Gaussian Integers and Dedekind's Creation of an Ideal: A Number Theory Project

Janet Heine Barnett*

January 1, 2018

1 Introduction

In the historical development of mathematics, the nineteenth century was a time of extraordinary change during which the discipline became more abstract, more formal, and more rigorous than ever before. Within the subdiscipline of algebra, these tendencies led to a new focus on studying the underlying *structure* of various number (and number-like) systems related to the solution of various equations. The concept of a *group*, for example, was singled out by Évariste Galois (1811-1832) as an important algebraic structure related to the problem of finding all complex solutions of a general polynomial equation. Two other important algebraic structures — *ideals* and *rings* — emerged later in that century from the problem of finding all integer solutions of various equations in number theory. In their efforts to solve these equations, nineteenth-century number theorists were led to introduce generalizations of the seemingly simple and quite ancient concept of an integer. In this project, we examine ideas from algebraic number theory that eventually led to the new algebraic concepts of an 'ideal' and a 'ring' in the work of German mathematician Richard Dedekind (1831-1916).

A native of Brunswick (Braunschweig) in Germany, Dedekind spent most of his life in his hometown, first as a youth and student, and later as a professor at the Brunswick Polytechnikum. In 1850, he entered the University of Göttingen and attended his first course with the celebrated mathematician Carl Friedrich Gauss (1777-1855); he completed his doctorate under Gauss' supervision just two years later. Dedekind remained at Göttingen to complete his *habilitation* degree in order to qualify as a university teacher, completing that degree in 1852. He then taught as an instructor at the University of Göttingen until 1858, when he accepted a teaching position at the Polytechnikum in Zürich. Dedekind remained in Zürich until his return to

*Department of Mathematics and Physics; Colorado State University-Pueblo; Pueblo, CO 81001 - 4901; janet.barnett@csupueblo.edu.

Brunswick in 1862. A lifetime bachelor, he lived out the remainder of his days in Brunswick with his sister Julia, a novelist, until her death in 1914. Following his retirement from the Brunswick Technische Hochschule (a university with an engineering focus) in 1894, he continued publishing and occasionally teaching. By the time of his own death in 1916, he was already something of a legend among the next generation of mathematicians.[1] Today, Dedekind is widely recognized for his contributions to algebraic number theory, the foundations of the real numbers, the early development of set theory, and abstract algebra, especially the theory of ideals.

While teaching at Göttingen, Dedekind attended courses taught by two other important nineteenth century mathematicians, Peter Gustav Lejeune Dirichlet (1805-1855) and Bernhard Riemann (1826-1866). Later in his life, he also became a close associate and friend of Georg Cantor (1845-1918), the creator of set theory, whom he met while both were on holiday in the Black Forest in 1874. The work of these three men, along with that of Gauss, had a significant influence on Dedekind's understanding of and approach to mathematics. In its turn, Dedekind's unique approach to mathematics was a major influence on and inspiration for subsequent generations. The highly influential algebraist Emmy Noether (1882-1935), for instance, is reported to have frequently told her own students during discussions of her own theory of ideals that "Alles steht schon bei Dedekind" ("Everything is already in Dedekind").

A key feature of Dedekind's approach was the formulation of a new conceptual framework for studying problems that were previously treated algorithmically. Dedekind himself described his interest in solving problems through the introduction of new concepts as follows [Dedekind, 1888, p. 16]:

> The greatest and most fruitful progress in mathematics and other sciences is through the creation and introduction of new concepts; those to which we are impelled by the frequent recurrence of compound phenomena which are only understood with great difficulty in the older view.

Notice here Dedekind's emphasis on *abstraction*: the creation of new concepts through the identification of the common properties that frequently recur in a collection of related phenomena. Another distinguishing characteristic of Dedekind's work was his insistence on formulating concepts in terms that did not depend on their notational representation, so as to obtain the greatest *generality* possible.

[1] In *Men of Mathematics*, E. T. Bell tells the following amusing anecdote [Bell, 1937, p. 519]:

> [Dedekind] lived so long that although some of his works ... had been familiar to all students of analysis for a generation before his death, he himself had become almost a legend and many classed him with the shadowy dead. Twelve years before his death, Teubner's *Calendar for Mathematicians* listed Dedekind as having died on September 4, 1899, much to Dedekind's amusement. The day, September 4, might possibly prove to be correct, he wrote to the editor, but the year certainly was wrong. "According to my own memorandum I passed this day in perfect health and enjoyed a very stimulating conversation on 'system and theory' with my luncheon guest and honored friend Georg Cantor of Halle."

Dedekind's quest for abstraction and generality, together with his careful methodology, frequently required long periods of study and gestation before he felt satisfied with his creations. Between 1871 and 1894, for example, he published four different versions of his theory of ideals[2], none of which was simply a revision of an earlier paper. Instead, each of these four publications described a new version of the theory of ideals in which Dedekind reformulated the underlying concepts in clearer and more abstract terms.[3] Each of the four also went through repeated early drafts in Dedekind's working notebook (or *Nachlass*), as was the case with all his publications. Both the brilliant mathematical insights resulting from these patient years of working (and re-working) his ideas, and the precision and clarity with which he expressed those ideas, have justifiably earned Dedekind renown as one of the most influential mathematicians of the nineteenth century.

In this project, we will encounter Dedekind's brilliance first hand through excerpts from his 1877 version of this theory of ideals, *Theory of Algebraic Integers* [Dedekind, 1966]. Section 2 begins with Dedekind's description of the number-theoretic properties of two sets of numbers: the set of integers, denoted $\mathbb{Z}$, and the set of Gaussian integers, denoted $\mathbb{Z}[i]$. In that section, we will begin to explore the basic properties of Gaussian integer divisibility, and see how they mirror the familiar properties that hold in $\mathbb{Z}$. In Section 3, we continue to explore those parallels by extending the notion of a prime number to the set of Gaussian integers, and consider a connection between Gaussian primes from the set $\mathbb{Z}[i]$ and a useful number-theoretic relationship (called the Sum of Two Squares Theorem) which holds in the set $\mathbb{Z}$. In Section 4, we then delve deeper into the number-theoretic properties satisfied by the Gaussian primes, before encountering, in Section 5, a new integer system in which some of these properties break down. The mathematical after-effects of this 'break down' will then be briefly described in the concluding Section 6.

2 The Gaussian Integers

In this section, we examine Dedekind's description of the motivating idea behind the theory of ideals through excerpts from Chapter 2 of his monograph [Dedekind, 1966]. We begin with an excerpt in which Dedekind reminded his readers of some basic integer properties. Notice that Dedekind used the expression 'rational integer' here, where we would typically just say 'integer.' Because he did so for a very good reason (which will become clear as we read later excerpts), we adopt Dedekind's terminology throughout this project. We do, however, denote the *set* of all rational integers by $\mathbb{Z}$, whereas Dedekind himself did not use any special notation for this set.[4]

---

[2] Three of Dedekind's four publications on ideals appeared (in 1871, 1879, and 1894) as appendices to the second, third, and fourth editions of Dirichlet's *Vorlesungen über Zahlentheorie* (*Lectures on Number Theory*), a text that Dedekind edited based on lectures that he himself attended. The third version of Dedekind's theory of ideals first appeared in French as a series of articles in 1876-1877, and was later published as an independent monograph in 1877. The excerpts we will read in this project are taken from John Stillwell's 1966 English translation of that monograph [Dedekind, 1966].

[3] For more details about Dedekind's work on ideal theory, see [Edwards, 1980] or the preface to [Dedekind, 1966].

[4] The now-standard notation $\mathbb{Z}$ for the set of integers comes from the German word *Zahlen*, which means 'number.'

§ 5. The rational integers[5]

The theory of numbers is at first concerned exclusively with the system of rational integers $0, \pm 1, \pm 2, \pm 3, \ldots$, and it will be worthwhile to recall in a few words the important laws that govern this domain.[6] Above all, it should be recalled that these numbers are closed under addition, subtraction and multiplication, that is, the sum, difference and products of any two members in this domain also belong to the domain. The theory of *divisibility* considers the combination of numbers under multiplication. The number a is said to be divisible by the number b when $a = bc$, where c is also a [rational] integer. The number 0 is divisible by any number; the two units ± 1 divide all numbers, and they are the only numbers that enjoy this property. If a is divisible by b, then $\pm a$ will also be divisible by $\pm b$, and consequently we can restrict ourselves to the consideration of positive numbers. Each positive number, different from unity, is either a *prime* number, that is, a number divisible only by itself and unity, or else a *composite* number. In the latter case we can always express it as a product of prime numbers and — which is the most important thing — in only one way. That is, the system of prime numbers occurring as factors in this product is completely determined by giving the number of times a designated prime number occurs as factor. This property depends essentially on the theorem that a prime divides a product of two factors only when it divides one of the factors.

The simplest way to prove these fundamental propositions of number theory is based on the algorithm taught by Euclid, which serves to find the greatest common divisor of two numbers.[7] This procedure as we know, is based on repeated application of the theorem that, for a positive number m, any number z can be expressed in the form $qm + r$, where q and r are also integers and r is [non-negative and] *less* than m. It is for this reason that the procedure always halts after a finite number of divisions.[8]

---

[5] To set them apart from the project narrative, all original source excerpts are set in sans serif font and bracketed by the following symbol at their beginning and end: ∞∞∞∞∞∞∞∞∞∞∞∞∞

[6] Note that Dedekind used the word 'domain' to refer to the system of rational integers together with its arithmetic operations; there is no connection here to the way we use the word 'domain' when talking about functions. However, the term 'integer domain' is still used in abstract algebra today to describe structures that have algebraic properties analogous to those satisfied by the set of rational integers.

[7] Dedekind's footnote: See, for example, the *Vorlesungen über Zahlentheorie* of Dirichlet.

[8] As a reminder of how this process works, consider the following example in which we determine $\gcd(1386, 13090)$:

- Divide 13090 by 1386 to obtain: $13090 = 9(1386) + 616$ $\quad (m_1 = 1386,\ q_1 = 9,\ r_1 = 616)$
- Divide 1386 by 616 to obtain: $1386 = 2(616) + 154$ $\quad (m_2 = 616,\ q_2 = 2,\ r_2 = 154)$
- Divide 616 by 154 to obtain: $616 = 4(154)$ $\quad (m_3 = 154,\ q_3 = 4,\ r_3 = 0)$

Since the last non-zero remainder is 154, we conclude that $\gcd(1386, 13090) = 154$.

Task 1 This task examines some of the terminology used by Dedekind in the preceding excerpt.

(a) What did Dedekind mean by the term 'unit'? How many units are there in $\mathbb{Z}$?

(b) What did Dedekind mean by the term 'unity'? What special properties are satisfied only by the unity? (Name at least two such properties.)

(c) Notice that Dedekind explicitly excluded unity from the set of prime numbers. In fact, this exclusion dates back to Euclid's work, and remains in place today. Why do you think mathematicians do not consider unity to be a prime number? Is unity a composite number? Why or why not?

As Dedekind noted, the ideas in this excerpt were well known at least since the time of Euclid (born c. 300 BCE). Notice that Dedekind identifed (at the end of the first paragraph) two theorems as being especially important:

- *Unique Factorization Property*[9] Every (positive) rational integer has a unique factorization as a product of primes (up to the order of the factors).
- *Prime Divisibility Property*[10] A (rational) prime number divides a product of two rational integer factors only if it divides one of the two factors.

Task 2 This task examines Dedekind's description of the two theorems stated above.

Go back to read what Dedekind said about these two theorems towards the end of the first paragraph of the preceding excerpt. Does his statements of these theorems differ in some way from the statements of each given above? If so, in what way(s)?

What did Dedekind say is "the most important thing" when describing the first of these theorems? Explain why you think Dedekind considered this to be especially important.

Also summarize what Dedekind said about how these two theorems are related.
In particular, which of the two theorems depends on the other according to Dedekind?

Dedekind's specific motivation for singling out these two important theorems in his paper was due to their connection to nineteenth-century efforts to determine integer solutions of certain number-theoretic equations. A famous example is the equation in Fermat's Last Theorem, which asserts that $x^n + y^n = z^n$ has no non-trivial[11] integer solutions for $n \geq 3$. To their dismay, mathematicians found that certain approaches to proving this theorem for larger values of n that initially seemed quite promising were ultimately blocked by technical difficulties related to the

[9] The Unique Factorization Property is also often called the *Fundamental Theorem of Arithmetic*.

[10] The Prime Divisibility Property is also often called *Euclid's Lemma*.

[11] *Trivial* integer solutions of the equation $x^n + y^n = z^n$ are those in which the value of at least one variables is zero, such as $(-1)^3 + (1)^3 = 0^3$, or $x^n + 0^n = x^n$ for any $x \in \mathbb{Z}$ and any $n \in \mathbb{N}$.

Unique Factorization and Prime Divisibility Properties.[12] The work that we are reading in this project grew out of Dedekind's effort to remove those technical obstacles.

Another nineteenth century number theory problem related to these two theorems involved 'polynomial' congruence[13] equations of the form $x^m \equiv p \pmod{q}$, where p and q are odd primes and $x, m \in \mathbb{Z}^+$. An especially famous result of this type is the *quadratic reciprocity law* which describes a relation between the solvabilty of the equations $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$ for two different odd primes p, q. This difficult and beautiful result was first proven by Gauss in his important 1801 treatise on number theory, *Disquisitiones Arithmeticae*.[14] Gauss also looked for reciprocity laws for higher powers, eventually formulating a law for the 'biquadratic' case $[x^4 \equiv p \pmod{q}]$ by introducing a new set of 'integers.' These 'complex integers', also known as the 'Gaussian integers,' were described in our next excerpt from Dedekind.

§ 6. The complex integers of Gauss

The first and greatest step in the generalisation of these notions was made by Gauss, in his second memoir on biquadratic residues, when he transported them to the domain of complex integers $x + yi$, where x and y are any rational integers and i is $\sqrt{-1}$, that is, a root of the irreducible quadratic equation $i^2 + 1 = 0$. The numbers in this domain[15] are closed under addition, subtraction and multiplication, and consequently we can define divisibility for these numbers in the same way as for rational numbers.

Using today's notation, we can denote and define the set of Gaussian complex integers by $\mathbb{Z}[i] = \{x+yi \mid x, y \in \mathbb{Z}\}$. Notice that both x and y must be rational integers here! Take a moment to verify Dedekind's assertion that the set $\mathbb{Z}[i]$ is indeed closed under addition, subtraction and multiplication. Then complete the following task to make sure you see how divisibility is defined in this number system.

