TD 14 Arithmétique.

Jeudi 19 Décembre 2024

Divise-Se factorise

Exercice 1. [Correction]

Montrer par récurrence que, pour tout $n \in \mathbb{N}$, 11 divise $\left(9^{5n+2} - 4\right)$

Exercice 2. [Correction] En utilisant le binôme, montrer que n^2 divise $(1+n)^n - 1$.

Exercice 3. [Correction] Somme Géo et factorisation (D'après une exercice d'oral de Centrale)

> On sait que : $\forall\, q \neq 1,\ 1 + q + q^2 + \cdots + q^{n-1} = \dfrac{1-q^n}{1-q} = \dfrac{q^n - 1}{q-1}$
>
> Ainsi on a la factorisation : $\square^n - 1 = (\square - 1)\left(1 + \square + \square^2 + \cdots + \square^{n-1}\right)$ avec $\square \in \mathbb{N}$

Soit $n \in \mathbb{N}$ et $M_n = 2^n - 1$.
On suppose que n est non-premier/composé, CàD n admet des diviseurs intermédiaires
, CàD $n = ab$ avec $2 \leqslant a \leqslant \sqrt{n} \leqslant b \leqslant n-1$

1. Démontrer que $M_a = 2^a - 1$ se factorise de M_n et que $M_a \geqslant 2$

   Conclusion : M_n admet des diviseurs intermédiaires donc M_n est composé/non-premier.
2. Expliciter la contraposée.

Congruence

Exercice 4. [Correction]

Montrer que : $\forall\, n \in \mathbb{N},\ 10^{3n+2} - 4^{n+1} \equiv 0 \mod [6]$.

Exercice 5. [Correction]

1. Calculer 2^{29} modulo 9.
2. On admet que le nombre 2^{29} possède neuf chiffres, tous distincts (parmi $0,1,2,3,4,5,6,7,8,9$).

   Quel est le chiffre manquant ?

Premier entre eux.

Exercice 6. [Correction]

1. Montrer que : Pour tout $n \in \mathbb{N}$, les entiers $3n^2 + 2n$ et $n+1$ sont premier entre eux.
2. *Bonus* Soit n est un diviseur commun positif de $3a^2 + 4a - 1$ et $2a + 1$.

   Montrer que $n = 1, 3$ *ou* 9. Conclusion : $pgcd\left(3a^2 + 4a - 1, 2a + 1\right) = 1\ ou\ 3\ ou 9$

Exercice 7. [Correction] Soit n un entier.

1. Montrer qu'il existe $(a_n, b_n) \in \mathbb{N}^2$ tel que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$.

   Exprimer a_{n+1}, b_{n+1} en fonction a_n et b_n.
2. Montrer que : $(a_n)^2 - 2(b_n)^2 = (-1)^n$
3. En déduire que a_n et b_n sont premier entre eux

Exercice 8. [Correction] Soit n un entier. On note F_n le nombre

$$F_n = 2^{2^n} + 1$$

On suppose que $a \geqslant 1$ est un diviseur commun de F_n et F_{n+1}.

> Calculer $2^{2^{n+1}}$ en fonction de 2^{2^n}
> En déduire F_{n+1} en fonction de F_n.

> En déduire que : a divise 2 puis que $a = 1$. Conclusion : F_n et F_{n+1} sont premiers entre eux.

Bonus : Démontrer en suivant la même démarche que : F_n et F_{n+k} sont premiers entre eux.

Gauss is Great.

Exercice 9. [Correction] On va démontrer un résultat sur le triangle de Pascal.

1. Écrire le triangle de Pascal jusqu'à la ligne n°7.
   Je vous donne la ligne 11 : 1, 11, 55, 165, 330, 462, 462, 330, 165, 55, 11, 1.
   On constate que lorsque p est premier,
   alors "tous" les coefficients de la ligne p du triangle sont divisibles par p.
2. On va démontrer ce résultat.
   (a) Pour $k \in \{1, 2, .., (p-1)\}$, exprimer $\binom{p}{k}$ en fonction $\binom{p-1}{k-1}$.
   (b) En déduire, avec Gauss, que : lorsque p est premier alors $\forall\ k \in \{1, 2, .., (p-1)\},\ p$ *divise* $\binom{p}{k}$.

Triplets pythagoriciens.

Exercice 10. [Correction] Soit $x, y, z \in \mathbb{Z}$ avec x et y premiers entre eux.

