

PREAMBULE

Si l'idée merveilleuse de Fermat était :

Où choisir un couple de paramètres p et q , formant un triplet de racines carrées : x' , y' , z' vérifiant l'égalité

$$X + Y = Z \text{ tel que } x^N + y^N = z^N \quad ?$$

La formule des triplets pythagoriciens donne un triplet de racines carrées.

$\sqrt{X}, \sqrt{Y}, \sqrt{Z}$; avec $X = x^N$; $Y = y^N$ et $Z = z^N$.

Elle donne toutes les solutions entières, $X + Y = Z$. soit : $(p^2 - q^2)^2 + (2pq)^2 = (p^2 + q^2)^2$ avec p et q , qui parcourent l'ensemble des entiers naturels, dans la puissance $N=1$.

En utilisant la relation du théorème de Pythagore on vérifie par la même une équation de Fermat sans perte de généralité !

$$p^2 - q^2 = \sqrt{X}, 2pq = \sqrt{Y}, \text{ et } p^2 + q^2 = \sqrt{Z}$$

Contrairement à l'idée générale, en démontrant le cas $N > 2$ et pair ; peut on alors résoudre de façon générale le cas N premier > 2 . C'est ce que l'on va montrer.

Des lors il a pu se demander :

Est ce qu'un couple p' et q' : réels, algébriques ou non, peut donner un triplet d'entiers, vérifiant son égalité, dans un premiers temps pour $N > 2$ et pair ; qui ne serait pas donné, ou différent , de ceux donné par p et q entiers non nuls premiers entre eux !

Avec un facteur commun K ; pour $K > 1$; il y en a une infinité pour le premier ; $p' = 2 (\sqrt{2})$, et $q' = \sqrt{2}$ donné par $p=2$, $q=1$ et $K=2$; soit le triplet 6, 8 et 10 .

Donc les seules solutions qui nous intéressent sont les primitives avec $K = 1$; car bien entendu, ces solutions multiples d'une solution primitive, données par p' et q' réels, ne sont pas différentes de celle donnée justement par p et q et un facteur $K > 1$, ce qui n'apporte rien de plus ni une contradiction!

Dans un triplet pythagoricien défini par la formule pythagorique, $p^2 - q^2 = X$, $2pq = Y$ et $p^2 + q^2 = Z$, avec X, Y et Z entiers naturels non nuls, premiers entre eux ; où p et q sont choisis dans les racines carrées c'est-à-dire dans les entiers naturels à la puissance $N=1$; premiers entre eux et de parité différente, et où X, Y et Z sont trois racines carrées entières ; donc des produits de puissance $N = 1, 2, 3 \dots n$ premiers !

Il est impossible d'obtenir une solution, dans une puissance pair > 2 ; tel que :

$$(p^2 - q^2)^2 + (2pq)^2 = (p^2 + q^2)^2. \text{ Soit l'égalité } X^2 + Y^2 = Z^2.$$

(« Equivalents à la notation $X + Y = Z$ dans $N = 1$; ex : $9 + 16 = 25$ qui vérifie l'équation de Fermat pour $N = 2$, et la relation de Pythagore, en mettant les segments du triangle rectangle aux carrés, soit : 3, 4 et 5 pour cet exemple. Bien entendu $9^1 + 16^1 = 25^1$, Ne peut en aucun cas être un triplet Pythagoricien 9 et 16 formerait un angle plat 180° sur lequel se superpose, l'hypoténuse ! »)

Du fait qu'il ne peut exister, tout d'abord ; pour $N = 4$:

a) x^2 et y^2 dans un triplet pythagoricien tel que $p^2 - q^2 = x^2 = X$, et $2pq = y^2 = Y$

(« Descente infinie de Fermat et les lemmes 4,3,2 et 1 en annexe A, à la fin, qui vont avec, pour démontrer le cas $N = 4$, voir sur internet. Dont Fermat n'avait nul besoin à priori, et ceci est valable pour p' et q' réel. Donc si il existe x^2 et y^2 alors, **z n'est pas un entier** et ce triplet ne pourrait être donné par p et q entier. Ceci fait remarquer : que p' et q' ne donnent un tel triplet primitif dans $N=1$ ainsi que dans $N=2$, avec **z entier** !»)

b) x^2 et z^2 dans un triplet pythagoricien tel que $p^2 - q^2 = x^2 = X$, et $p^2 + q^2 = z^2 = Z$
En effet :

