Summer 2017

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

Janet Heine Barnett
Colorado State University-Pueblo, janet.barnett@csupueblo.edu

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

Janet Heine Barnett*

April 7, 2017

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 the 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 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

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

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 [5, 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.

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

[1] In *Men of Mathematics*, E. T. Bell tells the following amusing anecdote [1, 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."

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* [4]. Section 2 begins with Dedekind's description of the number theoretic properties of two sets of numbers: the set of integers, denoted $\mathbf{Z}$, and the set of Guassian integers, denoted $\mathbf{Z}[i]$. 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 $\mathbf{Z}$. In Section 3, we will delve deeper into the number theoretic properties satisfied by the Gaussian primes. We will then encounter, in Section 4, another number domain in which certain of these number theoretic properties break down. The mathematical after-effects of this 'break down' will then be briefly described in the concluding Section 5.

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 [4]. We begin with a short excerpt in which Dedekind reminded his readers of some basic integer properties. Notice that Dedekind uses 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 $\mathbf{Z}$, 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 the (1996) English translation of that monograph.

[3]For more details about Dedekind's development of ideal theory, see [7] or the preface to [4].

[4]The now-standard notation $\mathbf{Z}$ 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 *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]Notice that Dedekind used the word 'domain' here 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.

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

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

As Dedekind noted, the ideas in this excerpt were well-known at least since the time of Euclid. Of particular importance in what follows are the theorems mentioned at the end of the first paragraph:

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

Dedekind's interest in these particular theorems was due to their importance in nineteenth century efforts to determine the integer solutions of certain number theoretic equations. A famous example of such an equation appears in *Fermat's Last Theorem*, which states that the equation $x^n + y^n = z^n$ has no non-zero integer solutions for $n \geq 3$. Although the details of the connection go beyond this project, nineteenth century efforts to prove Fermat's Last Theorem for larger values of n turned out to be intimately connected with precisely the two theorems listed above.[10]

Another type of number theory problem related to these two theorems involved 'polynomial' congruence equations of the form $x^m \equiv p \pmod{q}$, where p and q are odd primes and $x, m \in \mathbf{Z}^+$. An especially famous result of this type is the *quadratic reciprocity law* which describes a reciprocal 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 proven in Gauss' important 1801 treatise on number theory, *Disquisitiones Arithmeticae*.[11] 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', are described in our next excerpt from Dedekind. Note especially Dedekind's assertion that both the *Unique Factorization Theorem* and the *Prime Divisibility of a Product Theorem* (stated above) hold in the set of Gaussian integers.

[9] This theorem is often called 'Euclid's Lemma' in the mathematical literature.

[10] See [8] for additional detail.

[11] 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 iff $x^2 \equiv q \pmod{p}$ is solvable.
If $q \equiv 3 \pmod{4}$, then $x^2 \equiv p \pmod{q}$ is solvable iff $x^2 \equiv -q \pmod{p}$ is solvable.

§ 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[12] 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 $\mathbf{Z}[i] = \{x + yi \,|\, x, y \in \mathbf{Z}\}$. Notice that both x and y must be rational integers here! Take a moment to verify Dedekind's assertion that the set $\mathbf{Z}[i]$ 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.

Task 1 This task looks at the divisibility relationship in $\mathbf{Z}[i]$. As in the set of rational integers, given $z, w \in \mathbf{Z}[i]$, we say that z is divisible by w (or that w divides z) if and only if there is some Gaussian integer $q \in \mathbf{Z}[i]$ 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.
Hint? The quotient $\frac{z}{w}$ can be computed using the conjugate of w.

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

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

Let's now continue to read Dedekind's description of the Gaussian integers:

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

§ 6. The complex integers of Gauss

One can establish very simply, as Dirichlet showed in a very elegant manner,[13] 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 detailed proofs, Dedekind has described the *mathematical tool* that Dirichlet used to prove that the *Unique Factorization Theorem* and the *Prime Divisibility of a Product Theorem* hold in $\mathbf{Z}[i]$ — namely, the existence of a *norm* for Gaussian integers which allows us to find a greatest common divisor of two Gaussian integers via Euclid's Division Algorithm. The omission of these details was intentional on Dedekind's part, since his focus in this paper was not the Gaussian integers per se. Since our own motivations for reading this paper relate to how number theory ideas about rational integers can be generalized to the Gaussian integers, let's pause in our reading of his text here to see how the norm of a complex integer is computed and used to find a greatest common divisor (gcd) of two Gaussian integers within an adaptation of Euclid's Division Algorithm.

