The number 26, between 25 and 27

Resolution of the diophantine equation $y^3 - x^2 = 2$

Axel Gougam & Julien Baglio

May 28, 2006

Abstract

The goal of this article is to demonstrate a funny property of the number 26 : it is the only integer which is at a discrete distance of one from a square and a cube : $25 = 5^2 \leq 26 \leq 27 = 3^3$. This problem is related to Pierre de Fermat, a french mathematician of the XVIIe century, who stated that there should exist five integers which verify the property exposed above. It has been proved after that he was somewhat wrong for there is a unique solution to the problem. We here divide our work in two parts. First we expose the basic ideas which come to mind and lead to the solution which is then exposed in the second part.

1 Introduction to the problem, basic ideas

The problem discussed in this article can be formally exposed as :

If we take an integer $p > 0$ which verify $p - 1 = k^2$ and $p + 1 = k'^3$, then it implies that $p = 26, k = 5$ and $k' = 3$.

If we subtract the first equality with the second one, we obtain $-2 = k^2 - k'^3$, that is to say (k, k') is a solution of the diophantine equation $y^3 - x^2 = 2$ with $(x, y) \in \mathbb{N}^2$. In fact, the problem is to resolve this equation. Thus, we will prove that

Theorem 1 (Particular case of the Catalan problem) *The unique solution of the diophantine equation in $\mathbb{N}^2$*

$$y^3 - x^2 = 2 \tag{1}$$

is $x = 5$ and $y = 3$

The first idea is to study the parity of the solutions. It leads to

Lemma 1 *If (x, y) is a solution of the equation (1), then both x and y are odd numbers*

We have, taken in $\mathbb{Z}/2\mathbb{Z}$, $x^n = x$ for any integer x, n. That leads to $y^3 = y$, $x^2 = x$ and $y - x = 0$. The integers y and x have the same parity. In order to identify it, we take the equation in $\mathbb{Z}/4\mathbb{Z}$: for any integer class a we have $a^3 = a$ according to Euler's theorem which extends Fermat's theorem about rests in division by prime integer. Thus we have $y = x^2 + 2$. If we suppose that $2|x$ then $x^2 = 0$ and $y^3 = y = 2$. But we also have $2|y$, and then $y^3 = 0$: we have proved that $0 = 2$ if we suppose that x is an even number. That is of course a wrong inequality, and it implies that both x and y are odd numbers.

There are other properties which, even if there are interesting, are less important for the resolution of the equation (1).

Property 1 *If (x, y) is solution of (1), then $x \wedge y = 1$*

Let's suppose that $x = qm$ and $y = q'm$ with $m \geq 2$. We have $x^2 = q^2m^2$ and $y^3 = q'^3m^3$, then $2 = m^2(q'^3m - q^2)$. It means that $m^2|2$ which implies that $m = 1$, contradictory to the initial statement of $m \geq 2$. The conclusion is that $x \wedge y = 1$.

We now examine the equation in $\mathbb{Z}/3\mathbb{Z}$: it reduces the degree and we obtain $y - x^2 = 1$ because of Fermat's theorem which states that $x^2 = 1$ for any class integer x in $\mathbb{Z}/3\mathbb{Z}$. The resolution is easy and leads to $x = 3$ or $y = 3$ in $\mathbb{Z}/3\mathbb{Z}$. But we have $y < x$: if it was the contrary, the difference between y^3 and x^2 would never have been equal to 2 because of the comparative growth of the functions $x \mapsto x^2$ and $x \mapsto x^3$. Thus it leads to the unique solution $x = 5$ and $y = 3$ if we suppose x and y both prime numbers.

We wonder now if it is possible to use this result in order to achieve the demonstration. But if we continue onto this path, we do not obtain interesting results, and it is very fastidious. But it leads to the following idea : using another ring in order to achieve the demonstration, especially unique factorization domain.

2 Complete solution using unique factorization domain

In the section above, we have exposed clearly the problem and some basic properties. The lemma 1 will be very useful at the end.

We first remind the reader the definition of a unique factorization domain.

