Examples of Units and Primes in Some Integral Domains

William Gasarch, Samuel Wang, Owen Shu, Shriram Masanam, Sumedh Vangara

August 2026

Introduction

Understanding units and primes in an integral domain is essential for analyzing its structure and properties. In this paper, we explore the characterization of such elements across several integral domains.

Definitions and Examples

Integral Domains

Definition. An integral domain is a set $\mathbb{D}$ with two operations $+, \times$ where

- $+, \times$ are commutative, associative, and distributive.
- There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.
- There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x \times 1 = x]$.
- For all $x \in \mathbb{D}$ there exists $-x \in \mathbb{D}$ such that $x + (-x) = 0$.

Units

Definition. Let $\mathbb{D}$ be an integral domain. A unit is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$.
Let $\mathbb{U}$ be the set of units.

Primes

Definition. A prime is a $p \in \mathbb{D}$ such that if $p \mid ab$ then $p \mid a$ or $p \mid b$.
Note: primes p and q are equivalent if there exists $u \in \mathbb{U}$ such that $p = uq$.

Irreducibles

Definition. An irreducible is a $p \in \mathbb{D}$ such that if $p = ab$ then $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
Let $\mathbb{I}$ be the set of of irreducibles.

When Primes and Irreducibles are the Same

All primes are irreducibles but not all irreducibles are primes.

Unique Factorization Domains

Definition. An integral domain $\mathbb{D}$ is called a Unique Factorization Domain (UFD) if

- every element of $\mathbb{D}$ that is neither 0 or a unit can be factored into a product of a finite number of irreducibles
- if $p_1p_2 \cdot \ldots \cdot p_r$ and $q_1q_2 \cdot \ldots \cdot q_s$ are two factorizations of the same element of $\mathbb{D}$ into irreducibles, then $r = s$, and after reordering the indices, each p_i is an associate of q_i.

Euclidean Domains

Definition. A domain $\mathbb{D}$ is called a Euclidean domain if there exists a function

$$v : \mathbb{D} \setminus \{0\} \to \mathbb{N}$$

such that the following conditions are satisfied:

- for all $a, b \in \mathbb{D}$ with $b \neq 0$, there exists $q, r \in \mathbb{D}$ such that $a = bq + r$, where either $r = 0$ or $v(r) < v(b)$
- for all $a, b \in \mathbb{D} \setminus \{0\}, v(a) \leq v(ab)$

$\mathbb{Z}[\sqrt{-k}]$ is a UFD

Let $\mathcal{P}$ denote the primes and Irr denote the irreducibles, for problems 1, 2, and 3. Furthermore, for $x \in \mathbb{Z}[\sqrt{-k}]$, let $N(x) = x \times \overline{x}$, where $\overline{x}$ is the complex conjugate of x. We prove that $\mathbb{Z}[\sqrt{-k}]$ is a Euclidean Domain, and thus a UFD, if $k \leq 2$. We start with some lemmas.

Lemma 0.1
In $\mathbb{Z}[\sqrt{-k}]$ for $k > 0$, every multiple by an element of $\mathbb{Z}[\sqrt{-k}]$ of the number $x + y\sqrt{-k}$ can be written in the form $a(x + y\sqrt{-k}) + b(-ky + x\sqrt{-k})$ for $a, b \in \mathbb{Z}$.

Proof. Note that any multiple by an element of $\mathbb{Z}[\sqrt{-k}]$ of $x + y\sqrt{-k}$ can be written in the form $(a + b\sqrt{-k})(x + y\sqrt{-k})$ for $a, b \in \mathbb{Z}$ by definition of a multiple. We then have

$$\begin{aligned}(a + b\sqrt{-k})(x + y\sqrt{-k}) &= ax + ay\sqrt{-k} + bx\sqrt{-k} - byk \\ &= a(x + y\sqrt{-k}) + b(-ky + x\sqrt{-k})\end{aligned}$$

□

Thus, by Lemma **??**, every multiple of $x \in \mathbb{Z}[\sqrt{-k}]$ can be written as a sum of integer multiples of x and $x\sqrt{-k}$. We make the following claim:

Lemma 0.2
Multiples of $x \in \mathbb{Z}[\sqrt{-k}]$, when plotted in the complex plane, form a rectangular array (possibly tilted) formed of rectangles with side length $\sqrt{N(x)}$, $\sqrt{kN(x)}$.

Proof. Note that we already proved that the multiples of x have x and $\sqrt{-k}x$ as their basis. Thus, it suffices to prove that x and $x\sqrt{-k}$ are orthogonal in the complex plane and have the stated magnitudes. But this is true since $x\sqrt{-k} = x \times i \times \sqrt{k}$, and it's well known that multiplication by i corresponds to 90° rotation in the complex plane.

