D.M. 10, solution : autour des nombres parfaits

1 Nombres parfaits pairs :

a) Propriétés de la fonction σ : (i) On sait, par propriété de la décomposition en facteurs premiers que si on note $\Delta(n)$ l'ensemble des diviseurs de n dans $\mathbb{N}$, alors :

$$\Delta(n) = \{p_1^{\beta_1} \dots p_r^{\beta_r}, \quad \text{avec } \forall\, i \in [\![1, r]\!], \ \ 0 \le \beta_i \le \alpha_i\}.$$

Donc :

$$\sum_{d|n} d = \sum_{\beta_1 \le \alpha_1, \dots, \beta_r \le \alpha_r} p_1^{\beta_1} \dots p_r^{\beta_r} = \Big(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\Big) \dots \Big(\sum_{\beta_r=0}^{\alpha_r} p_r^{\beta_r}\Big) \quad \text{par simple distributivité.}$$

D'où l'expression :

$$\boxed{\sigma(n) = \frac{1-p_1^{\alpha_1+1}}{1-p_1} \cdots \frac{1-p_r^{\alpha_r+1}}{1-p_r}.}$$

Remarque (qui ne sert pas ici mais servira au § 2) Si on note $d(n) = \mathrm{Card}(\Delta(n))$, le nombre de diviseurs de n, avec les mêmes notations, on a :

$$d(n) = (\alpha_1 + 1) \dots (\alpha_r + 1).$$

(ii) Si deux nombres a et b sont premiers entre eux, on pourra écrire $\sigma(a) = \dfrac{1-p_1^{\alpha_1+1}}{1-p_1} \cdots \dfrac{1-p_r^{\alpha_r+1}}{1-p_r}$. et $\sigma(b) = \dfrac{1-p_{r+1}^{\alpha_{r+1}+1}}{1-p_{r+1}} \cdots \dfrac{1-r_s^{\alpha_s+1}}{1-p_s}$. en notant $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $b = p_{r+1}^{\alpha_{r+1}} \dots p_s^{\alpha_s}$, et comme $a \wedge b = 1$, on sait que $p_1, \dots, p_r, p_{r+1}, \dots, p_s$ sont *deux à deux distincts.*

Alors la formule du (i) appliquée à ab donne que $\boxed{\sigma(ab) = \sigma(a).\sigma(b)}$.

b) Comme $2^n \wedge b = 1$, on sait, par a) (ii), que : $\sigma(n) = \sigma(2^n).\sigma(b)$. Or par la formule du a) (i), $\sigma(2^n) = \dfrac{1-2^{n+1}}{1-2} = 2^{n+1} - 1$.

D'où la formule : $\boxed{\sigma(n) = (2^{n+1} - 1)\sigma(b)}$.

c) Notons qu' au b), on n'a pas utilisé le fait que n était parfait. Mais avec $\sigma(n) = 2n$, la relation du b) devient $2n = (2^{a+1} - 1)\sigma(b)$ autrement dit :

$$2^{a+1}b = (2^{a+1} - 1)\sigma(b) \quad (*).$$

Comme $2^{a+1} \wedge (2^{a+1} - 1) = 1$, on sait alors par lemme de Gauss appliqué à $(*)$ que $2^{a+1} | \sigma(b)$ autrement dit qu'il existe un $c \in \mathbb{N}$ tel que $\boxed{\sigma(b) = 2^{a+1}c \quad (1)}$

En remplaçant dans l'équation $(*)$, on obtient $\boxed{b = (2^{a+1} - 1)c \quad (2)}$.

d) Considérons les deux égalités obtenues au c). Avec (2) on a : $b = 2^{a+1}c - c$ donc

$$2^{a+1}c = b + c \quad (2').$$

Avec (1), on obtient :

$$\sigma(b) = b + c \quad (1').$$

Supposons, *par l'absurde* que $c > 1$, alors avec $b = (2^{a+1} - 1).c$ on aurait une décomposition non triviale de b car $c > 1$ et $2^{a+1} - 1 > 1$ (car $a \ge 1$).

Donc en particulier, c étant un diviseur non trivial de b, on aurait $\sigma(b) \ge 1 + b + c$ (en faisant la somme des deux diviseurs triviaux de b et c). Or ceci est une *contradiction* avec $(1')$.

Ainsi $c = 1$ et $b = (2^{a+1} - 1)$ et $\sigma(b) = 2^{a+1}$ mais cette dernière égalité signifie que $2^{a+1} - 1$ n'admet comme diviseurs que les triviaux puisque $1 + (2^{a+1} - 1)$ fait déjà 2^{a+1}.

Donc $\boxed{2^{a+1} - 1 \text{ est premier}}$.

e) On a bien montré que si $\boxed{n \text{ est parfait pair alors } n = 2^a(2^{a+1} - 1) \text{ avec } 2^{a+1} - 1 \text{ qui est premier.}}$

La réciproque, plus facile, a fait l'objet d'un exercice de la planche.

