

   Hérédité.

   Soit $n \in \mathbb{N}^*$ tel que $\mathcal{H}_0, \dots, \mathcal{H}_{n-1}$.
   Montrons $\mathcal{H}_n$. Fixons $m \in \mathbb{N}$.
   • Comme $n \neq 0$, on peut effectuer la division euclidienne de m par n :

$$m = nq + r \quad \text{avec } 0 \leqslant r < n$$

   D'après le lemme de la PCSI (qui n'utilise pas la condition sur r), on a $\boxed{m \wedge n = n \wedge r}$.
   • D'autre part, la question précédente dit $\boxed{F_m \wedge F_n = F_n \wedge F_r}$.
   • Utilisons à présent l'hypothèse de récurrence. Comme $r \in [\![0, n-1[\![$, on sait que $\mathcal{H}_r$ est vraie. Ainsi (en particularisant, dans la $\forall$-assertion, à n) :

$$\boxed{F_n \wedge F_r = F_{n\wedge r}}$$

   Maintenant, il suffit « d'agiter » les trois encadrés. Plus précisément, partons du dernier encadré, et utilisons les deux précédents. On obtient :

$$F_m \wedge F_n = F_{m\wedge n}$$

   D'où $\mathcal{H}_n$.

Une remarque très générale pour finir cet exercice.
Le lemme fondamental dit : si $a = bq + r$ (avec aucune condition sur b et r), alors $a \wedge b = b \wedge r$.
Ce que l'on peut écrire $b \wedge (r + bq) = b \wedge r$.
Autrement dit, en lisant la formule de droite à gauche $\leftarrow$, on voit que l'on peut ajouter un multiple du premier indice :

$$\begin{aligned} b \wedge \Big(\big((r+2b)+b\big)\Big) &= b \wedge \big((r+2b)\big) \\ b \wedge \Big(\big((r+b)+b\big)\Big) &= b \wedge \big((r+b)\big) \\ b \wedge \big((r+b)\big) &= b \wedge r \end{aligned}$$

1. • Commençons par le cas $b \in \mathbb{N}$.
   Par récurrence.
   Notons $\mathcal{H}_b$ la propriété « Pour tout $a \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = a \wedge b$ ».

   Initialisation.
   Soit $a \in \mathbb{Z}$.
   On a $a \wedge b = a \wedge 0 = |a|$.
   Si $a \in \mathbb{N}$, alors $a \times 1 + b \times 0 = |a| = a \wedge b$.
   Si $a \in \mathbb{Z} \setminus \mathbb{N}$, alors $a \times (-1) + b \times 0 = |a| = a \wedge b$.
   D'où $\mathcal{H}_0$.

   Hérédité. Soit $b \in \mathbb{N}^*$.
   On suppose que $\mathcal{H}_r$ est vraie pour tout $r \in [\![0,\, b-1]\!]$,
   autrement dit, on suppose $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{b-1}$.
   Montrons $\mathcal{H}_b$.
   Soit $a \in \mathbb{Z}$.
   Écrivons la division euclidienne $a = bq + r$ (licite car $b \neq 0$).
   • D'après le lemme fondamental de la PCSI, on a $a \wedge b = b \wedge r$.
   • On a $r \in [\![0, b-1]\!]$. Donc $\mathcal{H}_r$ est vraie.
   En utilisant la $\forall$-assertion de $\mathcal{H}_r$ avec b, on obtient
   qu'il existe $u, v \in \mathbb{Z}$ tel que $bu + rv = b \wedge r$.
   • Il n'y a plus qu'à remplacer tous les (b, r) par (a, b) : on obtient $bu + (a - bq)v = a \wedge b$.
   En réagençant, on obtient $av + b(u - qv) = a \wedge b$.
   D'où $\mathcal{H}_b$.

   • Traitons le cas $b \in \mathbb{Z} \setminus \mathbb{N}$.
   Alors $-b \in \mathbb{N}$. Donc d'après le cas précédent, il existe u, v tel que $au + (-b)v = \text{pgcd}(a, -b)$.
   D'après le cours, on a $\text{pgcd}(a, -b) = \text{pgcd}(a, b)$.
   On en déduit $au + b(-v) = \text{pgcd}(a, b)$.
   On a donc obtenu une relation de Bézout entre a et b.
2. Par hypothèse, $a \wedge b = 1$.
   Écrivons une relation de Bézout entre a et b, disons $au + bv = 1$.
   Multiplions-la par c. On obtient $acu + bcv = c$.
   Comme $a \mid bc$ (hypothèse), on en déduit que (WHY ?) $a \mid acu + bcv$, d'où $a \mid c$.