[12] For additional details about the connection of these theorems to Fermat's Last Theorem, see [Kleiner, 2009].

[13] Recall that for $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, we say that a, b are *equivalent modulo* m if and only if $m \mid (a - b)$. This implies that a and b have the same remainder when divided by m, and can thus be treated as equivalent as far as division by m is concerned. The theory of congruences was first systematically developed by Gauss, who also introduced the notation '$a \equiv b \pmod{m}$.'

[14] Gauss stated the quadratic reciprocity law for primes p, q as follows:

> If $q \equiv 1 \pmod{4}$, then $x^2 \equiv p \pmod{q}$ is solvable if and only if $x^2 \equiv q \pmod{p}$ is solvable.
> If $q \equiv 3 \pmod{4}$, then $x^2 \equiv p \pmod{q}$ is solvable if and only if $x^2 \equiv -q \pmod{p}$ is solvable.

[15] Recall from footnote number 6 that Dedekind used the word 'domain' to refer to a system of numbers under certain arithmetic operations.

Task 3 This task looks at the divisibility relationship in $\mathbb{Z}[i]$. As in the set of rational integers, given $z, w \in \mathbb{Z}[i]$, we say that z is divisible by w (or that w divides z) if and only if there is some Gaussian integer $q \in \mathbb{Z}[i]$ such that $z = qw$.

(a) Let $z = 9 + 8i$ and $w = 2 + 5i$.
Show z is divisible by w by verifying that the quotient $\frac{z}{w}$ is a Gaussian integer.
(To compute $\frac{z}{w}$, multiply by $\frac{\overline{w}}{\overline{w}}$, where $\overline{w} = 2 - 5i$ is called the *conjugate of* w.)

(b) For each of the following pairs, determine whether z is divisible by w in $\mathbb{Z}[i]$.

(i) $z = 9 - 3i$, $w = 1 + 4i$ (ii) $z = 5 + 14i$, $w = 3 - 2i$

Let's now continue to read Dedekind's description of the 'complex integers of Gauss', which we will refer to in this project more simply as the 'Gaussian integers.'

One can establish very simply, as Dirichlet showed in a very elegant manner,[16] that the general propositions on the composition of numbers from primes continue to hold in this new domain, as a result of the following remark. If we define the *norm* $N(w)$ of a number $w = u + vi$, where u and v are any rational numbers, to be the product $u^2 + v^2$ of the two conjugate numbers $u + vi$ and $u - vi$, then the norm of a product will be equal to the product of the norms of the factors, and it is also clear that for any given w we can choose a complex *integer* q such that $N(w - q) \leq 1/2$. If we now let z and m be any Gaussian integers, with m nonzero, it follows by taking $w = z/m$ that we can put $z = qm + r$ where q and r are Gaussian integers such that $N(r) < N(m)$. We can then find a greatest common divisor of any two Gaussian integers by a finite number of divisions, exactly as for rational numbers, and the proofs of the general laws of divisibility for rational integers can be applied word for word in the domain of Gaussian integers.

Notice that without giving any actual proofs, Dedekind has described the *mathematical tool* — namely, the existence of a *norm* for Gaussian integers — which Dirichlet used to elegantly show that "the general propositions on the composition of numbers from primes continue to hold in this new domain." The omission of the proof details was intentional on Dedekind's part, since his own primary focus was not the Gaussian integers per se. Since our motivations for reading Dedekind's monograph is to see how to generalize and transfer proofs of number-theoretic propositions about the rational integers over to the Gaussian integers, let's pause in our reading of Dedekind to see how the norm of a complex integer is computed. Recalling Dedekind's earlier assertion (on page 4 above) that "The simplest way to prove these fundamental propositions of number theory [in the rational integers] is based on the algorithm taught by Euclid, which serves to find the greatest common divisor of two numbers," let's also examine how that norm is used to find a greatest common divisor (gcd) of two Gaussian integers via an adaptation of Euclid's gcd algorithm for the rational integers.

[16] Dedekind's footnote: *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes* (Crelle's Journal, 24).

Task 4 This task explores the geometric meaning of the definition of the *norm* of a complex number $w = u + iv$, where $N(u + iv) = (u + iv)(u - iv) = u^2 + v^2$ for all $u, v \in \mathbb{R}$.

(a) Begin by plotting the following complex numbers in the imaginary plane.
Use the standard convention of plotting the real component on the horizontal axis and the imaginary component on the vertical axis.

(i) $w = 3 + 4i$ (ii) $x = -4 + 3i$ (iii) $x = -3 + 4i$
(iv) $x = 5 + 2i$ (v) $x = -8 + 6i$ (vi) $x = -2.7 + 4.6i$

(b) Now compute the norm of each of the complex numbers in part (a).
Describe how the norm of each number relates to their geometric placement.

(c) Geometrically describe the set of complex numbers q for which $N(q) = 1$.

Task 5 This task examines computations and a proof related to Dedekind's claims concerning the norm of a complex number in the previous excerpt.

(a) Show that the norm of the product of two complex numbers w, q is the product of their norms; that is, for all $w, q \in \mathbb{C}$, $N(wq) = N(w)N(q)$.

(b) For $w = 4.7 + 3.2i$, show that the complex *integer* $q = 5 + 3i$ satisfies $N(w - q) \leq 1/2$.

(c) For $w = -1.2 + 2.56i$, find a complex *integer* q such that $N(w - q) \leq 1/2$.
Now find a *second* complex integer q_2 that also satisfies $N(w - q_2) \leq 1/2$.
Do you think there will be other complex integers that are also $\leq 1/2$ 'close' to w, in the same way that q and q_2 are? Why or why not?

(d) Given an arbitrary $w = u + vi \in \mathbb{C}$, describe in general how to find a complex *integer* q with $N(w - q) \leq 1/2$. Describe what this means geometrically.
Also explain why there could be more than one such complex integer.
In what case, if any, will there be a unique complex integer q with this property?

Let's now look at an example of how the Euclidean algorithm for computing the gcd of two natural numbers can be adapted to find the greatest common divisor of two complex integers. Take particular note of how the norm is used in this proof as a tool for determining that the remainder is indeed 'smaller than' the divisor at each step.

Example In this example, we let $z = -8 + 51i$ and $m = -8 - i$ and find $\gcd(z, m)$.

- *Step 1* Since $N(z) = 2665 > 65 = N(m)$, we begin by dividing z by m; that is, we begin by finding complex *integers* $q_1, r_1 \in Z[i]$ such that $z = q_1 m + r_1$ and $N(r_1) < N(m)$. To estimate the quotient q_1, we use the complex conjugate of m in order to divide z by m:

$$\frac{z}{m} = \frac{-8 + 51i}{-8 - i} = \frac{-8 + 51i}{-8 - i} \cdot \frac{-8 + i}{-8 + i} = \frac{13 - 416i}{65} = \frac{13}{65} - \frac{416}{65}i$$

  Rounding the real and complex components of this quotient separately to the nearest rational *integers*, we obtain the *complex integer* $q_1 = 0 - 6i$.

  To obtain the corresponding remainder, we solve $z = q_1 m + r_1$ for r_1 to obtain:

$$r_1 = z - q_1 m = (-8 + 51i) - (-6i)(-8 - i) = -2 + 3i$$

  This concludes the first step of the process, giving us $\boxed{z = \underbrace{(-6i)}_{q_1} m + \underbrace{(-2 + 3i)}_{r_1}.}$

  Note that $N(r_1) = 13 < 65 = N(m)$.

- *Step 2* We next repeat this process, but now we divide the previous divisor m by the previous remainder r_1 in order to find complex *integers* $q_2, r_2 \in Z[i]$ with $m = q_2 r_1 + r_2$ and $N(r_2) < N(r_1)$:

$$\frac{m}{r_1} = \frac{-8 - i}{-2 + 3i} = \frac{-8 - i}{-2 + 3i} \cdot \frac{-2 - 3i}{-2 - 3i} = \frac{13 + 26i}{13} = 1 + 2i$$

  Since this quotient is already a complex integer, there is no need to round in this step; we simply set $q_2 = 1 + 2i$ and $r_2 = 0$. Note that $N(r_2) = 0 < 13 = N(r_1)$.

Having arrived at a zero remainder,[17] we now conclude that the sought-after gcd is the final non-zero remainder r_1; that is, $\boxed{\gcd(z, m) = -2 + 3i}$.

To verify that $-2 + 3i$ is a common divisor in this example, we can 'unravel' the results of the two steps to obtain the following:

$$\begin{aligned} m &= \underbrace{(1 + 2i)}_{q_2}\underbrace{\mathbf{(-2+3i)}}_{r_1} \\ z &= \underbrace{(-6i)}_{q_1}\underbrace{(1 + 2i)\mathbf{(-2+3i)}}_{m} + \underbrace{\mathbf{(-2+3i)}}_{r_1} \\ &= [\,(-6i)(1 + 2i) + 1\,]\mathbf{(-2+3i)} \\ &= (13 - 6i)\mathbf{(-2+3i)} \end{aligned}$$

This verifies that $-2 + 3i$ is a common divisor of m and z. As for the sense in which it is a *greatest* common divisor, here again the norm provides just the tool we need to talk about which

[17] Had we obtained a non-zero remainder in step 2, we would have repeated the process until we reached a stage with a zero remainder. Note that we can be confident that this process will halt since the norms of these remainders form a decreasing sequence of non-negative rational integers.

of two common divisors is the 'greater' of the two. We will say more about this idea later in this project. First, let's get some more basic practice with the Euclidean algorithm in $\mathbb{Z}[i]$.

Task 6 This task provides additional examples of the Euclidean algorithm for finding greatest common divisors, adapted to the Gaussian integers $\mathbb{Z}[i]$.

(a) Let $z = 12 - 23i$ and $m = 7 - 5i$. Complete just the first step of the Euclidean gcd algorithm by finding $q, r \in \mathbb{Z}[i]$ such that $z = qm + r$, where $N(r) < N(m)$.

(b) Use the Euclidean gcd algorithm to show that $d = -i$ is a greatest common divisor of $z = 9 + 5i$ and $m = 2 - 3i$.

(c) Use this algorithm to find a greatest common divisor for each of the following pairs.

(i) $z = 11 + 17i$ and $m = 5 + 3i$ (ii) $z = 16 - 120i$ and $m = 52 + 68i$

(d) Now that you have completed several examples of the Euclidean gcd algorithm adapted to the set $\mathbb{Z}[i]$, compare and contrast it with the basic algorithm as it applies to the set $\mathbb{Z}$. Identify at least one similarity and at least one difference.

Looking back at the example above the last task, notice that we could also have written these factorizations as follows:

$$\begin{aligned} m &= (1+2i)(-2+3i) \\ &= (1)[(1+2i)(-2+3i)] \\ &= (-i^2)[(1+2i)(-2+3i)] \\ &= \underbrace{(2-i)}_{-i(1+2i)}\ \underbrace{(-3-2i)}_{i(-2+3i)} \end{aligned} \qquad \begin{aligned} z &= (13-6i)(-2+3i) \\ &= (1)[(13-6i)(-2+3i)] \\ &= (-i^2)[(13-6i)(-2+3i)] \\ &= \underbrace{(-6-13i)}_{-i(13-6i)}\ \underbrace{(-3-2i)}_{i(-2+3i)} \end{aligned}$$

Since $N(-3-2i) = 13 = N(-2+3i)$, notice also that neither $-3-2i$ or $-2+3i$ is 'bigger' than the other when using their norms to compare them. In other words, we could just as well say that $\gcd(z, m) = -3 - 2i$. In fact, since $N(\pm(-2+3i)) = N(\pm i(-2+3i))$, there are four different complex integers that can be considered to be a gcd of z and m in this example!

The fact that each non-zero pair of Gaussian integers has four greatest common divisors may seem disquieting at first ... until we remember that something similar occurs with rational integers. For instance, in the positive integers, we say that $\gcd(12, 15) = 3$, but since $12 = (-4)(-3)$ and $15 = (-5)(-3)$, it would make sense to also say that -3 is a 'greatest common divisor' of 12 and 15. Of course, we typically avoid this issue with rational integers by limiting our attention to just positive integer factors, as Dedekind pointed out in his comments on the rational integers (on page 4 above). The situation with Gaussian integers is more complicated simply because, once we know that $d = \gcd(a, b)$, there is no straightforward way to decide which of the four numbers $\pm d$, $\pm id$ should have 'priority' as *the* gcd.[18] This is because of a special role that the four numbers 1, -1, i, $-i$ play within the set of Gaussian integers. In the next section

[18] In our example above, these four numbers are $d = -2 + 3i$, $-d = 2 - 3i$, $id = -3 - 2i$ and $-id = 3 + 2i$

of this project, we will see how Dedekind incorporated the special nature of these four Gaussian integers into his definition of what it means for a complex integer to be 'prime.' First, we close this section with two tasks that consider the special nature of these four Gaussian integers a bit further, and examine an aspect of quotients and remainders in the set of Gaussian integers that is even more unusual than what occurs with greatest common divisors.

Task 7 This task considers the special properties of the four Gaussian integers ± 1, $\pm i$.

Other than the connection that we have seen in the examples we have considered of greatest common divisors in $\mathbb{Z}[i]$, what do you think is particularly special about ± 1, $\pm i$? Identify at least two mathematical properties that are satisfied only by these four Gaussian integers.

Task 8 This task illustrates that the quotient and the remainder of two given Gaussian integers need not be uniquely determined, even if multiples of ± 1, $\pm i$ are considered equivalent.

Let $z = -51 + 8i$ and $m = 6 + 7i$ throughout this task.

(a) Verify that $-51 + 8i = (-3 + 5i)(6 + 7i) + (2 - i)$, and that $N(2 - i) < N(6 + 7i)$. Dividing z by m, what values does this give us for the quotient and remainder?

(b) Verify that $-51+8i = (-3+4i)(6+7i)+(-5+5i)$, and that $N(-5+5i) < N(6+7i)$. Dividing z by m, what values does this give us for the quotient and remainder?

(c) Now go back to the arithmetic statements given in part (a):

$$-51 + 8i = (-3 + 5i)(6 + 7i) + (2 - i) \quad , \quad N(2 - i) < N(6 + 7i)$$

Treat this as the first step in the Euclidean algorithm for finding a gcd of z and m, and continue with that algorithm to find a greatest common divisor of z and m.

(d) Also go back to the arithmetic statements that you verified in part (b):

$$-51 + 8i = (-3 + 4i)(6 + 7i) + (-5 + 5i) \quad , \quad N(-5 + 5i) < N(6 + 7i)$$

Treat this as the first step in the Euclidean algorithm for finding a gcd of z and m, and continue that algorithm to find a greatest common divisor of z and m.