Analyse : On suppose que : $x^2 + y^2 = z^2$

1. Montrer que : x et z premiers entre eux. On montre de même que : y et z premiers entre eux.
2. Soit $n \in \mathbb{N}$. Montrer que $n^2 \equiv 0\, mod\, [4]$ ou $n^2 \equiv 1\, mod\, [4]$
   En déduire, par contraposée, que : x ou y est pair.

   `Quitte à les permuter, on suppose désormais` y `pair.`
3. On considère $\beta = \dfrac{z+x}{2}$ et $\gamma = \dfrac{z-x}{2}$
   Montrer que β et γ sont des entiers et qu'ils sont premiers entre eux.
4. Montrer que qu'il existe $\alpha \in \mathbb{N}$ tel que $\beta.\gamma = \alpha^2$.
   En déduire (en utilisant les valuations/multiplicité) que β et γ sont des carrés. *(classique mais difficile)*
5. En déduire qu'il existe $b, c \in \mathbb{Z}$ tel que $x = b^2 - c^2$, $y = 2bc$ et $z = b^2 + c^2$.
6. Synthèse : Vérifier que les triplets de la forme précédente conviennent (et que b et c sont premier entre eux car x et y premiers entre eux).
7. Complément Lorsque que on suppose que x, y ne sont pas premier entre eux.
   Alors $d = pgcd(x, y) \geqslant 2$ et on peut factoriser le $pgcd$, CàD $x = d\,x'$ et $y = d\,y'$ et $pgcd(x', y') = 1$
   > Montrer que : d^2 divise z^2.
   > Avec les valuations/multiplicités, montrer que : d divise z, CàD $z = d\,z'$
   Conclusion : x', y' sont premier entre eux et $(x')^2 + (y')^2 = (z')^2$.

Conclusion final : Les solutions, dans $\mathbb{Z}$, de $x^2 + y^2 = z^2$ sont : $x = b^2 - c^2$, $y = 2bc$ et $z = b^2 + c^2$ avec $b, c \in \mathbb{Z}$

——— BAC is back Polynésie 2011 (5 points) ———

Exercice 11.

Partie A On considère l'équation (E) : $25x - 108y = 1$ où x et y sont des entiers relatifs.

1. Déterminer une solution particulière (x_0, y_0) de l'équation (E)
2. Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).

Partie B Dans cette partie, a désigne un entier naturel.
Les nombres c et g sont des entiers naturels vérifiant la relation $25g - 108c = 1$.

On admettra le théorème suivant, dit petit théorème de Fermat
Si p est un nombre premier et a un entier non divisible par p,
alors a^{p-1} est congru à 1 modulo p que l'on note $a^{p-1} \equiv 1\ [p]$.

1. Soit x un entier naturel.
   Démontrer que si $x \equiv a\ [7]$ et $x \equiv a\ [19]$, alors $x \equiv a\ [133]$.
2. Une congruence.
   (a) On suppose que a n'est pas un multiple de 7.
   Démontrer que $a^6 \equiv 1\ [7]$ puis que $a^{108} \equiv 1\ [7]$.
   En déduire que $\left(a^{25}\right)^g \equiv a\ [7]$.
   (b) On suppose que a est un multiple de 7.
   Démontrer que $\left(a^{25}\right)^g \equiv a\ [7]$.
   (c) On admet que pour tout entier naturel a, $\left(a^{25}\right)^g \equiv a\ [19]$.
   Démontrer que $\left(a^{25}\right)^g \equiv a\ [133]$.

Partie C On note $\mathcal{A}$ l'ensemble des entiers naturels a tels que : $1 \leqslant a \leqslant 26$.

Un message, constitué d'entiers appartenant à $\mathcal{A}$, est codé puis décodé.

$>$ La phase de codage consiste à associer, à chaque entier a de $\mathcal{A}$, l'entier r tel que $a^{25} \equiv r\ [133]$ avec $0 \leqslant r < 133$.
$>$ La phase de décodage consiste à associer à r , l'entier r_1 tel que $r^{13} \equiv r_1\ [133]$ avec $0 \leqslant r_1 < 133$.

1. Justifier que $r_1 \equiv a\ [133]$.
2. Un message codé conduit à la suite des deux entiers suivants : $128 \qquad 59$.
   Décoder ce message et lire le message.

Correction.

