Some Applications of Properties of the Extensions of the Ring of Integers

Marcel Teleuca, Larisa Sali

Abstract

This article presents some considerations related to the application of ring algebra concepts to solving problems proposed in mathematics competitions. The content can be useful to mathematics teachers and high school students.

Keywords: Gaussian integers, division theorem, factorization, greatest common divisor.

1 Introduction

The topics we will study are extensions of common properties of the Gaussian integers $Z[i] = \{a + bi | a, b \in Z\}$.

The objective of this investigation aims at the didactic transposition of the mathematical contents for the familiarization of students with some applications of concepts related to extension of the ring Z. Some properties of this structure are successfully used in solving problems. For this purpose, the following facts can be examined: the norm on $Z[i]$; divisibility in $Z[i]$; the division theorem in $Z[i]$; the Euclidean algorithm in $Z[i]$; unique factorization in $Z[i]$; primes in $Z[i]$; modular arithmetic in $Z[i]$; applications of $Z[i]$ to the arithmetic of Z.

Definition 1. *For $\alpha = a + bi \in Z[i]$, its norm is the product $N(\alpha) = (a + bi)(a - bi) = a^2 + b^2$.*

The norm of every Gaussian integer is a non-negative integer, but it is not true that every non-negative integer is a norm. Indeed, the norms are the integers of the form $a^2 + b^2$ and not every positive integer is a

©2024 by Marcel Teleuca, Larisa Sali

sum of two squares. It's preferable to deal with norms on $Z[i]$ instead of absolute values on $Z[i]$ because norms are integer.

Definition 2. *We say β divides $\alpha \in Z[i]$ (and write $\beta|\alpha$) if $\alpha = \beta\gamma$ for some $\gamma \in Z[i]$.*

Definition 3. *For non-zero α and $\beta \in Z[i]$ a greatest common divisor of α and β (denoted $gcd(\alpha, \beta)$) is a common divisor with maximal norm.*

We can speak about **a greatest** common divisor, but not about **the greatest** common divisor. If δ is a greatest common divisor of α and β, then its unit multiples $-\delta, i\delta, -i\delta$ (at least) are greatest divisors too.

Definition 4. *When α and $\beta \in Z[i]$ only have unit factors in common, we call them relatively prime.*

Some contest problems can be solved using the Eisenstein's ring of integers $Z[\omega] = \{\alpha = a + b\omega | a, b \in Z\}$, where $\omega = \dfrac{-1 + i\sqrt{3}}{2} = e^{\frac{2\pi i}{3}}$. Its norm is the product $N(\alpha) = a^2 - ab + b^2$. Units in this ring are $\pm 1, \pm\omega, \pm(1 + \omega) = \mp\omega^2$.

2 Some properties of the concepts in $Z[i]$

Theorem 1. *The norm is multiplicative: for α and β in $Z[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Theorem 2. *If $N(x)$ is prime, then x is also prime.*

Corollary 1. *The only Gaussian integers which are invertible in $Z[i]$ are $\{-i; i; -1; 1\}$.*

Theorem 3. *A Gaussian integer for $\alpha = a + bi$ is divisible by an ordinary integer c if and only if $c|a$ and $c|b$ in Z.*

We may prove that Euclidean Algorithm holds in this rings. Not every unique factorization domain (UFD) is Euclidean, but every Euclidean ring is a UFD. We won't prove either of these facts, some of the proofs can be found in [1]. Lets move onto problem examples.

3 Applications of algebraic number fields to Olympiad problem solving

We will start with a problem proposed for IMO. For these problems we will need the following important lemma.

Lemma. If a, b, c, d are elements of a unique factorization domain K, satisfying $ab = cd$, then there exist $m, n, p, q \in K$, such that $a = mn$, $b = pq$, $c = mp$, $d = nq$.

Proof. Let $gcd(a, c) = n$, then since $a \mid cd$, $\frac{a}{n} = m \mid d$, analogously if $gcd(b, c) = p$, then $\frac{b}{p} = q \mid d$. We get $a = mn$, $b = pq$, $c = mp$, $d = nq$. Notice since we are working in UFD all operations are well defined.

More notes on application of this lemma may be found in [2].

Problem 1. Let x, y and z be natural numbers satisfying $xy = z^2 + 1$. Prove that there exist integers a, b, c, d such that $x = a^2 + b^2$, $y = c^2 + d^2$ and $z = ac + bd$.

Solution. We will factor the right side of our equation and apply previously stated lemma to get $x = uv$, $y = tw$, $z + i = uw$, $z - i = vt$, for some $u, v, t, w \in Z[i]$. Because x and y are natural numbers, we must have $v = q\overline{u}$ and $t = p\overline{w}$ with $p, q \in Q$. Since $z + i = uw$ and $z - i = vt$, we conclude that $p = q = 1$. Now setting $u = a + bi$, $w = c - di$ yields $x = a^2 + b^2$, $y = c^2 + d^2$ and $z = ac + bd$.

