Integral Domains and Fermat's Two Squares Theorem

Tahseen Rabbani

University of Virginia

November, 2014

1 Integral Domains

The purpose of this paper is to discuss various properties and classes of integral domains, such as principal ideal domains (PID's), unique factorization domains (UFD's), and Euclidean domains. We will eventually use these concepts to prove Fermat's Two Squares Theorem.

Definition 1.1 *Let R be a commutative ring. We call R an **integral domain** if whenever $ab = 0$ for $a, b \in R$, then either $a = 0$ or $b = 0$. A nonzero $c \in R$ is called a **unit** if it has a multiplicative inverse.*

Throughout this paper, we shall assume any ring R is an integral domain, unless stated otherwise.

Of course, if every nonzero element of R is a unit, then R is a field, and every field is identifiable as an integral domain. Thus, subrings of fields are integral domains.

A typical example of an integral domain is $\mathbb{Z}$, whose units are ± 1. In fact, integral domains are considered generalizations of $\mathbb{Z}$, and as such, we may investigate how well-behaved divisibility and factorization are in these rings. Some other examples of integral domains:

- $R[x]$, for R an integral domain.
- The subring of $\mathbb{R}$, $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}, n \in \mathbb{Z}^+\}$.
- The subring of $\mathbb{C}$, $\mathbb{Z}[i\sqrt{n}] = \{a + bi\sqrt{n} \mid a, b \in \mathbb{Z}, n \in \mathbb{Z}^+\}$
- $\mathbb{Z}/p\mathbb{Z}$ for p prime.

For an interesting consequence, we consider those integral domains which are Artinian.

Definition 1.2 *A ring is **Artinian** if it satisfies the descending chain condition (DCC) on ideals, meaning for any (infinite) chain of ideals*

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$$

stabilizes, i.e., there is some positive integer n such that $I_n = I_{n+1} = I_{n+2} = \dots$

Proposition 1.3 *If R is an Artinian integral domain, then R is a field.*

Proof. Let nonzero $x \in R$ and consider the chain of ideals,

$$(x) \supseteq (x^2) \supseteq \dots$$

which stabilizes. Hence, $(x^{n+1}) = (x^n)$ for some n, which implies that $x^n = rx^{n+1}$ for some $r \in R$. So, $1x^n = (rx)x^n$ which means that either $rx = 1$ or $x^n = 0$. However, the latter is not possible since R is an integral domain. Thus, $rx = 1$, so x is a unit. ■

There is one last relation between integral domains and fields we would like to establish.

Theorem 1.4 *If R is a finite integral domain, then R is a field.*

This is a special case of Wedderburn's Little Theorem, which states that any finite "domain" is a field. A domain is a ring which possesses the same key property as integral domains, but it can be non-commutative.

Definition 1.5 *For $a, b \in R$, we say a divides b, denoted $a \mid b$, if there exists some $c \in R$ such that $b = ac$.*

This is a generalization of division in the integers.

Definition 1.6 *A nonzero, non-unit $u \in R$ is **irreducible** if whenever $u = ab$ for $a, b \in R$, we have that a or b is a unit. For a nonzero, non-unit $p \in R$, we say p is **prime** if whenever $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Lemma 1.7 *If $p \in R$ is prime then p is irreducible.*

Proof. Let $p = ab$. Without loss of generality, let $p \mid a$. Then, $a = pc$ for some $c \in R$. So, $p = ab = pcb$, hence $cb = 1$, so b is a unit. ■

The converse of this lemma, however, is not true. For example, consider $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}, n \in \mathbb{Z}^+\}$. We have that $2 \mid 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, but 2 does not divide either factor since $\frac{1}{2} \pm \frac{1}{2}i\sqrt{5} \notin \mathbb{Z}[i\sqrt{5}]$. There is also something interesting to note about this example: 6 does not have a unique factorization in this ring! We will have more to say about this property later on. First, we will consider the conditions under which irreducible and prime elements of an integral domain are equivalent.

1.1 Principal Ideal Domains

Definition 1.8 *An **ideal** is principal if it is generated by a single element $a \in R$. If every ideal of R is principal, then we call R a **principal ideal domain** (PID).*

In a PID, we have a concrete ring-theoretic notion of a greatest common divisor (gcd). Let R be a PID and $a, b \in R$. We have then that $(a, b) = (c)$ for some $c \in R$. First of all, this implies $c \mid a$ and $c \mid b$ and write $c = ar + bs$ for some $r, s \in R$. Thus, every common factor of a and b will also divide c. Thus, c satisfies the definition of a gcd of a and b.