2 Des propriétés des nombres parfaits impairs... s'il en existe :

Soit $n \in \mathbb{N}^*$ un nombre parfait impair, en supposant que de tels nombres existent.

a) (i) *Montrons qu'on nombre parfait impair n'est pas le carré d'un entier.*

Par contraposée Soit n impair tel que $n = k^2$ avec $k \in \mathbb{N}^*$. Nous allons montrer que n ne peut pas être parfait.

Alors en écrivant la D.F.P. de k sous la forme $k = p_1^{k_1} \dots p_r^{k_r}$, on obtient la D.F.P. : $n = p_1^{2k_1} \dots p_r^{2k_r}$.

Avec la remarque du 1) a) (i), en notant $d(n)$ le nombre de diviseurs de n dans $\mathbb{N}$, on a alors :

$$d(n) = (2k_1 + 1) \dots (2k_r + 1).$$

Donc $d(n)$ est un nombre *impair*.

Or comme n est impair tous les diviseurs de n sont des nombres *impairs*. Donc $\sigma(n)$ est la somme d'un nombre *impair* de *nombres impairs*. Donc $\sigma(n)$ est *impaire* (réduire modulo 2).

Donc $\sigma(n)$ ne peut pas être égal à $2n$ donc n n'est pas parfait, ce qui achève la preuve par contraposée.

(ii) *Par l'absurde* supposons existe deux nombres premiers distincts p et q tels que $v_p(n) \equiv 1\,[2]$ et $v_q(n) \equiv 1\,[2]$.

On considère l'expression de $\sigma(n)$ trouvée au 1) a) (i) à savoir : $\sigma(n) = \dfrac{1-p_1^{\alpha_1+1}}{1-p_1} \cdots \dfrac{1-p_r^{\alpha_r+1}}{1-p_r}$.

Quitte à reindexer les facteurs premiers $p_1, \dots, p_r$ apparaissant dans la D.F.P., on peut prendre $p_1 = p$ et $p_2 = q$.

Et donc avec les notations précédentes, $\alpha_1 \equiv 1\,[2]$ et $\alpha_2 \equiv 1\,[2]$.

On s'intéresse alors à la parité des deux facteurs $\dfrac{1-p_1^{\alpha_1+1}}{1-p_1}$ et $\dfrac{1-p_2^{\alpha_1+1}}{1-p_2}$.

Comme n est impair, on sait que p_1 et p_2 sont des nombres premiers impairs.

En revenant à l'écriture de $\dfrac{1-p_1^{\alpha_1+1}}{1-p_1}$ sous la forme de la somme géométrique $\sum_{k=0}^{\alpha_1} p_1^k$ on constate que cette somme est formée de $(\alpha_1 + 1)$ termes, tous impairs, donc la somme est *paire*.

Ainsi, on obtient que $2 \mid \dfrac{1-p_1^{\alpha_1+1}}{1-p_1}$ et $2 \mid \dfrac{1-p_2^{\alpha_2+1}}{1-p_2}$, donc $\boxed{4 \mid \sigma(n)}$.

Or par hypothèse n est parfait donc $\sigma(n) = 2n$ donc $4 \mid 2n$ et finalement $2 \mid n$, ce qui est une *contradiction* avec le fait que n est *impair*.

Conclusion de ce raisonnement par l'absurde : il existe au plus un nombre premier $p \in \mathbb{P}$ tel que $v_p(n) \equiv 1\,[2]$.

Mais d'autre part, avec le (i), on sait que n n'est pas un carré, donc on sait qu'il n'est pas possible que toutes les valuations p-adiques de n soient paires.

On a donc montré $\boxed{\text{l'existence (i) et l'unicité (ii) d'un nombre premier } p \text{ tel que } v_p(n) \equiv 1\,[2].}$

(iii) Comme p est impair, on sait que $p \equiv 1\,[4]$ ou $p \equiv -1\,[4]$.

Par l'absurde si $p \equiv -1\,[4]$, alors $\sum_{k=0}^{a} p^k \equiv \sum_{k=0}^{a} (-1)^k\,[4]$.

Mais comme a est *impair* cette somme $\sum_{k=0}^{a} (-1)^k$ a un nombre *pair* de termes, donc il y a autant de termes valant 1 que de termes valant +1.

Ainsi $\sum_{k=0}^{a} p^k \equiv 0\,[4]$.

Comme cette somme $\sum_{k=0}^{a} p^k$ est un des facteurs de la formule donnant $\sigma(n)$, on conclut une nouvelle fois que $4 \mid \sigma(n)$, ce qui, comme au (ii), donne une *contradiction*.

Ainsi, on a montré que $\boxed{p \equiv 1\,[4]}$.