Furthermore, in the complex plane, the norm of x is $\sqrt{N(x)}$, and since norm is multiplicative, the norm of $x\sqrt{-k}$ is $\sqrt{kN(x)}$. Thus, since the set of multiples of x has orthogonal basis vectors of lengths $\sqrt{N(x)}$ and $\sqrt{N(x)k}$, it must be a rectangular grid of $\sqrt{N(x)}$ by $\sqrt{N(x)k}$ rectangles. □

With these two lemmas in mind, we now claim that for $k \le 2$, $\mathbb{Z}[\sqrt{-k}]$ is a Euclidean Domain using the norm N.

Lemma 0.3

Letting $v(x)$ (from the Definition of a Euclidean Domain) be $N(x)$, we claim that $\mathbb{Z}[\sqrt{-k}]$ is a Euclidean Domain using the norm N for $k \le 2$.

Proof. First, we check that the domain of $N(x)$ is all $x \in \mathbb{Z}[\sqrt{-k}]$, and the range is the nonnegative integers (since $N(a + b\sqrt{-k}) = a^2 + b^2k \in \mathbb{Z}^{\ge 0}$.

Now, we prove that for all $a, b \in \mathbb{Z}[\sqrt{-k}]$, $\exists q, r \in \mathbb{Z}[\sqrt{-k}]$ such that $a = qb + r$, $N(r) = 0$ or $N(r) < N(b)$.

Consider any such (a, b), and plot both a and the set of multiples of b in the complex plane. Note that by Lemma **??**, the multiples of b form a grid of rectangles with side lengths $\sqrt{N(b)}$ and $\sqrt{kN(b)}$. Note that a must lie on the boundary or in the interior of one of these rectangles; Call that rectangle W.

We now prove that there exists q, r satisfying $a = qb + r$, $r = 0$ or $N(r) < N(b)$. Consider the vertex kb of W such that $N(a - kb)$ is minimized. If this is 0, then a is a multiple of b, so $r = 0$ and we're done.

Otherwise, suppose $N(a - kb) \neq 0$. Note that this is just the euclidean distance between a and kb in the complex plane. Since a lies in the rectangle W, this minimum distance of a to one of the vertices of the rectangle is minimized when a is in the center of the rectangle. In this case,

$$N(a - kb) = \left|\frac{b}{2}\right|^2 + \left|\frac{b\sqrt{-k}}{2}\right|^2 = \frac{N(b)}{4} + \frac{kN(b)}{4}$$

So we have $N(a - kb) < N(b) \iff \frac{k+1}{4}N(b) < N(b) \iff k \le 2$. □

Note that for $k \ge 3$, this norm N does not give the Euclidean-domain argument above. Intuitively, this is because as we choose a b with an arbitrarily large magnitude, we can choose an $a \in \mathbb{Z}[\sqrt{-k}]$ arbitrarily close to the center of one of the rectangles of the grid of multiples of b, and then we'll have $\frac{k+1}{4}N(b) \not< N(b)$. This only shows that this particular norm does not work; it does not prove that $\mathbb{Z}[\sqrt{-k}]$ cannot be a Euclidean domain with respect to some other Euclidean function.

Problem 1: Find all units in $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

We must find all x such that $N(x) = -1$ or 1, since

$$N(x) \in \{-1, 1\} \quad \text{if } x \in \mathbb{U}.$$

The norm is

$$N(x) = x\overline{x} = a^2 - 2b^2.$$

Also, note that $N(x)$ is multiplicative. Consider $x = 1 + \sqrt{2}$. Then

$$N(x) = 1 - 2 = -1,$$

so x is a unit. Then, since $N(x)$ is multiplicative, numbers of the form $\pm(1+\sqrt{2})^k$ and their conjugates will also satisfy $N(x) = -1$ or 1. And these are all the units in $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

If there were another unit u, then for some k,

$$(1+\sqrt{2})^k < u < (1+\sqrt{2})^{k+1}.$$

Multiplying by the inverse of $(1+\sqrt{2})^k$, we would obtain

$$1 < u(1+\sqrt{2})^{-k} < 1 + \sqrt{2},$$

but no other number in $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ exists between 1 and $1 + \sqrt{2}$.

Problem 2: Find all units and primes in the algebraic integers.

Let I denote the set of algebraic integers.

Characterization of the Units:

We start with a definition.

Definition 0.4. We define the **norm** $N(x)$, $N : I \to \mathbb{Z}$ of an Algebraic Integer to be the product of all the roots of its unique minimal polynomial. In particular, $N(x)$ is multiplicative.

This definition comes from Galois theory, though we can prove, using basic methods, that the minimal polynomial is unique.

Lemma 0.5

The minimal polynomial (monic) of an algebraic integer is unique

Proof. Suppose FTSOC we have monic polynomials $f(x)$ and $g(x)$, such that for some algebraic integer α, $f(\alpha) = g(\alpha) = 0$, and the degrees of f and g are minimal.

