Résolution de l'équation $n^2 + 100 = q^3$

Vincent Lefèvre

6 octobre 1996

0 Préliminaire sur les entiers de Gauss

Pour résoudre l'équation $n^2 + 100 = q^3$, nous nous placerons dans l'anneau $\mathbb{Z}(i)$ des entiers de Gauss, nombres complexes $a + bi$ avec $(a, b) \in \mathbb{Z}^2$.

Nous utiliserons le fait que cet anneau est factoriel, c'est-à-dire que tout entier de Gauss non nul admet une unique décomposition (à un ordre près) en facteurs irréductibles (à une unité près). Nous aurons donc des propriétés de divisibilité similaires à celles dans $\mathbb{Z}$, qui est factoriel.

Plus précisément, en considérant l'application N de $\mathbb{Z}(i)$ dans $\mathbb{N}$ définie par $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$, on montre les propriétés suivantes : les éléments inversibles (unités) de $\mathbb{Z}(i)$ sont 1, i, -1, $-i$; les facteurs irréductibles de $\mathbb{Z}(i)$ sont les nombres premiers p de $\mathbb{Z}$ ne pouvant pas se mettre sous la forme d'une somme de deux carrés (ce sont les nombres premiers p de la forme $4k+3$) et les nombres $a + bi$ tels que $N(a + bi)$ est un nombre premier dans $\mathbb{Z}$.

1 Analyse du problème

Dans l'anneau des entiers de Gauss $\mathbb{Z}(i)$, l'équation s'écrit

$$(n + 10i)(n - 10i) = q^3.$$

La résolution de cette équation sera basée sur la décomposition en facteurs irréductibles des deux membres, qui est unique car $\mathbb{Z}(i)$ est factoriel.

La décomposition en facteurs irréductibles de q^3 est particulière. Nous avons déjà trois facteurs identiques q. Ensuite, on peut décomposer q en facteurs premiers dans $\mathbb{Z}$. Il reste à décomposer un facteur premier p de $\mathbb{Z}$. On a deux possibilités : soit p est irréductible, soit p se décompose en produit $(a+bi)(a-bi)$ de deux facteurs irréductibles.

Montrons qu'il n'existe pas de facteur premier p de q dans $\mathbb{Z}$, qui soit irréductible dans $\mathbb{Z}(i)$. S'il en existe un, il divise l'un des deux facteurs $n + 10i$ ou $n - 10i$ (en fait, il divise même les deux), donc p divise n et 10, parce que $p \in \mathbb{Z}$. Donc $p = 2$ ou $p = 5$. Dans ces deux cas, p n'est pas irréductible dans $\mathbb{Z}(i)$: $2 = (1 + i)(1 - i)$ et $5 = (2 + i)(2 - i)$. Donc tout facteur irréductible de q dans $\mathbb{Z}(i)$ est de la forme $a + bi$ avec $ab \neq 0$.

Considérons un facteur premier p de q. Sa décomposition en facteurs irréductibles est de la forme : $p = (a+bi)(a-bi)$. On a :

$$(a+bi)^3(a-bi)^3 \mid (n+10i)(n-10i).$$

Quitte à changer le signe de b, on peut supposer que $(a+bi)^2 \mid n+10i$. On a alors les deux possibilités suivantes :

$$p \mid n+10i \quad \text{ou} \quad (a+bi)^3 \mid n+10i,$$

suivant que $a+bi \mid n-10i$ ou $a+bi \mid (n+10i)/(a+bi)^2$. Mais évidemment, ces deux possibilités ne sont pas exclusives.

Suivant la valeur de $n \wedge 10$ (où $\wedge$ dénote le PGCD), on peut déterminer si la première possibilité peut avoir lieu, auquel cas l'équation peut se « simplifier ». Une fois l'équation complètement simplifiée, on ne pourra avoir que la deuxième possibilité, qui mènera en fait à une égalité du type $(a+bi)^3 = r+si$, avec une relation linéaire entre r et s.

On va considérer les 4 cas possibles suivants : $n \wedge 10 = 1$, $n \wedge 10 = 2$, $n \wedge 10 = 5$ et $n \wedge 10 = 10$.

2 Cas $n \wedge 10 = 1$

Pour tout facteur premier p de q, on ne peut pas avoir $p \mid n+10i$. Donc il existe $(a,b) \in \mathbb{Z}^2$ tel que

$$(a+bi)^3 = n+10i$$

(et $(a-bi)^3 = n-10i$). Par conséquent

$$\left\{ \begin{array}{rcl} a^3 - 3ab^2 & = & n \\ 3a^2b - b^3 & = & 10 \end{array} \right.$$

De la seconde égalité $b(3a^2 - b^2) = 10$, on déduit $b \mid 10$. On a alors les différents cas suivants :

$$\left\{ \begin{array}{lcl} |b| = 1 & \rightarrow & 3a^2 = 1 \pm 10 \\ |b| = 2 & \rightarrow & 3a^2 = 4 \pm 5 \\ |b| = 5 & \rightarrow & 3a^2 = 25 \pm 2 \\ |b| = 10 & \rightarrow & 3a^2 = 100 \pm 1 \end{array} \right.$$

La seule solution possible est $a+bi = \pm 3 + 5i$, ce qui donne $n = 198$. On n'a pas $n \wedge 10 = 1$. Néanmoins $n = 198$ conduit bien à une solution correcte : on a $q = 34$; on retrouvera évidemment cette solution plus tard.