De même, on sait déjà que a est impair par déf. de a. Donc $a \equiv 1\,[4]$ ou bien $a \equiv -1\,[4]$.

En considérant toujours la même somme : $\sum_{k=0}^{a} p^k \equiv \sum_{k=0} 1\,[4]$ puisque $p \equiv 1\,[4]$.

Donc $\sum_{k=0}^{a} p^k \equiv (a+1)\ [4]$.

Mais si $a \equiv -1\ [4]$, on aurait encore $\sum_{k=0}^{a} p^k \equiv 0\ [4]$ et toujours la même contradiction.

Donc $\boxed{a \equiv 1\ \ [4].}$

Conclusion : comme demandé par l'énoncé, on a montré qu'il existe un unique nombre p tel que $v_p(n)$ est impair donc en notant $a = v_p(n)$, on sait que $n = p^a \prod_{i=2}^{r} p_i^{2k_i} = p^a m^2$ en posant $m = \prod_{i=2}^{r} p_i^{k_i} \in \mathbb{N}$. Et on a montré aussi que a et p sont congrus à 1 mod. 4.

b) (i) et (ii) *Comme je l'avais indiqué dans l'énoncé, ces deux résultats sont plus « classiques » que le reste du sujet. Mais ils ne sont pas autant « faciles » et le sujet était assez méchant de les demander sans décomposer en questions ! Il faut dire que c'était un sujet de préparations d'olympiades internationales pour élèves de terminales (très) « entrainés ». Je l'ai laissé tel quel pour voir (et je n'ai pas été déçu, au contraire !). Entre temps, une réponse au b) (ii) a été proposée à l'aide d'un exercice de la planche 20.5, même si nous verrons que ce n'est pas la seule approche possible ! Pour ne pas allonger ici,* **la solution complète du b) (i) sera traitée en appendice**. *Mais faisons déjà la remarque clef suivante pour le b) (i)*

b) (i) Notons $S = \{n \in \mathbb{N},\ \exists\ (a,b) \in\ \mathbb{N}^2, n = a^2+b^2\}$. Autrement dit S est l'ensemble des sommes de deux carrés.

Propriété clef : $\boxed{\text{l'ensemble } S \text{ des sommes de deux carrés est stable par produit.}}$

dém. Soit $(m,n) \in S^2$. On les note $m = a^2 + b^2$ et $n = c^2 + d^2$.

Là arrive *une idée assez géniale qui consiste à utiliser les nombres complexes !*

On remarque que $m = |(a+ib)|^2$ et $n = |(c+id)|^2$, donc

$$mn = |(a+ib)(c+id)|^2 = |(ac-bd)+i(ad+bc)|^2 = (ac-bd)^2 + (ad+bc)^2.$$

Donc $mn \in S$. □

Remarquer

Bien sûr qu'on peut vérifier *la formule :*

$$\boxed{(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2}$$

sans connaître les nombres complexes, mais c'est il est moins évident de trouver la formule.

b) (ii) Sens facile : sens $\Leftarrow$: supposons qu'il existe un $m \in \mathbb{N}$ tel que $m^2 \equiv -1\ [p]$,.

Comme p est premier, on sait par petit théorème de Fermat que $m^{p-1} \equiv 1\ [p]$.

Comme p est impair, $(p-1)/2$ est un entier, et on peut considérer $(-1)^{(p-1)/2} = (m^2)^{(p-1)/2} = m^{p-1} \equiv 1\ [p] \quad (*)$.

Or $(-1)^k \equiv 1\ [p]$ ssi k est pair. Donc ici avec $(*)$, on sait $(p-1)/2$ est pair, et on conclut bien que $p \equiv 1\ [4]$.

Sens $\Rightarrow$: par générosité voici pas moins de *trois méthodes, dont deux ne donneront cependant une solution complète qu'avec quelques compléments.*

(M1) Avec le théorème de Wilson : exercice de la planche 20. 5 :

Je renvoie au corrigé de cet exo où l'on montre que, dans $\mathbb{Z}/p\mathbb{Z}$:

$$\left(\prod_{k=1}^{(p-1)/2} \overline{k} \right)^2 = -\overline{1},$$

ce qui non seulement montre que $-\overline{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ mais donne une expression de ses deux racines carrées. □

(M2) et (M3) elles reposent sur un argument plus abstrait relatif à la taille de l'ensemble $\mathcal{C}$ des carrés dans $\mathbb{Z}/p\mathbb{Z}*$.

Partie commune à (M2) et (M3) :

On note $\mathcal{C}^* = \{x^2,\ x \in \mathbb{Z}/p\mathbb{Z}^*\}$ l'ensemble des carrés des éléments de $\mathbb{Z}/p\mathbb{Z}^*$.