119

1. On écrit $x = 18x', y = 18y'$ avec $x' \wedge y' = 1$. En particulier, on a

$$x \vee y = (18x') \vee (18y') = 18\,(x' \vee y') = 18x'y'$$

puisque x' et y' sont premiers entre eux. Ainsi, le système revient à trouver les couples (x', y') d'entiers premiers entre eux pour lesquels $x'y' = 30$. On trouve les couples $(30, 1), (15, 2), (10, 3), (6, 5)$ et leurs symétriques. Les couples (x, y) recherchés sont donc $(540, 18), (270, 36), (180, 54), (108, 90)$ et leurs symétriques.

121

• Une condition nécessaire est clairement que $d \mid m$ (le pgcd divise toujours le ppcm).
• Réciproquement, si $d \mid m$, alors il existe k tel que $m = kd$.
Montrons que le système admet au moins une solution.
Analyse. Supposons qu'il existe une solution (x, y).
Alors $d = x \wedge y$ et on peut écrire $x = dx', y = dy'$ avec $x' \wedge y' = 1$.
Le système se réduit (WHY ?) à l'équation $x'y' = k$.
Cette dernière équation admet toujours des solutions entières.
Par exemple le couple $(x', y') = (k, 1)$.
On a alors $x = dk$ et $y = d$.
Synthèse. Posons $(x, y) = (dk, d)$. On a $\begin{cases} \mathrm{d}k \wedge d = d(k \wedge 1) = d \times 1 & = & d \\ dk \vee d = d(k \vee 1) = dk & = & m \end{cases}$
Donc le système possède au moins une solution.

BILAN : le système admet donc une solution si et seulement si $d \mid m$

122

Raisonnons par l'absurde et supposons qu'il y ait un nombre fini de nombres premiers de la forme $4k+3$ et considérons $n = 3 \times 7 \times 11 \times 19 \dots$ le produit fini de ces nombres.
Considérons le nombre $N = 4n - 1$ et sa décomposition en facteurs premiers.
Soit $p \in \mathcal{P}$ divisant N. Examinons p modulo 4.
Tout d'abord, $p \neq 2$, car N est impair.
Si $p \equiv 3$, alors il divise n. Ainsi, p divise N et n, donc divise $N - 4n = -1$, ce qui n'est pas possible.
Donc les premiers qui apparaissent dans la DFP de N sont congrus à 1 modulo 4.
Par produit de premiers congrus à 1 modulo 4, on a $N \equiv 1 \bmod 4$.
D'où la contradiction (car $N \equiv -1 \bmod 4$).

124

Considérons un diviseur premier p de $n!+1$ (cela existe car $n!+1 \geqslant 2$).
Montrons qu'un tel diviseur p est nécessairement supérieur à $n+1$.
Si p était $< n$, alors p diviserait $n!$.
Donc p diviserait la différence $(n!+1)-(n!)=1$.
Ce qui n'est pas possible car p est premier.
Ainsi, $p \geqslant n+1$.

Redémontrons l'infinitude des nombres premiers.
On a donc montré

$$\forall\, n \in \mathbb{N}^*,\ \exists p \in \mathcal{P},\ p \geqslant n+1$$

D'où l'infinitude des nombres premiers.

125

On a $7 \mid n \iff 10d + u \equiv 0 \bmod 7$.
Ce qui est encore équivalent (WHY, ce n'est pas du tout évident) à $-20d - 2u \equiv 0 \bmod 7$, ce qui est équivalent à (facile) $d - 2u \equiv 0 \bmod 7$.
On a $413 = 41 \times +3$. Ona $d - 2u = 41 - 6 = 35$ qui est multiple de 7, donc 413 est multiple de 7.

