THE NUMBER 26, BETWEEN 25 AND 27. RESOLUTION OF THE DIOPHANTINE EQUATION $y^3 - x^2 = 2$ USING THE FACTORIAL RING $Z[i\sqrt{2}]$

GEORGIANA VELICU[1]
Valahia University of Targoviste, Faculty of Science and Arts, Bd.Unirii, nr. 18-24
Targoviste, Romania
neacsugeorgiana@yahoo.com

Abstract: *In this article I try to demonstrate, using the factorial ring* $Z[i\sqrt{2}]$ *an important property of the number 26, meaning that it's the only integer which is a discrete distance of one from a square and a cube:* $25 = 5^2 \le 26 \le 27 = 3^3$. *This problem is related to Pierre Fermat, a French mathematician of the XVII century above. It has proved after that he was somewhat wrong for there is a unique solution to the problem. The paper is divided in two parts. First I expose the basic ideas witch come to mind and lead to the solution witch 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 $-2 = k^2 - k'^3$ and then (k, k') is a solution of the diophantine equation $y^3 - x^2 = 2$ with $(x, y) \in N^2$. In fact, the problem is to solve this equation. Thus, we will prove that:

Theorem 1. (Particular case of the Catalan problem) The unique solution of the diophantine equation in N^2

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

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

First we 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.

Prof. If x is an even number, then x is $x = 2m, m \in Z$. We have that $y^3 = 4m^2 + 2$, and then also y is an even number.

If x is odd number, then x is $x = 2m + 1$, $m \in Z$. It results that $y^3 = 4m^2 + 4m + 3$, then also y is an odd number.

From the Euler's theorem we have that: $a^{\varphi(n)} \equiv 1 \pmod{n}$, for $(a, n) = 1$, where $\varphi(n)$ is Euler's indicatory, $\varphi(n) = n\prod_{i=\overline{1,m}}\left(1 - \frac{1}{p_i}\right)$, for $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, p_i - prime numbers, $i = \overline{1,m}$.

The theorem can be write: $a^{\varphi(n)+1} \equiv a \pmod{n}$, $(a, n) = 1$.

Solving the equation (1) in $Z/4Z = Z_4$, we have for $n = 4 = 2^2$, $\varphi(4) = 4\left(1-\frac{1}{2}\right) = 2$, and then $y^3 \equiv y \pmod 4, (y,4) = 1$. From there it results that $y \equiv x^2 + 2 \pmod 4$.

If we assume that $2|x \Rightarrow 4|x^2 \Rightarrow y \equiv 2 \pmod 4 \Rightarrow y \equiv y^3 \equiv 2 \pmod 4$. But, also, we have $2|y$ (x and y have the same parity), so $8|y^3$, from where results $y^3 \equiv 0 \pmod 4$, contradiction with $y^3 \equiv 2 \pmod 4$. The supposition we made is false, then x can't be an even number, so we have 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 a solution of (1), then $(x,y) = 1$.

Prof. Let $d = (x,y)$.

Then $x = d \cdot x_1$ and $y = d \cdot y_1$, $x_1, y_1 \in Z$. We have that $d^3 y_1^3 = d^2 x_1^2 + 2 \Rightarrow d^2\left(dy_1^3 - x_1^2\right) = 2$. From there we have $d^2|2$, and also $d = \pm 1$. The conclusion is that $(x,y) = 1$.

We now examine the equation in $Z/3Z = Z_3$. For $n = 3$, we have $\varphi(n) = 3\left(1-\frac{1}{3}\right) = 2$, then, from the Euler's theorem result that $y^2 \equiv 1 \pmod 3, (y,3) = 1$ or $y^3 \equiv y \pmod 3$. It reduces the degree and we obtain $y = x^2 + 2 \pmod 3$. But $x^2 \equiv 1 \pmod 3, (x,3) = 1$, and $y \equiv 3 \pmod 3 \Leftrightarrow y \equiv 0 \pmod 3$. The resolution is easy and leads to $x = 3$ or $y = 3$ in $Z/3Z = Z_3$. But we have that $y < x$: if it was the contrary, the difference between y^3 and x^2 would never been equal to 2 because of the comparative growth of the functions $x \to x^2$ and $y \to y^3$. Thus it leads to the unique solution $x = 5$ and $y = 3$, if we suppose that x and y are 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 direction, we don't obtain interesting results, and it is very fastidious. But it leads to the following idea: to use 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 some definitions.

Let R be a commutative ring with no divisors of zero.

Definition 1. An element $p \in R$ it is *a prime element* in R if and only if:

1) $p \neq 0$ and $p \notin U(R)$;

2) For every $a, b \in R$ with $p|ab$, it results that $p|a$ or $p|b$.

Definition 2. A commutative ring *R* is called *a factorial ring* if has no divisors of zero, and if there exists a decomposition of any element in unique product (without taking account of the order) of prime elements of the ring.

Definition 3. A commutative ring *R* is called an *Euclidian ring* if there exist an application $N: R \setminus \{0\} \to \mathrm{N}$ with the property: for every $a, b \in R$, $b \neq 0$ exists q and r in *R*, with:

$$a = bq + r, \text{ where } r = 0 \text{ or } N(r) < N(b).$$

The application N is called the *norm* application in *R*.

Theorem. If R is an Euclidian ring, then *R* is a factorial one.
The prof of the theorem is in [1].

