Vers le théorème de Fermat - Wiles

Au XVIIe siècle, le mathématicien français Pierre de Fermat écrit dans la marge de son exemplaire du livre d'arithmétique de Diophante avoir trouvé une preuve "absolument merveilleuse" du théorème suivant :

Théorème (Wiles) : Soit $n \geq 3$ un entier. Alors il n'existe aucun triplet $(x, y, z) \in \mathbb{N}^*$ solution de l'équation suivante :

$$x^n + y^n = z^n \qquad (E_n)$$

Cependant, on sait aujourd'hui qu'il ait à peu près impossible que Fermat ait effectivement obtenu une preuve de ce théorème, qui sera démontré seulement en 1994 par le britannique Andrew Wiles, en utilisant des technologies bien plus avancées que celles dont disposait Fermat (courbes elliptiques, formes modulaires).

1 Introduction

1. Expliquez pourquoi il suffit de traiter le cas où $n = 4$ ou n est premier impair pour démontrer le théorème de Wiles.

2 Les triplets pythagoriciens

Dans cette section, on va résoudre l'équation :

$$a^2 + b^2 = c^2 \qquad (E_2)$$

d'inconnues $a, b, c \in \mathbb{Z}$.

2. Montrer que résoudre cette équation revient à trouver tous couples de rationnels $(p, q) \in \mathbb{Q}^2$ tels que :

$$p^2 + q^2 = 1$$

On fixe donc $p, q \in \mathbb{Q}$ tels que $p^2 + q^2 = 1$.

3. On suppose dans cette question que $(p, q) \neq (-1, 0)$.

a) Montrer que la pente t de la droite reliant $(-1, 0)$ et (p, q) est rationnelle.

b) Montrer les égalités :

$$p = \frac{1 - t^2}{1 + t^2} \qquad q = \frac{2t}{1 + t^2}$$

4. Montrer que les solutions de l'équation (E_2) sont exactement les triplets $(a, b, c) \in \mathbb{Z}$ s'écrivant (à échange près de a et b) :

$$a = d(x^2 - y^2) \qquad b = 2dxy \qquad c = d(x^2 + y^2)$$

pour $d, x, y \in \mathbb{Z}$.

3 Le cas $n = 4$.

On va montrer dans cette section que l'équation :

$$a^4 + b^4 = c^2$$

n'a aucune solution entière pour laquelle a et b sont non nuls. Soit donc $(a, b, c) \in (\mathbb{N}^*)^3$ tel que $a^4 + b^4 = c^2$.

4. Montrer qu'on peut supposer sans perte de généralité que a, b, c sont deux à deux premiers entre eux, et que b est pair. On fera cette hypothèse dans la suite.

5. a) Montrer l'existence de $p, q \in \mathbb{N}^*$ tels que :

$$a^2 = p^2 - q^2 \qquad b^2 = 2pq \qquad c = p^2 + q^2$$

b) Montrer que p, q et a sont premiers entre eux deux à deux.

c) Montrer à partir de l'équation $a^2 + q^2 = p^2$ que q est pair et p impair.

6. a) Montrer l'existence de $x, y \in \mathbb{N}^*$ tels que :

$$a = x^2 - y^2 \qquad q = 2xy \qquad p = x^2 + y^2$$

b) Montrer que x, y et p sont deux à deux premiers entre eux.

c) En remarquant que $b^2 = 4pxy$, en déduire que p, x et y sont des carrés parfaits, qu'on notera respectivement p'^2, x'^2 et y'^2 avec $p', x', y' \in \mathbb{N}$.

d) Montrer que $p' < c$ et que :

$$p'^2 = x'^4 + y'^4$$

7. a) Conclure par le principe de la descente infinie de Fermat que l'équation $a^4 + b^4 = c^2$ n'a aucune solution $(a, b, c) \in \mathbb{N}$ pour laquelle a et b sont non nuls.

b) En déduire que l'équation $x^4 + y^4 = z^2 \qquad (E_4)$ n'a aucune solution formée d'entiers strictement positifs.