127

On a $164 = 4 \times 41$.
Pour savoir où l'on va, on peut se rappeler que $164 \mid n \iff (4 \mid n \text{ et } 41 \mid n)$ (ceci à cause du fait que $4 \wedge 41 = 1$).
Un nombre à 6 chiffres se terminant par 164 est un nombre n de la forme

$$\begin{aligned} n &= a10^5 + b10^4 + c10^3 + 164 \\ &= 10^3(a10^2 + b10^1 + c) + 164 \\ &= 4 \times \big(250(\underbrace{a10^2 + b10^1 + c}_{m}) + 41\big) \end{aligned}$$

avec $a \neq 0$ (pour imposer les 6 chiffres).
Ainsi $164 = 4 \times 41 \mid n \iff 41 \mid 250m + 41 \iff 41 \mid 250m$.
Comme 41 est un nombre premier, le lemme d'Euclide fournit

$$164 \mid n \iff 41 \mid m$$

Ainsi m est multiple de 41 et est compris entre 100 et 999.

$$3 \times 41 = 123, \quad 4 \times 41 = 164, \quad \ldots, \quad 23 \times 41 = 943, \quad 24 \times 41 = 984$$

qui sont au nombre de 22.
Il y a donc 22 nombres à six chiffres se terminant par 164 qui sont multiples de 164.

128

Soit $n \geqslant 7$.

— Cas n impair. On a $n = 2 + (n-2)$, et comme n est impair, on a $\text{pgcd}(2, n-2) = 1$.

— Cas n multiple de 4, disons $n = 4k$. Comme $n \geqslant 7$, on a $k \geqslant 2$. Ainsi $n = (2k-1) + (2k+1)$ est une somme de deux entiers $\geqslant 2$. Et $\text{pgcd}(2k-1, 2k+1) = 1$.

— Cas n congru à 2 modulo 4, disons $n = 4k+2$. Comme $n \geqslant 7$, on a $k \geqslant 2$, donc $n = (2k-1) + (2k+3)$ est une somme de deux entiers $\geqslant 2$. Et $\text{pgcd}(2k-1, 2k+3) = 1$ (on utilise le fait que $2k+3$ est impair).

129

2 n'est pas la somme de deux nombres premiers. On peut donc se limiter à rechercher les nombres premiers impairs qui sont à la fois la somme et le produit de deux nombres premiers.
En particulier, pour des raisons de parité, 2 doit alors intervenir à la fois dans la somme et dans la différence. Il s'ensuit que l'on recherche en fait les nombres premiers impairs q qui s'écrivent à la fois sous la forme $p+2$ et sous la forme $r-2$, avec p et r premiers (nécessairement impairs).
Autrement dit, il s'agit de chercher les nombres premiers q tels que $q \pm 2$ soit également premier.
Le point-clef est que $q-2$, q et $q+2$ ont nécessairement trois restes différents dans la division par 3. Il s'ensuit que l'un de ces nombres doit être multiple de 3. Puisqu'il s'agit de nombres premiers, l'un de ces nombres doit en fait valoir 3.
On a alors directement $q-2=3$, $q=5$ et $q+2=7$, qui est effectivement possible.
En résumé, le seul nombre premier possédant la propriété de l'énoncé est

$$5 = 7-2 = 3+2.$$

130

Soit $x \in \mathbb{N}^*$ et $A \in \mathbb{N}$ tel que

$$x(x+1)(x+2) = A^n.$$

Écrivons $A = \prod_{k=0}^{r} p_k^{e_k}$, avec $p_0 = 2$.
À part 2, aucun p_k ne peut diviser deux des trois termes du produit. Autrement dit, on a des décompositions d'un des deux types suivants

— Si x est pair, on a une partition I, J, K de $[\![1, r]\!]$ et deux entiers tels que $a+b = ne_0$, vérifiant

$$x = 2^a \prod_{k\in I} p_k^{ne_k}, \qquad x+1 = \prod_{k\in J} p_k^{ne_k} \quad \text{et} \quad x+2 = 2^b \prod_{k\in K} p_k^{ne_k}.$$

En particulier, $x+1$ et $x(x+2) = 2^{ne_0} \prod_{k\in I\cup K} p_k^{ne_k}$ sont des puissances n-ièmes.

— Si x est impair, on a une partition I, J, K de $[\![1, r]\!]$ vérifiant

$$x = \prod_{k\in I} p_k^{ne_k}, \qquad x+1 = 2^{ne_0} \prod_{k\in J} p_k^{ne_k} \quad \text{et} \quad x+2 = \prod_{k\in K} p_k^{ne_k}.$$

En particulier, x, $x+1$ et $x+2$ sont des puissances n-ièmes. *A fortiori*, le produit $x(x+2)$ également.

Dans tous les cas, on a deux entiers a et b tels que $x+1 = a^n$ et $x(x+2) = b^n$.
Or, on a

$$\begin{aligned} x(x+2) &= ((x+1)-1)((x+1)+1) \\ &= (x+1)^2 - 1 \\ &= a^{2n} - 1, \end{aligned}$$

donc $b^n = a^{2n} - 1$. Cela fournit deux puissances n-ièmes consécutives, ce qui est impossible ($\forall y \in \mathbb{N}^*, \forall n \in \mathbb{N}^*, (y+1)^n > y^n + 1$, d'après le binôme de Newton).