On va démontrer le lemme plus général suivant :

Lemme (Euler) :

$$\boxed{\forall\, x \in \mathbb{Z}/p\mathbb{Z}^*,\ x \in \mathcal{C}^* \Leftrightarrow x^{(p-1)/2} = \overline{1} \text{ dans } \mathbb{Z}/p\mathbb{Z}.}$$

Comme $(-\overline{1})^{(p-1)/2} = \overline{1} \Leftrightarrow p \equiv 1\ [4]$, on aura en particulier montré l'équivalence demandée dans ce b).

Bien sûr on a déjà vu le sens $\Leftarrow$ de l'équivalence du lemme. Pour le sens $\Rightarrow$ on peut utiliser deux arguments mais qui tous deux demandent un peu plus de culture mathématique

(M2) avec quelques notions sur les polynômes : Notons $\mathcal{S}$ l'ensemble des $x \in \mathbb{Z}/p\mathbb{Z}$ tels que $x^{(p-1)/2} = \overline{1}$.

On sait déjà que $\mathcal{S} \subset \mathcal{C}^*$, on veut montrer l'égalité de ces deux ensembles, on peut comparer leurs cardinaux.

• Pour l'ensemble $\mathcal{C}^*$ c'est assez facile :

On considère l'application : $\varphi : \mathbb{K}^* \to \mathbb{K}^*$, $x \mapsto \varphi(x) = x^2$.

On remarque que $\mathcal{C}^* = \varphi(\mathbb{K}^*)$. Par intégrité de $\mathbb{K}^*$, chaque élément de $\mathcal{C}^*$ a exactement deux antécédents distincts par φ.

Ceci démontre que $\boxed{\text{Card}(\mathcal{C}^*) = (p-1)/2}$ (*ce que nous avons vu dans beaucoup d'exemples concrets*).

• Pour l'ensemble $\mathcal{S}$: $\mathcal{S}$ est l'ensemble des zéros de la fonction polynomiale $x \mapsto x^{(p-1)/2} - \overline{1}$ de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même.

Si l'on admet qu'une telle fonction polynomiale n'a pas plus de $(p-1)/2$ zéros, comme dans le cas vu pour les fonctions polynomiales réelles ou complexes, on obtient tout de suite que $\text{Card}(\mathcal{S}) \leq (p-1)/2$.

Comme $\mathcal{C}^* \subset \mathcal{S}$ et que $\text{Card}(\mathcal{C}^*) = (p-1)/2 \geq \text{Card}(\mathcal{S})$ on conclut bien que $\mathcal{S} = \mathcal{C}^*$ ce qui démontre le lemme d'Euler.

N.B. Bien sûr resterait à démontrer le résultats sur les zéros des polynômes. Nous traiterons cela plus tard avec le chapitre sur les polynômes sur un corps quelconque. Il faut être quand même un peu prudent avec les fonctions polynomiales sur un corps finis (il n'y pas unicité de l'écriture de la fonction, par exemple $x \mapsto x^p - x$ est la fonction nulle sur $\mathbb{Z}/p\mathbb{Z}$ par petit théorème de Fermat, mais le résultat utilisé ici est vrai, et suffisamment intuitif pour que certains d'entre vous l'aient utilisé dans leur rédaction.

(M3) avec quelques notions en plus de théorie des groupes : voir D.M. 9 de l'an dernier.

On montre facilement que $(\mathcal{C}^*, \times)$ est un groupe, et (D.M. 9 de l'an dernier mais nous reprendrons cela forcément à un moment), si $(G, \times)$ est un groupe fini à N éléments, on peut montrer que pour tout $x \in G$, $x^N = e$ le neutre de G.

Donc ici pour tout $x \in \mathcal{C}^*$, $x^{(p-1)/2} = \overline{1}$ et c'est déjà fini. □

b) (iii) **Remarque :** Considérons les carrés dans $\mathbb{Z}/4\mathbb{Z}$: $\overline{2}^2 = \overline{0}$ et $\overline{3}^2 = (-\overline{1})^2 = \overline{1}$. Donc $\overline{0}$ et $\overline{1}$ sont les seuls carrés dans $\mathbb{Z}/4\mathbb{Z}$.

Sens $\Rightarrow$ si $p = a^2 + b^2$. Alors dans $\mathbb{Z}/4\mathbb{Z}$, d'après la remarque ci-dessus, $\overline{p} = \overline{a}^2 + \overline{b}^2 \in \{\overline{0}, \overline{1}, \overline{2}\}$.

Mais comme p est impair, la seule possibilité est que $p \equiv 1\ [4]$.

Sens $\Leftarrow$: si $p \equiv 1\ [4]$. Par le (ii), il existe un $a \in \mathbb{Z}$ tel que $a^2 \equiv -1\ [p]$. Donc $a^2 + 1 \equiv 0\ [p]$.