Task 2 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.

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

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

Task 3 This task includes some computations and a proof related to Dedekind's claims concerning the 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 $w, q \in \mathbf{C}$, $N(wq) = N(w)N(q)$.

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

(c) For $q = -1.2 + 2.56i$, find a complex *integer* w such that $N(w - q) \leq 1/2$.

(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.

Let's now look at an example to see how to adapt the Euclidean algorithm for computing the gcd of two natural numbers in order to find a gcd of two Gaussian integers.

Example In this example, we let $z = 28 - 3i$ and $m = 1 + 5i$ and find $\gcd(z, m)$.

- *Step 1* Since $N(z) = 793 > 26 = N(m)$, 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:

$$\frac{z}{m} = \frac{28 - 3i}{1 + 5i} = \frac{28 - 3i}{1 + 5i} \cdot \frac{1 - 5i}{1 - 5i} = \frac{13 - 163i}{26} = \frac{13}{26} - \frac{163}{26}i$$

  Rounding this quotient to the nearest complex *integer*, we obtain $q_1 = 0 - 6i$. To obtain the corresponding remainder, we solve $z = q_1 m + r_1$ for r_1 to obtain:

$$r_1 = z - q_1 m = (28 - 3i) - (-6i)(1 + 5i) = -2 + 3i$$

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

  Note that $N(r_1) = 13 < 26 = N(m)$.
- *Step 2* We 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 $N(r_2) < N(r_1)$:

$$\frac{m}{r_1} = \frac{1 + 5i}{-2 + 3i} = \frac{1 + 5i}{-2 + 3i} \cdot \frac{-2 - 3i}{-2 - 3i} = \frac{13 - 13i}{13} = 1 - i$$

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

Having arrived at a zero remainder,[14] we now conclude that the sought-after gcd is the final non-zero remainder r_1; that it, $\boxed{\gcd(z, m) = -2 + 3i}$.

[14] Had we obtained a non-zero remainder in step 2, we would 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.

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:

$$m = \underbrace{(1-i)}_{q_2}\underbrace{(-2+3i)}_{r_1} \qquad z = \underbrace{(-6i)}_{q_1}\underbrace{(-2+3i)(1-i)}_{m} + \underbrace{(-2+3i)}_{r_1}$$

$$= [(-6i)(1-i)+1](-2+3i)$$

$$= (-5-6i)(-2+3i)$$

This verifies that $-2+3i$ is indeed a common divisor[15] of m and z.

Task 4 This task provides some additional examples of finding $\gcd(z,m)$ for $z, m \in \mathbf{Z}[i]$, using the adaptation of the Euclidean Algorithm for the Greatest Common Divisor illustrated in the last example.

(a) Let $z = 12-23i$ and $m = 7-5i$. Complete just the first step of the Euclidean gcd Algorithm by finding $q, r \in \mathbf{Z}[i]$ 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) Apply the Euclidean gcd 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 $m = 52+68i$

Looking back at the example above the last task, remember that we found $\gcd(z,m) = -2+3i$, where $m = (1-i)(-2+3i)$ and $z = (-5-6i)(-2+3i)$. But notice that we could also have written these factorizations as follows:

$$m = (1-i)(-2+3i) \qquad z = (-5-6i)(-2+3i)$$

$$= (1)[(1-i)(-2+3i)] \qquad = (1)[(-5-6i)(-2+3i)]$$

$$= (-i^2)[(1-i)(-2+3i)] \qquad = (-i^2)[(-5-6i)(-2+3i)]$$

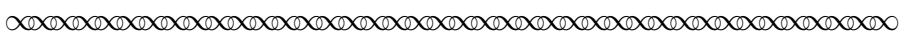
$$= \underbrace{(-1-i)}_{-i(1-i)}\ \underbrace{(-3-2i)}_{i(-2+3i)} \qquad = \underbrace{(-6+5i)}_{-i(-5-6i)}\ \underbrace{(-3-2i)}_{i(-2+3i)}$$

Since $N(-3-2i) = 13 = N(-2+3i)$, notice also that neither of the two Gaussian integers $-3-2i$ and $-2+3i$ is 'bigger' than the other when we use their norms to compare them. In

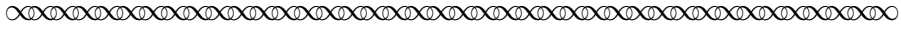
[15] The verification that $-2+3i$ is a *greatest* of the common divisors of z and m is less relevant to the questions we are studying in this section, and is thus postponed until Section 3.