1) Un triplet Pythagoricien n'est jamais solution, sans être mis au carré, ou la formule qui donne les triplets Pythagoricien serait fausse, (« elle ne peut donner une solution qui soit un triplet, avec le même couple de paramètres !(les deux côtés doivent former un angle de 90°) »)

2) si $p^2 - q^2 = X = x'^2$, alors p , q et x' sont pythagoriques, p et q ont été choisis dans un triplet pythagorique inférieur, donné par p_1' et $q_1' < p$ et q . On peut dire $p = z'$ et $q = y'$ soit :

$z'^2 - y'^2 = x'^2$ (« **note et par supposition** : p' et q' peuvent être des entiers, réels ou réels algébriques »)

Mais si $p^2 + q^2 = Z = z^2$, p , q et z sont aussi pythagoriques ; et p et q ont été choisis dans le même triplet pythagorique inférieur, donné par le même couple de paramètre p_2' et q_2' ; ce qui est absurde, $X \neq Z$ ou $z'^2 + y'^2 = z^2$; $z' \neq x'$; $p^2 - q^2 \neq p^2 + q^2$. (« L'hypoténuse ne peut être **égale au côté opposé à l'hypoténuse**.

Donc le triplet ne peut être donné par la formule pythagorique. p et q change de valeur pour chaque triplet Pythagoricien ; mais il en ressort, que ceci est aussi valable pour p' et q' réels, ils ne pourraient donner ces deux triplets. **Mais surtout**, ils ne pourraient avoir paramétrés ces deux solutions : $z'^2 + y'^2 = z^2$ et $z'^2 - y'^2 = x'^2$ Donc pas de triplets de ce types dans $N = 1$ et 2 »)

Conclusion et propriété : un triplet Pythagoricien, ne peut être solution par addition et soustraction tel que :

$p^2 - q^2 = X = x^2$ vrai, (donc il existe une solution inférieur $z'^2 - y'^2 = x^2$, avec un couple de paramètre $< p$ et q !) Mais $p^2 + q^2 = Z = z^2$ soit

$z'^2 + y'^2 = z^2$, il faudrait que $z' = x'$, ce qui est absurde, donc $p = z'$ ou x' **mais pas les deux !**

Ou de façon différente, il existerait :

$2p_1'q_1' = q = y'$ ainsi que $2p_2'q_2' = q = y'$ c'est-à-dire : $p_1' = p_2' = p''$ et $q_1' = q_2' = q''$
deux triplets donnés par un même couple de paramètre p'' et q'' ce qui est absurde !

Alors **si et seulement si** il existe dans un triplet Pythagoricien, tel que défini, x^2 et z^2 ; les paramètres p et q **ne peuvent être** des entiers et $2pq = Y$ non plus ! par conséquent **ce ne pourrait être** une solution primitive dans $N = 2$, **avec Y entier**, en choisissant p' et q' dans les réels algébriques ou non ; à la rigueur une solution dans $N = 1$ uniquement, par exemple : $1 + 80 = 81$!

(« il devient déjà évident , que p et q vont ce généraliser et interdire une solution dans une puissance pair > 2 , c'est-à-dire que p et q , ne peuvent être deux produits de puissance N premier et devant donner x^N et z^N par addition et soustraction, ce que nous verrons en détail. »)

3)

Démonstration du cas Z^2 et Y^2 égale à : $p^2 + q^2$ et à $2pq$

c) Il ne peut exister, z^2 et y^2 dans un triplet pythagoricien tel que :
 $p^2 + q^2 = Z = z^2$ et $2pq = Y = y^2$. En effet : idem 2) de b) car :

3) si $p^2 + q^2 = Z = z^2$ et $2pq = Y = y^2$ alors p, q et d tel que $d = p - q$ sont pythagoricien. Car, dans un triplet primitif, $(p^2 + q^2) - (2pq) = (p - q)^2$ donc $z^2 - y^2 = d^2$, par conséquent : p, q et d, sont pythagoriciens, c'est à dire, choisis dans un triplet inférieur donné par p' et $q' < p$ et q ; ce qui est impossible car:
 $[d^2 = (p - q)^2] \neq [X = p^2 - q^2]$ et encore moins la solution : $(p^2 + q^2)^2 - (2pq)^2 = (p - q)^2$, mais plutôt $(p^2 - q^2)^2$!

a')

Le contraire laisserait supposer que $d^2 + y^2 = z^2$ vérifie le théorème de Pythagore sans que les deux côtés y^2 et z^2 l'hypoténuse, soit mis au carré !

