On Rings and Gaussian Integers

Texas A&M University – San Antonio

Sean Zachary Roberson

In abstract algebra, one is concerned about the structures that particular sets have under some binary operation. For example, the set of planar rotations of a square form a group under the operation of function composition, where the functions are the rotations (such as quarter-turns and reflections). However, some sets, such as integers (including congruence classes), matrices, and polynomials are endowed with more than one operation. In this paper, we will examine the structure of rings and analyze the set of Gaussian integers – the set of complex numbers that lie on lattice points. Furthermore, we will see how Gaussian integers can be used to prove results that originate from the ordinary integers.

Before introducing the Gaussian integers, one must understand the concept of the algebraic structure known as a ring. The study of rings can be related to Fermat's Last Theorem, which states that the Diophantine equation $x^n + y^n = z^n$ has no solutions when $n \geq 3$. Leonhard Euler began work on the case when $n = 3$. In his attempts, Euler extended the rules of addition and multiplication in the integers to numbers of the form $a + b\sqrt{-3}$, where a and b are integers. This set forms a ring, but Euler was not concerned about their algebraic structure. In 1847, the mathematician Gabriel Lamé claimed he had a solution for Fermat's Last Theorem, but Joseph Liouville argued that any proof would rely on the property of unique factorization of primes. Here, the primes would not necessarily be typical integers, but numbers similar to those that Euler had worked on. Similar work continued until Richard Dedekind began analyzing complex numbers similar to Euler. Dedekind stated the concept of "ideal complex numbers," and, more generally, ring ideals. The ideal, to Dedekind, was characterized by closure under certain operations. The concept of prime numbers was extended by Dedekind to prime ideals, abstracting the property of irreducibility. Although many concepts of rings were thought of by Dedekind, the word "ring" was not coined by him. David Hilbert, another German mathematician, used the word *Zahlring*, meaning “number ring,” to describe the structures that Dedekind considered. While much of early ring theory branched from number theory, other mathematicians, such as Benjamin Peirce, noted that rings do not have to be composed of numerical objects. For example, he noted that Arthur Cayley’s matrices satisfied the modern ring axioms (O'Connor & Robertson, 2004). While ring theory started as an extension of number theory, it holds a connection to the study of algebra as a whole. It may be of interest, then, to study not only the group structure of particular sets of objects such as integers and matrices, but also their ring structure.

Typically, students of abstract algebra first learn about groups, and then proceed to rings. Students are familiar with some notable groups – the group of integers modulo *n*, the dihedral group of order *2n*, and the group of permutations on *n* symbols, just to name a few. However, of these aforementioned sets, only one is endowed with another natural operation. The set of integers modulo *n* (which we will now write as $\mathbf{Z}_n$) naturally contain a sort of addition and a sort of multiplication. However, when concerned about group structure, only addition is considered. It is well known that $\mathbf{Z}_n$ is an abelian group under addition, but when multiplication is considered as an operation, the same set does not form a group. A new algebraic structure can be built using the same set and the operations of addition and multiplication modulo *n*. This new structure is called a ring. Gallian’s text on abstract algebra (Contemporary Abstract Algebra, 2012, p. 245) lists the ring axioms by first showing the group structure under addition (that is, associativity, existence of inverses and identities, and the commutative nature), then the two properties a ring must possess under multiplication. The two multiplicative properties are recognized as associative multiplication and distribution of multiplication over addition. In some familiar rings, such as the integers and the real numbers, a multiplicative identity, named a unity according to Gallian's text (Contemporary Abstract Algebra, 2012, p. 246), may exist within the ring. However, other books require that a ring possess a unity (Sethuraman, 1996, p. 33). The existence of a unity may then be listed as an axiom. Rings can also be classified as commutative if the operation of multiplication within the ring is commutative. Special elements called units may exist in rings if there are multiplicative inverses (Gallian, p. 246). The usual properties and notions of integers can carry over to other rings of different elements, and so one can make connections to the ring of integers.

As is the case with groups, one may be interested of subsets of rings. In particular, one may wish to know if a certain subset of a ring also forms a ring under the same operations. The test to see if a subset is indeed a subring is similar to those for subgroups. Gallian's subring test requires that the subset is closed under subtraction and multiplication, provided the set is not empty (Contemporary Abstract Algebra, 2012, p. 248). However, Sethuraman's subring test requires closure under addition and multiplication, as well as the existence of a unity and additive inverses (Rings, Fields, and Vector Spaces, 1996, p. 43). To justify this, if the additive inverse is in a subset *S* of *R*, then the ring will be closed under subtraction. Subrings can explain some properties of parent rings, just as subgroups describe parent groups. For example, the set $\{a + bi : a, b \in Z\}$ is a subring of the complex numbers. Later on, this set, known as the Gaussian integers, will be used to describe various results of the ordinary integers.