Solution de l'exercice 1 (Énoncé)

Montrer par récurrence que, pour tout $n \in \mathbb{N}$, 11 divise $\left(9^{5n+2}-4\right)$

On fait par récurrence $H_{<n>}$: 11 divise $\left(9^{5n+2}-4\right)$

> Initialisation $n=0$

Comme $9^{5.0+2}-4=9^2-4=81-4=77$, $H_{<0>}$ est vrai

> Hérédité. On suppose $H_{<n>}$

On va montrer $H_{<n+1>}$, CàD 11 divise $\left(9^{5(n+1)+2}-4\right)$

On cherche le lien entre $9^{5(n+1)+2}-4$ et $9^{5n+2}-4$ puis on applique $H_{<n>}$

$$\begin{aligned}
9^{5(n+1)+2}-4 &= 9^5.9^{5n+2}-4\\
&= 9^5.\left(9^{5n+2}-4\right)+4.9^5-4\\
&= 9^5.\left(9^{5n+2}-4\right)+4.\left(9^5-1\right)\\
&= 9^5.\left(9^{5n+2}-4\right)+4.59048\\
&= 9^5.\left(9^{5n+2}-4\right)+4.11.5368\\
&\quad \textit{On applique } H_{<n>}\\
&= 9^5.11\times k+4.11.5368 = 11\times\left(9^5.k+4.5368\right)
\end{aligned}$$

Donc $H_{<n+1>}$ est vraie.

Solution de l'exercice 2 (Énoncé)

En utilisant le binôme, montrer que n^2 divise dans $(1+n)^n-1$.

On a

$$\begin{aligned}
(1+n)^n-1 &= \left[\sum_{k=0}^{n}\binom{n}{k}n^k\right]-1\\
&= \sum_{k=1}^{n}\binom{n}{k}n^k \qquad \textit{car } \underbrace{1}_{k=0}\\
&= \underbrace{\binom{n}{1}\times n}_{k=1} + \underbrace{\sum_{k=2}^{n}\binom{n}{k}n^k}_{\textit{Ici } k\geqslant 2 \textit{ donc } n^2 \textit{ se factorise.}}\\
&= n^2+n^2\left(\sum_{k=2}^{n}\binom{n}{k}n^{k-2}\right)\\
&= n^2\times Entier
\end{aligned}$$

Conclusion : n^2 divise dans $(1+n)^n-1$.

Solution de l'exercice 3 (Énoncé)

1. Démontrer que $M_a=2^a-1$ se factorise de M_n et que $M_a\geqslant 2$

   On utilise la factorisation géo

$$\begin{aligned}
M_n=2^n-1=2^{ab}-1=(2^a)^b-1 &= \square^b-1\\
&\quad \text{On utilise la factorisation géo}\\
&\quad C\text{à}D\ \square^b-1=(1-\square)\left(1+\square+\square^2+\cdots+\square^{b-1}\right)\\
&= (2^a-1)\left(1+[2^a]+[2^a]^2+\cdots+[2^a]^{n-1}\right)\\
&= M_a\times Entier
\end{aligned}$$

   De plus $M_a=2^a-1\geqslant 2^2-1=4-1=3$. Ainsi M_a est bien un diviseur intermédiaire de M_n

2. Expliciter la contraposée.

   On vient de démontrer que : Si/Lorsque n est composée alors M_n est composé/non-premier

Par contraposée, on a : Si/Lorsque M_n est premier alors n est premier.

Moralité : Les nombres premiers de la forme $2^n - 1$
sont à chercher parmi les n *premier, CàD* $n = 2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Solution de l'exercice 4 (Énoncé)
Montrer que : $\forall\, n \in \mathbb{N},\ 10^{3n+2} - 4^{n+1} \equiv 0 \mod [6]$.

Pour $n \in \mathbb{N}$, on

$$\begin{aligned} 10^{3n+2} - 4^{n+1} &\equiv \overline{10}^{3n+2} - \overline{4}^{n+1} \mod [6] \\ &\quad \textit{Or on a } \overline{10} \equiv 4 \mod [6] \\ &\equiv 4^{3n+2} - 4^{n+1} \mod [6] \\ &\equiv \left[\left(4^3\right)^n.4^2 - 4^n.4^1\right] \mod [6] \\ &\equiv [64^n.16 - 4^n.4] \mod [6] \\ &\quad \textit{Or } \overline{64} \equiv 4 \mod [6] \textit{ et } \overline{16} \equiv 4 \mod [6] \\ &\equiv [4^n.4 - 4^n.4] \mod [6] \\ &\equiv O \mod [6] \qquad \texttt{Fini} \end{aligned}$$