(e) Note that the quotients from part (a) and part (b) respectively can *not* be obtained from each other via multiplication by any of the special Gaussian integers ± 1, $\pm i$. Note also that this is also the case for the remainders from part (a) and part (b). Verify that, in contrast, the greatest common divisors of z and m that you obtained in parts (c) and (d) respectively *can* be obtained from each other via multiplication by one of the special Gaussian integers ± 1, $\pm i$. Also state the values of the other two greatest common divisors of z and m — but without using the Euclidean algorithm!

(f) Suppose we consider two Gaussian integers x, y to be equivalent provided $x = \pm y$ or $x = \pm iy$. Given $z, m \in \mathbb{Z}[i]$ with $N(m) \leq N(z)$, how many distinct non-equivalent quotients and remainder do you think are possible when z is divided by m? Explain why you believe this is the case.

3 Gaussian Primes, and the Sum of Two Squares

At the end of the previous section, we saw that the four numbers ± 1, $\pm i$ play a special role within the set of Gaussian integers. Namely, if d is any particular greatest common divisor of two given Gaussian integers, then the four numbers $\pm d$, $\pm id$ are also greatest common divisors of those two Gaussian integers. In our next excerpt from Dedekind, we will see how he incorporated another special characteristic of these Gaussian integers into a definition of what it means for a Gaussian integer to be 'prime.'

There are four units ± 1, $\pm i$, that is, four numbers which divide all numbers, and whose norm is consequently 1. Every other nonzero number is either a composite number, so called when it is the product of two factors, neither of which is a unit, or else it is a prime, and such a number cannot divide a product unless it divides at least one of the factors. Every composite number can be expressed uniquely as a product of prime numbers, provided of course the four associated primes $\pm q$, $\pm qi$ are regarded as representatives of the same prime number q.

Task 9 This task examines the definitions given by Dedekind in the previous excerpt.

(a) Based on Dedekind's description of *units* in the preceding excerpt, complete the following to give a general definition that would apply in an arbitrary number domain.

Let D be any domain[19], and $u \in D$.
We say u is a unit in D if and only if _____.

(b) Use your definition from part (a) to verify that:

(i) ± 1 are units in the domain $\mathbb{Z}$; and

(ii) ± 1 and $\pm i$ are units in the domain $\mathbb{Z}[i]$.

(c) After describing a defining characteristic for units, Dedekind asserted that "every other nonzero number" in $\mathbb{Z}[i]$ falls into one of two categories: composite numbers and prime numbers. Explain why Dedekind considered units to be neither composite nor prime.

(d) Complete the following to give Dedekind's definition of a composite number for the domain $\mathbb{Z}[i]$, making sure that your definition excludes units.

Given $z \in \mathbb{Z}[i]$, we say z is a composite number if and only if
_____.

(e) Now, carefully negate your definition of composite number to provide a formal definition of a Gaussian prime, again making sure your definition excludes units.

Given $z \in \mathbb{Z}[i]$, we say z is a prime number if and only if
_____.

[19] We are using the term 'domain' here in Dedekind's sense of a system of numbers together with certain arithmetic operations.

Task 10 This task examines Dedekind's claims about Gaussian primes in the preceding excerpt.

(a) In addition to describing what the terms 'unit,' 'composite number' and 'prime number' mean, Dedekind stated two theorems about Gaussian primes in the preceding excerpt. Identify the complete statements of these two theorems in that excerpt, and label each with the name used in this project for the corresponding theorems about rational primes.

(b) In what way(s), if any, is Dedekind's statement of these two theorems for the Gaussian integers different from how we have stated them for the rational integers?

Task 11 In this task, you will prove Dedekind's claim that ± 1 and $\pm i$ are the only units in $\mathbb{Z}[i]$.

(a) Begin by explaining why $N(\omega) \in \mathbb{Z}^+$ for every non-zero $\omega \in \mathbb{Z}[i]$.

(b) Recall Dedekind's description of a 'unit', stated in the following formal definition:

> **Definition**
> Given $u \in \mathbb{Z}[i]$, we say u is a unit if and only if every $z \in \mathbb{Z}$ is divisible by u.

Use this definition, the result of part (a), and the fact that "the norm of a product is the product of the norms" to complete the following proof.

> Assume $u \in \mathbb{Z}[i]$ is a unit; that is, assume u divides every complex integer.
> In particular, u must be a divisor of 1. Use this to first show that $N(u) = 1$.
> Then use the definition of norm to show that $u = \pm 1$ or $u = \pm i$.
>
> *Note: If $u = \pm 1$ or $u = \pm i$, then clearly $N(u) = 1$.*
> *The last part of this task asks is to prove the converse of this fact!*

Look back at your answers to Task 9(e), and notice how Dedekind's definition of a composite number in the set of Gaussian integers mirrors the definition of a rational composite as a rational integer with a non-trivial factorization in $\mathbb{Z}$. Consequently, Dedekind's (implied) definition of the Gaussian primes gives us the set of non-zero non-unit Gaussian integers that have only trivial factorizations. In other words, to show that a given non-zero non-unit Gaussian integer is a prime, we need to verify that it can not be factored as the product of any two non-unit Gaussian integers. *(Make sure you see why the phrase 'non-unit' is needed here!)* Intriguingly, numbers that are prime in $\mathbb{Z}$ may not be prime in $\mathbb{Z}[i]$. For example, it is possible to factor the number 2 within $\mathbb{Z}[i]$ as $2 = (1+i)(1-i)$; since neither $1+i$ nor $1-i$ is a unit in $\mathbb{Z}[i]$, the rational prime number 2 thus does have a non-trivial factorization in the Gaussian integers. In other words, 2 is *not* a prime number in the Gaussian integers!

On the other hand, the number 7 *is* a prime in $\mathbb{Z}[i]$. To see this, suppose that we factor 7 in $\mathbb{Z}[i]$ to obtain $7 = wq$ with $w, q \in \mathbb{Z}[i]$. Then $N(7) = N(wq) = N(w)N(q)$, where we also know that $N(7+0i) = 7^2 + 0^2 = 49$. This gives us $N(w)N(q) = 49$, where $N(w)$ and $N(q)$ are positive integers. If we now assume that both $N(w) \neq 1$ and $N(q) \neq 1$ (so that neither w or q is unit), it

would have to be the case that $N(w) = N(q) = 7$. Setting $w = u + iv$ with $u, v \in \mathbb{Z}$, this would imply that $7 = N(w) = u^2 + v^2$. But a moment's reflection shows that the equation $7 = u^2 + v^2$ has *no* integer solutions! In other words, the only way to obtain $7 = wq$ with $w, q \in \mathbb{Z}[i]$ is to have either $N(w) = 1$ or $N(q) = 1$. This means that 7 is the product of two factors in $\mathbb{Z}[i]$ only if one of the factors (either w or q) is a unit. Since 7 has no non-trivial factorization in the set of Gaussian integers, we conclude that 7 is a prime number in that set. We can thus refer to 7 as both a *rational prime* and a *Gaussian prime*.

Perhaps unsurprisingly, it turns out that there are also 'new' primes in the Gaussian integers which do not even exist in the the set of rational integers. For instance, the Gaussian integers which we used above to factor 2 in $\mathbb{Z}[i]$ — that is, $1 \pm i$ — can be shown to have no non-trivial factorization in $\mathbb{Z}[i]$. This is one of the examples considered in the next task.

Task 12 This task provides additional examples of primes and composites in the Gaussian integers.

(a) Show that each of the following is NOT a Gaussian prime.

(i) 5 (*Hint:* $5 = 1 + 4$) (ii) 13 (iii) $6 + 7i$

(b) Show that each of the following IS a Gaussian prime.

(i) 3 (ii) $1 + i$ (iii) $10 + 9i$

(c) Determine which of the following is a Gaussian prime.
Be sure to justify your answers with an appropriate proof or factorization.

(i) 17 (ii) $1 - 4i$ (iii) $3 + 4i$

Task 13 This task considers the question of which Gaussian integers are Gaussian primes.

The following table shows the Gaussian integers that we know are or are not Gaussian primes thus far:

Gaussian Primes	Not Gaussian Primes
3	2
7	5
1+i	13
10+9i	6+7i

Add your answers from part (c) of the previous task to this table.

Then use the examples in this table to develop a conjecture for predicting whether a particular Gaussian integer $z = a + bi$ is a prime.

Test your conjecture with a few more examples.

Hint: It may be useful to look at the value of $N(z)$.

As you worked on the previous task, you may have noticed a pattern about which rational prime numbers are also Gaussian primes in the set of Gaussian integers. In the next excerpt, Dedekind gave a complete description of the set of Gaussian primes.

The set of all prime numbers q in the domain of Gaussian integers consists of:

1. All the rational prime numbers (taken positively) of the form $4n + 3$;
2. The number $1 + i$, dividing the rational prime $2 = (1 + i)(1 - i) = -i(1 + i)^2$;
3. The factors $a + bi$ and $a - bi$ of each rational prime p of the form $4n + 1$ with norm $a^2 + b^2 = p$.

The existence of the primes $a \pm bi$ just mentioned, which follows immediately from the celebrated theorem of Fermat on the equation $p = a^2 + b^2$, and which likewise implies that theorem, can now be derived without the help of the theorem, with marvellous ease. It is a splendid example of the extraordinary power of the principles we have reached through generalisation of the notion of integer.

The 'celebrated theorem of Fermat' mentioned in Dedekind's justification for the third class of Gaussian primes is a theorem in number theory known as the *Sum of Two Squares Theorem*:[20]

The Sum of Two Squares Theorem
An odd prime p is the sum of two squares if and only if p is of the form $4n + 1$.

Notice that Dedekind's interest in this number-theoretic result centered on how its connection to the Gaussian integers demonstrates the power of generalization. In later sections of this project, we will see how Dedekind continued to pursue this notion of 'generality' by looking at number systems of the form $\mathbb{Z}[\theta] = \{x + y\theta \mid x, y \in \mathbb{Z}\}$ for values of $\theta \neq i$. Before we leave the Gaussian integers to look at those other systems, we will take a closer look at what Dedekind had to say about prime factorization in $\mathbb{Z}[i]$ in the next section. But first, let's close this section with a few tasks related to the rational integer number-theoretic result stated in the Sum of Two Squares Theorem and its connection to Dedekind's description of Gaussian primes.

[20] The problem of determining whether an integer is the sum of two squares, and in how many ways, dates back to the ancient Greek mathematician Diophantus (c. third century). In a posthumously published note of 1634, the French mathematician Albert Girard (1595-1632) observed that every prime of the form $4n+1$ can be written as the sum of two squares. Pierre de Fermat (1601-1655) asserted this same claim (without proof) in a letter to Marin Mersenne (1588-1648) dated December 25, 1640, stating that "every prime of the form $4n+1$ is the hypotenuse of a right triangle in a single way." For this reason, the theorem is sometimes called *Fermat's Christmas Theorem*. Although Fermat claimed to have a proof in his correspondence with Mersenne and others, the first published proof was due to Leonhard Euler (1707-1783) in 1755. This history is further described in [Dickson, 2005].

Task 14 This task examines a proof of the Sum of Two Squares Theorem based on Dedekind's description of the Guassian primes.

Let's call the theorem that tells us which Gaussian integers are Gaussian primes (described in our last excerpt from Dedekind) the *Gaussian Primes Theorem*. According to Dedekind, this theorem both follows from and implies the Sum of Two Squares Theorem.

Prove the latter part of this claim, by assuming the Gaussian Primes Theorem holds, then deriving both directions of the Sum of Two Squares Theorem as follows.

(a) First assume $p \in \mathbb{Z}$ is an odd rational prime such that for some $a, b \in \mathbb{Z}^+$, $p = a^2 + b^2$. Use the definition of Gaussian prime to explain why p must also be a Gaussian prime. Then apply part 1 of the Gaussian Primes Theorem to conclude that $p \equiv 1 \pmod 4$.

(b) Now assume $p \in \mathbb{Z}$ is an odd rational prime such that $p \equiv 1 \pmod 4$. By the Gaussian Primes Theorem, we know that p is not a Gaussian prime. There thus exist $w, x \in \mathbb{Z}[i]$, neither of which is a unit, for which $p = wx$. Use this factorization together with facts about complex norms to prove that there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

Task 15 This task considers how to prove the Sum of Two Squares Theorem completely within $\mathbb{Z}$. As we saw in the previous task, it is straightforward to prove the Sum of Two Squares Theorem using the Gaussian Primes Theorem stated in our last excerpt from Dedekind. However, the Sum of Two Squares Theorem itself just talks about rational integers, and was proven by Euler well before either Gauss of Dedekind worked on the Gaussian integers. Complete the following direct proof for one direction of the Sum of Two Squares Theorem without making use of the Gaussian Primes Theorem.[21] Do this as follows:

> Assume $p \in \mathbb{Z}$ is an odd rational prime such that for some $a, b \in \mathbb{Z}^+$, $p = a^2 + b^2$.
>
> Use the fact that p is prime to prove that $p \equiv 1 \pmod 4$.

Task 16 This task examines several consequences of the Sum of Two Squares Theorem.

The Sum of Two Squares Theorem only tells use which rational *primes* can be written as a sum of two squares — but there are also rational composite numbers of this form. For example, $50 = 7^2 + 1^2$. The following identity is useful for finding sum-of-two-squares representations for certain composite numbers:

$$\text{For all } a, b, c, d \in \mathbb{Z}, \quad (a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2 \qquad (\star)$$

This says that if we start with two rational integers k, n, both of which can be written as a sum of two squares (say, $k = a^2 + b^2$ and $n = c^2 + d^2$), then their product kn can also be written as a sum of two squares.

[21] It is also possible to prove the second direction of the Sum of Two Squares Theorem independently of the Gaussian primes, by making use of the quadratic reciprocity law (stated in footnote 14). Although the quadratic reciprocity law is studied in many undergraduate courses on number theory, it is a fairly sophisticated number-theoretic tool which goes beyond the scope of this project.

Task 16 - continued

(a) Use the identity ($\star$) stated above to write each of the following as a sum of squares.
(i) $377 = 13 \cdot 29$ (ii) $1450 = 29 \cdot 50$ (iii) $18850 = 13 \cdot 29 \cdot 50$

(b) Recall that we earlier proved that $N(wq) = N(q)N(q)$ for all $w, q \in \mathbb{Z}[i]$.
Use this fact in order to prove the identity ($\star$).

