$x^5 - y^2 = 4$ AND GAUSSIAN INTEGERS

Albertas ZINEVIČIUS
Faculty of Mathematics and Informatics, Vilnius University,
Naugarduko str. 24, LT-03225 Vilnius, Lithuania;
e-mail: albertas.zinevicius@gmail.com

Abstract. The article offers a short exposition to a classical technique of solving Diophantine equations by solving $x^5 - y^2 = 4$ with the help of unique factorization in the ring of Gaussian integers $\mathbb{Z}[i]$.

Key words and phrases: Diophantine equation, Gaussian integers, factorization.

2010 Mathematics Subject Classification: 11D41, 11H45.

1. Solution to $x^5 - y^2 = 4$

“Determine all pairs $(x, y)$ of integers such that $x^5 - y^2 = 4$.”

The problem was proposed in [4]. The reader can find an elementary solution in the next issue. We offer a different solution that demonstrates how the basic knowledge of the ring of Gaussian integers may be employed in a Diophantine problem. This approach is well-known (e.g., see the survey article [2]) and dates back at least to [3]. In Section 2, we shortly discuss a more general problem.

Theorem 1. There is no pair of integers $(x, y)$ such that $x^5 - y^2 = 4$.

Proof. Assume that there is such a pair $(x, y)$. If $x$ is even, then $x = 2x'$. We hence have

$$32x'^5 = y^2 + 4.$$

We see that $y^2$ must be divisible by 4. Thus, $y = 2y'$. Therefore,

$$32x'^5 = 4y'^2 + 4 \iff 8x'^5 = y'^2 + 1.$$
Since the left-hand side of the last equation is even, we see that \( y' \) must be odd. But then, the right-hand side equals 2 modulo 4, while the left-hand side equals 0 modulo 4. Thus, \( x \) cannot be even. So, \( x \) is odd. We can write

\[
x^5 = (y + 2i)(y - 2i)
\]

over the ring of Gaussian integers \( \mathbb{Z}[i] \). If there is a Gaussian prime \( p \in \mathbb{Z}[i] \) such that \( p|y + 2i, y - 2i \), then \( p|y + 2i - (y - 2i) = 4i \). Thus \( p \) is a divisor of 2 and, therefore, is an associate of \( 1 + i \). Then, \( 1 + i|\alpha^5 \). Therefore, \( \text{N}(1 + i) = 2\text{N}(\alpha^5) = x^{10} \). This, however, cannot happen since \( x \) is odd. Consequently, \( y + 2i, y - 2i \) are coprime and, since their product is a 5th power, they both must be associates of 5th powers of some elements of \( \mathbb{Z}[i] \).

In particular,

\[
e(y + 2i) = (k + li)^5 = \sum_{j=0}^{5} \binom{5}{j} k^{5-j} (li)^j
\]

\[
= (k^5 - 10k^3l^2 + 5kl^4) + (5k^4l - 10k^2l^3 + l^5)i,
\]

where \( k, l \in \mathbb{Z} \) and \( e \in \{ \pm 1, \pm i \} \) is a unit. Therefore, either

\[
2ie = k^5 - 10k^3l^2 + 5kl^4,
\]

or

\[
2ie = (5k^4l - 10k^2l^3 + l^5)i.
\]

We claim that neither \( k^5 - 10k^3l^2 + 5kl^4 \), nor \( 5k^4l - 10k^2l^3 + l^5 \) can be an associate of 2. Observe that it is enough to show the first, as the other follows by renaming \( k \) by \( l \) and vice versa. If

\[
k^5 - 10k^3l^2 + 5kl^4 = k(k^4 - 10k^2l^2 + 5l^4) = \pm 2,
\]

then \( k|2 \). Thus, \( k = \pm 1 \) or \( k = \pm 2 \). In the first case,

\[
k^4 - 10k^2l^2 + 5l^4 = 1 - 10l^2 + 5l^4 = \pm 2.
\]

One can verify that for \( l^2 = 0, 1 \) this is not the case, while for \( l^2 \geq 4, 1 - 10l^2 + 5l^4 \geq 1 - l^2(10 - 20) > 2 \). Hence, the first case cannot happen.

