IMAGINARY QUADRATIC EUCLIDEAN DOMAINS

RICHARD CHEN

Abstract. The purpose of this paper is to give an introduction to some elementary but important concepts in Algebraic Number Theory. To this end, the first part of this paper discusses Euclidean Domains and Unique Factorization Domains. In particular, we show that every Unique Factorization Domain is a Greatest Common Divisor Domain and that every Euclidean Domain is a Unique Factorization Domain. The second part of this paper discusses structures called Imaginary Quadratic Domains. Building upon the previous section, we give a complete characterization of which Imaginary Quadratic Domains are Euclidean.

Contents

1. Euclidean Domain and Unique Factorization Domain

Definition 1.1. A *commutative ring* is a set R with two binary operations on R called addition, denoted $+$, and multiplication, denoted $\cdot$, satisfying the following *ring axioms*:

(1) (Commutative Laws) For all $a, b \in R$, $a + b = b + a$ and $a \cdot b = b \cdot a$.
(2) (Associative Laws) For all $a, b, c \in R$, $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(3) (Identity Laws) There exist elements $0, 1 \in R$ such that $a + 0 = a$ and $a \cdot 1 = a$ for all $a \in R$.
(4) (Inverse Law) For any $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.
(5) (Distributive Law) For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

For convenience, generally we will use ab to denote $a \cdot b$, and we will use the ring axioms implicitly.

Remark 1.2. Let R be a commutative ring. Let $a \in R$. We will use the notation a^n with $n \in \mathbb{N}$ to denote $\underbrace{a \cdots a}_{\text{n times}}$.

Lemma 1.3. *Let R be a commutative ring. Let $a \in R$. Then $a \cdot 0 = 0$.*

Proof. We have $a \cdot (1 + 0) = a \cdot 1 + a \cdot 0 = a + a \cdot 0$ and $a \cdot (1 + 0) = a \cdot (1) = a$. Then $a + a \cdot 0 = a$. Subtracting a, this gives the result. □

Definition 1.4. An *integral domain* is a commutative ring R such that for all $a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$.

Lemma 1.5. *Let R be an integral domain. Let $a, b, c \in R$ such that $c \neq 0$ and $ac = bc$. Then $a = b$.*

Proof. We have $ac = bc$. Rearranging, we obtain $ac - bc = c(a - b) = 0$. Since $c \neq 0$, then $a - b = 0$, so $a = b$. □

Definition 1.6. Let R be an integral domain. Let $a, b \in R$ with $b \neq 0$. We say that b *divides* a in R (denoted $b \mid_R a$) if there exists $r \in R$ such that $a = rb$. When obvious, we will not specify the integral domain in which b divides a and simply write $b \mid a$.

Observation 1.7. Let R be an integral domain. If $a \in R$ is non-zero, then $a \mid a$ since $a \cdot 1 = a$.

Lemma 1.8. *Let $a, b, c \in R$ such that $a = b + c$. Suppose $r \neq 0 \in R$ such that $r \mid b$ and $r \mid c$. Then $r \mid a$.*

Proof. We have $b = xr$ and $c = yr$ for some $x, y \in R$. Then $a = xr + yr = r(x + y)$. Thus $r \mid a$. □

Lemma 1.9. *Let R be an integral domain. Let $a \in R$ and some non-zero $b, c \in R$ such that $c \mid b$ and $b \mid a$. Then $c \mid a$.*

Proof. By definition, $b = rc$ and $a = sb$ for some $r, s \in R$. Then $a = s(rc) = (rs)c$ by substitution. By definition, $c \mid a$. □

Definition 1.10. Let R be an integral domain. The units of R are the elements which divide 1. Equivalently, $u \in R$ is called a unit if and only if there exists $v \in R$ such that $uv = 1$. We call v the *multiplicative inverse* of u and denote it u^{-1}.

Observation 1.11. By commutativity, the multiplicative inverse of any unit in an integral domain is a unit itself.

Observation 1.12. Let R be an integral domain. For any $a \in R$ and unit $u \in R$, $a = a \cdot 1 = a(uu^{-1}) = (au^{-1})u$. Thus $u \mid a$.