Hint: Starting with arbitrary $a, b, c, d \in \mathbb{Z}$, it is possible to define several different Gaussian integers w and q with norms $a^2 + b^2$ and $c^2 + d^2$, respectively.

(c) Let $x \in \mathbb{N}$. Prove that if the prime factorization of x does not include any primes $p \equiv 3 \pmod 4$, then x can be written as a sum of two squares.

Task 17 This task explores another rational number-theoretic result related to the Sum of Two Squares Theorem.

In part (c) of the last task, you proved that any positive rational integer that has no prime factors that are equivalent to 3 modulo 4 can be written as a sum of squares. But notice that $637 = (14)^2 + (21)^2$ can also be written as the sum of squares ... even though the prime factorization of $637 = 7^2 \cdot 13$ includes the prime 7, where $7 \equiv 3 \pmod 4$.

Explore the conditions under which a composite number with primes $p \equiv 3 \pmod 4$ in its prime factorization can nevertheless be written as a sum of squares.

Be sure to organize any data you collect clearly, and use that data to write an explanation of why you believe your final conjecture is correct.

Task 18 This task examines a generalization of the Sum of Two Squares Theorem.

We know from the Sum of Two Squares Theorem that some rational prime numbers can *not* be written as the sum of two integer squares. The same is true when we look at the sum of *three* integer squares, even if one of the terms is allowed to be 0 (e.g., $5 = 0^2 + 1^2 + 2^2$).

(a) Collect some data about which rational prime numbers $p \in \mathbb{Z}$ can be written as the sum of three squares. Include primes that use '0^2' as one of the three possible terms in your 'can be done' list. Be sure to organize your data is some clear fashion.

(b) Use your data from part (a) to state a conjecture concerning the Sum of Three Squares problem; write your conjecture in the following form:

(i) If p is a rational prime that satisfies condition(s) _____, then p is a sum of three squares.

(ii) If p is a rational prime that satisfies condition(s) _____, then p is *not* a sum of three squares.

Your completed conjecture should cover all possible rational primes p.
Your data from part (a) should also provide clear support for your conjecture.[22]

[22] You do not need to prove your conjecture; in fact, a proof of part (i) is quite difficult! However, it could be useful to think about a proof of part (ii) to test your conjecture.

Somewhat surprisingly, it turns out that every positive rational *integer* — not just the primes! — can be written as the sum of *four* squares. The first published proof of the Sum of Four Squares Theorem was given in 1770 by the French mathematician J. L. Lagrange (1736-1813). Before then, Fermat claimed to have a proof (but did not write it down!), and Euler made substantial progress towards a proof, but was unable to complete it. Euler was able, however, to prove the following identity that allows us to rewrite a product of two four-square-sums as the sum of four four-square-sums:

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2)\\&\quad=(ax+by+cz+dw)^2+(ay-bx-cw+dz)^2+(az+bw-cx-dy)^2+(aw-bz+cy-dx)^2.\end{aligned}$$

Note the similarity of this four square identity to the identity ($\star$) which you proved in Task 16, using facts about the norms of complex integers. In much the same way that the two square identity is related to the set of complex integers, it is possible to derive Euler's four square identity by way of integers in the set of *quaternions*,[23] a non-commutative system of 'imaginary' numbers that were discovered nearly a century after Euler's own algebraic proof of his identity!

4 Gaussian Primes and Unique Factorization

Before we look at the notion of primes in other number systems, let's go back and re-read what Dedekind reported about the properties satisfied by Gaussian primes.

> There are four units ± 1, $\pm i$, that is, four numbers which divide all numbers, and whose norm is consequently 1. Every other nonzero number is either a composite number, so called when it is the product of two factors, neither of which is a unit, or else it is a prime, and such a number cannot divide a product unless it divides at least one of the factors. Every composite number can be expressed uniquely as a product of prime numbers, provided of course the four associated primes $\pm q$, $\pm qi$ are regarded as representatives of the same prime number q.

[23] Introduced by the Irish mathematician William Rowan Hamilton (1805-1865), *quarternions* are 'imaginary' numbers of the form $a+bi+cj+dk$ subject to certain non-commutative rules, such as $ij = k = -ji$. The problem that led Hamilton to the discovery of quarternions was the search for an algebraic system which would represent the three-dimensional space of physics, in a manner analogous to the interpretation of the algebra of complex numbers $a + bi$ as a representation of a two-dimensional plane. Although this geometrical interpretation of the complex numbers is now standard, it was discovered only in the early 1800s and was thus relatively new in Hamilton's time. After six years of unsuccessful work on the three-dimensional problem, Hamilton found a solution only by abandoning commutativity for multiplication. He also replaced 'triplets' by the 'four-dimensional' quaternion $a + bi + cj + dk$. By the end of the nineteenth century, physicists found a way to use just the 'vector part' $bi + cj + dk$ of a quaternion to represent three-dimensional space. Although vectors have replaced quarternions in physics, the vector cross product operation retains the non-commutativity of quarternion multiplication.

As we saw in the previous section, Dedekind's definition of a composite number implicitly defined a Gaussian prime as follows:

Definition
Given $p \in \mathbb{Z}[i]$ with $p \neq 0$. We say that p is a *Gaussian prime* if and only if:

1. p is not a unit; and
2. p has no non-trivial factorization; that is,
   if $w, q \in \mathbb{Z}[i]$ with $p = wq$, then either w is a unit or q is a unit.

Notice also the first property of Gaussian primes that Dedekind highlighted in this excerpt; namely that "such a number cannot divide a product unless it divides at least one of the factors." In other words, the Prime Divisibility Property which we stated above (on page 5) for the rational integers also holds in the Gaussian integers! Tasks 20 and 21 examine this amazing fact further. But first, it will be useful to generalize the important result from the set of rational primes which asserts that the greatest common divisor of any two given rational integers can be written as a linear combination of the given integers. Or, stating this more formally, we have the following:

Linear Combination Property of Rational Integer gcd's
For any $a, b \in \mathbb{Z}^+$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

Before proceeding to the next task, you may wish to look back at the proof of this property for rational integers given in a modern Number Theory textbook. To prove that this property transfers over to the Gaussian integers, we begin by adapting the definition of 'greatest common divisor' for rational integers to the set of Gaussian integers.

Definition
Given $a, b, g \in \mathbb{Z}[i]$ with $a, b \neq 0$.
We say that g is *a greatest common divisor* of a, b if and only if:

1. g is a common divisor of a and b; and
2. For all $d \in \mathbb{Z}[i]$, if $d|a$ and $d|b$, then $d|g$.

Task 19 This task proves that every greatest common divisor of two given Gaussian integers may be written as a linear combination of those two Gaussian integers.

(a) Begin by proving the following lemma:

> **Lemma** Given $a, b \in \mathbb{Z}[i]$.
> If $u, v, g \in \mathbb{Z}[i]$ are such that $g = au + bv$ and g has the least non-zero norm of all linear combinations of a and b, then g is a common divisor of a and b.
>
> *Note:* To say "g has the least non-zero norm of all linear combinations of a and b" means that for all $x, y \in \mathbb{Z}[i]$, $\quad 0 < N(g) \leq N(ax + by)$.

Hint: To show $g|a$, apply the Division Algorithm in $\mathbb{Z}[i]$ to write $a = gq + r$, where $q, r \in \mathbb{Z}[i]$ and $0 \leq N(r) < N(g)$. Then carefully prove that $N(r) = 0$.

Task 19 - continued

(b) Now use the lemma from part (a) of this task to complete the following:

Let $a, b \in \mathbb{Z}[i]$ and assume that a, b are relatively prime;
that is, assume that every common divisor of a and b is a unit.
Show that we can write 1 as a linear combination if a and b;
that is, show that there exists $z, w \in \mathbb{Z}[i]$ such that $az + bw = 1$.

Hint: Use the set $S = \{ax+by \,|\, x, y \in \mathbb{Z}[i]\,,\, xy \neq 0\}$ to first obtain an element $g \in \mathbb{Z}[i]$ that has the properties required by the hypothesis of the lemma in part (a).
(To do this, it will be important that $N(z) \in \mathbb{Z}^+$ for all $z \in \mathbb{Z}$.)
Once you have obtained g, be careful not to just assume $g = 1$!

Task 20 This task adapts a standard proof of the Prime Divisibility Property in the set of rational integers $\mathbb{Z}$ to the Gaussian integers $\mathbb{Z}[i]$.

As appropriate, review the rational integer proof in a modern Number Theory textbook. Then use the result of Task 19(b) to carefully prove the following:

Prime Divisibility Property for Gaussian Integers
Given $q, w \in \mathbb{Z}[i]$ and a Gaussian prime $p \in \mathbb{Z}[i]$.
If $p|qw$, then either $p|q$ or $p|w$.

Hint: Consider the two cases $p\,|q$ and $p \not| q$. For the second case, apply the theorem in Task 19(b) to an appropriate pair of Gaussian integers, but be sure to first carefully explain how you know that the Gaussian integer pair in question satisfies that theorem's hypothesis!

Task 21 This task examines the relationship between the definition of Gaussian prime given at the start of this section and Prime Divisibility Property in $\mathbb{Z}[i]$.

In the previous task, you showed that the standard definition of Gaussian prime implies that the Prime Divisibility Property holds in $\mathbb{Z}[i]$. Now show that we could, in fact, have instead used the Prime Divisibility Property as an alternate definition of 'Gaussian prime.'

Do this by proving the following:

Suppose $z \in \mathbb{Z}[i]$ is non-zero and satisfies the following property:

For all $q, w \in \mathbb{Z}[i]$, if $z|qw$, then either $z|q$ or $z|w$.

Then either z is a unit, or z is Gaussian prime.

Before returning to Dedekind's assertions about the properties of primes in $\mathbb{Z}[i]$, complete the following task to show that the norm really does provide us with just the right tool for determining whether a common divisor is, in fact, a *greatest* common divisor.

Task 22 This task formalizes the sense in which the norm allows us to measure which common divisors are greatest common divisors.

Use the definition of greatest common divisor for Gaussian integers and the theorem in Task 19(b) to prove the following:

> Let $a, b, g \in \mathbb{Z}[i]$ and assume g is a common divisor of a and b.
> Then g is a greatest common divisor of a and b if and only if
> for every $d \in Z[i]$ which is a common divisor of a and b, $N(d) \leq N(g)$.

We close this section with two tasks related to Dedekind's assertion that — once we make the proper adjustment to allow for units — the Unique Factorization Property also holds in $\mathbb{Z}[i]$. Let's first take another look at Dedekind's description about how to make that adjustment, stated in the following excerpt.

> Every composite number can be expressed uniquely as a product of prime numbers, provided of course the four associated primes $\pm q$, $\pm qi$ are regarded as representatives of the same prime number q.

Task 23 In this task, we examine how 'unique factorization' means something slightly different in the Gaussian integers than it did in the case of the rational integers.

Notice that 3 is, of course, one factor of 21, but Dedekind wrote that we need to regard the four Gaussian primes $\pm 3, \pm 3i$ as equivalent representations of the prime factor 3.

(a) Use this idea to write 21 as a product of Gaussian primes in four ways, using each of these four representations of 3.

(b) Given the result of part (a), explain why Dedekind nevertheless maintained that the Unique Factorization Property holds in the Gaussian integers.

Task 24 This task examines the proof of the Unique Factorization Property in $\mathbb{Z}[i]$.

Look back at the proof of the Unique Factorization Property for the set of rational integers $\mathbb{Z}$ in a modern Number Theory text. (Remember that this theorem is often referred to as the Fundamental Theorem of Arithmetic.) Then adapt that proof to show that the Unique Factorization Property holds in the set of Gaussian integers $\mathbb{Z}[i]$, provided that the four associated primes $\pm q$, $\pm qi$ are regarded as representatives of the same prime number q. *Indicate clearly where the Prime Divisibility Property is required in your proof.*

(There are, in fact, several ways to approach this proof in $\mathbb{Z}$ — you might again find that the proof by contradiction is most readily adaptable to the Gaussian integers.)

5 Uniqueness Lost?

Earlier in this project, we read Dedekind's description of the rational integers, in which he asserted that the Unique Factorization Property "depends essentially on the theorem that a prime divides a product of two factors only when it divides one of the factors." In the previous section of this project, you showed that this is also the case in the set of Gaussian integers by proving that the Prime Divisibility Property implies the Unique Factorization Property in that set. In this section, we continue our reading of Dedekind's analysis of more general number domains, to see how the Prime Divisibility Property, and consequently the Unique Factorization Property, can both break down. Dedekind began his analysis of such number domains as follows.

§ **7. The domain**[24]

There are still other numerical domains which can be treated in absolutely the same manner. For example, let θ be any root of any of the five equations

$$\theta^2 + \theta + 1 = 0, \quad \theta^2 + \theta + 2 = 0,$$

$$\theta^2 + 2 = 0, \quad \theta^2 - 2 = 0, \quad \theta^2 - 3 = 0,$$

and let x, y be rational integers. Then the numbers $x + y\theta$ form a corresponding numerical domain. In each of these domains it is easy to see that one can find the greatest common divisor of two numbers by a finite number of divisions, so that one immediately has general laws of divisibility agreeing with those for rational numbers, even though there happen to be an infinite number of units in the last two examples.

Notice that Dedekind once more omitted any proof that it is always possible to "find the greatest common divisor of two numbers by a finite number of divisions" within the five particular numerical domains $\mathbb{Z}[\theta]$ discussed in the previous excerpt, and instead simply stated that each of these sets can be treated "in absolutely the same manner" as the set of complex integers $\mathbb{Z}[i]$. In fact, Dedekind had little interest in these 'well behaved' numerical systems, and mentioned them primarily to provide contrast for the much more interesting domain $\mathbb{Z}[\theta]$ of numbers $x + y\sqrt{-5}$. As we will soon see, this latter system turns out to be interesting precisely because *the general laws of divisibility do not hold in it!!* Furthermore, it was precisely this anomalous behavior of the

[24] Recall from footnote 6 that Dedekind used the word 'domain' to refer to a system of numbers under certain arithmetic operations. Here and elsewhere, Dedekind denoted this particular number domain by '$\mathfrak{o}$.' In order to have consistent notation for this set in the primary source excerpts from Dedekind and in the project commentary on those excerpts, Dedekind's notation '$\mathfrak{o}$' has either been omitted or replaced by the notation $\mathbb{Z}[\theta]$ throughout this section of the project.

domain $\mathbb{Z}[\sqrt{-5}]$ that provided the motivation for the concept of 'an ideal number,' which in turn motivated the concept of an 'ideal'. We thus forego commentary on the more tame numerical systems mentioned in the previous excerpt, and move directly to Dedekind's discussion of how the notion of 'ideal numbers' arises out of the intriguing behavior of $\mathbb{Z}[\sqrt{-5}]$. As we do so, we will pause at various points in our reading in order to work through some of the details omitted by Dedekind.