3 Cas $n \wedge 10 = 2$

Posons $n = 2k$. Alors $n^2 + 100 = 4(k+5i)(k-5i)$. Puisque $2 \mid q$, on a $2 \mid (k+5i)(k-5i)$, d'où $1+i \mid k+5i$. Soit $(a,b) \in \mathbb{Z}^2$ tel que $(1+i)(a+bi) = k+5i$; (a,b) vérifie :

$$\left\{ \begin{array}{l} a - b = k \\ a + b = 5 \end{array} \right.$$

$a+b$ est impair, donc k aussi. Posons $k = 2\ell+1$. Alors $a = \ell+3$ et $b = -\ell+2$. En résumé :

$$n^2 + 100 = 2^3((\ell+3) - (\ell-2)i)((\ell+3) + (\ell-2)i).$$

$n \wedge 10 = 2$, donc $k \wedge 5 = 1$, et $(\ell+3) \wedge (\ell-2) = 1$, i.e. il existe $(a, b) \in \mathbb{Z}^2$ tel que

$$(a + bi)^3 = (\ell+3) + (\ell-2)i.$$

Par conséquent

$$\begin{cases} a^3 - 3ab^2 &= \ell+3 \\ 3a^2b - b^3 &= \ell-2 \end{cases}$$

ce qui donne l'équation suivante :

$$a^3 - 3a^2b - 3ab^2 + b^3 = 5,$$

que l'on peut factoriser :

$$(a+b)((a+b)^2 - 6ab) = 5.$$

On a soit $|a+b| = 1$, soit $|a+b| = 5$. La seule solution acceptable donne $\ell = 49$. On retrouve la solution $n = 198$, $q = 34$.

4 Cas $n \wedge 10 = 5$

Posons $n = 5k$. Alors $n^2 + 100 = 25(k+2i)(k-2i)$. Puisque $5 \mid q$, on a $5 \mid (k+2i)(k-2i)$, d'où $1+2i$ divise $k+2i$ ou $k-2i$. Soit $s = \pm 1$ tel que $1+2i \mid k+2si$. Soit $(a, b) \in \mathbb{Z}^2$ tel que $(1+2i)(a+bi) = k+2si$; (a, b) vérifie :

$$\begin{cases} a - 2b = k \\ 2a + b = 2s \end{cases}$$

D'où

$$a = \frac{k+4s}{5} \quad \text{et} \quad b = \frac{2s-2k}{5}.$$

a et b sont entiers, donc k est de la forme $5\ell + s$. On a alors :

$$n^2 + 100 = 5^3((\ell+s) - 2\ell i)((\ell+s) + 2\ell i).$$

Là encore $(\ell+s) \wedge 2\ell = 1$ (puisque n est impair). Donc il existe $(a, b) \in \mathbb{Z}^2$ tel que

$$(a+bi)^3 = (\ell+s) + 2\ell i.$$

Par conséquent

$$\begin{cases} a^3 - 3ab^2 &= \ell+s \\ 3a^2b - b^3 &= 2\ell \end{cases}$$

ce qui donne l'équation suivante :

$$2a^3 - 3a^2b - 6ab^2 + b^3 = 2s.$$

Cette fois, le polynôme X^3-6X^2-3X+2 est irréductible : on a une équation de Thue, i.e. elle est de la forme $P(a,b) = r$, où P est un polynôme homogène de $\mathbb{Z}[X,Y]$ irréductible et de degré supérieur ou égal à 3, et r une constante entière. Le logiciel Magma V2 permet de résoudre de telles équations. Pour l'équation ci-dessus, les solutions sont : $(1,-1)$, $(-1,1)$, $(1,0)$, $(-1,0)$. Elles conduisent à $q^3 = 5^3 \times 8$ et à $q^3 = 5^3 \times 1$, i.e. $q = 10$ et $q = 5$. Bien que correcte, la solution $q = 10$ est ici à rejeter (on la retrouvera dans la section suivante). La solution $q = 5$ convient.

5 Cas $n \wedge 10 = 10$

On reprend l'équation :

$$n^2 + 100 = 5^3((\ell + s) - 2\ell i)((\ell + s) + 2\ell i).$$

Puisque $2 \mid n + 10i$, ℓ est impair. En posant $\ell = 2m - s$, on montre que m est de la forme $2r + s$, et on obtient l'équation

$$n^2 + 100 = 10^3((3r + s) + ri)((3r + s) - ri),$$

puis

$$a^3 - 9a^2b - 3ab^2 + 3b^3 = s.$$

On a encore une équation de Thue, qui admet pour solutions $(1,0)$ et $(-1,0)$, ce qui donne $q = 10$.

6 Conclusion

En conclusion, les seules solutions de l'équation $n^2 + 100 = q^3$ sont :

$$\begin{cases} n = 5 \\ q = 5 \end{cases} \qquad \begin{cases} n = 30 \\ q = 10 \end{cases} \qquad \begin{cases} n = 198 \\ q = 34 \end{cases}$$

Note : en remarquant que $1 + i = i(1 - i)$, on aurait pu omettre les cas $n \wedge 10 = 2$ et $n \wedge 10 = 10$ (en gardant toutes les solutions des deux autres cas).

Je tiens à remercier Geoff Bailey pour m'avoir donné les deux résultats des équations de Thue, ainsi que les autres lecteurs du newsgroup `sci.math` pour leurs informations sur les équations de Thue.