We would like to continue with the classic Fermat's Last Theorem for the case $n = 3$. Proof presented below is due to Gauss.

Problem 2. Prove that the equation $x^3 + y^3 = z^3$ has no solutions in integers.

Solution. Suppose that x, y, z are nonzero elements of $Z[\omega]$ (the ring of Eisenstein's integers, where $\omega = \frac{-1 + i\sqrt{3}}{2} = e^{\frac{2\pi i}{3}}$), which satisfy the equation. We can assume that they are pairwise coprime. Lets consider $\delta = 1 - \omega$. It is prime and $\overline{\delta} = 1 - \omega^2 = (1 + \omega)\delta$. For some $\phi \in Z[\omega]$, $\delta \mid \phi$ iff $\delta \mid \overline{\phi}$. We also want to prove that every number in $Z[\omega]$ is congruent to $-1, 0$ or $1 \pmod{\delta}$. It follows from the congruence $a + b\omega \equiv (a + b) \mod \delta$ and $a + b = 3q + r \equiv r$

(mod δ), where $r \in \{-1, 0, 1\}$. Another important fact that we will use is that $\phi \equiv \pm 1 \pmod{\delta}$ (with $\phi \in Z[\omega]$) implies $\phi^3 \equiv \pm 1 \pmod{\delta^4}$. Returning back to our initial equation we notice that exactly one of the numbers x, y, z must be divisible by δ, because otherwise we get that x, y, z are congruent to $\pm 1 \pmod{\delta^4}$, which implies false congruence. We assume without loss of generality that $\delta \mid z$. Also $\delta^4 \mid z^3$, so $\delta^2 \mid z$.

Let $k \geq 2$ be the smallest natural number for which there exists solution with x, y, z pairwise coprime and $\delta^k \mid z$, but δ^{k+1} does not divide z. Factoring the equation we obtain $z^3 = (x+y)(\omega x+\omega^2 y)(\omega^2 x+\omega y)$, noticing that the factors are congruent (mod δ) and their sum is 0, we may denote them as $x + y = A\delta$, $\omega x + \omega^2 y = B\delta$ and $\omega^2 x + \omega y = C\delta$, where $A, B, C \in Z[\omega]$ are pairwise coprime and $A + B + C = 0$. Because $ABC = \left(\frac{z}{\delta}\right)^3$ is a perfect cube we must have $A = \varepsilon\alpha^3$, $A = \zeta\beta^3$, $A = \eta\gamma^3$, for some pairwise coprime $\alpha, \beta, \gamma \in Z[\omega]$ and $\varepsilon, \zeta, \eta \in \{\pm 1, \pm\omega, \pm\omega^2\}$. Therefore $\varepsilon\alpha^3 + \zeta\beta^3 + \eta\gamma^3 = 0$. Since $\varepsilon\zeta\eta$ is a unit and a perfect cube it must be equal to ± 1. On the other hand, $ABC = \left(\frac{z}{\delta}\right)^3$ is divisible by δ (because $\delta^2 \mid z$), so exactly one of the numbers α, β, γ is divisible by δ, let it be γ. In fact, $\gamma^3 \mid ABC$ and $\delta^{3k-3} \mid ABC$, and δ^{3k-2} does not divide ABC. So, $\delta^{k-1} \mid \gamma$ and δ^k does not divide γ. Now since α, β are not divisible by δ, evaluating $\varepsilon\alpha^3 + \zeta\beta^3 + \eta\gamma^3 = 0 \pmod{\delta^4}$ gives us $\varepsilon \pm \zeta \equiv 0 \pmod{\delta^4}$, therefore $\varepsilon = \pm\zeta$ and $\varepsilon\zeta\eta = \pm 1$, implies $\eta = \pm\zeta$. Canceling ζ in equation yields $\alpha^3 \pm \beta^3 \pm \gamma^3 = 0$, which is another nontrivial solution to the initial equation with α, β, γ being pairwise coprime. However, in this solution $\delta^{k-1} \mid \gamma$ and δ^k does not divide γ, which contradicts choice of k.

Problem 3. Prove that a prime number p can't be written as a sum of 2 squares of positive integers in more than one way.