Donc $p | (a^2 + 1^2)$, avec $a \wedge 1 = 1$ donc par le (i), on conclut que p est la somme de deux carrés.

b) (iv) Soit n un nombre imparfait impair. Alors par le a), il existe $(p, a, m) \in (\mathbb{N}^*)^3$ tel que $n = p^a.m^2$ avec $p \in \mathbb{P}$, $p \equiv 1\ [4]$ et $a \equiv 1\ [4]$.

Comme $p \in \mathbb{P}$ et $p \equiv 1\ [4]$, par le (iii), il existe $(\alpha, \beta) \in \mathbb{N}^2$, $p = \alpha^2 + \beta^2$.

Donc $n = (\alpha^2 + \beta^2)^a.m^2$. Comme l'ensemble S des sommes de deux carrés est stable par produit (cf. la prop. clef du b) (i)), et que $(\alpha^2 + \beta^2) \in S$ et $m^2 = m^2 + 0^2 \in S$, on conclut que $n \in S$. □

b) (v) Soit n un nombre parfait pair. D'après le résultat de la première partie, il s'écrit $n = 2^a(2^{a+1} - 1)$ où $2^{a+1} - 1$ est premier.

(Remarquons qu'on sait aussi que si $2^{a+1} - 1$ est premier alors $a + 1 = p \in \mathbb{P}$ d'après l'exercice sur les nombres de Mersenne).

On note donc plutôt $n = 2^{p-1}(2^p - 1)$.

Si $n = a^2 + b^2$ avec $(a, b) \in \mathbb{N}^2$, on a donc $a^2 + b^2 = 2^{p-1}(2^p - 1)$.

Soit $d = a \wedge b$, on note $a = a_1 d$ et $b = b_1 d$ avec $a_1 \wedge b_1 = 1$.

On obtient $d^2(a_1^2+b_1^2)=2^{p-1}(2^p-1)$. Donc $d^2|2^{p-1}(2^p-1)$ et comme $2^p-1\in\mathbb{P}$, on en déduit : $d^2|2^{p-1}$.

Or les diviseurs de 2^{p-1} sont de la forme 2^k pour un certain $k\leq p-1$. Donc $d^2=2^k$ pour un certain $k\in[\![0,p-1]\!]$.

On peut écrire $2^k(a_1^2+b_1^2)=2^{p-1}(2^p-1)$, donc $(a_1^2+b_1^2)=2^{p-1-k}(2^p-1)$ avec $p-1-k\geq 0$.

Ainsi le nombre premier 2^p-1 divise $a_1^2+b_1^2$.

Par le (i), on en déduit que peut s'écrire $2^p-1=\alpha^2+\beta^2$.

Or 2^p-1 est un nombre premier impair, donc par le (iii) (sens facile), comme il s'écrit comme somme de deux carrés, $2^p-1\equiv 1\ [4]$. Donc $2^p\equiv 2\ [4]$.

Mais ceci force $p=1$ ce qui est impossible car alors $n=2^0(2-1)=1$, qui n'est pas pair.

D'où la *contradiction.*

c) (i) Par le théorème de Pythagore, un nombre n est l'hypoténuse d'un triangle rectangle à côté de longueur entière ssi il existe $(a,b)\in(\mathbb{N}^*)^2$ tel que $n^2=a^2+b^2$.

Il est important de bien spécifier que a et b sont tous les deux **non nuls**, *sinon il est trivial avec $a=n$ et $b=0$ que la condition est vérifiée pour tout entier $n\in\mathbb{N}$.*

Soit n un nombre parfait impair.

On a montré au b) (iv) que $n=a^2+b^2\quad(*)$ avec $(a,b)\in\mathbb{N}^2$.

Comme n est un nombre parfait impair, on sait par le a) (i) que n n'est *pas* un carré d'entier.

Donc dans l'égalité $(*)$ les deux nombres a et b sont non nuls.

Alors $n^2=(a^2+b^2)^2=A^2+B^2$ avec $A=(a^2-b^2)$ et $B=2ab$ par la formule donnée au b) (i).

Comme a et b sont non nuls on sait que $B\neq 0$.

Reste à montrer que $A\neq 0$.

Par l'absurde si $A=0$, on aurait $a=b$ donc $n=2a^2+2b^2$ et n serait pair, ce qui est exclu.

Donc $A\neq 0$, et donc $n^2=A^2+B^2$ avec $A\neq 0$ et $B\neq 0$, c.q.f.d.

c) (ii) Cette fois, le résultat du b) (v) ne suffit pas. Soit n un nombre parfait pair ; on sait que $n\notin S$, mais cela ne suffit certes pas pour dire quelque chose sur n^2...

En revanche, on peut reprendre la *démonstration* du b) (v).

On note $n=2^{p-1}(2^p-1)$.

Par l'absurde si $n^2=a^2+b^2$ avec $(a,b)\in(\mathbb{N}^*)^2$, on a donc $a^2+b^2=(2^{p-1}(2^p-1))^2$.

Soit $d=a\wedge b$, on note $a=a_1d$ et $b=b_1d$ avec $a_1\wedge b_1=1$.