(« de plus $X = p^2 - q^2 = d^2 + (d n)$, avec $n = 2$, pour $q = 1$, d'où $n = 2q$; et $q + d = p$; exemple avec le triplet 15, 8 et 17 : $X = 15$, $d^2 = 9$, $(d n) = 6$
 $(d n) / d = 2q = 2$, soit $2/2 = q = 1$ et $1 + d = p = 4$ soit $4^2 - 1^2 = X = 15$; formule permettant de retrouver p et q en fonction de x, y et z quel qu'ils soient. »)

b')

Le carré de l'hypoténuse (« et non l'hypoténuse ») est égal, à la somme des carrés des côtés de l'angle droit,

(« et non avec un côté Y et sa différence d au carré, avec l'hypoténuse ! c'est-à-dire :
 $(p^2 + q^2)^2 - (2pq) = (p - q)^2$, ce qui est absurde. »)

Là encore la formule des triplets Pythagoriciens, serait fausse, ainsi que l'égalité suivante :
 $(z^2 + y^2)(z^2 - y^2) \neq (x^2)^2$ du fait de la propriété pythagorique qui donne :
 $(z + y)(z - y) = (X)^2$, avec X qui peut être un carré des l'instant où p et q sont pythagoricien
 $= z'$ et y' !

Sans oublier la contradiction 2) de b) ci-dessus, qui serait aussi fausse, en remplaçant z et y par p et q, soit : $p^2 + q^2 = u^2$ (1) et $p^2 - q^2 = v^2$ (2) ; où $(u^2 v^2) = (x^2)^2$ ou tout simplement X^2 .

On en déduit bien que si z et y était deux carrés alors X et d, ne serait des entiers ; et ceci est toujours aussi valable pour p' et q' réels !

Soit l'égalité : $((p^2 + q^2) + (2pq))((p^2 + q^2) - (2pq)) = (p^2 - q^2)^2$.

Enfin, si z et y avait été deux carrés, on retombe dans une descente infini d'entiers (que le lecteur pourra vérifier, Mais dont Fermat n'ignorait pas) ; car ces deux nombres $(z^2 + y^2)$ et $(z^2 - y^2)$ devant donner $(x^2)^2$ et comme ils sont premiers entre eux deux à deux, il sont eux même des carrés $(z^2 + y^2) = u^2$ et $(z^2 - y^2) = v^2$. ce que l'on vient de montrer impossible, par addition et soustraction.

(« $p^2 + q^2 = z^2$ et $2pq = y^2$. Il existe alors : p' et $q' < p$ et q tel que :
 $p'^2 - q'^2 = p = x'$ et $2p' q' = q = y'$. Ce qui donne bien : $x'^2 + y'^2 = z^2$ et $2x' y' = y^2$; or si $2pq = y^2$, (« p est un carré et q un demi carré ») ceci est équivalent à :
 $2(p'^2 - q'^2)(2p' q') = y^2$ qui est égale à $4(p'^2 - q'^2)(p' q')$!

On retrouve la descente infinie découverte par Fermat. $(p'^2 - q'^2)$ doit être un carré donc x'^2 , ainsi que $(p' q')$, c'est-à-dire que l'on retrouve $p' = a'^2$ et $q' = b'^2$, et comme :

$p'^2 - q'^2 = x'^2$, est égal à : $(a'^2)^2 - (b'^2)^2$; il suffit de remplacer a'^2 par z'^2 et bien sur, b'^2 par y'^2 ; pour retrouver une solution inférieure !

Nous voyons bien que quelque soit la nature de p' et q' , qui par supposition sont choisis dans les racines carrées entière ; quand bien même ils seraient des réels, il ne peuvent donc donner un triplet d'entiers avec une telle solution, le cas $N=4$ serait alors faux, mais aussi le théorème de Fermat, ainsi que la formule des triplets pythagoriciens, qui donne toutes les solutions entières, avec p et q entiers ; le contraire serait absurde !»)