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 Gaussian integers that can be considered to be a gcd of z and m is this example!

The situation we just described may seem disquieting at first ... until we remember that something similar occurs within the set of 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. 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[16]. This is because the four numbers 1, -1, i, $-i$ play a special role within the set of Gaussian integers. Notice in the next excerpt how Dedekind incorporated this special feature of the Gaussian integers into his definition of what it means for a complex 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 5 In this task, you will prove Dedekind's claim that ± 1 and $\pm i$ are the only units in $\mathbf{Z}[i]$.

(a) Explain why $N(\omega) \in \mathbf{Z}^+$ for every non-zero $\omega \in \mathbf{Z}[i]$.

(b) Now use part (a) and the fact that "the norm of a product is the product of the norms" to complete the following proof.

> Assume $u \in \mathbf{Z}[i]$ is a unit; that is, assume u is a divisor of 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!*

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

Notice how Dedekind's definition of a prime within the set of Gaussian integers $\mathbf{Z}[i]$ mirrors the definition of prime within the set of rational integers $\mathbf{Z}$. Intriguingly, numbers that are prime in the set $\mathbf{Z}$ may not be prime in the set $\mathbf{Z}[i]$. For example, it is possible to factor the number 2 within $\mathbf{Z}[i]$ as $2 = (1+i)(1-i)$; since neither $1+i$ nor $1-i$ is a unit in $\mathbf{Z}[i]$, the rational prime number 2 is thus *not* a prime complex integer!

On the other hand, the number 7 *is* a prime in $\mathbf{Z}[i]$. To see this, suppose that we factor 7 in $\mathbf{Z}[i]$ to obtain $7 = wq$ with $w, q \in \mathbf{Z}[i]$. 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 $u, v \in \mathbf{Z}$, 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 $w, q \in \mathbf{Z}[i]$ is to have either $N(w) = 1$ or $N(q) = 1$. This means that 7 is the product of two factors in $\mathbf{Z}[i]$ only if one of the factors (either w or q) is a unit, so that 7 is a prime number in the set of Gaussian integers. We can thus refer to 7 as both a *rational prime* and a *Gaussian prime*.

Task 6 This task examines ideas related to units and primes in the set of Gaussian integers. Recall from the previous excerpt that the norm of a product is the product of the norms. Use this fact to complete each of the following.

(a) Show that the following are NOT Gaussian primes; that is, that they are not primes in the set of Gaussian integers:

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

(b) Show that the following ARE Gaussian primes; that is, that they are primes in the set of Gaussian integers:

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

(c) Take a look back at 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

Make a conjecture about how to predict whether the complex integer $z = a + bi$ will be a Gaussian prime. Test your conjecture with a few more examples.

Hint? It may be useful to look at $N(z)$.

As you worked the previous task, you may have noticed a pattern in terms of 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 complex primes is a theorem in number theory that is known today as the *Two Square Theorem*:[17]

An odd prime p is the sum of two squares if and only if it 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 $\mathbf{Z}[\theta] = \{x + y\theta \mid x, y \in \mathbf{Z}\}$ for values of $\theta \neq i$. Before we leave the Gaussian integers to look at those other systems, we will first take a closer look in at what Dedekind had to say about prime factorization in $\mathbb{Z}[i]$ in Section 3. But first, let's close this section with some number theoretic tasks related to the Two Square Theorem.

[17]The number theoretic 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 in his correspondence with Mersenne and others to also have a proof, the first published proof was due to Leonhard Euler (1707-1783) in 1755. This history is further described in [6].

Task 7 This task examines some number theoretic consequences of the Two Square Theorem.