Theorem 1.9 *In a PID, irreducible elements are prime.*

Proof. Let R be a PID, $p \in R$ irreducible. Suppose $p \mid ab$ and without loss of generality, assume $p \nmid b$. We will show that $p \mid a$. We have that $(p, b) = (c)$ for some $c \in R$, so $c \mid p$. Since p is irreducible, c is either a unit or $c = pu$ for some unit u. In the latter case, we have that $(p, b) = (c) = (p)$. However, this implies that $b \in (p)$, so $p \mid b$, which contradicts our assumption.

So c is a unit and without loss of generality, we may assume that $c = 1$. We may write $1 = rp + sb$ for some $s, r \in R$. Multiplying by a on both sides, we have that $a = rpa + sba$. Since p divides both terms on the RHS, $p \mid a$. ∎

Proposition 1.10 *$\mathbb{Z}$ is a PID.*

Proof. Let $I \subseteq \mathbb{Z}$ be an ideal. If $I = \{0\}$ then $I = (0)$, so it is principal. So assume I is nonzero and let $0 \neq n \in R$. We may multiply by ± 1 to obtain an element $n > 0$. By the well-ordering principle, we can find a smallest positive integer $j \in I$. We will show that $I = (j)$.

Clearly $(j) \subseteq I$. Now let $a \in I$. By the division algorithm, we can write $a = qj + r$ for $0 \leq r < j$. Since $j \in I$, we have that $qj \in I$, thus, $r = a - qj \in I$. If r is nonzero, then $0 < r < j$, which contradicts the minimality of j, thus $r = 0$, and $a = qj$. Hence, $a \in (j)$ giving us the other inclusion, so $I = (j)$. ∎

It is important to note that polynomial rings over PID's are not always PID's. For instance, $\mathbb{Z}[x]$ is not a PID since $(2, x)$ (among other example) is not principal.

Definition 1.11 *A ring is **Noetherian** if it satisfies the ascending chain condition (ACC) on ideals, meaning any (infinite) chain of ideals*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

stabilizes, i.e., there is some positive integer n such that $I_n = I_{n+1} = I_{n+2} = \dots$

Proposition 1.12 *If R is a PID then R is Noetherian.*

Proof. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals in R. Set

$$I = \bigcup_{i=1} I_i.$$

Clearly, I is an ideal. Since R is a PID, $I = (k)$ for some $k \in R$, so $k \in I_n$ for some n. Hence, $(k) \subseteq I_n$. Now, $I_n \subset I = (k)$, so $I_n = I$, hence for all $N \geq n$, $I_N = I$. ∎

1.2 Unique Factorization Domains

Definition 1.13 *We say R is a **unique factorization domain** (UFD) if every nonzero $n \in R$ can be written uniquely (up to re-ordering) as*

$$n = u \prod {p_i}^{\alpha_i}$$

for u a unit, α_i nonzero, and p_i irreducible.

By the Fundamental Theorem of Arithmetic, $\mathbb{Z}$ is a UFD. Going back to our earlier example, $\mathbb{Z}[i\sqrt{5}]$ is not a UFD, since we have $6 = 2\cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$. These are two different factorizations, since the only units in this ring are ± 1 and $2, 3, 1+i\sqrt{5}, 1-i\sqrt{5}$ are irreducible (which we will not show here). In general, determining whether an integral domain is a UFD through factorial arguments alone is not an easy endeavor. However, we have a useful relation between PID's and UFD's.

Theorem 1.14 *If R is a PID then R is a UFD.*

Proof. See [2] §8.3, Theorem 14. ∎

As an example, we will show that a polynomial ring over a field is a UFD.

Proposition 1.15 *Let F be a field. Then $F[x]$ is a UFD.*

Proof. Let I be an ideal of $F[x]$. If $I = 0$ then $I = (0(x))$, the zero polynomial. Now let I be nonzero, so we can choose a polynomial $k(x) \in I$ of minimal degree. For $g(x) \in F[x]$, we have by polynomial long division that $g(x) = q(x)k(x) + r(x)$, for some $q(x) \in F[x]$ and $\deg(r(x)) < \deg(k(x))$. Rewriting $r(x) = -q(x)k(x) + g(x)$, we have that $r(x) \in I$ and by the minimality of $\deg(k(x))$, $r(x) = 0(x)$, so $k(x) \mid g(x)$. Thus, $g(x) \in I$ and $(k(x)) = I$, so $F[x]$ is a PID and a UFD by the above theorem. ∎

We also have that if R is a UFD, then so is $R[x]$, but these are not always PID's. For example, $\mathbb{Z}[x]$ is a UFD, but not a PID. In fact, $R[x]$ is a PID if and only if R is a field.