Although the Gaussian integers are complex numbers, they share similar structural properties of the integers. The relationship between the rings $\mathbf{Z}[i]$ and $\mathbf{Z}$ relies on properties of complex numbers and facts of the integers. To begin, one must first be aware of the norm function in $\mathbf{Z}[i]$. Various sources define the norm of a Gaussian integer $a + bi$ to be $a^2 + b^2$, which is the product of a Gaussian integer with its complex conjugate (Gethner, Wagon, &

Wick, 1998). The use of this norm function opens up doors to prove properties of the Gaussian primes. For example, one can prove a necessary condition for a prime Gaussian integer. That is, there is a way to determine if a Gaussian integer cannot be factored into non-trivial factors, much like the ordinary integers. The following proof is a variation on Keith Conrad's note on Gaussian integers.

Let α be a Gaussian integer, and suppose its norm is a prime number p. Then, since the norm is multiplicative, $N(\alpha) = N(\beta)N(\gamma)$. (Here, N is the norm function.) Since the ordinary integer p is prime, its only factors are 1 and p itself, so exactly one of $N(\beta)$ or $N(\gamma)$ must be the prime p. Now, if the norm of β is 1, then it follows that β is a unit (an element with a multiplicative inverse). So, γ is an element whose norm is prime, and α must be a Gaussian prime. (Conrad, p. 12)

With these properties of primes, one may have questions about the ordinary integers, since they belong to the ring of Gaussian integers (when treated as a complex number). In particular, some, not all, ordinary primes are not Gaussian primes. For example, the ordinary prime number 5 can be factored as $(2 + i)(2 - i)$. By the above proof, both $2 + i$ and $2 - i$ are Gaussian primes. On the other hand, 3 is a Gaussian prime, since it cannot be factored into a product of Gaussian primes (other than itself and the units ± 1 and $\pm i$). The above proof is one condition to find a Gaussian prime. Another condition, given by Gethner, Wagon, and Wick, states that if a Gaussian integer is of the form $\pm n$ or $\pm ni$, then such an integer is prime if and only if n is a prime whose absolute value is congruent to 3 modulo 4 (A Stroll Through the Gaussian Primes, 1998). Relating the properties of prime numbers to those in $\mathbf{Z}[i]$ is key, and is the basis for one unsolved problem in mathematics.

Aside from their ring structure, the Gaussian integers are used in a variety of applications, mainly in algebraic number theory. These integers can be used to examine Pythagorean triples, properties in geometry, and the spread of the Gaussian primes. The manipulations of complex numbers and the Gaussian integers help show results about ordinary integers, and, in the case of the gaps between primes, determine if one can travel the complex plane while only stepping on Gaussian primes.

The equation $x^2 + y^2 = z^2$ is known to many students as the statement of the Pythagorean Theorem. In number theory, it is of interest to solve this equation in the integers. The equation can be extended to complex numbers and the Gaussian integers, so it is of interest to solve $\alpha^2 + \beta^2 = \gamma^2$ in the ring $\mathbf{Z}[i]$. A paper by James T. Cross builds the solution to this equation by first extending the concept of divisibility and parity of integers to $\mathbf{Z}[i]$. The definition of “even” or “odd” Gaussian integers is based on division by a particular Gaussian prime, $1 + i$. To further the definition of parity, Cross states that this Gaussian prime divides any other Gaussian integer “if and only if $x \equiv y \ (mod\ 2)$.” That is, both the real and imaginary parts of the Gaussian integer must be both even or both odd. If that is the case, then the Gaussian integer is even; otherwise, it is odd (Primitive Pythagorean Triples of Gaussian Integers, 1986). To see why a parity definition in $\mathbf{Z}[i]$ is needed, one must examine the set of primitive Pythagorean triples in the ordinary integers. In such a triple, exactly one of the elements is even, and all entries are pairwise relatively prime. Similarly, in the Gaussian integers, a primitive Pythagorean triple must have exactly one “even” element, and all entries must be pairwise relatively prime, at least in $\mathbf{Z}[i]$. By extending the notion of Pythagorean triples to complex numbers, one can learn more about the structure of the Gaussian integers and sums of squares.