The Two Square Theorem only tells use which rational prime numbers can be written as a product of primes — but there are rational composite numbers of this form as well. For example, $50 = 7^2 + 1^2$. The following identity is useful for finding sum of square representations for certain composite numbers:

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

Note that this says that if we start with two rational integers m, n, both of which can be written as a sum of squares — say, $m = a^2 + b^2$ and $n = c^2 + d^2$ — then their product mn can also be written as a sum of squares.

(a) Use identity $(\star)$ 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 $N(zw) = N(z)N(w)$ for all $z, w \in \mathbb{Z}[i]$. Use this fact in order to prove that identity $(\star)$.

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

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

(d) Notice that $637 = (14)^2 + (21)^2$ *can* be written as the sum of squares ... even though the prime factorization of $45 = 7^2 \cdot 13$ includes the prime 7 which is NOT congruent to 1 (mod 4). Explore the conditions under which a composite number that includes primes $p \equiv 3 \pmod 4$ in its prime factorization can be written as a sum of squares.

Task 8 This task examines some number theoretic generalization of the Two Square Theorem. Using an identity similar to that given in Task 7, it is possible to prove that EVERY rational integer can be written as the sum of four squares.[18] The same, however, is not true for the sum of three squares.

(a) Collect some data to write a conjecture about which rational prime numbers p can be written as the sum of three squares; state it in the following form:
(i) If p satisfies _____, then p is a sum of three squares.
(ii) If p satisfies _____, then p is not a sum of three squares.

(b) Write a proof for part (ii) of your conjecture in part (a).
[You could also try to prove part (i), but that is quite difficult!]

[18]The first published proof of this theorem was given by the French mathematician J. L. Lagrange in 1770. 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 did prove the four square identity: $(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2)$ is equal to $(ax + by + cz + dw)^2 + (ay - bx - cw + dz)^2 + (az + bw - cx - dy)^2 + (aw - bz + cx - dx)^2$. It turns out that the four square identity is related to quarternions in much the same say that the two square identity is related to complex integers. Discovered in the 19th century by W. R. Hamilton, quarternions are 'imaginary' numbers of the form $a + bi + cj + dk$ subject to the non-commutative rules such as $ij = k = -ji$.

3 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 concerning Unique Factorization and the 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.

As we saw in Section 2, Dedekind's definition of a composite number implicitly defines a Gaussian prime as follows:

Definition Given $p \in \mathbb{Z}[i]$, we say that p is a Gaussian prime if and only if:

1. p is not a unit; and
2. For all $w, q \in \mathbb{Z}[i]$, if $p = wq$, then either w is a unit or q is a unit.

Notice also the second 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 short, the Prime Divisibility Property holds in the Gaussian integers! Tasks 9 and 10 examine this property further.

Task 9 This task proves that the Prime Divisibility Property holds in $\mathbb{Z}[i]$.

First, look at the proof of the Prime Divisibility Property in the set of rational integers $\mathbb{Z}$ in a modern Number Theory textbook. Then follow the outline below to adapt that proof to the Gaussian integers $\mathbb{Z}[i]$.

(a) Begin by proving the following lemma:

> *Lemma* Given $a, b \in \mathbb{Z}[i]$, if $x, y, g \in \mathbb{Z}[i]$ are such that $g = ax + by$ 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: The expression 'g has the least non-zero norm of all linear combinations of a and b' means that for all $z, w \in \mathbb{Z}[i]$, we have $0 < N(g) \leq N(az + bw)$.

Hint? To show that $g|a$, 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 use the given assumptions about g to prove that $N(r) = 0$.

(Task 9 continued)

(b) Apply the lemma from part (a) to complete the proof of the Prime Divisibility Property for Gaussian Integers:

Given $q, w \in \mathbb{Z}[i]$ and a Gaussian prime $p \in \mathbb{Z}[i]$ such that $p|qw$,
then either $p|q$ or $p|w$.

NOTE: Before applying the lemma in part (a) to a pair of Gaussian integers within your proof, be sure to carefully explain how to obtain $g, x, y \in \mathbb{Z}[i]$ with the properties required by the hypothesis of that lemma.

Task 10 This task examines the relationship between the definition of Guassian Prime given at the start of ths section and Prime Divisibility Property in $\mathbb{Z}[i]$.