1.3 Euclidean Domains

Definition 1.16 *A commutative ring R, not necessarily an integral domain, is* ***Euclidean*** *if there exists a function (norm) $N : R \setminus \{0\} \to \mathbb{Z}^+ \cup \{0\}$ such that*

1. *If a, $b \in R$ and $ab \neq 0$ then $N(a) \leq N(ab)$ and*

2. *If a, $b \in R$ and $b \neq 0$ then there exists $q, r \in R$ such that $a = qb + r$ with $N(r) < N(b)$.*

If R is an integral domain, we call it a ***Euclidean domain****.*

Essentially, a Euclidean ring is endowed with a division algorithm. Some examples of Euclidean domains are the following,

- $\mathbb{Z}$ with $N(a) =\mid a \mid$, the standard absolute value.

- For F a field, $F[x]$ with $N(f(x)) = \deg(f(x))$

- $\mathbb{Z}[i]$ with $N(a+bi) = a^2 + b^2$.

The last item, in particular, will be important to proving Fermat's Two Squares Theorem, and we will prove that function defined is indeed a norm.

Theorem 1.17 *If R is a Euclidean domain then R is a PID.*

Proof. Let R be a Euclidean domain and I a nonzero ideal. By the well-ordering principle, there is a nonzero element d of minimum norm. We will show that $(d) = I$.

We that have $(d) \subseteq I$. Now let $a \in I$. Using the division algorithm, we have that $a = qd + r$ with $r = 0$ or $N(r) < N(d)$. Since $a - qd = r \in I$, and by the minimality of $N(d)$, we have that $r = 0$ and $a = qd \in (d)$. So $I \subseteq (d)$ and $I = d$. ∎

The converse of this theorem is not true, however. The ring

$$R = \{a + b\frac{1+\sqrt{-19}}{2} \mid a, b \in \mathbb{Z}\}$$

is a PID, but not a Euclidean domain. For a (fairly long) proof of this, see [1]. For a non-Euclidean ring, we give an example borrowed from [3].

Definition 1.18 *Let K and F be fields. If F is a subfield of K, we call K an* ***extension field*** *of F. The extension fields of $\mathbb{Q}$ are referred to as* ***number fields****.*

Well-known extension fields of $\mathbb{Q}$ are $\mathbb{R}$ and $\mathbb{C}$.

Definition 1.19 *A complex number α is an* ***algebraic integer*** *if it is the root of a polynomial with integral coefficients. If K is a number field then the* ***integers in K*** *are*

$$\mathbb{Z}_K = \{\alpha \in K \mid \alpha \textit{ is an algebraic integer}\}.$$

It is a fact that $\mathbb{Z}_K$ is an integral domain. Describing $\mathbb{Z}_K$ can be intuitive sometimes – for example, $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$, but it is not always so simply determined. The ring of integers in

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q} \text{ and } d \text{ square-free}\}$$

d square-free varies significantly in complexity depending on the value of d modulo 4. For futher information, see [3] §2.7, Proposition 2.34.

Theorem 1.20 *Let $K = \mathbb{Q}[\sqrt{d}]$. Then $\mathbb{Z}_K$ is a Euclidean domain if and only if $d = -1, -2, -3, -7$ or -11.*

Proof. See [4] §6.2, Theorem 6.4 and 6.5. ∎

By our discussions in this entire section, we have established the following relationship:

$$\text{Euclidean Domains} \subsetneq \text{PID's} \subsetneq \text{UFD's}$$

2 Fermat's Two Squares Theorem

We shall use the machinery developed in the first section to prove the following theorem,

Theorem 2.1 (Fermat's Two Squares Theorem) *For p an odd prime, $p = x^2+y^2$, for $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$.*

Before we begin the proof, however, we will first need to study the Gaussian integers.

2.1 Gaussian Integers

The Gaussian integers are

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

Note that $(a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{Z}[i]$ and $(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$ so the Gaussian integers form a subring of $\mathbb{C}$, and thus they form an integral domain. It is our goal in this section to show that in the Gaussian integers, the prime and irreducible elements are equivalent.