Definition 1 *A ring is said to be a unique factorization domain if it is commutative, with no divisor of zero, and if there exists a decomposition of any element in a unique product (without taking account of the order) of irreductible elements of the ring. Those elements are the root of the decomposition, there are not a product of other elements.*

The first and classic exemple of unique factorization domain is the ring of relative integer $\mathbb{Z}$. In such rings, it is possible to define a gcd, as in $\mathbb{Z}$, and it is this property that will be used.

We have $x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2})$. We then examine the situation in the unique factorization domain $\mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2}, (a, b) \in \mathbb{Z}^2\}$. According to the last sentence, we have $y^3 = (x + i\sqrt{2})(x - i\sqrt{2})$.

Let's take δ as $\delta|(x + i\sqrt{2})$ and $\delta|(x - i\sqrt{2})$. We have $\delta|(x + i\sqrt{2} - x + i\sqrt{2})$. It means that any divisor of $x + i\sqrt{2}$ and $x - i\sqrt{2}$ is a divisor of $x + i\sqrt{2}$ and $2i\sqrt{2}$. In the same way, any divisor of $x + i\sqrt{2}$ and $2i\sqrt{2}$ is a divisor of $x + i\sqrt{2}$ and $x - i\sqrt{2}$. This implies that $\gcd(x + i\sqrt{2}, x - i\sqrt{2}) = \gcd(x + i\sqrt{2}, 2i\sqrt{2}) = \gcd(x + i\sqrt{2}, (i\sqrt{2})^3)$.

$i\sqrt{2}$ is of course irreductible. If we suppose that $i\sqrt{2}|(x + i\sqrt{2})$, we have $x + i\sqrt{2} = i\sqrt{2}(a + bi\sqrt{2}) = -2b + ia\sqrt{2}$. Thus, $a = 1$ and $x = -2b$, which means that x is an even number.

But the lemma 1 states that both x and y are odd numbers ; then we have to consider that $i\sqrt{2}$ does not divide $x + i\sqrt{2}$: $(x + i\sqrt{2}) \wedge i\sqrt{2} = 1$ and $(x + i\sqrt{2}) \wedge (x - i\sqrt{2}) = 1$.

We now use the unique factorization of both elements in $\mathbb{Z}[i\sqrt{2}]$: $x + i\sqrt{2} = z_1 z_2 ... z_n$ and $x - i\sqrt{2} = \bar{z_1}\bar{z_2}...\bar{z_n}$ (they are conjugate numbers). We have $(x + i\sqrt{2}) \wedge (x - i\sqrt{2}) = 1$, which implies that we have $z_i \neq \bar{z_j}$ for every (i, j) ; combined with $y^3 = (x + i\sqrt{2})(x - i\sqrt{2})$ it means that each z_i is present three times in the factorization. Thus there exists $(a, b) \in \mathbb{Z}^2$ with $x + i\sqrt{2} = (a + bi\sqrt{2})^3$.

Expending the expression, we obtain $3a^2b - 2b^3 = 1$ which is the same equality as $b(3a^2 - 2b^2) = 1$. It means that either $b = 1$ and $3a^2 - 2b^2 = 1$ or $b = -1$ and $3a^2 - 2b^2 = -1$. If we examine the second set of equalities, we have $3a^2 = 1$, which has no integer solutions. Therefore we have $b = 1$ and $a^2 = 1$.

Finally, $x + i\sqrt{2} = (\pm 1 + i\sqrt{2})^3$. Expending it, we obtain $x + i\sqrt{2} = \pm 5 + i\sqrt{2}$. Recalling that $x > 0$, we obtain $x = 5$.

If we use equation (1) and replace x by its value 5, we have to resolve $y^3 = 27$. It has a unique trivial solution $y = 3$ in $\mathbb{N}$. We end the demonstration by assuring that $(x, y) = (5, 3)$ is a valid solution of the equation (1).

References

[1] Forumeurs. *Forum mathématiques de l'enseignement supérieur.* FuturaSciences, 2006.
URL : http://forums.futura-sciences.com/thread81165.html