Solution de l'exercice 5 (Énoncé)

1. Calculer 2^{29} modulo 9.

On a $2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 = 16 \equiv 7 \mod [9]$

$2^5 = 2^4.2 \equiv 7.2 \mod [9] \equiv 14 \mod [9] \equiv 5 \mod [9]$

$2^6 = 2^5.2 \equiv 5.2 \mod [9] \equiv 10 \mod [9] \equiv 1 \mod [9]$

$$\text{Ainsi on a } 2^{29} = 2^{6.4+5} = \left(2^6\right)^4.2^5 \equiv 1^4.5 \mod [9] \\ \equiv 5 \mod [9]$$

2. On admet que le nombre 2^{29} possède neuf chiffres, tous distincts (parmi $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$).
   Quel est le chiffre manquant ?

On sait que : n modulo [9] est est égale à la somme des chiffres (en base 10), ainsi

$$\begin{aligned} 2^{29} &\equiv (\textit{somme des chiffes}) \mod [9] \\ &\equiv (0+1+2+3+4+5+6+7+8+9-a) \mod [9] \quad \textit{avec } a \textit{ le chiffre manquant} \\ &\equiv (O - a) \mod [9] \\ &\equiv -a \mod [9] \end{aligned}$$

Ainsi : $2^{29} \equiv -a \mod [9]$ et $2^{29} \equiv 5 \mod [9]$

Conclusion : $-a \equiv 5 \mod [9]$ et $a \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
Donc $a = 4$

Confirmation : On sait grâce à Python que : $2^{29} = 536870912$. Donc Yes ! ! !

Solution de l'exercice 6 (Énoncé)

1. Montrer que : Pour tout $n \in \mathbb{N}$, les entiers $3n^2 + 2n$ et $n + 1$ sont premier entre eux.
2. Soit n est un diviseur commun positif de $3a^2 + 4a - 1$ et $2a + 1$. Montrer que $n = 1, 3$ *ou* 9.

On suppose que $n \geqslant 1$ divise $3a^2 + 4a - 1$ et $2a + 1$.
On a

$$\left.\begin{array}{r} n \text{ divise } 3a^2 + 4a - 1 \\ n \text{ divise } 2a + 1 \end{array}\right\} \Longrightarrow n \textit{ divise } (-2)(3a^2 + 4a - 1) + (3a)(2a + 1) = -5a + 2$$

On poursuit avec

$$\left.\begin{array}{r} n \text{ divise } 2a + 1 \\ n \text{ divise } -5a + 2 \end{array}\right\} \Longrightarrow n \textit{ divise } (2)(-5a + 2) + (5)(2a + 1) = 9$$

Conclusion n divise 9 donc $n = 1, 3$ *ou* 9.

Solution de l'exercice 7 (Énoncé)

1. Montrer qu'il existe $(a_n, b_n) \in \mathbb{N}^2$ tel que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$. Exprimer a_{n+1}, b_{n+1} en fonction a_n et b_n.

   Par récurrence.

2. Montrer que : $(a_n)^2 - 2(b_n)^2 = (-1)^n$

   Par récurrence.

3. En déduire que a_n et b_n sont premier entre eux

   On suppose $a \geqslant 1$ divise a_n et b_n. On a

$$\left.\begin{array}{l} a \text{ divise } a_n \\ a \text{ divise } b_n \end{array}\right\} \Longrightarrow a \textit{ divise } (a_n)(a_n) - (2b_n)(b_n) = (-1)^n$$

   Donc $a = 1$.

Conclusion : 1 est le seul diviseur commun de a_n et b_n
donc a_n et b_n sont premiers entre eux.

Solution de l'exercice 8 (Énoncé)

$>$ Calculer $2^{2^{n+1}}$ en fonction de 2^{2^n}

En déduire F_{n+1} en fonction de F_n.

$>$ En déduire que : a divise 2 puis que $a = 1$.