Ou de façon plus explicite :

$$z^2 + y^2 = u^2 \quad (3)$$

$$z^2 - y^2 = v^2 \quad (4)$$

L'égalité (3) est une équation de Pythagore, qui admet pour solution primitive le triplet : $(z, y \text{ et } u)$ paramétrés de manière unique par le couple p_1 et q_1 tels que :

$$\begin{aligned} p_1^2 + q_1^2 &= u \\ p_1^2 - q_1^2 &= z \\ 2 p_1 q_1 &= y \end{aligned} \quad (5)$$

L'égalité (4) est également une équation de Pythagore, qui admet pour solution primitive le triplet :

$(v, y \text{ et } z)$ paramétrés de manière unique par le couple p_2 et q_2 tels que :

$$\begin{aligned} p_2^2 + q_2^2 &= z \\ p_2^2 - q_2^2 &= v \\ 2 p_2 q_2 &= y \end{aligned} \quad (6)$$

Or, $2 p_1 q_1 = y$ et $2 p_2 q_2 = y$; alors : $p_1 = p_2 = p'$ et $q_1 = q_2 = q'$ ce qui nous donne deux triplets $(z, y \text{ et } u)$ et $(v, y \text{ et } z)$ donnés par un même couple de paramètres p' et q' ! Ce qui est impossible, et évidemment il en est de même si p' et q' étaient deux réels !

D'où : p' et q' réels ne peuvent paramétrer un triangle rectangle primitif avec des produits de puissance $N \geq 1$, qui ne serait donné par p et q entiers !

.....

Cas $N = 4$:

si dans un triplet pythagoricien, X est un carré Y ne peut en être un! (1)

si dans un triplet pythagoricien, X est un carré Z ne peut en être un! (2)

si dans un triplet pythagoricien, y est un carré Z ne peut en être un! (3)

de ces trois égalités, il devient évident qu'un couple de paramètres p' et q' réels, ne peut donner un triplet primitif avec solution dans $N = 2$; qui ne serait donné par p et q entiers ! Propriété (A)

note:

(il en serait de même, pour un triplet multiple d'un primitif où p' et q' ne pourraient donner un triplet différent, qui ne serait pas donné par p et q et un facteur $K > 1$ entier non nul! $K \mid 2pq$, $K \mid p^2 - q^2$, et $K \mid p^2 + q^2$)

l'égalité (2) confirme (3) et inversement

si un triplet x^2, y^2 et z^2 paramétré par p et q , soit la solution :

$$(x^2)^2 + (y^2)^2 = (z^2)^2$$

on obtiendrait la contradiction 2, qui correspond à l'égalité (2) !

$p^2 - q^2 = (x^2)$ et $p^2 + q^2 = (z^2)$ impossible, $z \neq x$. ref 2): démonstration du cas x^2 et z^2 .

de plus on obtient propriété (B)

$(x^2)^2 = (z^2 + y^2)(z^2 - y^2)$ impossible, z^2 et y^2 ne peuvent exister contradiction 2 et 3, correspondant à l'égalité (2) et (3)! ref 3): démonstration du cas y^2 et z^2

(B) nous indique que z et y premiers entre eux, donnent deux carrés, en effet le produit de ces deux nombres, premiers entre eux deux à deux doivent donner : $(x^2)^2$; tel que :

$$(z^2 + y^2) = u^2 \text{ et } (z^2 - y^2) = v^2. \text{ d'où :}$$

$(x^2)^2 = (u^2 v^2)$ si et seulement si (B) était faux !

de (B), on en retire une autre évidence, propriété (c)

en effet:

$(z^2 + y^2) = u^2$ ainsi que $(z^2 - y^2) = v^2$; est équivalent à l'égalité (2) c'est à dire que je pourrais remplacer z et y par p et q si de tel triplets existaient, c'est-à-dire si l'égalité (2) était fausse!

ou encore mieux, je peux utiliser deux réels algébriques p' et q' , choisis dans les racines carrées des entiers à la puissance $N > 2$ et premier : 3, 5, 7...etc!

qui me donnerait: $p'^2 + q'^2 = u^2$ et $p'^2 - q'^2 = v^2$ avec solution dans $(N^{(3+2)})$ mais aussi dans $N=2$, « car on pourrait supposer que u et v sont des produits de puissance 3...etc ainsi que p'^2 et q'^2 »

ce qui est absurde le cas $N = 4$ serait faux ainsi que l'égalité (3) et (2)

Donc deux "réels algébriques" choisis dans les racines carrées, des entiers à la puissance $N=2$ sont deux entiers p et q ; Mais devient impossible pour $N > 2$ et premier, car en mettant ces deux réels algébriques p' et q' au carré, on obtient la contradiction (3),(2)..etc!

deux réels, non algébriques ne peuvent non plus exister et me donner ces deux solutions primitives, en paramétrant un tel triplet !

c'est à dire me donner un triplet de racines carrée entières dans $N=1$! ni même dans $N=2$!

en démontrant le cas $N=4$, il devient évident que p et q entiers, ne sauraient donner un triplet de produits de puissance $N > 2$, car l'égalité (2) et (3) serait contredite!

en remplaçant l'exposant 2, par N premier, car il faudrait bien choisir p et q dans les racines carrées de ces entiers à la puissance $N > 2$ et pair!