As you read through the remainder of this section, keep in mind that Dedekind began this discussion (in the first sentence of the excerpt below) by explicitly stipulating that θ is a root of the equation $\theta^2 + 5 = 0$; **throughout the rest of this section, we will thus set $\theta = \sqrt{-5}$**.

On the other hand, this method [of finding the greatest common divisor of two numbers by a finite number of divisions] is not applicable to the domain of integers

$$\omega = x + y\theta$$

where θ is a root of the equation

$$\theta^2 + 5 = 0,$$

and x, y again take all rational integer values. Here we encounter the phenomenon which suggested to Kummer[25] the creation of ideal numbers, and which we shall now describe in detail by means of examples.

The numbers ω of the domain we shall now be concerned with are closed under addition, subtraction and multiplication, and we therefore define the notions of divisibility ... of numbers exactly as before. Also, if we define the norm $N(\omega)$ of a number $\omega = x+y\theta$ to be the product $x^2 + 5y^2$ of the two conjugate number $x \pm y\theta$, then the norm of a product will be equal to the product of the norms of the factors. ..... If μ is a unit, and hence divides all numbers, then we must have $N(\mu) = 1$ and therefore $\mu = \pm 1$.

Before continuing with your reading of Dedekind, pause to look at the following task to make sure the details of the ideas presented in the previous excerpt are clear.

[25] The German mathematician Ernest Kummer (1810–1893) was the first to recognize that the approach which nineteenth-century number theorists were pursuing in their attempts to prove Fermat's Last Theorem simply could not work — precisely because the Unique Factorisation property fails in systems of complex numbers such as the one Dedekind considered in this excerpt. As noted by Dedekind, this led Kummer to try to restore this uniqueness property to these number domains by introducing 'ideal' numbers into them.

Task 25 This task examines properties of the domain $\mathbb{Z}[\theta] = \{x + y\theta \,|x, y \in \mathbb{Z}\}$, where $\theta = \sqrt{-5}$, that Dedekind mentioned in the previous excerpt.

(a) Verify Dedekind's claim that $\mathbb{Z}[\sqrt{-5}]$ is closed under addition, subtraction and multiplication. Identify the additive identity and the multiplicative identity of this domain; justify both your answers.

(b) Given $\omega \in \mathbb{Z}[\sqrt{-5}]$ with $\omega = x + y\theta$, $x, y \in \mathbb{Z}$, note that Dedekind's definition of the norm of ω is exactly analogous to the definition of norm for the complex integers:

$N(\omega) = N(x + y\theta) = (x + y\theta)(x - y\theta) = x^2 - y^2\theta^2 = x^2 - y^2(\sqrt{-5})^2 = x^2 + 5y^2$

Find the norm of each of the following elements of $\mathbb{Z}[\sqrt{-5}]$.

(i) $\omega_1 = 4 - 7\theta$ (ii) $\omega_2 = -3 + 2\theta$ (iii) $\omega_1\omega_2$

Then use these values to verify that $N(\omega_1\omega_2) = N(\omega_1)N(\omega_2)$ in this case.

(c) Verify Dedekind's claim that any unit $\mu \in \mathbb{Z}[\sqrt{-5}]$ satisfies $N(\mu) = 1$.
Then explain why this implies that $\mathbb{Z}[\sqrt{-5}]$ contains only two units, $\mu = \pm 1$.

Task 26 This task provides computational practice in $\mathbb{Z}[\theta] = \{x + y\theta \,|x, y \in \mathbb{Z}\}$, where $\theta = \sqrt{-5}$.

Given $z, m \in \mathbb{Z}[\theta]$, define $m|z$ in the usual way.

Determine whether $m|z$ for each of the following pairs.

(a) $z = 113 + 22\theta$, $m = 4 - 3\theta$ (b) $z = 94 + 23\theta$, $m = 3 + 2\theta$

Task 27 This task establishes another 'sum of squares' identity in the set of rational integers.

Recall (from Task 16) that the following property can be proven using norms in $\mathbb{Z}[i]$:

For all $a, b, c, d \in \mathbb{Z}$, $(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2$ $(\star)$

(a) Use properties of norms in $\mathbb{Z}[\theta]$, $\theta = \sqrt{-5}$, to prove the following new identity:

For all $a, b, c, d \in \mathbb{Z}$, $(a^2+5b^2)(c^2+5d^2) = (ac+bd)^2+5(ad-bc)^2$ $(\diamondsuit)$

(b) Write each of the following in the form $u^2 + 5v^2$, with $u, v \in \mathbb{Z}$,
using property $(\diamondsuit)$ as needed.

(i) 29 (ii) 89 (iii) 2581 (iv) 229,709

Returning now to our reading of Dedekind, we will see how $\theta = \sqrt{-5}$ leads to strange new divisibility behavior in the domain $\mathbb{Z}[\theta]$.

A number (different from zero and ± 1) is called *decomposable* when it is the product of two factors, neither of which is a unit. In the contrary case the number is called *indecomposable*. Then it follows from the theorem on the norm that each decomposable number can be expressed as the product of a finite number of indecomposable factors. However, in infinitely many cases an entirely new phenomenon presents itself here, namely, the same number is susceptible to several, essentially different, representations of this kind. The simplest examples are the following. It is easy to convince oneself that each of the following numbers is indecomposable.

$$\begin{array}{llll} a = 2, & b = 3, & c = 7; & \\ b_1 = -2 + \theta, & b_2 = -2 - \theta, & c_1 = 2 + 3\theta, & c_2 = 2 - 3\theta; \\ d_1 = 1 + \theta, & d_2 = 1 - \theta, & e_1 = 3 + \theta, & e_2 = 3 - \theta; \\ f_1 = -1 + 2\theta, & f_2 = -1 - 2\theta, & g_1 = 4 + \theta, & g_2 = 4 - \theta; \end{array}$$

In fact, for a rational prime p to be decomposable, and hence of the form $\omega\omega'$, it is necessary that $N(p) = p^2 = N(\omega)N(\omega')$, and since ω, ω' are not units we must have $p = N(\omega) = N(\omega')$, that is, p must be representable by the binary quadratic form $x^2 + 5y^2$. But the three prime numbers 2, 3, 7 cannot be represented in this way, as one sees from the theory of these forms,[26] or else by a small number of direct trials. They are therefore indecomposable. It is easy to show the same thing similarly, for the other twelve numbers, whose norms are products of two of these three primes.

Task 28 This task examines the ideas introduces by Dedekind in the previous excerpt.

(a) Write down the formal definitions of 'decomposable' and 'indecomposable' numbers given by Dedekind in this excerpt. Why do you think he used the words 'decomposable' and 'indecomposable' here, rather than the words 'composite' and 'prime' that he used to describe the rational integers $\mathbb{Z}$ and the Gaussian integers $\mathbb{Z}[i]$?

(b) The previous excerpt also included a list of fifteen indecomposable numbers in $\mathbb{Z}[\theta]$, which Dedekind claimed will allow us to write down numbers that are "susceptible to several, **essentially different**, representations" as products of two indecomposable factors. Explain why you think that Dedekind emphasized that these factorizations are 'essentially different.' How do you think this will be different than what we saw in the previous section about Gaussian primes, where each composite Gaussian integer also has several different representations as products of Gaussian primes?
[Don't worry if you don't see why these fifteen numbers are indecomposable in $\mathbb{Z}[\theta]$; we'll look at this further in a moment.]

[26] Dedekind's footnote: See Dirichlet's *Vorlesungen über Zahlentheorie*, § *71*.

Notice that Dedekind's discussion of the 'indecomposability' of the numbers listed in the previous excerpt was simply the first part of his description of the 'entirely new phenomenon' that occurs within $\mathbb{Z}[\sqrt{-5}]$. Before we read more about this phenomenon, let's pause to consider this list of numbers and the definition of 'indecomposable' more carefully.

At first glance, the fact that the numbers 2, 3, 7 are indecomposable in $\mathbb{Z}[\sqrt{-5}]$ may seem to need no proof — after all, each of these numbers is prime in the set of rational integers. By virtue of this fact, we know that the numbers 2, 3, 7 each fails to have a non-trivial factorization in $\mathbb{Z}$, and this is exactly what it means to say these numbers are *indecomposable* in that set. But remember the situation in the Gaussian integers $\mathbb{Z}[i]$, where $2 = (1-i)(1+i)$ and neither of these factors is a unit in $\mathbb{Z}[i]$. In other words, 2 is *decomposable* in that set. Thus, the same number can be decomposable or not depending on the number domain in which we are working.

Dedekind's argument about the indecomposability of rational prime numbers (e.g., 2, 3, 7) in $\mathbb{Z}[\sqrt{-5}]$ was thus not simply belaboring the obvious . . . a proof really is needed. Let's consider the details of that proof for the specific value[27] $p = 2$. Arguing by contradiction, suppose that 2 is decomposable in $\mathbb{Z}[\theta]$. By definition of decomposable, 2 would then have a non-trivial factorization, which would give us non-units $\omega, \omega' \in \mathbb{Z}[\theta]$ with $\omega\omega' = 2$. Taking norms, we have $N(\omega\omega') = N(2) = N(2+0\theta) = 2^2 + 5(0^2) = 4$, which implies that $N(\omega)N(\omega') = 4$. Since neither ω nor ω' is a unit, we also know that $N(\omega) \neq 1$ and $N(\omega') \neq 1$. The only way for this to occur (i.e., $N(\omega)N(\omega') = 4$, $N(\omega) \neq 1$, $N(\omega') \neq 1$) would be if $N(\omega) = N(\omega') = 2$. *(It's important to remember that the norm of a number in $\mathbb{Z}[\sqrt{-5}]$ is necessarily a non-negative rational integer ... do you see why?)* But this implies that there exist $x, y \in \mathbb{Z}$ such that $\omega = x + y\theta$ and $N(\omega) = x^2 + 5y^2 = 2$. However, this latter equation clearly has no integer solutions. Our conclusion? The rational prime number $a = 2$ is indecomposable in the set $\mathbb{Z}[\sqrt{-5}]$.

Task 29 This task establishes the indecomposability of two other numbers in $\mathbb{Z}[\theta]$, where $\theta = \sqrt{-5}$.

(a) Let $b_1 = -2 + \theta$. Assume that b_1 is decomposable in $\mathbb{Z}[\theta]$, so that $b_1 = \omega\omega'$ for some non-units $\omega, \omega' \in \mathbb{Z}[\theta]$. Use the fact that the product of norms is the norm of products, together with the fact that $N(x + iy) = x^2 + 5y^2$ for any $x + iy \in \mathbb{Z}[\theta]$, to derive a contradiction.

(b) Use a similar proof to show that $e_2 = 3 - \theta$ is indecomposable in $\mathbb{Z}[\theta]$.

Let's now return to Dedekind's discussion of how the indecomposability of the fifteen numbers listed in the previous excerpt leads to an 'entirely new phenomenon' for divisibility in $\mathbb{Z}[\sqrt{-5}]$.

[27] You can check your understanding of the general proof simply by replacing '2' by 'p' (and $2^2 = 4$ by p^2), where p is an arbitrary prime, throughout this paragraph.

However, despite the indecomposability of these fifteen numbers, there are numerous relations between their products, which can all be deduced from the following.

$$
\begin{array}{lccc}
(1) & ab = d_1 d_2, & b^2 = b_1 b_2, & ab_1 = d_1^2 \\
(2) & ac = e_1 e_2, & c^2 = c_1 c_2, & ac_1 = e_1^2 \\
(3) & bc = f_1 f_2 = g_1 g_2, & af_1 = d_1 e_1, & ag_1 = d_1 e_2
\end{array}
$$

In each of these ten relations, the same number is represented in two or three *different* ways as a product of indecomposable numbers. Thus one sees that an indecomposable number may very well divide a product without dividing any of its factors. Such an indecomposable number therefore does not possess the property which, in the theory of rational numbers, is characteristic of a *prime number*.

If you were puzzled about why Dedekind used the term 'indecomposable' (rather than the more familiar term 'prime') to describe a number that can not be factored except as the product of itself and a unit, his reason for having done so should now be clear! Remember the following theorem from Euclid about prime rational integers, a property that we now know also holds for the Gaussian integers:

> *Prime Divisibility Property:* A (rational) prime number divides a product of two (rational) integer factors only when it divides one of the factors.

Yet each of the relationships in this last excerpt from Dedekind directly violates this theorem within $\mathbb{Z}[\sqrt{-5}]$! Take the first relationship on the list, for instance: $ab = d_1 d_2$. It is easy to verify that $ab = 6$ (since $a = 2$ and $b = 3$), and also that $d_1 d_2 = 6$ (since $d_1 = 1 + \sqrt{-5}$ and $d_2 = 1 - \sqrt{-5}$). But d_1 and d_2 are both indecomposable in $\mathbb{Z}[\sqrt{-5}]$, so that neither d_1 nor d_2 is divisible by 2 within this domain. We thus have a product $d_1 d_2$ which is divisible by the indecomposable number 2, and yet neither of the factors d_1 , d_2 of that product is divisible by 2. In other words, the number 2 does *not* satisfy our expectations concerning how prime numbers should behave, and therefore should *not* be called a prime number. Yet the number 2 *does* have the feature of having no factors other than itself and 1 (up to units), which certainly merits a special designation (i.e., 'indecomposable').

Task 30 This task further examines the failure of the Prime Divisibility Property in $\mathbb{Z}[\sqrt{-5}]$.

(a) Choose another of the equalities listed in (1), (2) and (3) of the previous excerpt (other than the equality $ab = d_1d_2$), and verify the details of that equality. (For instance, if you choose the equality '$ag_1 = d_1e_2$', explain why this equality holds.)

Then explain how your chosen equality illustrates the fact that "an indecomposable number may very well divide a product without dividing any of its factors" within the number domain $\mathbb{Z}[\sqrt{-5}]$.

(b) Choose yet another of the equalities listed in (1), (2) and (3) of the previous excerpt, and verify its details. Again explain how your chosen equality illustrates the fact that "an indecomposable number may very well divide a product without dividing any of its factors" within the number domain $\mathbb{Z}[\sqrt{-5}]$.

Task 31 This task reflects on the meaning and status of unique factorization in $\mathbb{Z}[\sqrt{-5}]$.

Begin by reviewing the equalities listed in (1), (2) and (3) of the previous Dedekind excerpt. Also look back also at your answer to Task 24 of the previous section, where you proved that the Unique Factorization Property holds in the Gaussian integers $\mathbb{Z}[i]$.