131

1. Sans perte de généralités, supposons $a < b$ de sorte que $b - a > 0$ (cela va servir à la fin de la preuve).

   On a $b + n = (a + n) + (b - a)$, donc $\text{pgcd}(a + n, b + n) = \text{pgcd}(a + n, b - a)$.

   La question se reformule donc « trouver une infinité de $n \geqslant 1$ tel que $\text{pgcd}(a+n, b-a) = 1$ ».

   Soit $k \in \mathbb{N}$ quelconque de sorte que $n = k(b - a) + 1 - a$ soit $\geqslant 1$ (c'est possible prendre k égal à $k_0 = \lfloor \frac{a-1}{b-a} \rfloor + 1$; c'est là que l'on utilise que $b-a > 0$). On a alors $a+n = k(b-a)+1$, donc $\text{pgcd}(a + n, b - a) = 1$.

   Dans le cas où $a < b$, on a bien trouvé une infinité de n tels que $\text{pgcd}(a + n, b + n) = 1$: prendre tous les n qui s'écrivent $n = k(b-a)+1-a$ pour k assez grand, précisément supérieur à k_0.

2. $a = 2$, $b = 3$, $c = 4$ et $d = 5$ convient : si n est pair, $a + n$ et $c + n$ sont tous les deux pairs, donc ils ne peuvent pas être premiers entre eux ; si n est impair, c'est $b + n$ et $d + n$ qui sont tous les deux pairs.

132

Si $n = 2^a$ est une anagramme de $m = 2^b$, ils ont particulier le même nombre r de chiffres. Cela signifie que $10^{r-1} \leqslant n, m < 10^r$. Or, comme $2^4 = 16 > 10$, on ne peut jamais trouver cinq puissances de 2 ayant le même nombre de chiffres. (En fait, le nombre de puissances de 2 ayant k chiffres vaut toujours 3 ou 4, mais on n'en a pas besoin ici).
Par ailleurs, si deux nombres sont anagrammes l'un de l'autre, la somme de leurs chiffres est la même, et ils sont donc congrus modulo 9. Or, les puissances de 2, modulo 9, sont périodiques de période 6 : $2^6 = 64 \equiv 1 \mod 9$:

k modulo	0	1	2	3	4	5
2^k modulo 9	1	2	4	8	7	5

Ainsi, quatre puissances consécutives de 2 n'auront des sommes de chiffres égales, donc, en particulier, les puissances de 2 ne sont jamais des anagrammes l'une de l'autre.

133

Tout carré parfait est congru à 0, 1 ou 4 modulo 8. En effet, si $n = 2k$, $n^2 = 4k^2 \equiv 0, 4 \mod 8$; si $n = 2k + 1$, $n^2 = 4k^2 + 4k + 1 \equiv 1 \mod 8$ car $k^2 + k$ est pair.
Par ailleurs, $\forall e \in \mathbb{N}$, $3^e \equiv 1, 3 \mod 8$. Ainsi, le nombre $1 + 3^n + 3^m$ peut être congru à 3, 5 ou 7 modulo 8, mais pas à 1, donc ce n'est pas un carré parfait.

134

Déjà, l'équation implique que p et q sont distincts.
Comme il s'agit de nombres premiers, ils sont premiers entre eux.
Modulo $p+q$, on a la congruence $p-q \equiv -2q$, donc l'équation se réduit en

$$0 \equiv (p-q)^3 \equiv (-2q)^3 \equiv -8q^3 \mod p+q.$$

Autrement dit, $p+q \mid 8q^3$.
De plus, $(p+q) \wedge q = 1$ (si ce n'était pas le cas, comme q est premier, on aurait $q \mid p+q$, donc $q \mid p$, mais c'est impossible car $p \wedge q = 1$).
D'après le lemme de Gauss, on obtient $p+q \mid 8$.
Comme p et q valent au moins 2, cela entraîne $p+q \in \{4,8\}$. Mais la seule façon de décomposer 4 en somme de deux nombres premiers est $4 = 2+2$ et la seule façon de décomposer 8 est $8 = 5+3$.
Or $p = q = 2$ n'est pas une solution de notre équation, contrairement à $p = 5$ et $q = 3$.