Exemple, avec le triplet:

x^4, y^4 et z^4 , alors il existe, de par la propriété de Pythagore

$(x^4)^2 = (z^4 + y^4)(z^4 - y^4)$; où : comme pour $N=2$ je devrais obtenir deux produits de puissance $N = 3$

soit:

$$(x^4)^2 = (u^3)^3 (v^3)^3; \text{ mais aussi } (x^4)^3 = (u^2)^3 (v^2)^3 !$$

deux solutions par addition et soustraction comme la contradiction du cas $N=4$,

de plus, si p et q sont des racines carrées entières on aurait aussi p^3 et q^3 qui doivent donner z^3 et x^3 avec $2p^3q^3 = y^3$!

$$(z^3 + y^3) = (u^3)$$

$$(z^3 - y^3) = (v^3), \text{ on pourrait remplacer } z \text{ et } y \text{ par } p \text{ et } q.$$

(la démo de Euler serait fausse.. mais aussi 2) et 3)..etc)

propriété (D)

il ne peut exister deux réel algébriques p' et q' ; qui donne un triplet de produits cubique, et plus généralement de produit de puissance première; avec p' et q' qui seraient choisis dans les racines carrée entières ou non, de ces produits de puissance N premier! ni deux réels! On en conclut :

Pas de solution quelque soit N pair > 2 !

Propriété (D')

il ne peut alors, exister deux réels qui auraient paramétré ces deux solutions cubiques, $(z^3 + y^3) = (u^3)$ et $(z^3 - y^3) = (v^3)$ dans $N=3$; (« car il existerait un triplet de produits de puissance 3 ce que l'on vient de monter impossible ! »)

C'est-à-dire : ces deux triangles rectangles mesurés par des réels algébriques; que sont les racines carrées des entiers x , y et z à la puissance 3, ou x , y et z ne peuvent être 3 carrés parfait, au maximum il pourrait en exister qu'un ! (« de part la supposition, leurs racines carrées n'étant pas entières »)!

Observation sur(D'):

Ce cas nous indique clairement, que deux couples de réel p' , q' et p'' , q'' ne peuvent en aucun cas donner deux solutions de cette forme ; donc ne peuvent paramétrer un triplet primitif d'entiers, à la puissance N premières ≥ 2 , ainsi qu'un triplet primitif dans $N=1$, ni à plus forte raison, deux triplets de racines carrées algébriques, puisque ces deux solutions sont paramètres par un seul couple p et q comme le cas 2) de b)!

Mais cela ne peut résoudre de façon formel le cas $N=3$, car il pourrait exister un triplet de racines algébriques, et donner quand même une solution dans $N=3$; c'est le même cas que $N=4$ il n'existe pas deux solutions, de cette forme avec z^2 et y^2 , mais il existe des solutions dans $N=2$ paramétrés par p et q entiers, choisis dans les racines carrées, c'est à dire dans $N=1$!

Ce qui indique que si : ces deux solutions existe avec z^2 et y^2 , donné par deux couples de réels, tel que : $z^2 + y^2 = u^2$ et $z^2 - y^2 = v^2$, alors u et v ne sont des entiers ce qui est idiot, z^2 et y^2 sont des carrés parfaits par supposition !

Or supposons, qu'il existe un triplet de racines algébriques d'entiers à la puissance 3, alors il existe p' et q' algébriques qui peuvent être choisis dans ces racines carrées, comme pour $N=2$; et redonner une solution qui est supposée existé, (« soit par addition ou soustraction ») en recréant un triplet supérieur.

Ce qui est impossible ! En effet en mettant p' et q' au carré, on se retrouve avec deux entiers X et Z ce qui est contraire à cette supposition, il me faudrait 3 racines non entières, algébriques et au minimum 2! De plus :

X et Z sont supposés être deux produits de puissance $N=3$ pour cet exemple, puisque l'on cherche deux racines carrées algébriques dans $n=3$, ce qui est absurde on retrouve la contradiction 2) du cas générale pour N pair !

Il est donc impossible de trouver et choisir deux réel algébriques p' et q' supposer vérifier et redonner un triplet de racines algébriques quelque soit la

puissance N première ≥ 3 , c'est à dire reconstruire un triplet de racines supposé existé ! Ce qui n'est pas le cas pour N=2 avec p et q entiers, 1 et 2 !