Then write a 1–2 paragraphs in which you reflect upon the following questions.

- What is problematic about the Unique Factorization Property in the domain $\mathbb{Z}[\sqrt{-5}]$?
- How do these problems relate to failure of the Prime Divisibility Property in $\mathbb{Z}[\sqrt{-5}]$?
- Is there some portion or variation of the Unique Factorization Property that we *can* prove within $\mathbb{Z}[\sqrt{-5}]$, even without the Prime Divisibility Property?
- How might we be able re-define or extend the concept of what counts as a 'prime' for the domain $\mathbb{Z}[\sqrt{-5}]$ so that it does make sense to talk about the the Unique Factorization Property for this domain?

6 Ideal Numbers, and Uniqueness Restored!

In the next part of his paper, Dedekind further analyzed the fifteen indecomposable numbers that we examined in the last section of this project, with an eye towards restoring the Prime Divisibility Property to $\mathbb{Z}[\theta]$, where $\theta = \sqrt{-5}$. As you read the beginning of this analysis in the next excerpt, don't be concerned if you don't see how to "easily deduce" the relationships stated by Dedekind — as we see from his footnote, the English translator of Dedekind's paper found these deductions mysterious as well!

NOTE: The numbered sets of equations (1), (2) and (3) referenced in Dedekind's computations in this section were given in the last Dedekind excerpt of the preceding section, and are reproduced here for the reader's convenience:

$$\begin{array}{lccc} (1) & ab = d_1d_2, & b^2 = b_1b_2, & ab_1 = d_1^2 \\ (2) & ac = e_1e_2, & c^2 = c_1c_2, & ac_1 = e_1^2 \\ (3) & bc = f_1f_2 = g_1g_2, & af_1 = d_1e_1, & ag_1 = d_1e_2 \end{array}$$

If we imagine for a moment that the fifteen preceding numbers are rational integers then, by the general laws of divisibility, we easily deduce from the relations (1) that there are decompositions of the form[28]

$$\begin{aligned} a &= \mu\alpha^2, & d_1 &= \mu\alpha\beta_1 & d_2 &= \mu\alpha\beta_2 \\ b &= \mu\beta_1\beta_2, & b_1 &= \mu\beta_1^2 & b_2 &= \mu\beta_2^2 \end{aligned}$$

and from the relations (2) that there are decompositions of the form[29]

$$\begin{aligned} a &= \mu'\alpha'^2, & e_1 &= \mu'\alpha'\gamma_1 & e_2 &= \mu'\alpha'\gamma_2 \\ c &= \mu'\gamma_1\gamma_2, & c_1 &= \mu'\gamma_1^2 & c_2 &= \mu'\gamma_2^2 \end{aligned}$$

where all the Greek letters denote rational integers. And it follows immediately, by virtue of the equation $\mu\alpha^2 = \mu'\alpha'^2$, that the four numbers f_1, f_2, g_1, g_2 appearing in the relations (3) will likewise be *integers*.[30]

These decompositions are simplified if we make the additional assumptions that a is prime to b and c, since this implies $\mu = \mu' = 1$, $\alpha = \alpha'$ and hence the fifteen numbers can be expressed as follows in terms of the five numbers α, β_1, β_2, γ_1, γ_2:

$$(4) \qquad \begin{cases} a = \alpha^2, & b = \beta_1\beta_2, & c = \gamma_1\gamma_2 & \\ b_1 = \beta_1^2, & b_2 = \beta_2^2, & c_1 = \gamma_1^2 & c_2 = \gamma_2^2 \\ d_1 = \alpha\beta_1, & d_2 = \alpha\beta_2, & e_1 = \alpha\gamma_1 & e_2 = \alpha\gamma_2 \\ f_1 = \beta_2\gamma_1, & f_2 = \beta_2\gamma_2, & g_1 = \beta_1\gamma_2 & g_2 = \beta_2\gamma_1 \end{cases}$$

Now even though our fifteen numbers are in reality indecomposable, the remarkable thing is that they behave, in all questions of divisibility in the domain $\mathbb{Z}[\theta]$, exactly as if they were composed, in the manner indicated above, of five different *prime numbers* α, β_1, β_2, γ_1, γ_2.

---

[28] In the following proof provided by the translator of Dedekind's monograph, note that the statement (in line 5 below) that "μ, μ_1, μ_2 are square free" is not a new assumption, but simply an acknowledgement that we can collect all even powered factors of a, b_1, b_2 together as part of α^2, β_1^2, β_2^2, respectively.

> **Translator's footnote:** Since these decompositions do not seem obvious to me, I include the following proof of the consequences of (1) as an example. Note first that $ab_1 = d_1^2$ and $b_1b_2 = b^2$ are both squares. Suppose that
>
> $$a = \mu\alpha^2, \;\; b_1 = \mu_1\beta_1^2, \;\; b_2 = \mu_2\beta_2^2,$$
>
> where μ, μ_1, μ_2 are square free. Then $ab_1 = \mu\mu_1\alpha^2\beta_1^2$ is not a square unless $\mu = \mu_1$. Similarly, b_1b_2 is not a square unless $\mu_1 = \mu_2$. Thus in fact $\mu = \mu_1 = \mu_2$ and hence
>
> $$a = \mu\alpha^2, \;\; b_1 = \mu\beta_1^2, \;\; b_2 = \mu\beta_2^2.$$
>
> Forming products of these, we get
>
> $$\begin{aligned} d_1^2 = ab_1 = \mu^2\alpha^2\beta_1^2 &\;\Rightarrow\; d_1 = \mu\alpha\beta_1, \\ d_2^2 = ab_2 = \mu^2\alpha^2\beta_2^2 &\;\Rightarrow\; d_2 = \mu\alpha\beta_2, \\ b^2 = b_1b_2 = \mu^2\beta_1^2\beta_2^2 &\;\Rightarrow\; b = \mu\beta_1\beta_2, \end{aligned}$$
>
> which completes the proof of the decompositions claimed by Dedekind.

[29] This second set of decompositions can be derived in a fashion similar to that illustrated by the translator's proof in the preceding footnote.

[30] As before, the conclusion that these four numbers are integers may not seem immediately obvious! The interested reader is invited to algebraically prove that this is indeed the case. It may be useful to first show that $\alpha = \alpha'$.

Task 32 This task examines Dedekind's assertions in the previous excerpt.

(a) At the start of this excerpt, Dedekind asked us to "imagine for a moment that the fifteen preceding numbers are rational integers". Explain what he meant by this. That is, what properties of the rational integers $\mathbb{Z}$ do not hold for the given fifteen numbers that it would be useful for us to imagine they did have?

(b) Explain what Dedekind meant at the end of the excerpt when he said the following. In particular, what properties will α, β_1, β_2, γ_1, γ_2 need to satisfy if they are, in fact, prime numbers?

> Now even though our fifteen numbers are in reality indecomposable, the remarkable thing is that they behave, in all questions of divisibility in the domain $\mathbb{Z}[\theta]$, exactly as if they were composed, in the manner indicated above, of five different *prime numbers* α, β_1, β_2, γ_1, γ_2.

(c) Now explain how we know that α, β_1, β_2, γ_1, γ_2 are NOT actually in $\mathbb{Z}[\sqrt{-5}]$ itself.

In a subsequent part of his monograph, Dedekind went on to analyze the divisibility properties of the number 2 in the domain $\mathbb{Z}[\theta]$ and arrived at the conclusion that "... the number 2 behaves in our domain as though it were the square of the prime number α." He further commented that:

> Although such a prime number α does not actually exist in the domain $\mathbb{Z}[\theta]$, it is by no means necessary to introduce it, since in fact Kummer managed in similar circumstances with great success by taking such a number α to be an *ideal* number, ...

Dedekind then demonstrated that this ideal number α *(as well as ideal numbers $\beta_1, \beta_2, \gamma_1, \gamma_2$ that appear in (4) above)* does indeed have the essential property of a prime; namely, if the product of two factors is divisible by α, then one of the factors must also be divisible by α! Although Dedekind's full analysis of the actual and ideal primes of $\mathbb{Z}[\theta]$ with $\theta = \sqrt{-5}$ goes beyond the scope of this project, here is how he summarized the conclusions of that analysis:

> By similar study of the whole domain of the numbers $\omega = x + \theta y$ (where $\theta = \sqrt{-5}$) we find the following results:
>
> 1. All the positive rational primes $\equiv 11, 13, 17, 19 \pmod{20}$ behave like actual prime numbers.
> 2. The number θ ... has the character of a prime number. The number 2 behaves like the square an ideal prime number α.
> 3. Each positive rational prime $\equiv 1, 9 \pmod{20}$ can be decomposed into two different factors, which really exist and have the character of primes.
> 4. Each positive rational prime $\equiv 3, 7 \pmod{20}$ behaves like the product of two different ideal prime numbers.
> 5. Each actual number ω different from zero and ± 1 is either one of the numbers mentioned above as having the character of a prime, or else it behaves in all questions of divisibility as a unique product of actual or ideal prime factors.

We will look more at Dedekind's fifth claim in a moment. First, check your understanding of the first four claims about his 'mod-20' test for determining the actual and ideal primes of $\mathbb{Z}[\theta]$ by completing the following task.

Task 33 This task looks at Dedekind's claims concerning actual and ideal primes in $\mathbb{Z}[\sqrt{-5}]$.

(a) Which of the following positive rational primes p are actual primes in $\mathbb{Z}[\theta]$? For each that is NOT an actual prime in $\mathbb{Z}[\theta]$, either write p as the product of actual primes in $\mathbb{Z}[\theta]$ or explain why this is not possible.

$$5 \ , \ 23 \ , \ 29 \ , \ 31 \ , \ 43 \ , \ 59 \ , \ 61 \ , \ 89$$

An Illustration: 41

41 is a rational prime, with $41 \equiv 1 \pmod{20}$.

By Dedekind's mod-20 test, 41 is decomposable into two different factors which have the character of primes.

- To factor, write $41 = (x + \theta y)(x - \theta y) = x^2 + 5y^2$.
  (Do you see why conjugate factors are necessary)
  Solving $41 = x^2 + 5y^2$ gives us $x = 6, y = 1$; thus $41 = (6 + \theta)(6 - \theta)$.
- To show $6 \pm \theta$ "have the character of primes," we verify indecomposability:
  Assume $6 \pm \theta = \omega\omega'$, where $\omega, \omega' \in \mathbb{Z}[\theta]$.
  Then $N(6 \pm \theta) = N(\omega)N(\omega')$, or $41 = N(\omega)N(\omega')$, with $N(\omega), N(\omega') \in \mathbb{Z}^+$.
  Because 41 is a rational prime, either ω or ω' must thus be a unit.
  Hence, $6 \pm \theta$ has trivial factorizations only, and is therefore decomposable.

Conclusion: 41 is composite in $\mathbb{Z}[\theta]$, with (actual) prime factorization $41 = (6+\theta)(6-\theta)$.

(b) Which of the following elements of $\mathbb{Z}[\theta]$ have prime factorizations that include ideal prime numbers? For each that does, indicate how many ideal prime factors it has.

$$817 \ , \ 2021 \ , \ 7667 \ , \ 22\theta \ , \ 29 + 58\theta \ , \ 33 + 44\theta$$

An Illustration: 437

- First factor over the rational primes, $437 = 19 \cdot 23$.
- Then apply Dedekind's mod-20 test to each factor:
  - 19 is an actual prime number, since $19 \equiv 19 \pmod{20}$
  - 23 behaves like the product of two ideal prime number, since $23 \equiv 3 \pmod{20}$

Conclusion: 437 is the product of 1 actual prime and 2 ideal prime factors.

Let's go back now and re-read Dedekind's Claim 5 in the preceding excerpt:

> Each actual number ω different from zero and ± 1 is either one of the numbers mentioned above as having the character of a prime, or else it behaves in all questions of divisibility as a unique product of actual or ideal prime factors.

In short, by creating 'ideal primes' for the integer domain $\mathbb{Z}[\theta]$, we can restore the Unique Factorization Propery (aka, the Fundamental Theorem of Arithmetic) to $\mathbb{Z}[\theta]$! The key to this proof is something that we have now encountered several times in this project. Namely, in order to prove that each number in a particular integer domain has a *unique* factorization as the product of prime numbers (either actual or ideal), we need to know that the domain satisfies the *Prime Divisibility Property*. By introducing ideal primes for the the integer domain $\mathbb{Z}[\sqrt{-5}]$, Dedekind was able to show that the Prime Divisibility Property held in $\mathbb{Z}[\theta]$ and, along with it, the Unique Factorizaton Property.

Here is what Dedekind went on to say about the proof that these two properties hold in the domain $\mathbb{Z}[\sqrt{-5}]$:

> However, to arrive at this result and to become completely certain that the general laws of divisiblity governing the domain of rational numbers extend to our domain $\mathbb{Z}[\sqrt{-5}]$, with the help of the ideal numbers we have introduced, it is necessary, as we shall soon see when we attempt a rigorous derivation, to make a very deep investigation, ... We can indeed reach the proposed goal with all rigor; however, as we have remarked in the Introduction, the greatest circumspection is necessary to avoid being led to premature conclusions. In particular, the notion of *product* of arbitrary factors, actual or ideal, cannot be exactly defined without going into minute detail. Because of these difficulties, it has seemed desirable to replace the ideal numbers of Kummer, which is never defined in its own right, but only has a divisor of actual numbers ω in the domain $\mathbb{Z}[\sqrt{-5}]$, by a *noun* for something which actually exists, and this can be done in several ways.

The '*noun*' to which Dedekind referred is a special type of algebraic structure that is known today as an *ideal*, a term first introduced by Dedekind in the paper from which we have been reading in this project. Here is how Dedekind himself defined an ideal. (In this excerpt, the symbol '$\mathfrak{o}$' represents an integer domain like $\mathbb{Z}[\theta]$, and the symbol '$\mathfrak{a}$' represents a subset of the given integer domain $\mathfrak{o}$.)

An *ideal* of an (integer domain) $\mathfrak{o}$ is a system $\mathfrak{a}$ of elements α in $\mathfrak{o}$ with the following two properties:

I. The sum and difference of any two elements in $\mathfrak{a}$ also belong to $\mathfrak{a}$;

II. The product $\alpha\omega$ of any element α in $\mathfrak{a}$ with an element ω in $\mathfrak{o}$ is an element in $\mathfrak{a}$.