On obtient $d^2(a_1^2+b_1^2)=2^{2p-2}(2^p-1)^2\quad(*)$. Donc $d^2|2^{2p-2}(2^p-1)^2$ donc $d|2^{p-1}(2^p-1)$.

Comme $2^p-1\in\mathbb{P}$, on connaît la forme de d, deux cas sont possibles :

• Cas 1 : $d=2^k$ avec $k\leq p-1$. On obtient dans ce cas la *même contradiction* qu'au b) (v).

En effet, dans ce cas, $(*)$ devient $2^{2k}(a_1^2+b_1^2)=2^{2p-2}(2^p-1)^2$ donc $a_1^2+b_1^2=2^{2p-2-2k}(2^p-1)^2$ avec $2p-2-2k\geq 0$.

Donc $(2^p-1)|a_1^2+b_1^2$ ce qui donne la même contradiction qu'au b) (v).

• Cas 2 : $d=2^k(2^p-1)$ avec $k\leq p-1$.

Alors $(*)$ devient $2^{2k}(2^p-1)^2(a_1^2+b_1^2)=2^{2p-2}(2^p-1)^2$.

Donc $a_1^2+b_1^2=2^{2p-2-2k}\quad(**)$ avec $2p-2-2k\geq 0$.

Mais $a_1\wedge b_1=1$, donc l'un a_1 et b_1 ne sont pas pairs tous les deux, donc l'un des deux termes a_1^2 ou b_1^2 est congru à 1 modulo 4 (l'autre pouvant être congru à 0 ou à 1 modulo 4).

Ainsi $a_1^2+b_1^2\equiv 0\ [4]$ ou $a_1^2+b_1^2\equiv 2\ [4]$.

Or si $k<p-1$, $2^{2(p-1-k)}=(2^2)^{p-1-k}=4^{p-1-k}\equiv 0\ [4]$ et donc l'égalité $(**)$ donne une contradiction.

Reste le cas où $k=p-1$, mais dans ce cas $(**)$ donne que $a_1^2+b_1^2=1$ ce qui est impossible avec $a_1\neq 0$ et $b_1\neq 0$, ce qui est supposé au départ puisque $(a,b)\in(\mathbb{N}^*)^2$.

Donc dans tous les cas, on a obtenu une *contradiction.*

Donc on a bien montré que n n'est pas l'hypoténuse d'un triangle rectangle.

d) (i) Soit n un nombre parfait impair. *Par l'absurde, supposons que* $n\equiv 5\ [6]$.

On a vu au a) que $n=p^am^2$ avec $p\equiv 1\ [4]$

Première étape :*on va en déduire par C.N. la classe de m et p modulo* 6

Classe de n modulo 4 : . Comme p est impair, m est impair et donc $m^2\equiv 1\ [4]$.

Donc $n\equiv p^am^2\equiv 1\ [4]$.

Classe de n modulo 6 : On veut montrer que $n\not\equiv 5\ [6]$.

Les carrés modulo 6 sont congrus à $0, 1, 3, 4$. Et comme m est impair, m^2 ne peut être congru qu'à 1 ou 3 modulo 6.

D'autre part p est un nombre premier impair donc p est congru à $1, 3$ ou 5 modulo 6. Mais mieux, p est un nombre premier congru à 1 modulo 4 donc en particulier $p \neq 3$. Or si $p \equiv 3$ [6], on aurait $3|p$, et comme p est premier, $p = 3$, ce qui est exclu. Donc $p \equiv 1$ ou $p \equiv -1$ modulo 6.

En résumé, on a :

• deux cas pour la classe de m^2 modulo 6 : $m^2 \equiv 1$ ou $m^2 \equiv 3$ modulo 6.

• deux cas pour la classe de p^a modulo 6 : $p^a \equiv 1$ ou $p^a \equiv -1$ modulo 6.

On obtient le tableau (de classe modulo 6) :

m^2	1	3	1	3
p^a	1	1	-1	-1
m^2p^a	1	3	-1	-3

Dans la dernière ligne de ce tableau, bien sûr $-3 \equiv 3$ [6]. Mais ce tableau nous dit que

si $m^2p^\alpha \equiv -1$ [6] alors $m^2 \equiv 1$ [6] et $p^a \equiv -1$ [6], et mieux, $p \equiv -1$ [6].

Deuxième étape : *en revenant à la condition n est parfait, on va obtenir une contradiction*

A partir de l'écriture $n = p^a m^2$ avec $p^a \wedge m^2 = 1$, on sait que $\sigma(n) = \sigma(p^a).\sigma(m^2) = \dfrac{p^{a+1}-1}{p-1}.\sigma(m^2)$.

Or $p \equiv -1$ [6] et on se souvient que $a \equiv 1$ [4] donc $a+1$ est pair donc $p^{a+1} - 1 \equiv 0$ [6].