Propriété E : c'est qu'il n'existe pas un triplet algébrique de racines carrées d'entiers à la puissance N = 3, où l'on pourrait choisir un couple de paramètres algébriques p' et q' Et de façon plus générale il en est de même pour N premier > 2 !

Ci cette propriété E. ne serait suffisante pour résoudre le cas N=3 :

Il ne reste plus qu'alors la solution avec :

P' et q' réels tout simplement ; or en démontrant le cas N=3, L. Euler montre que même sous cette condition, il n'existe pas un couple p' et q' réels pouvant donner un triplet primitif de racines algébriques dans N=3 ! Et de façon plus générale il en est de même pour N premier > 2, alors il n'existe pas de solution !

Ce qui est vrai pour N=1,2,3..etc, est aussi vrai pour les racines carrées algébriques des entiers à la puissance $N \geq 3$!

En démontrant le cas N pair, on démontre la propriété (D' et E) ; car au minimum il existerait des solution dans N=4, 3 et 6 si un couple de réel p'et q' avait existé, de plus un couple de réels p' et q' pourrait donner un triplet de racines carrées entières, dans une puissance première en commençant par N=2 !

P de Fermat c'est arrêté au cas N = 3, ce qui était largement suffisant.

Ce qui es parfaitement valable, pour avoir démontré ce théorème à son époque; mais aussi actuellement....

Ceci conclu mon raisonnement.

Annexe A

§§§§§§§§§§§§§§§§

Lemme 1.2.3.4 utilisés pour la descente infinie du cas N = 4.

Mais dont Fermat n'aurait pu utiliser, Gauss et postérieur à Fermat.

Néanmoins Fermat n'avait aucun problème pour X^2 et Y^2 impossible dans un triplet Pythagoricien.

Lemme 1 : si $p \wedge q = 1$, p et q de parité distincte, alors p + q et p - q sont premiers entre eux.

Preuve : si d est un diviseur premier commun à p + q et p - q, alors d divise 2p et 2q (par addition et soustraction). Si d divise 2, alors d = 2 : pas possible car vu la parité distincte de p et q, p + q et p - q sont impairs. Donc d divise p et d divise q (théorème de Gauss). Pas possible puisque $p \wedge q = 1$.

Lemme 2 : si $m \wedge n = 1$, alors $m^2 \wedge n^2 = 1$ et, de plus, les nombres m, n et $m^2 - n^2$ sont premiers entre eux (deux à deux).

Preuve : m et n peuvent s'écrire sous forme d'un produit des puissances de leurs facteurs premiers. Les diviseurs premiers de m^2 et de n^2 sont leurs facteurs premiers respectifs. La première assertion $m^2 \wedge n^2 = 1$ est donc évidente. Quant à la seconde, si d divise m, alors il

divise m^2 . Donc, si d divise m et $m^2 - n^2$, il divise aussi n^2 . Or $m^2 \wedge n^2 = 1$, donc $d = 1$. On raisonnerait de même avec n .

Lemme 3 : si $m^2 \wedge n^2 = 1$, alors $m \wedge n = 1$.

Lemme 4 : Si un produit de nombres premiers entre eux (deux à deux) est un carré, alors ces nombres sont eux-mêmes des carrés.

Preuve : Supposons $\text{pgcd}(p,q,r) = 1$ (pris 2 à 2, le pgcd est 1) et $pqr = t^2$. L'entier t se décompose en un produit de facteurs premiers. Par suite t^2 est un produit de facteurs premiers dont les exposants sont pairs. Puisque $pqr = t^2$, les diviseurs premiers de p , q et r sont extraits de ceux de t . Soit d un diviseur premier de t , apparaissant, dans t^2 , sous la forme d^{2n} . Il ne peut diviser deux des nombres p , q et r . S'il divise p , alors d^{2n} qui divise t^2 divise nécessairement p (théorème de Gauss). Donc, par épuisement des cas, p est un carré et on obtiendra que q et r sont des carrés.

Les lemmes 2 et 4 permet d'affirmer que p , q et $p^2 - q^2$ sont des carrés. Posons $p = m^2$, $q = n^2$ et $p^2 - q^2 = r^2$. Ainsi :

$$r^2 = p^2 - q^2 = m^4 - n^4 = (m^2 + n^2)(m^2 - n^2) ;$$

Contradiction, b) ; l'auteur aurait pu conclure le cas $N = 4$ à ce passage ! $z \neq x$