Proposition 2.2 *$\mathbb{Z}[i]$ is a PID.*

Proof. It is enough to show that $\mathbb{Z}[i]$ is a Euclidean domain. Clearly, the ring is an integral domain, so we must choose an appropriate norm and verify it satisfies the properties of a Euclidean norm. We will endow $\mathbb{Z}[i]$ with the complex modulus norm, i.e., $N(x + iy) = x^2 + y^2$.

For the first property, note that if $ab \neq 0$ for $a, b \in \mathbb{Z}[i]$, then a and b are nonzero, since $\mathbb{Z}[i]$ is an integral domain. We have then that $N(a)$ and $N(b)$ are greater than 0, but since a and b have integral coefficient as a complex number, the norm will be an integer greater than or equal to 1. Hence, $N(a) \leq N(ab)$.

For the second property, we will use an elegant geometric argument given in [4]. Consider $q = x + iy$ as points (x, y) in the plane. These points have integral coordinates so, in particular, they produce a square tiling of the plane. These squares tiles have side lengths of 1.

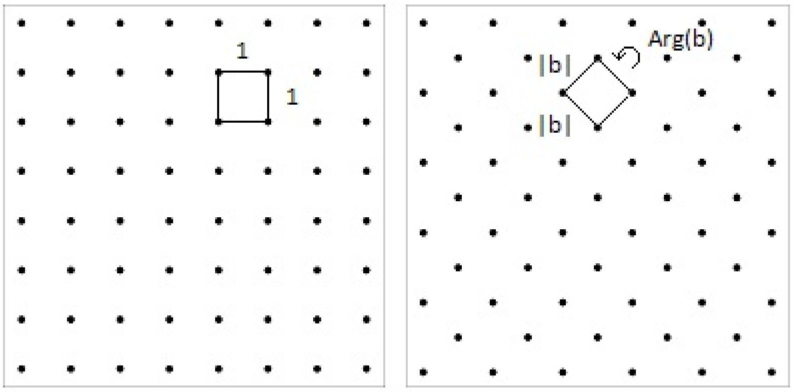
If $b \in \mathbb{Z}[i]$ is nonzero, then multiples qb with $q \in \mathbb{Z}[i]$ produce another square tiling – this multiplication will rotate the original lattice by $\text{Arg}(b)$, and stretch the side lengths by a factor of $|b|$. See Figure 1 for a depiction of this transformation.

We have that every complex number, and thus every $a \in \mathbb{Z}[i]$ is in one of these squares. The max distance from a to one of the vertices is $|b|/\sqrt{2}$, which happens if a is in the center of the square. Let q be such that qb is a vertex of the square in which a lies. Now define $r = a - qb$. Since $a, qb \in \mathbb{Z}[i]$, this implies that $r \in \mathbb{Z}[i]$. This gives us $|r| \leq |b|/\sqrt{2}$, so

$$N(r) = |r|^2 \leq |b|^2/2 < |b|^2 = N(b).$$

Thus, we have shown $\mathbb{Z}[i]$ is a Euclidean domain, so it is a PID by Theorem 1.17. ∎

Figure 1: A transformation of the square tiling.



2.2 The Proof

We will first show that if $p \equiv 3 \mod 4$, then it is not representable as a sum of two squares. To see this, note that $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 0$, and $3^2 \equiv 1 \mod 4$. Thus, p is not representable as the sum of two squares.

Now we must show that if $p \equiv 1 \mod 4$, it is representable as the sum of two squares. First, we show that there exists some integer x such that $x^2 \equiv 1 \mod p$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, let α be a generator. Since $p \equiv 1 \mod 4$, $\frac{p-1}{4} \in \mathbb{Z}$, so consider $x = \alpha^{\frac{p-1}{4}}$. We have that $(x^2)^2 \equiv 1 \mod 4$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, we have at most two solutions, and these are easily identifiable as $x^2 = \pm 1$. Since α is a generator, α^k assumes unique values for $k \in \{1, 2, \dots, p-1\}$, thus $x^2 = \alpha^{\frac{p-1}{2}} = -1$, since $\alpha^{p-1} = 1$. Thus, for every odd prime $p \equiv 1 \mod 4$, there exists some integer x such that $p \mid x^2 + 1$.