Donc avec l'égalité $(p-1)\sigma(n) = (p^{a+1}-1)m^2$, on obtient que $(p-1)\sigma(n) \equiv 0$ [6] et comme on a vu que $p \equiv -1$ [6], on obtient $-2\sigma(n) \equiv 0$ [6] ou encore $2\sigma(n) \equiv 0$ [6].

Ceci équivaut à dire que $2\sigma(n) = 6k$ avec $k \in \mathbb{N}$ donc $\sigma(n) = 3k$ avec $k \in \mathbb{N}$.

Mais *comme n est parfait (il faut bien l'utiliser à un moment)*, $\sigma(n) = 2n$ donc $3|2n$ et donc $3|n$.

Mais alors $n \equiv 0$ [6] ou $n \equiv 3$ [6] *contradiction avec notre hypothèse de départ* $n \equiv 5$ [6].

d) (ii) Par le (i), on sait que $n \equiv 1$ [4] et ($n \equiv 1$[6] ou $n \equiv 3$ [6]).

1er cas : si $n \equiv 1$ [6].

En particulier $n \equiv 1$ [3]. Comme $3 \wedge 4 = 1$, on sait que les deux conditions $n \equiv 1$ [4] et $n \equiv 1$ [3] donnent alors $\boxed{n \equiv 1\ [12]}$.

(Car 3 et 4 divisent $n-1$ et donc $ppcm(3,4) = 12$ divise $n-1$).

2ème cas : si $n \equiv 3$ [6].

Alors $n \equiv 0$ [3] et $n \equiv 1$ [4] ce qui peut se réécrire (à l'aide d'un représentant commun) : $n \equiv 9$ [3] et $n \equiv 9$[4].

On en déduit de même, comme $3 \wedge 4 = 1$, que $\boxed{n \equiv 9\ [12]}$.

Mais l'énoncé demande, mieux, de montrer que $n \equiv 9$ [36]*, alors on continue !* on note $n = 9 + 12k$.

Pour montrer que $n \equiv 9$ [36], il suffit de montrer que k est encore un multiple de 3.

Or, comme $n \equiv 9$ [12], on sait alors $3|n$.

Or $n = p^a m^2$ et p est premier différent de 3 (car $p \equiv 1$ [4]), donc $3|m^2$ donc $3|m$.

Donc $3^2|m^2$ donc $3^2|n$.

On a donc obtenu que $9|n$ et on savait que $n \equiv 9$ [12].

Parmi les trois représentants $9, 21, 33$ de 9 modulo 36, seul 9 est divisible par 9, on conclut donc enfin que $\boxed{n \equiv 9\ [36]}$.

Appendice : preuve du b) (i) et plus...

L'énoncé propose une méthode de descente de Fermat*. Il faut savoir qu'en effet Fermat a cité ce résultat, en disant qu'il en avait une preuve très sûre.. mais sans guère plus expliciter la démonstration qu'en faisant allusion à ce même argument de descente que nous avons déjà rencontré en exercice ! Cette question b) (i) est la seule qui n'a pas été traitée entièrement par un ou l'autre des courageux qui ont fait le DM.. et pour cause... c'était vraiment brut comme énoncé, mais les solutions esquissées n'étaient pas loin quand même ! Si ce qui suit vous rebute, sachez qu'il y a des méthodes plus agréables pour arriver à ce résultat par exemple grâce aux propriétés de l'anneau* $\mathbb{Z}[i]$.

Théorème de descente de Fermat : Soit $(a, b) \in \mathbb{Z}^2$ tel que $a \wedge b = 1$. Soit $p \in \mathbb{P}$ tel que $p|a^2 + b^2$. Alors p s'écrit $p = \alpha^2 + \beta^2$ avec $(\alpha, \beta) \in \mathbb{Z}^2$.

Pourquoi ce théorème de descente suffit pour répondre à la question posée : Soit $n \in \mathbb{N}^*$ tel que $n|a^2+b^2$. Par le théorème de descente, chaque facteur premier p_i apparaissant dans la D.F.P. de n s'écrit $p_i = \alpha_i^2 + \beta_i^2$.

Par la propriété de stabilité par produit de l'ensemble S des sommes de deux carrés mentionné au b) (i) dans le corps du corrigé, on en déduit que $n = p_1^{m_1} \dots p_r^{m_r}$ est aussi dans S. □

Preuve du théorème de descente : On utilisera le lemme suivant :

Lemme de division Notons $N = a^2+b^2$ où $a \wedge b = 1$. Supposons qu'on ait un diviseur premier q de N qui s'écrive sous la forme $q = x^2+y^2$ avec $(x,y) \in \mathbb{Z}^2$. Alors l'entier N/q s'écrit aussi c^2+d^2 avec $c \wedge d = 1$.