In today's terminology, note that Property I simply states that the set $\mathfrak{a}$ is closed under addition and subtraction. But as you may have already noticed, Property II is much *stronger* than asserting that $\mathfrak{a}$ is closed under multiplication! This is because Property II asserts that if we begin with some α in the ideal $\mathfrak{a}$ and look at *all* the possible products $\alpha\omega$ for *every element* ω *in the entire integer domain* $\mathfrak{o}$, then all of these products end up inside the ideal $\mathfrak{a}$ — regardless of whether ω comes from inside of $\mathfrak{a}$ or from outside of $\mathfrak{a}$. In contrast, checking that a set $\mathfrak{a}$ is 'closed under multiplication' requires us to consider the products $\alpha\omega$ only for elements α and ω that *both* lie inside the set $\mathfrak{a}$ itself. Dedekind's motivation for this stronger property (today called 'absorption of products') had to do with what Dedekind called two elementary theorems about divisibility:

1. If two integers $\alpha = \mu\omega$, $\alpha' = \mu\omega'$ are divisible by the integer μ, then so are their sum $\alpha + \alpha' = \mu(\omega + \omega')$, and their difference $\alpha - \alpha' = \mu(\omega - \omega')$, since the sum $\omega + \omega'$ and difference $\omega - \omega'$ are themselves integers.
2. If $\alpha = \mu\omega$ is divisible by μ, then each number $\alpha\omega' = \mu(\omega\omega')$ divisible by α will also be divisible by μ, since each product $\omega\omega'$ of integers ω, ω' is itself an integer.

Task 34 This task compares integer divisibility properties with Dedekind's definition of an ideal.

Complete the following restatements of Properties 1 and 2 for divisibility by an integer μ.

1. *The sum and difference of any two numbers that are divisible by* μ *are always* _____.
2. *The product of a number that is divisible by* μ *by any other number is always* _____.

Comment on how properties 1 and 2 for divisibility of integers (as re-stated in this task) relate to Properties I and II of an ideal $\mathfrak{a}$ (stated by Dedekind in the excerpt at the top of this page). How are these two pairs of properties the same? How are they different?

Dedekind's definition of an ideal brings us to the end of our number-theoretic study of his monograph. Dedekind himself went on in that monograph to extend the properties of rational integer divisibility to ideals themselves. In addition to defining what it means for one ideal to divide another ideal, he defined the notions of least common multiple of two ideals and the greatest common divisor of two ideals. He then introduced several special types of ideals. These included *principal ideals*, which correspond to the actual number in the underlying integer domain, and *prime ideals*, which allowed Dedekind to achieve his goal of restoring unique factorization to integer domains like $\mathbb{Z}[\sqrt{-5}]$. The general concept of an ideal, as well as the concept of an integer domain, is today part of an important Abstract Algebra topic known as *ring theory* — a sophisticated and highly applicable algebraic theory that was initially motivated by the simple desire to maintain the property of unique prime factorizations when working in integer domains!

References

E. T. Bell. *Men of Mathematics*. Simon and Schuster, New York, 1937.

A. Cayley. On the theory of groups, as depending on the symbolic equation $\theta^n = 1$, Part I. *Philosophical Magazine*, 7:40–47, 1854. and in *The Collected Mathematical Papers of Arthur Cayley*, Cambridge: Cambridge University Press, Vol. 2 (1889), 123–130.

L. Corry. *Modern Algebra and the Rise of Mathematical Structures*. Birkhäuser, Basel, second revised edition, 2004.

R. Dedekind. *Stetigkeit und irrationale Zahlen (Essays on the Theory of Numbers)*. F. Vieweg und Sohn, Braunschweig, 1888. English translation by Beman, The Open Court Publishing Company, Chicago, 1901.

R. Dedekind. *Theory of Algebraic Integers*. Cambridge University Press, Cambridge, 1966. English tranlation by J. Stillwell of *Sur la Théorie des Nombres Entiers Algébriques*, first published in 1877.

L. E. Dickson. *History of the Theory of Numbers, Volume II*. Dover, Mineola MN, 2005. First published in 1919.

H. M. Edwards. The genesis of ideal theory. *Archives for the History of the Exact Sciences*, 15: 321–378, 1980.

I. Kleiner. The roots of commutative algebra in algebraic number theory. In M. Anderson, V. Katz, and R. Wilson, editors, *Who Gave you the Epsilson? & Other Tales of Mathematical History*, pages 299–308. Mathematical Association of America, Washington DC, 2009.

Notes to Instructors

PSP Content: Topics and Goals

Developed as part of the Transforming Instruction in Undergraduate Mathematics via Primary Historical Sources (TRIUMPHS) program, the Primary Source Project (PSP) *Gaussian Integers and Dedekind's Creation of an Ideal: A Number Theory Project* offers students an in-depth exploration of the concept of 'prime number' through a guided reading of select excerpts from the 1877 version of Dedekind's theory of ideals. Characteristics of Dedekind's work that make it an excellent vehicle for students in a first course on number theory include his emphasis on abstraction, his continual quest for generality and his careful methodology. The 1877 version of his ideal theory (the third of four versions he developed in all) is an especially good choice for students to study, due to the care that Dedekind devoted therein to motivating the concept of an ideal as a means to restore unique prime factorization to integral domains that lack this familiar property. Through a careful choice of examples, Dedekind essentially asked, then answered, the question: *What makes a prime number 'prime'?*

Dedekind set the stage for his inquiry into this question by first considering the example of the Gaussian integers $\mathbb{Z}[i]$, itself a unique factorization domain. A core topic of the PSP is thus the study of divisibility and primes within $\mathbb{Z}[i]$, culminating with the proof that unique factorization holds therein. The connection of Gaussian primes to the Sum of Two Squares Theorem for rational integers is also considered via a series of student tasks. Dedekind's next example, $\mathbb{Z}[\sqrt{-5}]$, then provides students with a readily-accessible illustration of the insufficiency of 'indecomposability' as the defining property for the concept of a prime number. The PSP closes with a brief overview (omitting the technical details) of Kummer's notion of an *ideal prime*, and an even briefer preview of the more abstract algebraic structure of an *ideal* that Dedekind proposed as a replacement for Kummer's ideal primes.

The PSP's running theme of '*What makes a prime number 'prime'?*' has particular relevance for prospective secondary mathematics teachers, for whom a course in number theory is often a requirement. A second running theme throughout the project is the important concept of *uniqueness*, which is explored in connection with both divisibility in $\mathbb{Z}[i]$ and the Unique Factorization Property more generally. Project tasks further offer students the opportunity engage in a variety of activities that model how mathematicians work: extending and consolidating conceptual understanding through computation, making sense of and interpreting mathematical texts, generalizing familiar concepts to new contexts, using data to formulate conjectures, then testing, refining and proving those conjectures.

Student Prerequisites

No prior experience with complex numbers is assumed, beyond some familiarity with the basic operations of addition, subtraction and multiplication. The only significant number theory pre-requisite (needed for Section 4 and one task in Section 5) is some prior experience with one or more proofs that the following two properties hold for the rational integers $\mathbb{Z}$:

- *Unique Factorization Property* (or *Fundamental Theorem of Arithmetic*): Every (positive) integer has a unique factorization as a product of primes (up to the order of the factors).
- *Prime Divisibility Property* (or *Euclid's Lemma*): A prime number divides a product of two integer factors only if it divides one of the two factors.

Most of the other number-theoretic concepts required for completion of the project will be familiar to students from their K-12 experiences; these include the definitions (within $\mathbb{Z}$) of *prime*, *composite*,

divisor, and *greatest common divisor*. Euclid's algorithm for finding the greatest common divisor is also featured in Section 2, where it is extended (without proof) from the rational integers to the Gaussian integers; the example given in footnote 8 should suffice as a reminder of how this algorithm works for natural numbers. Congruence also plays a role in several tasks (identified in the PSP Design and Task Commentary description below), but primarily as a notational device, so that the definition given in footnote 13 is enough to allow even students who have not yet encountered this concept to proceed. And although Dedekind's own motivation in his 1877 monograph was to introduce the concept of an ideal to his readers, the PSP itself requires no prior formal study of abstract algebra. Indeed, Dedekind's own writing on the topic of ideals pre-dated what we today call ring theory!

PSP Design, and Task Commentary

The full PSP is divided into six sections described in more detail below. Although these sections are of differing page lengths, the five non-introductory sections can each be expected to take approximately the same number of class periods. An estimated number of class periods (based on a class length of 50 minutes) is given for each section. The actual number of class periods spent on each section naturally depends on the students' prior experience and background, on the instructor's goals, and on how the PSP is actually implemented with students. Estimates on the high end of the range assume most PSP work is completed by students working in small groups during class time.

- Section 1: Introduction (0 class days)

  This brief section includes some biographical and historical details related to Dedekind and his work, and provides an overview of the contents of other sections of the project.

- Section 2: The Gaussian Integers (1 – 2 class days)

  This section opens with Dedekind's summary of the essential divisibility properties for the set of rational integers, in which the Unique Factorization Property and Prime Divisibility Property make their first appearance. Its then moves quickly to the introduction of the Gaussian integers. Tasks 4 and 5 examine the geometry of the Gaussian integers, and begin to introduce the idea that uniqueness can fail in interesting new ways within the set of Gaussian integers.[31] Other tasks in this section provide computational practice with divisibility in $\mathbb{Z}[i]$ and the use of the norm operator to adapt the Euclidean algorithm for greatest common divisors to that set. The existence of four distinct but equivalent (up to multiplication by the units ± 1, $\pm i$) gcds for each pair of non-zero Gaussian integers is presented by way of project narrative. The closing task further emphasizes this notion of equivalence, while illustrating how the different quotients and remainders of a given pair of non-zero Gaussian integer may fail to be equivalent in this sense.

  Note that three tasks in this section (Tasks 1, 2 and 7) call for student reflection on mathematical ideas in anticipation of material that will be encountered again, in later sections of the PSP. In particular, Task 7 provides a segue into the discussion of units/associates in Section 3.

[31] For Task 4(c), students are expected to notice that the values of both $\mathrm{Re}(w)$ and $\mathrm{Im}(w)$ of the complex number w would need to have a fractional part of .5 for there to be more than two complex integers q with $N(w-q) \leq 1/2$. For Task 4(d), there will there be a unique complex integer q with this property only when $\mathrm{Re}(w)$ and $\mathrm{Im}(w)$ both have fractional parts near 0 or 1.

- Section 3: Gaussian Primes, and the Sum of Two Squares (1 – 2 class days)

  This section begins with Dedekind's descriptions of three special classes of Guassian integers: units, composites and primes. In Task 9, students are asked to re-cast his somewhat informal descriptions into formal definitions. **Note that two of these three definitions will be later revealed in the PSP (*unit* on page 13, and *Gaussian prime* on page 19); thus, Task 8 should be completed by students prior to assigning these later pages for student reading.**

  Task 10 continues to track the appearance of the Unique Factorization Property and the Prime Divisibility Property within Dedekind's thinking, but now within the set $\mathbb{Z}[i]$; a formal treatment this theme will be taken up in earnest in Section 4. In anticipation of that more formal treatment, a formal write-up of the proof that is requested in Task 11 of Section 3 is recommended as part of a homework assignment.

  The subsequent project narrative then offers examples of how to prove that a given rational prime is or is not a Gaussian prime, with additional examples of Gaussian primes and Gaussian composites (some with non-zero imaginary parts) appearing in Task 12. In Task 13, students are asked to organize this data in order to develop a conjecture for prediction if a given Gaussian integer is a prime. This is an excellent task for in-class small group work. **Note, however, that the answer to Task 13 is revealed in the Dedekind excerpt on page 15!!**

  This same Dedekind excerpt then leads to a discussion of the Sum of Two Squares Theorem for rational integers, which is further explored in Tasks 14–18. *Instructors who wish to focus exclusively on Gaussian integers could omit these five tasks and the closing paragraph of this section on page 18. In this case, Task 27 (from Section 5) should also be omitted.* Note that Task 17 is a more challenging exploratory task, so that students may need some additional guidance from instructors who assign it. Note also that congruence notation is employed in the tasks related to the Sum of Two Squares Theorem; this notation is defined in footnote 13.

- Section 4: Gaussian Primes and Unique Factorization (2 – 2.5 days)

  This section is the most challenging portion of the PSP in terms of the level of abstraction and formality involved in the Tasks. Starting with formal definitions of 'prime' and 'greatest common divisor' for the set of Gaussian integers, these tasks guide students towards an understanding of and formal proofs for both the Prime Divisibility Property and Unique Factorization Property in $\mathbb{Z}[i]$. **Note again that the PSP assumes that students have experienced a proof of both these properties for the rational integers $\mathbb{Z}$!** Task instructions in the PSP include the suggestion that students review these proofs for the rational integers in a modern Number Theory text prior to tackling the proofs for the Gaussian integers.

  Given both their challenging nature and fundamental importance to the PSP themes, the formal proofs requested Tasks 19, 20 and 24 are well-suited for discussion during class in small groups, followed by individualized formal write-up as homework. Tasks 21 and 22 also offer good opportunities for practice with formal proof writing.

- Section 5: Uniqueness Lost? (1 – 1.5 days)

  This section is based on Dedekind's discussion of the specific integral domain $\mathbb{Z}[\sqrt{-5}]$, which fails to satisfy the Prime Divisibility Property, and therefore also the Unique Factorization Property. Following some very concrete, computational tasks within $\mathbb{Z}[\sqrt{-5}]$, students are asked to read Dedekind's discussion of the entirely 'new phenomenon [that] presents itself here, namely, the same number is susceptible to several, essentially different, representations of this kind. This is where Dedekind offered his answer to the question *'What makes a prime number 'prime'?'* by distinguishing between 'indecomposability' and 'Prime Divisibility Property,, and emphasizing that it is the latter property which is required to have unique prime factorization. Although the concepts themselves are fairly sophisticated, most of the tasks in this section of the PSP involve little more than straightforward computations. The exception is the very open-ended Task 31, which calls for students to reflect on the the issues encountered within $\mathbb{Z}[\sqrt{-5}]$. Although instructors are encouraged to allow a wide range of responses to the questions posed in this task, it is hoped that students will realize that there is no difficulty in proving the *existence* of indecomposable factorizations in $\mathbb{Z}[\sqrt{-5}]$, but rather that these factorizations may not be unique due to the failure of the Prime Divisibility Property. Given its open-endedness, Task 31 is also well-suited to small group discussion and perhaps even small group (versus individual) write-ups.