The geometry of complex numbers can be used to prove particular properties of the Gaussian integers. A short paper by Walter Rudin gives a proof of the unique factorization property of $\mathbf{Z}[i]$ using a geometric argument. A preliminary lemma is first given, describing that a square whose center lies on a circle has at least one vertex in the interior of the circle. Rudin then proceeds to prove the unique factorization of Gaussian integers into primes. The factorization is, however, unique up to arrangement of the primes and their representation (Unique Factorization of Gaussian Integers, 1961). The representation of these primes may appear different, since they may be a rotation of 90 degrees of a respective prime in the complex plane. A geometric proof of unique factorization is one way the structure of the complex plane is used to show properties of the ring $\mathbf{Z}[i]$.

Geometry can also be used to show the existence of a division algorithm in the Gaussian integers. Jack S. Calcut uses a geometric argument to show that a division algorithm similar to the ordinary integers exists in $\mathbf{Z}[i]$, and he uses this to show unique factorization. First, a Gaussian integer w is selected and is used to rotate the plane by the argument of w, which is equivalent to multiplying all Gaussian integers by w. Next, any Gaussian integer in the original, untouched lattice is taken within a certain distance of an integer in the rotated lattice so that the norm of the difference of these two complex numbers in minimal. This procedure can continue until a complex "remainder" is obtained whose norm is less than that of the integer in the rotated lattice (Gaussian Integers and Arctangent Identities for π, 2009). This is analogous to how division is done in the integers, where the remainder must be selected to be as small as possible. Through the geometry of complex numbers, the Gaussian integers can reveal many parallels to the ordinary integers.

One unsolved problem in mathematics involves the Gaussian primes and how far apart they are from each other. The problem, known as the Gaussian moat problem, asks if it is possible for one to find an infinite sequence of Gaussian primes for which the difference between terms is bounded. The problem is also stated as a walk to infinity, using the Gaussian primes as stepping stones. An article by Ellen Gethner gives a basic understanding of the problem. Posed by UCLA mathematician Basil Gordon in 1962, the Gaussian moat problem is one that asks about gaps between the primes, in terms of Euclidean distance. The size of a moat is given by the maximum distance between any two primes. One question in the article asks, “If you keep walking forever, will you, every once in a while, have to take longer and longer steps?” (In Prime Territory, 1996). An expanded article by Gethner, along with Stan Wagon and Brian Wick, shows more results about the problem. The problem is reduced to a walk on the line within the complex plane. This line contains two or more distinct Gaussian integers, and it is proven that there is another integer on this line so that all Gaussian integers within a particular distance of it are composite. So, there is no line in the complex plane for which one can walk to infinity while using the Gaussian primes as stepping stones (A Stroll Through the Gaussian Primes, 1998, p. 7). The unsolved problem eludes mathematicians as they try to learn more about the Gaussian integers and the gaps between their irreducible elements.

In closing, the Gaussian integers are a ring contained within the complex numbers. Their structure allows various questions to be answered about ordinary integers or elements of the ring $\mathbf{Z}[i]$. While geometry can connect the Gaussian integers and the ordinary integers, there are still mysteries of the prime elements in $\mathbf{Z}[i]$. These integers can still be seen as an extension of the ordinary integers, and allow mathematicians to draw more connections to them in algebra and number theory.

Bibliography

Calcut, J. S. (2009, June). Gaussian Integers and Arctangent Identities for π. *The American Mathematicial Monthly, 116*(6), 515-530.

Conrad, K. (n.d.). The Gaussian Integers.

Cross, J. T. (1986, April). Primitive Pythagorean Triples of Gaussian Integers. *Mathematics Magazine, 59*(2), 106-110.

Gallian, J. A. (2012). *Contemporary Abstract Algebra* (8th ed.). Cengage Learning.

Gethner, E. (1996, April). In Prime Territory. *Math Horizons, 3*(4), pp. 8-13.

Gethner, E., Wagon, S., & Wick, B. (1998). A Stroll Through the Gaussian Primes. *The American Mathematical Monthly, 105*(4), 327-337.

Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). *An Introduction to the Theory of Numbers* (5th ed.).

O'Connor, J. J., & Robertson, E. F. (2004, September). Ring Theory. Retrieved from http://www-history.mcs.st-andrews.ac.uk/HistTopics/Ring_theory.html

Rudin, W. (1961, November). Unique Factorization of Gaussian Integers. *The American Mathematical Monthly, 68*(9), 907-908.

Sethuraman, B. A. (1996). *Rings, Fields, and Vector Spaces.* Springer.