The significance of the above result is that $x^2 + 1$ splits over $\mathbb{Z}[i]$, so $p \mid x^2 + 1 = (x+i)(x-i)$. If p is irreducible, then by Proposition 2.2, p is prime, so it should divide $(x+i)$ or $(x-i)$. However, this is clearly not the case, since $\frac{x}{p} + \frac{1}{p}i \notin \mathbb{Z}[i]$. So, p is not irreducible, meaning it can be expressed as the product of two non-units, $p = (a+bi)(c+di)$.

It is not difficult to show that the norm of $\mathbb{Z}[i]$ preserves multiplication, that is, $N(ab) = N(a)N(b)$. So taking the norm on both sides of $p = (a+bi)(c+di)$, we have that $p^2 = (a^2+b^2)(c^2+d^2)$. Neither factor on the right is equal to 1, since the norm of an element is equal to 1 if and only if the element is a unit (also simple to show). Since we are now working within $\mathbb{Z}$, we must have that $a^2 + b^2 = p = c^2 + d^2$, finishing the proof.

2.3 A Complete Characterization

We will now explicitly describe the set of positive integers which are representable as the sum of two squares.

Lemma 2.3 *For every odd prime p, there exists some integer x such that $p \mid x^2 + 1$ if and only if $p \equiv 1 \mod 4$.*

Proof. We have shown one direction already in the proof of Fermat's two squares theorem. For the other direction, see [4] §7.3, Theorem 7.6 and Corollary 7.7 ■

Theorem 2.4 *A positive integer n is the sum of two squares if and only if for every prime factor $q \equiv 3 \mod 4$ of n, q is raised to an even power.*

Proof. We will first show that the product of two numbers which are the sum of two squares is also the sum of two squares:

$$(a^2 + b^2)(c^2 + d^2) = (ac + cd)^2 + (ad - bc)^2$$

Furthermore, if we want to multiply any sum of two squares by an integer j to an even power e, we simply multiply every input by $j^{e/2}$. By Fermat's Sum of Two Squares Theorem, we can represent any power of an odd prime $p \equiv 1 \mod 4$ as the sum of two squares. Thus, a positive integer n such that

$$n = 2^k p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} q_1^{2b_1} q_2^{2b_2} \dots q_l^{2b_l}$$

where $k, a_i, b_i \in \mathbb{Z}^+ \cup \{0\}$; $p_i \equiv 1 \mod 4$, and $q_i \equiv 3 \mod 4$ is representable as the sum of two squares.

To show the other direction, assume we have a positive integer $n = x^2 + y^2$ with a prime factor $q_i \equiv 3 \mod 4$ of n such that the maximal power f such that $q_i^f \mid n$ is odd. If $d = \gcd(x, y)$ then $x = ad$ and $y = bd$ where $\gcd(a, b) = 1$. Hence, $n = (a^2 + b^2)d^2$ and $nd^{-2} = a^2 + b^2$. If j is the maximal power such that $q^j \mid d$, then q^{f-2j} is odd (thus, nonzero), so $q^{f-2j} \mid nd^{-2}$. Since $f - 2j$ is odd, we have that $q \mid nd^{-2} = a^2 + b^2$, so $a^2 \equiv -b^2 \mod q$. Since a and b are coprime, q cannot divide both of them, so without loss of generality, $q \nmid b$ and $b \in (\mathbb{Z}/q\mathbb{Z})^\times$. Hence,

$$a^2(b^{-1})^2 = (ab^{-1})^2 \equiv -b^2(b^{-1})^2 \equiv -1 \mod q$$

However, by Lemma 2.3, there cannot exist such a square for an odd prime $q \equiv 3 \mod 4$, so this is a contradiction. Thus, n cannot have such a prime factor. ■

Acknowledgements

This paper was written as part of a semester-long research seminar taught by Professor Andrei Rapinchuk. I would like to thank Professor Rapinchuk for encouraging me to pursue this topic and for providing many valuable resources. I would also like to thank the anonymous referee, whose comments helped to improve the quality and coherency of this exposition.

References

[1] O.A. Cámpoli, "A principal ideal domain that is not a Euclidean domain," Amer. Math. Monthly, vol. 95 no. 9 (Nov. 1988), 868–871.

[2] D. Dummit and R. Foote, *Abstract Algebra.* John Wiley and Sons Inc., 2004.

[3] F. Jarvis, *Algebraic Number Theory.* Springer, 2014.

[4] G. A. Jones and J.M. Jones, *Elementary Number Theory.* Springer, 1998.