In the second case,

\[
k^4 - 10k^2l^2 + 5l^4 = 16 - 40l^2 + 5l^4 = \pm 1.
\]

By checking values of \( l^2 = 0, 1, 4 \) and seeing that when \( l^2 \geq 9 \), holds \( 16 - 40l^2 + 5l^4 \geq 16 - l^2(40 - 45) > 1 \), one concludes that this case cannot happen as well. We conclude that the equation \( x^5 - y^2 = 4 \) cannot have integer solutions.
2. On integer solutions to $x^{2n+1} - y^2 = 4$

This approach allows us to say a bit more.

**Theorem 2.** For $n \geq 2$, the equation $x^{2n+1} - y^2 = 4$ has a solution in integers $(x, y)$ precisely when the equation

$$y + 2i = \pm(l + 2i)^{2n+1}$$

has a solution in integers $(y, l)$.

**Proof.** First, observe that if $(x, y)$ is a solution, then, in the same manner as above, $x$ must be odd and $y + 2i, y - 2i$, therefore, have to be coprime. Hence, $y + 2i, y - 2i$ both have to be associates of $2n + 1$th powers of Gaussian integers. Thus,

$$e(y + 2i) = (k + li)^{2n+1},$$

where $k, l \in \mathbb{Z}$ are integers and $e \in \{\pm 1, \pm i\}$ is a unit. By the binomial expansion, we have

$$e(y + 2i) = \sum_{j=0}^{2n+1} \binom{2n+1}{j}k^{2n+1-j}(li)^j.$$

The real and imaginary parts of the binomial expansion are

$$\sum_{j=0}^{n} \binom{2n+1}{2j}k^{2n+1-2j}(li)^{2j}, \sum_{j=0}^{n} \binom{2n+1}{2j+1}k^{2n-2j}(li)^{2j},$$

respectively. One of them must equal $\pm 2$. Up to renaming $k$ by $l$ and vice versa, we may assume that it is the first one. Then $k|2$, and thus, either $k = \pm 1$, or $k = \pm 2$. We will show that $k = \pm 1$ is not possible. Say, $k = \pm 1$. Then

$$\pm 2 = \sum_{j=0}^{n} \binom{2n+1}{2j}k^{2n+1-2j}(li)^{2j} = \sum_{j=0}^{n} \binom{2n+1}{2j}(-l^2)^j.$$

By observing that the first summand of the binomial expansion is equal to 1 and subtracting it from both sides, we obtain

$$\sum_{j=1}^{n} \binom{2n+1}{2j}(-l^2)^j \in \{-3, 1\}.$$
Thus \(l^2 \mid 3\), and, therefore, \(l = \pm 1\). Hence, the complex number \(k + li\) has norm equal to 2. We can see that the norm of \((k + li)^{2n+1}\) is an even number, while the norm of \(e(y + 2i)\) is odd. Therefore, the equality \(e(y + 2i) = (k + li)^{2n+1}\) is not possible. Hence, \(k = \pm 1\) is not possible. Thus, \(k = \pm 2\). Then we have \(e(y + 2i) = (\pm 2 + li)^{2n+1}\). By multiplying both sides by a unit, we thus obtain

\[
y + 2i = e(l + 2i)^{2n+1},
\]

where \(e\) denotes a unit again. Since \(y\) is odd, \(l\) must be odd too. Then \((l + 2i)^{2n+1}\) has an odd real part and an even imaginary part. Since, after multiplication by \(e\), the real part must equal \(y\) and thus remain odd, we conclude that \(e = \pm 1\). Therefore,

\[
y + 2i = \pm(l + 2i)^{2n+1}.
\]

Conversely, say that

\[
y + 2i = \pm(l + 2i)^{2n+1}
\]

holds for integers \((y, l)\). By multiplying both sides of the equality by their conjugates, we obtain

\[
y^2 + 4 = (l^2 + 4)^{2n+1}.
\]

Thus, \((x, y) = (l^2 + 4, y)\) is a solution.

The equation \(y + 2i = \pm(l + 2i)^{2n+1}\) can be interpreted geometrically. It may be interesting to ask whether \(n\) for which it has an integer solution could be arbitrarily large. It turns out that the answer is known to be negative. In fact, for \(n \geq 2\), the corresponding equation has no integer solutions. The result follows from the work of T. Nagell [5], as referenced to in [1]. Very generally, a conjecture of S. S. Pillai states that each positive integer occurs at most finitely many times as a difference of two perfect powers (see, e.g., [6]).

Acknowledgement. I would like to thank \textit{Mathematical Excalibur} for mailing their magazine.

References


$x^5 - y^2 = 4$ and Gaussian integers


Received
9 January 2012