Preuve du lemme division :

Fil directeur pour ce qui suit : on veut obtenir un écriture de $N = q.N/q$ de la forme :

$$a^2+b^2 = (x^2+y^2)(c^2+d^2) \quad (C)$$

Or par la relation mentionnée au b) (i) du corps du corrigé, on sait que :

$$(x^2+y^2)(c^2+d^2) = (xc-yd)^2 + (xd+yc)^2$$

Donc pour montrer le lemme, c'est-à-dire avoir une égalité comme (C), il suffit de trouver des entier c et d tels que :

$$\begin{aligned} a &= cx - dy, \\ b &= dx + cy. \end{aligned}$$

Comme $q = x^2+y^2$ divise $N = a^2+b^2$, on peut aussi remarquer que q divise $x^2N - a^2q$. Or

$$\begin{aligned} x^2N - a^2q &= x^2(a^2+b^2) - a^2(x^2+y^2), \\ &= x^2b^2 - a^2y^2 = (xb-ay)(xb+ay). \end{aligned}$$

Comme q est premier, q doit diviser un des deux facteurs $(xb-ay)$ ou $(xb+ay)$ et quitte à changer le signe de a, ce qui ne change pas N, on peut supposer SRdG que $q|xb-ay$, ce qu'on écrira $xb-ay = qd$ où $d \in \mathbb{Z}$.

Affirmation : $x|(a+dy)$.

Preuve de l'affirmation :

$$\begin{aligned} (a+dy)y &= ay + dy^2 = xb - dq + dy^2, \\ &= xb - d(x^2+y^2) + dy^2 = xb - dx^2, \end{aligned}$$

et ce denier terme est visiblement divisible par x. □

Retour à la preuve du lemme : Grâce à l'affirmation précédente, on peut noter $a+dy = cx$ où $c \in \mathbb{Z}$.

Ceci permet d'avoir l'écriture sympathique recherchée aussi bien pour a que pour b :

$$\begin{aligned} a &= cx - dy, \\ b &= dx + cy \end{aligned}$$

et démontre le lemme (c et d sont premiers entre eux car tout diviseur commun à c et d donnerait immédiatement un diviseur commun à a et b vu que $a = cx-dy$ et $b = dx+cy$). □

Application du lemme à la preuve du théorème de descente de Fermat :

Soit p un nombre premier impair qui divise $N = a^2+b^2$ où $a \wedge b = 1$. (Le cas où $p = 2$ est trivial, car $2 = 1^2+1^2$).

Par l'absurde si p ne s'écrit pas comme somme de deux carrés.

On considère a_1 (resp. b_1) l'unique représentant de a (resp. de b), modulo p tel que $|a_1| < p/2$ (resp. $|b_1| < p/2$).

(Ceci est toujours possible car $]\!]-(p-1)/2, (p-1)/2]\!]$ fournit un système complet de représentants modulo p).

Alors, en notant $N_1 = a_1^2 + b_1^2$, on a encore $N_1 \equiv N \equiv 0\ [p]$, mais avec l'avantage que $|N_1| < (p/2)^2 + (p/2)^2 = p^2/2$. On ne connaît pas le p.g.c.d. de a_1 et b_1, mais si on note $d = a_1 \wedge b_1$, on sait que p ne divise pas d, car sinon, il diviserait aussi a et b. En considérant $a_2 = a_1/d$ et $b_2 = b_1/d$, et $N_2 = a_2^2 + b_2^2$, on dispose maintenant d'un nombre $N_2 = a_2^2 + b_2^2$ avec $a_2 \wedge b_2 = 1$, tel que $p|N_2$, et $|N_2| < p^2/2$.

Alors avec l'inégalité $|N_2| < p^2/2$, on sait que tous les autres diviseurs premiers q_i de N_2 vérifient l'inégalité que $q_i < p$. Mieux, si on écrit la D.F.P. de N_2 sous la forme $N_2 = pq_1^{m_1} \dots q_r^{m_r}$, on sait que $q_1^{m_1} \dots q_r^{m_r} < p/2$.

Si tous les q_i s'écrivent sous la forme $q_i = \alpha_i^2 + \beta_i^2$, alors en appliquant de manière répétée le lemme de division [1], on obtiendra que $p = N/(q_1^{m_1} \dots q_r^{m_r})$ est aussi une somme de deux carrés, ce qui est contraire à notre hypothèse.

Donc il existe un diviseur premier $q_{i_0} < p$ qui ne s'écrit pas comme somme de deux carrés. Mais alors on peut alors reprendre le même raisonnement en remplaçant p par q_{i_0} et on construit ainsi une suite strictement décroissante de nombres premiers, ce qui donne une *contradiction*, ouf ! □

1. On l'applique m_1 fois avec q_1 pour obtenir successivement que N_2/q_1, puis N_2/q_1^2, jusqu'à N_2/q_1^{m-1} sont somme de deux carrés, puis de même avec les autres q_i