In Task 9, you showed that the given definition of Guassian 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 $z \in \mathbb{Z}[i]$ satisfies the following property $(\star)$:

If $q, w \in \mathbb{Z}[i]$ are such that $z|qw$, then either $z|q$ or $z|w$. $(\star)$

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

At the end of the previous excerpt, Dedekind further asserted that Unique Factorization holds in $\mathbb{Z}[i]$. The last two tasks in this section examine this property of the Gaussian Integers further — in the next section, we will then see how it can break down in other number domains!

Task 11 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 never-the-less maintained that Unique Factorization holds in the Gaussian integers.

Task 12 This task examines the proof of Unique Factorization in $\mathbb{Z}[i]$.

Look back at the proof of Unique Factorization within the set of rational integers $\mathbb{Z}$ in a modern Number Theory text. Then adapt that proof to show that Unique Factorization 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.)

4 Uniqueness Lost?

In this section, we continue our reading of Dedekind's analysis of more general number domains. He began this analysis as follows.

§ **7. The domain**[19] **of numbers** $x + y\sqrt{-5}$

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 $\mathbf{Z}[\theta]$ 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 $\mathbf{Z}[i]$. 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 $\mathbf{Z}[\theta]$ 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 domain $\mathbf{Z}[\sqrt{-5}]$ 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 $\mathbf{Z}[\sqrt{-5}]$. 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** $\theta = \sqrt{-5}$.

[19]Recall from footnote number 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 today's notation $\mathbf{Z}[\theta]$ throughout this section of the project. The author apologizes for this historical anachronism, which has been committed in the interest of greater clarity for the reader.

On the other hand, this method 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[20] 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.

Task 13 This task examines properties of the domain $\mathbf{Z}[\theta] = \{x + y\theta \,|x, y \in \mathbf{Z}\}$, where $\theta = \sqrt{-5}$, mentioned by Dedekind in the previous excerpt.

(a) Verify Dedekind's claim that $\mathbf{Z}[\sqrt{-5}]$ is closed under addition, subtraction and multiplication. What is the additive identity of this set? What is the multiplicative identity of this set?

(b) Given $\omega \in \mathbf{Z}[\sqrt{-5}]$ with $\omega = x+y\theta$, $x, y \in \mathbf{Z}$, 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 $\mathbf{Z}[\sqrt{-5}]$.

(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 $\mu \in \mathbf{Z}[\sqrt{-5}]$ satisfies $N(\mu) = 1$.
Then explain why this implies that $\mathbf{Z}[\sqrt{-5}]$ contains only two units, $\mu = \pm 1$.

[20]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 14 This task provides computational practice in $\mathbf{Z}[\theta] = \{x + y\theta \,|\, x, y \in \mathbf{Z}\}$, where $\theta = \sqrt{-5}$. Given $z, m \in \mathbf{Z}[\theta]$, define $m|z$ in the usual way. Determine if $m|z$ for the following pairs.

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

Task 15 This task establishes another 'sum of squares' identity in the set of rational integers. Recall from Task 7 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 $u, v \in \mathbb{Z}$.

(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 $\mathbf{Z}[\theta]$.

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 number 2, 3, 7 cannot be represented in this way, as one sees from the theory of these forms,[21] 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.

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

Task 16 This task examines the ideas introduces by Dedekind in the previous excerpt.

(a) Write down the definitions of 'decomposable' and 'indecomposable' numbers given by Dedekind in this excerpt. Why do you think that 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 from what we saw in Section 3 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 are indecomposable in $\mathbb{Z}[\theta]$; we'll look at this further in a moment.]

Notice that Dedekind's discussion of the 'indecomposability' of the numbers listed in the previous excerpt is simply the first part of his description of the 'entirely new phenomenon' that occurs within $\mathbf{Z}[\sqrt{-5}]$. Before we read more about this phenomenon, let's pause to consider this list of numbers and the definition of 'indecomposable' more carefully. The fact that the numbers 2, 3, 7 are indecomposable in $\mathbf{Z}[\sqrt{-5}]$ may seem at first glance to need no proof ... after all, each of these numbers is prime (and therefore indecomposable) within the set of rational integers $\mathbf{Z}$. But remember the situation in the Gaussian integers $\mathbf{Z}[i]$, where 2 is *not* prime since $2 = (1-i)(1+i)$, and neither of these factors is a unit in $\mathbf{Z}[i]$.