The first and the classical example of Euclidian and also factorial ring is **Z,** the ring of the integers. Another examples: $Z[i]$ - the ring of Gauss' integers, $Z[i\sqrt{2}]$, $Z\left[\frac{1+i\sqrt{3}}{2}\right]$, $Q[x]$. Examples of rings that are not factorial rings: $Z[i\sqrt{6}]$, $Z[i\sqrt{5}]$, $Z[i\sqrt{26}]$, $Z[i\sqrt{n}]$ with $n = 4k+1, n \geq 3, \sqrt{n} \in \mathrm{Z}$.

In factorial rings we can define a gcd (the greatest common divisor) , as in **Z**, and that is the property will be used.

Definition. Let $a, b \in R$. An element $d \in R$ is a gcd of *a* and *b* if and only if:
1) $d \mid a$ and $d \mid b$ (*d* is a common divisor of *a* and *b*);
2) if there $\exists d' \in R$ so that $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Now we return to the equation (1). We have $x^2 + 2 = \left(x + i\sqrt{2}\right)\left(x - i\sqrt{2}\right)$, and $y^3 = \left(x + i\sqrt{2}\right)\left(x - i\sqrt{2}\right)$.

Then we study the equation in the factorial ring $Z[i\sqrt{2}] = \left\{a + bi\sqrt{2} \mid a, b \in \mathrm{Z}\right\}$, with the norm application $N: Z[i\sqrt{2}] \setminus \{0\} \to \mathrm{N}$, $N(a + bi\sqrt{2}) = a^2 + 2b^2$. We know that the norm application have the following properties:

1) $N(z_1 z_2) = N(z_1)N(z_2), \forall z_1, z_2 \in Z[i\sqrt{2}]$;
2) if $z_1 \mid z_2$ in $Z[i\sqrt{2}]$, then $N(z_1) \mid N(z_2)$ in **N.**

Assume that $d = g.c.d.(x + i\sqrt{2}, x - i\sqrt{2})$. It follows that $d \mid x + i\sqrt{2}$ and $d \mid x - i\sqrt{2}$. Let $d = a + bi\sqrt{2}, a, b \in \mathrm{Z}$. We obtain $d \mid 2i\sqrt{2}$, so $N(d) \mid N(2i\sqrt{2})$ and $N(d) \mid 8 \Leftrightarrow N(d) \in \{1,2,4,8\}$. But $d \mid x \pm i\sqrt{2} \Rightarrow N(d) \mid N(x \pm i\sqrt{2}) \Leftrightarrow N(d) \mid x^2 + 2$. We know that x in an odd number, also $x^2 + 2$ is odd, then *N*(*d*) is odd, but $N(d) \in \{1,2,4,8\}$, and we have *N*(*d*) = 1. It follows that $a^2 + 2b^2 = 1$, with the solution $a = \pm 1$ and $b = 0$ in **N**. We obtain d =1 and $g.c.d.(x + i\sqrt{2}, x - i\sqrt{2}) = 1$.

We now use the unique factorization of both elements in $Z[i\sqrt{2}]$: $x+i\sqrt{2}=z_1z_2...z_n$ and $x-i\sqrt{2}=\bar{z}_1\bar{z}_2...\bar{z}_n$ (they are conjugate numbers). We have $g.c.d.(x+i\sqrt{2},x-i\sqrt{2})=1$, 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 $(a,b)\in Z^2$ with $x+i\sqrt{2}=(a+bi\sqrt{2})^3$.

Expending the expression, we obtain $x+i\sqrt{2}=(a+bi\sqrt{2})^3=$ $=(a^3-6ab^2)+i\sqrt{2}(3a^2b-2b^3)$ and $3a^2b-2b^3=1\Leftrightarrow b(3a^2-2b^2)=1$. It means that $b=1$ and $3a^2b=-2b^2=1$, or $b=-1$ and $3a^2b=-2b^2=-1$. If we examine the second set of equalities, we have $3a^2=1$, which has no integer solution. Therefore we have $b=1$ and $a^2=1$.

Finally, $x+i\sqrt{2}=(1+i\sqrt{2})^3$. Expending it, we obtain $x+i\sqrt{2}=\pm5+i\sqrt{2}$. Recalling that $x>0$, we obtain $x = 5$.

If we use equation (1) and replace *x* by its value 5, we have to solve $y^3=27$. It has a unique trivial solution $y = 3$ in **N**.

We end the demonstration by saying that $(x,y)=(5,3)$ is a valid solution of the equation (1).

3. Another examples of diophantine equations witch can be solved using factorization domains:

3.1. The equation $y^2=x^3-4$ can be solved using **Z**[*i*] (the ring of Gauss' integers) and we have the solutions $(5,\pm11)$ and $(2,\pm2)$.

3.2. The equation $x^2+7=2^y$ can be solved using $Z\left[\frac{1+i\sqrt{7}}{2}\right]$ and we have the solutions: $(\pm1,3)$, $(\pm3,4)$, $(\pm5,5)$, $(\pm11,7)$ and $(\pm181,15)$.

References

[1] Nastasescu, C. Nita, C., Vraciu, C., *Bazele algebrei*, vol. I, Editura Academiei R.S.R., 1986

[2] Nastasescu, C. Nita, C., Vraciu, C., *Aritmetica si algebra*, Editura Didactica si Pedagogica Bucuresti, 1993

[3] Nastasescu, C. Nita, C., Vraciu, C., *Aritmetica si algebra*, Editura Uviversitatii Bucuresti, 1986