On a $2^{2^{n+1}} = 2^{2^n.2} = \left(2^{2^n}\right)^2$

$$\text{Ainsi } F_{n+1} - 1 = 2^{2^{n+1}} = \left(2^{2^n}\right)^2 = (F_n - 1)^2 = (F_n)^2 - 2F_n + 1$$

Conclusion : $F_{n+1} = (F_n)^2 - 2F_n + 2$

On suppose $a \geqslant 1$ divise F_{n+1} et F_n

On a

$$\left.\begin{array}{c} a \text{ divise } F_{n+1} \\ a \text{ divise } F_n \end{array}\right\} \Longrightarrow a \textit{ divise } (1)(F_{n+1}) - (F_n - 2)(F_n) = \cdots = +2$$

Donc forcément $a = 2$ ou $a = 1$.

Mais 2 ne divise pas F_n car $F_n = 2^n + 1$ est impair.

Conclusion : 1 est le seul diviseur commun de F_{n+1} et F_n
donc F_{n+1} et F_n sont premiers entre eux.

BONUS : Démontrer en suivant la même démarche que : F_n et F_{n+k} sont premiers entre eux.

On a $2^{2^{n+k}} = 2^{2^n.2^k} = \left(2^{2^n}\right)^{2^k}$

Ainsi $F_{n+k} - 1 = 2^{2^{n+k}} = \left(2^{2^n}\right)^{2^k} = (F_n - 1)^{2^k}$

$$\begin{aligned} \text{Conclusion : } F_{n+1} = (F_n - 1)^{2^k} + 1 &= \left[\sum_{p=0}^{2^k} \binom{2^k}{p} (F_n)^p (-1)^{2^k - p}\right] + 1 \\ &= \underbrace{\sum_{p=1}^{2^k} \binom{2^k}{p} (F_n)^p (-1)^{2^k - p}}_{\textit{Ici } F_n \textit{ se factorise car } p \geqslant 1} + \underbrace{1}_{p=0} + 1 \\ &= F_n \times Entier + 2 \end{aligned}$$

On suppose $a \geqslant 1$ divise F_{n+k} et F_n

On a

$$\left.\begin{array}{c} a \text{ divise } F_{n+k} \\ a \text{ divise } F_n \end{array}\right\} \Longrightarrow a \textit{ divise } \Big[(1)(F_{n+k}) + (-Entier)(F_n)\Big] = 2$$

Donc forcément $a = 2$ ou $a = 1$.

Mais 2 ne divise pas F_n car $F_n = 2^n + 1$ est impair.

Conclusion : 1 est le seul diviseur commun de F_{n+k} et F_n
donc F_{n+k} et F_n sont premiers entre eux.

Solution de l'exercice 9 (Énoncé)

1. Écrire le triangle de Pascal jusqu'à la ligne n°7.

   1,7,21,35,35,21,7,1

2.
   (a) Pour $k \in \{1, 2, .., (p-1)\}$, exprimer $\binom{p}{k}$ en fonction $\binom{p-1}{k-1}$.

   On a $\binom{p}{k} = \cdots = \frac{p}{k}\binom{p-1}{k-1}$.

   (b) En déduire, avec Gauss, que : lorsque p est premier alors $\forall\ k \in \{1, 2, .., (p-1)\}$, p *divise* $\binom{p}{k}$.

   On a $k\binom{p}{k} = p\binom{n-1}{k-1}$
   Comme $k \in \{1, 2, .., (p-1)\}$ et que p est premier DONC p est premier avec k, ainsi

$$\left.\begin{array}{r} p \text{ divise } k\binom{p}{k} \\ \\ p \text{ est premier avec } k \end{array}\right\} \xrightarrow{Thm\ Gauss} p \text{ divise } \binom{p}{k}$$

Solution de l'exercice 10 (Énoncé)

1. Montrer que : x et z premiers entre eux. On montre de même que : y et z premiers entre eux.

   Si/Lorsque a et b ne sont pas premier eux alors $d = pgcd(a, b) \geqslant 2$ donc un diviseur premier de d est un diviseur premier commun de a et b

Rappel/Complément : Ainsi Si a et b ne sont pas premier entre eux $\Longrightarrow$ a et b admettent un diviseur premier commun Par contraposée : a et b n'ont pas de diviseur premier commun $\Longrightarrow$ a et b sont premier entre eux

   On suppose que p est un diviseur premier commun de x et z
   Ainsi p divise $z.z - x.x = y^2$
   De plus p est premier et p divise $y.y$
   Donc p divise y et p est un diviseur commun de x et y
   Donc $p = 1$ OUPS (car p est premier)

   x et z n'ont pas de diviseur premier commun
   $\Longrightarrow$ x et z sont premier entre eux.