- Section 6: Ideal Numbers, and Uniqueness Restored! (1 – 1.5 days)

  This section continues Dedekind's discussion of the integer domain $\mathbb{Z}[\sqrt{-5}]$ and his argument that every element can be viewed as behaving as if it were composed of prime numbers, provided that 'ideal numbers' are introduced to serve in the place of the prime factors which are essentially missing from $\mathbb{Z}[\sqrt{-5}]$. Although there is considerable algebraic manipulation behind his conclusions in the key excerpt on page 29, these manipulations are peripheral to the main point of his analysis, and can thus be briefly skimmed or omitted altogether. In fact, most of the details of Dedekind's analysis related to actual and ideal primes are omitted from the PSP altogether, although the statement of his final 'mod-20' test for characterizing how elements of $\mathbb{Z}[\sqrt{-5}]$ can be factored into actual and ideal primes is included. An illustration of how to apply this test is given as part of Task 33, which is essentially intended to provide additional practice in verifying indecomposability.

  The section (and the PSP!) closes with Dedekind's description of how the Unique Factorization Property can be restored either through the introduction of ideal numbers, as suggested by Kummer, or by making use of a 'noun for something that actually exists' — that is, an *ideal*. In the closing task of the project, students examine Dedekind's first definition of an ideal, together with his explanation of how that definition is motivated simply by thinking about properties of the divisibility relationship for rational integers. Since studying the algebraic structure of ideals goes beyond the scope of this project, nothing beyond the definition is discussed. This final portion of the project (pages 32–34) could thus simply be assigned for students to complete outside of class (including Task 34), with minimal discussion of its content in class.[32]

[32] Instructors who are interested in having students work with the algebraic structure of an ideal itself may wish use portions of the author's PSP *Dedekind and the Creation of Ideals: Early Developments in Ring Theory*, which is designed for use in a first course on Abstract Algebra and is available at `http://webpages.ursinus.edu/nscoville/TRIUMPHS.html`.

Possible Modifications of the PSP

Although there are many options for omitting particular tasks during implementation of this project (or adding new tasks to it!), the following two options are notable variations that could be adopted depending on the instructor's goals for the course.

- Instructors who wish to study only the Gaussian Integers could complete Sections 1–4 of the project, and also omit Tasks 14–18 pertaining to the Sum of Two Squares Theorem.
- Instructors who teach a more informal course could omit some or all of Section 4, which focuses on formal proofs of properties of the Gaussian integers, as well as some or all of the following 'formal proof' exercises: Tasks 11, 14, 15, 16(c)

The author is available to discuss other options for modifying the project to better suit an instructor's goals for the course. LaTeXcode of the entire PSP may also be requested should an instructor be interested in project modifications that go beyond simply skipping parts of the project. In such cases, the author requests that a copy of the LaTeXcode for the modified PSP and an Instructor Implementation Report be returned to her following class completion of the modified version.

Suggestions for Classroom Implementation

To reap the full mathematical benefits offered by this PSP, students should be required to read assigned sections in advance of any in-class discussion, or to work through reading excerpts together in small groups in class. The author's method of ensuring that advance reading takes place is to require student completion of daily "Reading Guides" based on the assigned reading for the next class meeting; see pages 44–46 for a sample guide. Reading Guides typically include "Classroom Preparation" exercises (drawn from the PSP Tasks) for students to complete prior to arriving in class; they may also include "Discussion Questions" that ask students only to read a given task and jot down some notes in preparation for class discussion. On occasion, tasks are also assigned as follow-up to a prior class discussion. In addition to supporting students' advance preparation efforts, these guides provide helpful feedback to the instructor about individual and whole class understanding of the material. The author's students receive credit for completion of each Reading Guide (with no penalty for errors in solutions).

With regard to PSP implementation, a combination of whole class discussions, small group work, student presentations and homework assignments drawn from the PSP tasks is recommended in order to take advantage of the variety of questions provided in the PSP. The Sample Implementation Schedule below include suggestions concerning instructional strategies that are especially well-suited to different parts of the PSP. For small group work on individual tasks, the author recommends providing students with a copy of the task (with space provided to complete each part thereof). LaTeXcode of the entire PSP may be requested from author to facilitate preparation of such 'in-class task sheets'.

Sample Implementation Schedule (based on a 50 minute class period)

The following sample schedule assumes completion of the entire PSP.

- **Advance Preparation Work for Day 1** (to be completed before class)
  Read pages 1 – 9 in Sections 1 and 2, completing work on Tasks 1–4 for class discussion along the way, per the sample Reading Guide on pages 44–46 below.

- **Day 1 of Class Work**
  - (Optional) Brief whole class discussion of the historical and mathematical ideas from Section 1.
  - Whole class and/or small group discussion of the assigned reading and related tasks in Section 2, to include comparison of answers to Tasks 1, 3a, 4a. Students' Reading Guide answers to Task 2 could also be compared in small groups, or simply reviewed by the instructor after class.
  - Small group completion of Tasks 3(b), 4, 5(a–c)
  - Time permitting, begin small group work on Task 6a.
  - **Homework**: A complete formal write-up of Task 5(d) could be assigned, to be due at a later date (e.g., one week after completion of the in-class work).

- **Advance Preparation Work for Day 2**
  In Section 2, read pages 9–11, completing Tasks 6a and 7 for class discussion along the way.

- **Day 2 of Class Work**
  - Whole class and/or small group discussion of the assigned reading and related tasks in Section 2, to include comparison of answers to Task 6a and 7.
  - Small group work on Task 6b, and possibly also parts of Task 8.
    (Alternatively, all of Task 8 could be assigned as homework.)
  - Begin individual or small group reading of Dedekind excerpt on page 12, and also Task 9.
  - **Homework**: A complete formal write-up of Tasks 6(c-d) and some or all of Task 8 (especially e-f) could be assigned, to be due at a later date (e.g., one week after completion of the in-class work).

- **Advance Preparation Work for Day 3** (to be completed before class)
  Read (or re-read) Section 3, pages 12 –14, preparing notes for class discussion of Tasks 9 and 10.

- **Day 3 of Class Work**
  - Whole class and/or small group discussion of Tasks 9 and 10. Students' Reading Guide answers to some or all parts of these tasks could also be compared in small groups, or simply reviewed by the instructor after class.
  - Whole class discussion of definitions of prime and composite for Gaussian primes, with answers to Task 5(a -i) and Task 5(b-i) used as examples.
  - Small group work on the remainder of Task 12 and on Task 13.
    Note: *Recall that the answer to Task 13 is revealed in the Dedekind excerpt on page 15, so that group work on Task 13 needs to be completed before continued reading is assigned.*
  - **Homework**: A complete formal write-up of Task 11 should be assigned, to be due at a later date (e.g., one week after completion of the in-class work).

- **Advance Preparation Work for Day 4** (to be completed before class)
  In Section 3, read page 15 and complete class notes for discussion on some or all of Tasks 14 and 16(a).
- **Day 4 of Class Work**
  - Small group work on some or all of Task 14, Task 16(a), Task 16(b).
  - Time (and instructor interest) permitting, small group work on Task 17 and/or Task 18.
  - **Homework**: A complete formal write-up of student work on Task 14, should be assigned, to be due at a later date (e.g., one week after completion of the in-class work). Write-up of Tasks 15, 16(b), 16(c)and 18 is also recommended for homework. As desired, additional class time could be spent on small group work on some or all of these tasks before they are assigned for individual homework.

- **Advance Preparation Work for Day 5** (to be completed before class)
  In Section 4, read pages 18–19, and prepare notes along the way for class discussion of Task 19.
- **Day 5 of Class Work**
  - Small group work on Tasks 19 and 20.
  - Time permitting, small group work on one of the following: Task 20, 21, 22.
  - **Homework:** A complete formal write-up of student work on Tasks 18 and 19 could be assigned, to be due at a later date (e.g., one week after completion of the in-class work). Write-up of one or more of Tasks 20–22 is also recommended for homework. As desired, additional class time coulde be spent on small group work on some or all of these tasks before they are assigned for individual homework.

- **Advance Preparation Work for Day 6** (to be completed before class)
  In Section 4, read the Dedekind excerpt on page 21, and complete Task 23 for class discussion along the way. Also prepare some initial notes for class discussion of Task 24.
- **Day 6 of Class Work**
  - As needed, continued small group work on Tasks 18 and 19 from Day 5. This could be supplemented by a whole group discussion of these tasks, or by student presentations of their group's work, depending on the instructor's instructional preferences.
  - Small group work on Tasks 24.
  - Time permitting, small group work on one of the following: Task 20, 21, 22.
  - **Homework:** A complete formal write-up of student work on Task 24 could be assigned, to be due at a later date (e.g., one week after completion of the in-class work).

- **Advance Preparation Work for Day 7** (to be completed before class)
  In Section 5, read pages 22–26, completing work on the following for class discussion along the way: Task 25(b), Task 25(c), Task 26, Task 28
- **Day 7 of Class Work**
  - Summarizing whole group discussion of definition of norm in $\mathbb{Z}[\sqrt{-5}]$, and of the definition and examples of *decomposability* introduced on pages 25–26, including answer to Task 28(a). If an example different than the one given in the PSP on page 26 is desired, then the indecomposability of either $p = 3$ or $p = 7$ could be verified during this discussion.
  - Small group work on Task 29(a).
  - Time permitting, begin individual or small group reading of Dedekind excerpt and subsequent commentary on page 27. Small group work on Task 30(a) could also be started, depending on how much time is spent on the whole group summarizing discussion.
  - **Homework:** A complete formal write-up of Task 25(a) and Task 27 could be assigned, to be due at a later date (e.g., one week after completion of the in-class work).

- **Advance Preparation Work for Day 8** (to be completed before class)
  Complete reading of Section 5, pages 27–28, and prepare notes for discussion of Tasks 30(a) and 31. Also begin reading Section 6, pages 28–29; students should be asked to jot down one comment and one question about the Dedekind excerpt on page 29.
- **Day 8 of Class Work**
  - Small group work on Tasks 30 and 31, possibly supplemented by a whole group discussion of the ideas in Task 31.
  - Small group work on Task 32, possibly supplemented by a whole group discussion of these ideas. Student presentations of group answers to Task 32 could also be useful to consolidate the ideas discussed by Dedekind on page 29.
  - Time permitting, continue individual or small group reading of page 30, and begin small group discussion of Task 33.
  - **Homework:** Complete formal write-up of student answers to Task 31 could be assigned, to be due at a later date (e.g., one week after completion of the in-class work). A write-up of Task 30(b) could also be assigned if the instructor feels that further consolidation of these ideas is needed.

- **Advance Preparation Work for Day 9** (to be completed before class)
  Complete reading of Section 6, pages 30–24, and prepare notes for class discussion of a subset of Task 33 and of Task 34.
- **Day 9 of Class Work**
  - Small group discussion of Task 33.
  - Final summarizing whole class discussion of the concepts of ideal numbers / ideals and how these relate to the Prime Divisibility Property and the Unique Factorization Property.

Acknowledgments

The development of this student project has been partially supported by the Transforming Instruction in Undergraduate Mathematics via Primary Historical Sources (TRIUMPHS) Program with funding from the National Science Foundation's Improving Undergraduate STEM Education (IUSE) Program under grant number 1523494. Any opinions, findings, and conclusions or recommendations expressed in this project are those of the author and do not necessarily represent the views of the National Science Foundation.

For more information about TRIUMPHS, visit
`http://webpages.ursinus.edu/nscoville/TRIUMPHS.html`.

SAMPLE READING GUIDE

Background Information: The primary goal of this two-page reading and tasks assigned in this guide is to familiarize students with the historical and mathmatical background of the project, and to prepare them for in-class small group work on Tasks 1 – 5.

****

Reading Assignment - *Gaussian Integers PSP* - pp. 1–9 (with some omissions)

1. Read the *Introduction* on pages 1–3. *Questions or comments?*

2. In *Section 2*, read pages 3–4. Much of this should sound familiar! *Questions or comments?*

3. In preparation for class discussion, **complete Task 1 (page 4)**.
   This is reproduced below for your convenience.

   Task 1 This task examines the terminology used by Dedekind in the excerpt on page 4.

   (a) What did Dedekind mean by the term 'unit'? How many units are there in $\mathbb{Z}$?

   (b) What did Dedekind mean by the term 'unity'? What special properties are satisfied only by the unity? (Name at least two such properties.)

   (c) Notice that Dedekind explicitly excluded unity from the set of prime numbers. In fact, this exclusion dates back to Euclid's work, and remains in place today. Why do you think mathematicians do not consider unity to be a prime number? Is unity a composite number? Why or why not?

4. In *Section 2*, read the paragraph below Task 1 on page 5; then **prepare notes for class discussion of Task 2 (page 5)**, reproduced below for your convenience.

> **Task 2** This task examines Dedekind's description of the two theorems stated on page 5.
>
> Go back to read what Dedekind said about these two theorems towards the end of the first paragraph of the excerpt on page 4. Does his statements of these theorems differ in some way from the statements of each given above? If so, in what way(s)?
>
> What did Dedekind say is "the most important thing" when describing the first of these theorems? Explain why you think Dedekind considered this to be especially important.
>
> Also summarize what Dedekind said about how these two theorems are related.
> In particular, which of the two theorems depends on the other according to Dedekind?

5. In *Section 2*, read pages 5–6. *Questions or comments?*

6. **Check your understanding of divisibility of Gaussian integers by completing Task 3, part a**. .

> **Task 3(a)** Let $z = 9 + 8i$ and $w = 2 + 5i$.
> Show z is divisible by w by verifying that the quotient $\frac{z}{w}$ is a Gaussian integer. (To compute $\frac{z}{w}$, multiply by $\frac{\overline{w}}{\overline{w}}$, where $\overline{w} = 2 - 5i$ is called the *conjugate of* w.)

7. In *Section 2*, read page 7.

   Write at least one question or at least one comment about this part of the assigned reading.

8. **Discussion: complete Task 4, parts a and b** in preparation for class work.

   Task 4 This task explores the geometric meaning of the definition of the *norm* of a complex number $w = u + iv$, where $N(u + iv) = (u + iv)(u - iv) = u^2 + v^2$ for all $u, v \in \mathcal{R}$.

   (a) Begin by plotting the following complex numbers in the imaginary plane.
   Use the standard convention of plotting the real component on the horizontal axis and the imaginary component on the vertical axis.

   (i) $w = 3 + 4i$

   (ii) $x = -4 + 3i$

   (iii) $x = -3 + 4i$

   (iv) $x = 5 + 2i$

   (v) $x = -8 + 6i$

   (vi) $x = -2.7 + 4.6i$

   (b) Now compute the norm of each of the complex numbers in part (a).
   Describe how the norm of each number relates to their geometric placement.