Definition 1.13. Let R be an integral domain. Let $a, b \in R$. We call b an *associate* of a in R if there exists some unit $u \in R$ such that $a = ub$. The set of all associates of a in R is denoted $[a]_R$, or simply [a].

Remark 1.14. One can show that in Definition 1.13, we have defined an *equivalence relation* on an integral domain that partitions it into *equivalence classes*. This means that if R is an integral domain, then

(1) For any $a \in R$, $a \in [a]$.
(2) For any $a, b \in R$, $a \in [b]$ if and only if $b \in [a]$.
(3) For any $a, b, c \in R$, if $a \in [b]$ and $b \in [c]$, then $a \in [c]$.

Moreover, it follows that for any $a, b \in R$, a and b are associates if and only if $[a] = [b]$. We will assume familiarity with these facts for brevity.

Observation 1.15. Let R be an integral domain. Let $a, b \in R$ such that they are associates. If $a = rb$ for some $r \in R$, then it can be shown that r is a unit by Lemma 1.5.

Lemma 1.16. *Let R be an integral domain. Let $a, b \in R$ be non-zero. Then a and b are associates if and only if $a \mid b$ and $b \mid a$.*

Proof. If a and b are associates, then $a \mid b$ and $b \mid a$ by definition. If a and b divide each other, then $a = rb$ and $b = sa$ for some $r, s \in R$. Then $a = r(sa)$. Rearranging, $a - r(sa) = a(1 - rs) = 0$. Since $a \neq 0$, we have $1 - rs = 0$, so $1 = rs$. Thus r and s are units, so a and b are associates. □

Lemma 1.17. *Let R be an integral domain. The set of all units in R is $[1]$.*

Proof. Suppose $u \in R$ is a unit. Then $1 = uu^{-1}$. By Definition 1.13, $u \in [1]$. Suppose $x \in [1]$. Then $1 = vx$ for some unit $v \in R$. By definition, x is unit. Thus, $r \in R$ is a unit if and only if $r \in [1]$, i.e., $[1]$ is the set of all units in R. □

Remark 1.18. Let R be an integral domain. Following Lemma 1.17, we will now call $[1]$ the set of all units in R.

Lemma 1.19. *Let R be an integral domain. Let $u, v \in R$. Then $u, v \in [1]$ if and only if $uv \in [1]$.*

Proof. Suppose $u, v \in [1]$. Then $(uv)(u^{-1}v^{-1}) = (uu^{-1})(vv^{-1}) = 1 \cdot 1 = 1$. Thus, $uv \in [1]$. Suppose $uv \in [1]$. Then $(uv)(uv)^{-1} = u(v(uv)^{-1}) = v(u(uv)^{-1}) = 1$. Thus, $u, v \in [1]$. □

Observation 1.20. Let R be an integral domain. By induction, $u_1, \ldots, u_n \in [1]$ if and only if $u_1 \cdots u_n \in [1]$.

Definition 1.21. Let R be an integral domain. An element $0 \neq \pi \in R$ is called *prime* if $\pi \notin [1]$ and for all non-zero $a, b \in R$, if $\pi \mid ab$, then $\pi \mid a$ or $\pi \mid b$.

Remark 1.22. Let R be an integral domain. By induction, if $\pi \in R$ is prime and $\pi \mid a_1 \cdots a_n$ for some $a_i \in R$, then $\pi \mid a_i$ for some i. We will use this fact implicitly.

Definition 1.23. Let R be an integral domain. An element $0 \neq \pi \in R$ is called *irreducible* if $\pi \notin [1]$, and if whenever $\pi = ab$ for some $a, b \in R$, then a or b must be a unit.