2. Soit $n \in \mathbb{N}$. Montrer que $n^2 \equiv 0\, mod\, [4]$ ou $n^2 \equiv 1\, mod\, [4]$.

   On sait que n modulo 4 est égale à $0, 1, 2$ ou 3

   $>$ Lorsque n modulo 4 est égale à 0 ou 2, CàD n pair, on a $n^2 \equiv 0\, mod\, [4]$

   $>$ Lorsque n modulo 4 est égale à 1 ou 3, CàD n impair on a $n^2 \equiv 1\, mod\, [4]$

   En déduire, par contraposée, que : x ou y est pair.

   On fait un RA. On suppose que x ET y sont impair
   Ainsi $z^2 = x^2 + y^2 \equiv [1 + 1] \mod [4] \equiv [2] \mod [4]$ IMPOSSIBLE/OUPS

   `Quitte à les permuter, on suppose désormais` y `pair.`

3. On considère $\beta = \dfrac{z+x}{2}$ et $\gamma = \dfrac{z-x}{2}$
   Montrer que β et γ sont des entiers premiers entre eux.

   Comme x et y sont premier entre eux et y pair Donc x impair.
   De même z et y sont premier entre eux et y pair Donc z impair.

   $$\text{Ainsi } \beta = \frac{z+x}{2} = \frac{Impair + Impair}{2} \in \mathbb{N} \text{ et de même } \gamma = \frac{z-x}{2} \in \mathbb{N}$$

   On suppose que n est un diviseur de β et γ
   Ainsi n divise $\beta + \gamma = z$ et $\beta - \gamma = x$ donc $n = 1$ car z et x sont premier entre eux

4. Montrer que qu'il existe $\alpha \in \mathbb{N}$ tel que $\beta.\gamma = \alpha^2$.

Comme y est pair, on a $y = 2.\alpha$

$$\text{Ainsi } x^2 + y^2 = z^2 \implies (2\alpha)^2 = z^2 - x^2$$
$$\implies \alpha^2 = \frac{(z+x)(z-x)}{4} = \beta.\gamma$$

En déduire que β et γ sont des carrés

Rappel/Complément : Si $ab = c$ alors $v_p(a) + v_p(b) = v_p(c)$ Si a, b sont premier entre eux alors $v_p(a) \geqslant 1 \implies v_p(b) = 0$ et symétriquement

Pour tout $p \in \mathscr{P}$, on a $\beta.\gamma = \alpha^2$ donc $v_p(\beta) + v_p(\gamma) = v_p(\alpha^2) = 2v_p(\alpha)$

De plus β, γ sont premier entre eux

donc $v_p(\gamma) = 0$ et $v_p(\beta) = 2v_p(\alpha)$ OU $v_p(\beta) = 0$ et $v_p(\gamma) = 2v_p(\alpha)$

Conclusion : $\forall\, p \in \mathscr{P},\ v_p(\beta)$ est pair, CàD β est un carré (et de même pour γ)

5. En déduire qu'il existe $b, c \in \mathbb{Z}$ tel que $x = b^2 - c^2$, $y = 2bc$ et $z = b^2 + c^2$.

On a $\dfrac{z+x}{2} = \beta = b^2$ et $\dfrac{z-x}{2} = \gamma = c^2$

Ainsi on a $z = \dfrac{z+x}{2} + \dfrac{z-x}{2} = b^2 + c^2$ et $x = \dfrac{z+x}{2} - \dfrac{z-x}{2} = b^2 - c^2$

De plus $y^2 = z^2 - x^2 = \left[b^2 + c^2\right]^2 - \left[b^2 - c^2\right]^2 = 4b^2.c^2$

Donc $y = 2bc$

Conclusion de l'analyse : Si $x^2 + y^2 = z^2$

Alors $x = b^2 - c^2$, $y = 2bc$ et $z = b^2 + c^2$ avec $b, c \in \mathbb{Z}$

6. Synthèse : Vérifier que les triplets de la forme précédente conviennent.

Il est facile de vérifier que : $\left(b^2 - c^2\right)^2 + (2bc)^2 = \left(b^2 + c^2\right)^2$

Il "faudrait" vérifier que $x = b^2 - c^2$ et $y = 2bc$ sont premier entre eux ! ! !

C'est le cas Ssi b et c sont premier entre eux (et $\neq 1, 1$).