Since $\mathbb{Z}[x]$ is a Euclidean Domain with norm being the degree of the polynomial, consider dividing f by g. Let $f(x) = q(x)g(x) + r(x)$. Then, we must also have $f(\alpha) = q(\alpha)g(\alpha) + r(\alpha) \implies 0 = r(\alpha)$, so α must also be a root of the monic polynomial $r(x)$. But by definition of an ED, $\deg(r(x)) < \deg(f(x))$, contradiction. □

We prove the following lemma.

Lemma 0.6

$x \in I$ is a unit only if $N(x) \in \{-1, 1\}$

Proof. First, note that $N(1) = 1$, since the minimal polynomial of 1 is $x - 1$, whose product of roots is simply 1.

Now, suppose for some $x \in I$, $\exists y \in I$ such that $xy = 1$. Then, taking the norm of both sides, we have

$$xy = 1 \implies N(xy) = N(1)$$

$$\implies N(x)N(y) = 1$$

But since the range of $N(x)$ is the integers, and the only unit integers are ± 1, we must have $N(x) \in \{-1, 1\}$. □

Lemma 0.7

$x \in I$ is a unit if $N(x) \in \{-1, 1\}$

Proof. Equivalently, it suffices to prove that for all $u \in I$ such that $u \neq 0$, if $|N(u)| = 1$ then $\frac{1}{u} \in I$.

Consider the unique minimal polynomial $P(x)$ of u. Note that its constant term must be (by Vieta's formulas, since by definition of norm the product of its roots must be ± 1) ± 1. Let

$$\deg(P(x)) = d$$

Now, consider the polynomial

$$Q(x) = x^d P(\frac{1}{x})$$

Note that this polynomial is essentially $P(x)$, but with the coefficients of the x^k and x^{d-k} terms swapped for all k. Then, since the coefficient of the constant term of $P(x)$ was ± 1, then so must the leading coefficient of $Q(x)$.

Now, let

$$R(x) = a_d Q(x)$$

where a_d is the leading coefficient of $Q(x)$. Note that $R(x)$ must then be monic, since if the leading coefficient of $Q(x)$ was 1, that of $R(x)$ remains unchanged, whereas of the leading coefficient of $Q(x)$ was -1, that of $R(x)$ must be flipped to 1.

We claim that $\frac{1}{u}$ is a solution to $R(x)$. Note that

$$R(\frac{1}{u}) = a_d Q(\frac{1}{u})$$

$$= a_d \left(\frac{1}{u}\right)^d P(u)$$

$$= 0$$

Thus, $\frac{1}{u}$ is an algebraic integer. □

Thus, we have proven that $x \in I$ is a unit if and only if $N(x) \in \{-1, 1\}$.

Characterization of the Primes:

We claim that there are no primes in I.

Lemma 0.8

For any $x \in I$, $\sqrt{x} \in I$

Proof. Let $P(x)$ be the minimal polynomial of x. Then, consider the monic polynomial $P(x^2)$. Note that $\sqrt{x}$ is a solution to $P(x^2)$, so $\sqrt{x} \in I$. □

Lemma 0.9

For any $x \in I$, $x^2 \in I$

Proof. This comes simply from the fact that I is closed under multiplication. □

We now prove that there are no primes in I. Suppose FTSOC that some $p \in I$ was prime. Then, knowing that $\sqrt{p} \in I$ by Lemma **??**, we have

$$p = \sqrt{p} \times \sqrt{p} \implies p \mid \sqrt{p} \implies \frac{\sqrt{p}}{p} = \frac{1}{\sqrt{p}} \in I$$

But then by Lemma **??**, we have

$$\frac{1}{\sqrt{p}} \in I \implies \frac{1}{p} \in I$$

Since both p and $\frac{1}{p} \in I$, p must be a unit, contradiction.

Problem 3: Find all units and primes in the set of rational numbers whose denominators are not divisible by a prime p.

Note that the inverse of a/b is b/a, so in order for the inverse of a number to be in that set (i.e., for it to be a unit), p must also not divide its numerator. Thus, the units are $\frac{a}{b}$ where $p \nmid a, b$.

Note also that in this set, x divides y iff $\nu_p(x) \leq \nu_p(y)$. Now, consider any potential prime q. Then we must have that for all a, b,

$$\nu_p(q) \leq \nu_p(a) + \nu_p(b)$$

which implies

$$\nu_p(q) \leq \nu_p(a) \quad \text{or} \quad \nu_p(q) \leq \nu_p(b).$$

Which is true only when $\nu_p(q) = 1 \quad \text{or} \quad \nu_p(q) = 0$. We drop the latter case, since a prime is defined not to be a unit. Thus, primes are just numbers such that p fully divides their numerator.

However, we consider two primes p and q equivalent if there exists a unit u such that $p = uq$.

Thus, the only prime in this set is p itself.