Dedekind's argument concerning the indecomposability of rational prime numbers (e.g., 2, 3, 7) in $\mathbf{Z}[\sqrt{-5}]$ is thus not simply belaboring the obvious ... a proof really is needed. Let's consider the details of that proof[22] for just one specific value, $a = 2$. Arguing by contradiction, suppose that 2 is decomposable in $\mathbf{Z}[\theta]$. By definition of decomposable, this would give us non-units $\omega, \omega' \in \mathbf{Z}[\theta]$ such that $\omega\omega' = 2$. Taking the norm, we then have $N(\omega\omega') = N(2) = N(2 + 0\theta) = 2^2 + 5(0^2) = 4$, which in turn implies that $N(\omega)N(\omega') = 4$ (since the norm of the product is the product of the norms). 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 $\mathbf{Z}[\sqrt{-5}]$ is necessarily a non-negative rational integer ... do you see why?)* But this implies that there exist $x, y \in \mathbf{Z}$ 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 $\mathbf{Z}[\sqrt{-5}]$.

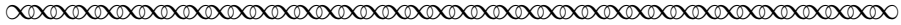
[22] You can check your understanding of the general proof simply by replacing '2' by 'p' (and $2^2 = 4$ by p^2), where p is an arbitrary prime, throughout this paragraph.

Task 17 This task proves the indecomposability of two other numbers in $\mathbf{Z}[\theta]$, where $\theta = \sqrt{-5}$.

(a) Let $b_1 = -2 + \theta$. Assume that b_1 is decomposable in $\mathbf{Z}[\theta]$, so that $b_1 = \omega\omega'$ for some non-units $\omega, \omega' \in \mathbf{Z}[\theta]$. 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 $x + iy \in \mathbf{Z}[\theta]$, to derive a contradiction.

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

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' with respect to divisibility within $\mathbf{Z}[\sqrt{-5}]$.



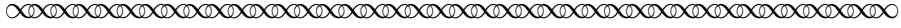
However, despite the indecomposability of these fifteen numbers, there are numerous relations between their products , which can all be deduced from the following.

$$(1) \qquad ab = d_1 d_2, \qquad b^2 = b_1 b_2, \qquad ab_1 = d_1^2$$

$$(2) \qquad ac = e_1 e_2, \qquad c^2 = c_1 c_2, \qquad ac_1 = e_1^2$$

$$(3) \qquad bc = f_1 f_2 = g_1 g_2, \quad af_1 = d_1 e_1, \quad ag_1 = d_1 e_2$$

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 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 $\mathbf{Z}[\sqrt{-5}]$! 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 $\mathbf{Z}[\sqrt{-5}]$, 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 factor 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), so that it makes sense to give it some special designation (i.e., 'indecomposable').

Task 18 This task further examines the failure of the *Prime Divisibility Property* in $\mathbf{Z}[\sqrt{-5}]$.

(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 $\mathbf{Z}[\sqrt{-5}]$.

(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 $\mathbf{Z}[\sqrt{-5}]$.

Task 19 This task asks you to reflect on the meaning and status of the *Unique Factorization Property* in $\mathbb{Z}[\theta]$, where $\theta = \sqrt{-5}$.

Begin by looking again at the equalities listed in (1), (2) and (3) of the previous excerpt.

Look back also at your answer to Task 12 in Section 3, 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 $\mathbb{Z}[\theta]$?
- How do these problems relate to the fact that the Prime Divisibility Property fails to hold in $\mathbb{Z}[\theta]$?
- Is there some portion or variation Unique Factorization Property that we *can* prove within $\mathbb{Z}[\theta]$, 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 $\mathbb{Z}[\theta]$ so that it does make sense to talk about the the Unique Factorization Property for this domain?

5 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 $\mathbf{Z}[\theta]$, 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 equations (1), (2) and (3) referenced in Dedekind's computations below and on the next page are given in the last Dedekind excerpt of Section 4 (page 20).

