Théorème 1. 26 est l'unique entier entre un carré et un cube.

L'essentiel du développement consiste à étudier l'équation $x^2+2=y^3$, en effet, si n est un entier entre un carré et un cube alors en notant $x^2=n-1$ et $y^3=n+1$ on a $x^2+2=y^3$. Pour résoudre cette équation on étudie l'anneau $\mathbb{Z}[i\sqrt{2}]$.

Lemme 1. L'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien pour le stathme du module.

Preuve.

Soit $(x,y)\in\mathbb{Z}[i\sqrt{2}]^2$ avec $y\neq 0$. On écrit $\dfrac{x}{y}=a+ib\sqrt{2}$ avec $(a,b)\in\mathbb{Q}^2$. On note u (resp. v) l'entier le plus proche de a (resp. b), si a ou b est un demi-entier on prend la partie entière (prendre la partie entière supérieure ne change rien). On a alors en notant $q=u+iv\sqrt{2}\in\mathbb{Z}[i\sqrt{2}]$:

$$\left|\frac{x}{y}-q\right|^2=(a-u)^2+2(b-v)^2\leq\frac{1}{4}+2\frac{1}{4}=\frac{3}{4}<1$$

Donc $x=yq+r$ avec $r=x-yq\in\mathbb{Z}[i\sqrt{2}]$ qui vérifie $r=0$ où $|r|<|q|$. □

Lemme 2. $\mathbb{Z}[i\sqrt{2}]^\times=\{\pm1\}$

Preuve.

Soit $z=a+ib\sqrt{2}\in\mathbb{Z}[i\sqrt{2}]^\times$, alors $1=\left|zz^{-1}\right|^2=|z|^2\underbrace{\left|z^{-1}\right|^2}_{\in\mathbb{N}}$ donc $|z|^2=1$ ie $a^2+2b^2=1$. Comme a et b sont des entiers les seuls couples solutions de l'équation précédente sont $(1,0)$ et $(-1,0)$, ce qui donne $z=\pm1$. Inversement, il est clair que ±1 sont inversibles dans $\mathbb{Z}[i\sqrt{2}]$. □

Lemme 3. L'élément $i\sqrt{2}$ est irréductible dans $\mathbb{Z}[i\sqrt{2}]$.

Preuve.

Déjà $i\sqrt{2}$ n'est pas inversible par le lemme précédent. Si on écrit $i\sqrt{2}=zz'$ avec $(z,z')\in\mathbb{Z}[i\sqrt{2}]^2$, nécessairement $2=|z|^2|z'|^2$ et donc $|z|=1$ ou $|z'|=1$ ie z ou z' inversible et cela conclut. □

Soit maintenant $(x,y)\in\mathbb{Z}^2$ solution de $x^2+2=y^3$. Notons d le pgcd de $x-i\sqrt{2}$ et $x+i\sqrt{2}$, on sait qu'il existe car $\mathbb{Z}[i\sqrt{2}]$ euclidien. L'élément d divise $x+i\sqrt{2}$ et $x-i\sqrt{2}$ donc d divise

$$(x+i\sqrt{2})-(x-i\sqrt{2})=2i\sqrt{2}=-(i\sqrt{2})^3$$

Or $i\sqrt{2}$ est irrédutible dans $\mathbb{Z}[i\sqrt{2}]$ donc par unicité de la décomposition en produits d'irréductibles dans l'anneau factoriel $\mathbb{Z}[i\sqrt{2}]$, d est de la forme $d=(i\sqrt{2})^k$. On va maintenant montrer que $d=1$ ie $k=0$. Supposons $k\neq0$, alors

$$i\sqrt{2}\mid d\mid x-i\sqrt{2}$$

donc,

$$i\sqrt{2}\mid(x-i\sqrt{2})+i\sqrt{2}=x$$

Donc $\left|i\sqrt{2}\right|^2$ divise $|x|^2$ (dans $\mathbb{N}$) ie 2 divise x^2 et x est pair et x^2 divisible par 4. Par suite, $y^3=x^2+2$ est pair donc 8 divise y^3. On réduit l'équation $x^2+2=y^3$ modulo 4 pour obtenir :

$$2\equiv0[4]$$

ce qui est absurde, donc $k=0$ et $d=1$ et $x+i\sqrt{2}$ est premier avec $x-i\sqrt{2}$. Comme de plus :

$$(x+i\sqrt{2})(x-i\sqrt{2})=x^2+2=y^3$$

Donc par factorialité de $\mathbb{Z}[i\sqrt{2}]$, $x+i\sqrt{2}$ et $x-i\sqrt{2}$ sont eux même des cubes. En écrivant $x+i\sqrt{2} = (a+ib\sqrt{2})^3$ avec $(a,b) \in \mathbb{Z}^2$ et en identifiant partie réelle et imaginaire on a :

$$\begin{cases} x = a(a^2 - 6b^2) \\ 1 = b(3a^2 - 2b^2) \end{cases}$$

La seconde équation donne $b = \pm 1$, mais si $b = -1$ alors la seconde équation $1 = -(3a^2 - 2)$ qui n'a pas de solution dans $\mathbb{Z}$. Donc $b = 1$ et $a^2 = 1$ ie $a = \pm 1$. En injectant dans la première équation on a $x = \pm 5$ et $y^3 = 25 + 2 = 27$ ie $y = 3$. Les couples solutions sont donc donnés par :

$$(5,3) \text{ et } (-5,3)$$

On peut maintenant conclure, si n est un entier entre un carré et un cube alors en notant $x^2 = n-1$ et $y^3 = n+1$ on a $y^2 = x^2 + 2$ donc $27 = y^3 = n+1$ et $n = 26$.

Remarque 1. La preuve peut se trouver dans le livre "131 Développements pour l'oral" à quelques détails près.