4 Le théorème de Sophie Germain

Dans cette partie, on va démontrer le théorème suivant, du à Sophie Germain :

Théorème : Soit p un nombre premier impair tel que $q = 2p + 1$ soit également premier. Alors, l'équation $x^p + y^p + z^p = 0$ n'a aucune solution $(x, y, z) \in (\mathbb{Z})^3$ pour laquelle $xyz \not\equiv 0 \mod p$.

On fixe donc un nombre premier p impair tel que $q = 2p + 1$ soit également premier. Soient $x, y, z \in \mathbb{N}^*$ tels que $x^p + y^p + z^p$. On veut montrer que p divise xyz. On suppose donc par l'absurde que $xyz \not\equiv 0 \mod p$.

8. Montrer qu'on peut supposer sans perte de généralité que x, y et z sont premiers entre eux.

9. a) Montrer que :

$$(x + y)\left(\sum_{k=0}^{p-1}(-1)^k x^k y^{p-1-k}\right) = (-z)^p$$

et que $x + y$ et $\displaystyle\sum_{k=0}^{p-1}(-1)^k x^k y^{p-1-k}$ sont premiers entre eux.

b) En déduire que $x + y = c^p$ pour un certain entier $c \in \mathbb{Z}$. Montrer de la même manière l'existence de $a, b \in \mathbb{Z}$ tels que $y + z = a^p$ et $x + z = b^p$.

10. Dans cette question, on suppose par l'absurde que q ne divise pas xyz

a) Montrer que $x^p \equiv \pm 1 \mod q$, et de même pour y et z. *On pourra utiliser le petit théorème de Fermat.*

b) Montrer que ceci mène à une contradiction.

11. a) Montrer que exactement un des entiers x, y, z est divisible par q. Sans perte de généralité, on suppose que c'est x.

b) Montrer alors que $y \equiv c^p \equiv \pm 1 \mod q$ et que $z \equiv b^p \equiv \pm 1 \mod q$.

c) En remarquant que $c^p + b^p - a^p = 2x$, montrer alors que q divise a.

d) Montrer que $y \equiv -z \mod q$.

e) En déduire les congruences :

$$\sum_{k=0}^{p-1} (-1)^k x^k y^{p-1-k} \equiv p y^{p-1} \equiv p \mod q$$

12. a) Montrer avec l'aide de 9.a) que l'entier :

$$\sum_{k=0}^{p-1} (-1)^k x^k y^{p-1-k}$$

est une puissance entière de p.

b) En déduire une contradiction avec la question 11.e), et conclure la preuve du théorème de Sophie Germain.

5 L'équation optique

On s'intéresse dans cette section à l'équation suivante, d'inconnues $x, y, z \in \mathbb{N}^*$:

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c} \qquad (E_{-1})$$

Le nom d' "équation optique" provient du fait qu'elle répond à la question de trouver deux lentilles optiques de vergences entières dont la concaténation est à vergence entière.

Soient donc $a, b, c \in \mathbb{N}^*$ tels que $\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$, i.e. $ab = c(a+b)$.

13. Montrer qu'on peut se contenter de traiter le cas où a, b, c sont premiers entre eux dans leur ensemble. On fera cette hypothèse dans la suite.

On pose $m = \text{pgcd}(a, c)$ et $k = \text{pgcd}(b, c)$.

14. On va montrer dans cette question que $c = mk$.

a) Montrer que $m \wedge k = 1$ et en déduire que mk divise c.

b) Montrer que l'entier $\frac{c}{k}$ divise ab et est premier avec b. En déduire que $\frac{c}{k}$ divise a.

c) Montrer que $\frac{c}{k}$ divise m.

d) Conclure que $c = mk$.

On écrit $a = xm$ et $b = yk$, où $x, y \in \mathbb{N}^*$.

15. a) Montrer que tout facteur premier commun à x et k divise a, b et c. En déduire que $x \wedge k = 1$.

b) Montrer que x divise yk puis que x divise y.

c) En déduire que $x = y = m + k$.

16. Montrer que les solutions $(a, b, c) \in (\mathbb{N}^*)^3$ de l'équation (E_{-1}) sont les triplets d'entiers strictement positifs (a, b, c) de la forme :

$$a = d(m^2 + mk) \qquad b = d(mk + k^2) \qquad c = dmk$$

où $d, m, k \in \mathbb{N}^*$ avec $m \wedge k = 1$.