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[23]

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

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

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

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

[23]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

$$a = \mu\alpha^2, \;\; b_1 = \mu_1\beta_2^1, \;\; b_2 = \mu_2\beta_2^2,$$

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

$$a = \mu\alpha^2, \;\; b_1 = \mu\beta_2^1, \;\; b_2 = \mu\beta_2^2.$$

Forming products of these, we get

$$d_1^2 = ab_1 = \mu^2\alpha^2\beta_1^2 \;\Rightarrow\; d_1 = \mu\alpha\beta_1,$$

$$d_2^2 = ab_2 = \mu^2\alpha^2\beta_2^2 \;\Rightarrow\; d_2 = \mu\alpha\beta_2,$$

$$b^2 = b_1b_2 = \mu^2\beta_1^2\beta_2^2 \;\Rightarrow\; b = \mu\beta_1\beta_2,$$

which completes the proof of the decompositions claimed by Dedekind.

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 $\mathbf{Z}[\theta]$, 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.

Task 20 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:

> 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 $\mathbf{Z}[\theta]$, 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.

In particular, what properties will α, β_1, β_2, γ_1, γ_2 need to satisfy if they are, in fact, prime numbers?

(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 paper, Dedekind went on to analyze the divisibility properties of the number 2 in the domain $\mathbf{Z}[\theta]$ 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 $\mathbf{Z}[\theta]$, 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 $\mathbf{Z}[\theta]$ 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'll look more at Dedekind's fifth claim in a moment. First, check your understanding of the first four claims concerning the actual and ideal primes in $\mathbf{Z}[\theta]$ by completing Task 21.

Task 21 This task looks at Dedekind's claims concerning actual and ideal primes in $\mathbb{Z}[\theta]$, where $\theta = \sqrt{-5}$.

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

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

(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.

$$437 \ , \ 817 \ , \ 2021 \ , \ 22\theta \ , \ 29 + 58\theta \ , \ 33 + 44\theta$$

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 Fundamental Theorem of Arithmetic back to $\mathbb{Z}[\theta]$! The key to this proof is something that we previously encountered in Task 13 of Section 4. 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 of this claim:

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 we are reading. 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 ω that lie inside the set $\mathfrak{a}$ itself. Dedekind's motivation for this stronger property 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 the 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 22 This tasks looks briefly at how the definition of an ideal relates to the integer divisibility properties.

Complete the following restatements of properties 1 and 2 for divisibility by the 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 here, relate to Dedekind's 'two fundamental properties' I and II for the principal ideal $\mathfrak{a}$ that corresponds to the number μ. How are these two pairs of properties the same? How are they different?

Having arrived at the definition of an ideal brings this project to the end of our number theoretic study of Dedekind's paper. Dedekind himself went on 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 also introduced notions such as the least common multiple and greatest common divisor of two ideals. He then went on define and study several special types of ideal. These included sets known as *principal ideals*, which correspond to the actual number in the underlying integer domain, and also sets known as *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 topic initially motivated by the simple desire to maintain the Unique Factorization property when studying integer domains!

References

[1] Bell, Eric Temple, *Men of Mathematics*, Simon and Schuster, New York, 1937.

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

[3] Corry, Leo *Modern Algebra and the Rise of Mahtematical Structures*, second revised edition, Birkhäuser, Basel, 2004.

[4] Dedekind, Richard. *Theory of Algebraic Integers*, J Stillwell (translator & editor), Cambridge University Press, New York, (first published in French in 1877), English Translation 1996.

[5] Dedekind, Richard, *Essays on the Theory of Numbers*, Beman, (translator), The Open Court Publishing Company, Chicao, (first published in German in 1888), English transalation 1901.

[6] Dickson, Leonard Eugene, *History of the Theory of Numbers*, Volume II, Dover, Mineola MN, (first published in 1919), Dover Reprint 2005.

[7] Edwards, H. M., The Genesis of Ideal Theory, *Archives for the History of the Exact Sciences*, 15, 1980, 8–17.

[8] Kleiner, Israel, The Roots of Commutative Algebra in Algebraic Number Theory, in *Who Gave you the Epsilson? & Other Tales of Mathematical History*, M Anderson, V Katz & R Wilson (editors), Mathematical Association of America, Washington DC, 2009, 299–308.