Solution. Let p be a prime number, which contradicts our assumption. Then we have $p = x^2 + y^2 = u^2 + v^2$, factoring yields $(x + iy)(x - iy) = (u + iv)(u - iv)$. Denoting $a = x + iy$, $b = u + iv$ the former condition may be rewritten as $a\overline{a} = b\overline{b}$. If $gcd(a, b) = n$, then $m = \dfrac{a}{n}$ must divide $\overline{b}$, following this logic we get $a = nm =$

$(\alpha+i\beta)(\gamma+i\delta)$ and $b = n\overline{m} = (\alpha+i\beta)(\gamma-i\delta)$. Now $x = Re(a) = \alpha\gamma-\beta\delta$ and $y = Im(a) = \beta\gamma + \alpha\delta$, going back to our first relation we get $p = x^2+y^2 = (\alpha\gamma-\beta\delta)^2+(\beta\gamma+\alpha\delta)^2 = (\alpha^2+\beta^2)(\gamma^2+\delta^2)$. For p to be prime one of the factors must be equal to 1, without loss of generality lets assume $\alpha^2+\beta^2 = 1$, this implies that $\alpha = 0, \beta = 1$ or $\alpha = 1, \beta = 0$. If $\alpha = 0$ then $x = -\delta$ and $u = \delta$, contradiction with assumption that integers are positive. If $\beta = 0$ the $x = \gamma = u$ and obviously $y = v$, contradiction with assumption that integers are different. So there aren't any primes p representable as sum of two squares in two different ways.

Problem 4. *(IMO 2001, Problem 6)* Let $a > b > c > d$ be positive integers such that $ac + bd = (b + d + a - c)(b + d - a + c)$. Prove that $ab + cd$ is not prime.

Solution. Initial condition is equivalent to $a^2-ac+c^2 = b^2+bd+d^2$, which may be factored as $(a + \omega c)(a + \omega^2 c) = (b - \omega d)(b - \omega^2 d) \Leftrightarrow (a + \omega c)\overline{(a + \omega c)} = (b - \omega d)\overline{(b - \omega d)}$. Lets denote $a + \omega c = x$ and $b - \omega d = y$. If $gcd(x, y) = n$ and $\dfrac{x}{n} = m$, then $m \mid \overline{y}$, resulting $gcd(x, \overline{y}) = m$. So we get $x = nm$, $y = n\overline{m}$ and $n = p+\omega q$, $m = r+\omega s$. Now going backwards we find that $a = pr - qs$, $c = qr + ps - qs$, $b = pr + qs - ps$ and $d = ps - qr$. Now $ab + cd = (pr - qs)(pr + qs - ps) + (qr + ps - qs)(ps - qr) = (p^2 - q^2)(r^2 - rs + s^2)$. For $ab + cd$ to be prime we must have $p^2 - q^2 = \pm 1$ or $r^2 - rs + s^2 = \pm 1$. First equation has solutions only if one of numbers p, q is 0, which would imply that $a + b = 0$ or $c = d$. Second equation has solutions only if one of the numbers r, s is 0 or $r = s$, all three cases leading to contradictions to initial condition. So $ab + cd$ is product of two integers with absolute values greater than 1, i.e. is composite.

Problem 5. *(BMO Shortlist 2010)* Find all pairs of integers (x, y), such that $x^3 = 2y^2 + 1$.

Solution. Rewrite original equation as $x^3 = (1+y\sqrt{-2})(1-y\sqrt{-2})$. Since $Z[\sqrt{-2}]$ is UFD and $gcd(1 + y\sqrt{-2}, 1 - y\sqrt{-2}) = 1$. We get that $1+y\sqrt{-2} = (u+v\sqrt{-2})^3 = u(u^2-6v^2)+v(3u^2-2v^2)\sqrt{-2}$. Therefore, $u(u^2 - 6v^2) = 1$, which implies $u = 1$ and $v = 0$. Consequently, $y = 0$ and $x = 1$, which are obviously solutions to the given equation.

4 Conclusion

This approach to solving some Olympiad problems is interesting because involves the application of algebraic facts, not studied in high school, but accessible to students for understanding. Through the didactic transposition of mathematical contents, high school students get familiar with various possibilities for making generalizations and abstractions. The contents give them the opportunity to reflect on the nature of mathematical knowledge.

Acknowledgments. The Institutional Research Program of the Moldova State University for 2024–2027 years, subprogram 011303 has supported part of the research for this paper.

References

[1] D. Djukic. *Arithmetic in Extensions of Q*. IMOMATH, 2007.

[2] I. Mitelman and M. Teleuca. *A parametrization for pairs of numbers with the same product in the ring of integers and some of its quadratic extensions in solving olympiad-type problems from number theory.* Mathematics in the modern school, 1/2012, pp. 40-45.(In ukrainean.)

[3] BMO Shortlist, 2010.

[4] www.artofproblemsolving.com

Marcel Teleuca[1], Larisa Sali[2]

[1]Moldovan State University, Vladimir Andrunachievici Institute of Mathematics and Computer Science
E–mail: marcel.teleuca@math.usm.md
ORCID: https://orcid.org/0000-0003-1730-5284

[2]Pedagogical State University "Ion Creanga"
E–mail: larisa.sali2018@gmail.com
ORCID: https://orcid.org/0000-0003-1172-3055