Lemma 1.24. *Let R be an integral domain. Let π be a prime of R. Then π is irreducible.*

Proof. Suppose $\pi = ab$ for some $a, b \in R$. Then $a \mid \pi$ and $b \mid \pi$. Since $\pi \mid ab$, by Definition 1.21 $\pi \mid a$ or $\pi \mid b$. Without loss of generality, let $\pi \mid a$. Then π and a are associates, so $b \in [1]$. □

Corollary 1.25. *Let R be an integral domain. Let $a, b \in R$ be prime. If $b \mid a$, then $[a] = [b]$.*

Proof. We have $a = rb$ for some $r \in R$. By Lemma 1.24, a is irreducible, so $r \in [1]$ since $b \notin [1]$ by Definition 1.21. Then $[a] = [b]$. □

Definition 1.26. Let R be an integral domain. R is called a *unique factorization domain* (UFD) if every non-zero, non-unit element $r \in R$ can be written as a unique product $r = u\pi_1 \cdots \pi_m$ for some irreducibles $\pi_j \in R$ and $u \in [1]$. This product is unique in that if $r = vq_1 \cdots q_n$ for some irreducible elements $q_i \in R$ and $v \in [1]$, then $m = n$, and there exists a permutation ϕ of $\{1, \ldots, m\}$ such that for all j, $[\pi_j] = [q_{\phi(j)}]$.

Remark 1.27. Let R be a UFD. One can show that every non-zero, non-unit element $r \in R$ can be written as a unique product $r = u\pi_1^{e_1} \cdots \pi_m^{e_m}$ for some distinct irreducibles $\pi_j \in R$, $e_j \in \mathbb{N}$, and $u \in [1]$. These irreducibles are distinct in that $[\pi_j] \neq [\pi_i]$ for all $i \neq j$. This product is unique in that if $r = vq_1^{p_1} \cdots q_n^{p_n}$ for some irreducibles $q_i \in R$, $p_i \in \mathbb{N}$, and $v \in [1]$, then $m = n$, and there exists a permutation ϕ of $\{1, \ldots, m\}$ such that for all j, $[\pi_j] = [q_{\phi(j)}]$ and $e_j = p_{\phi(j)}$. We will use this fact implicitly.

Lemma 1.28. *Let R be a UFD. Let $a, b \in R$ be non-zero, non-unit. Suppose $a = u\alpha_1 \cdots \alpha_m$ and $b = v\beta_1 \cdots \beta_n$ for some irreducibles $\alpha_j, \beta_i \in R$ and $u, v \in [1]$. Then $b \mid a$ if and only if $n \leq m$, and there exists a permutation ϕ of $\{1, \ldots, m\}$ such that for all i, $[\beta_i] = [\alpha_{\phi(i)}]$.*

Proof. Suppose $b \mid a$. We have $a = rb$ for some $r \in R$. Suppose $r \notin [1]$. Note $r \neq 0$, or else $a = 0$ by Lemma 1.3. Then $r = w\gamma_1 \cdots \gamma_l$ for some irreducibles $\gamma_k \in R$ and $w \in [1]$. Let $\beta_{n+k} = \gamma_k$ for all k. By substitution,

$$u\alpha_1 \cdots \alpha_m = (w\gamma_1 \cdots \gamma_l)(v\beta_1 \cdots \beta_n) = (vw)(\beta_1 \cdots \beta_{n+l}).$$

By Lemma 1.19 $vw \in [1]$. Then, by uniqueness, $m = n + l$, so $n < m$, and there exists a permutation ϕ of $\{1, \ldots, m\}$ such that for all i, we have $[\beta_i] = [\alpha_{\phi(i)}]$. The case for $r \in [1]$ follows similar logic.

Now suppose $n \leq m$, and there exists a permutation ϕ of $\{1, \ldots, m\}$ such that $[\beta_i] = [\alpha_{\phi(i)}]$ for all i. Then, for all i, we have $\alpha_{\phi(i)} = x\beta_i$ for some $x \in [1]$. Thus

$$a = (u)(\prod_{i=1}^{n} \alpha_{\phi(i)})(\prod_{j=n+1}^{m} \alpha_{\phi(j)}) = (u)(\prod_{i=1}^{n} x_i\beta_i)(\prod_{j=n+1}^{m} \alpha_{\phi(j)})$$

for some $x_i \in [1]$. Since $1 = vv^{-1}$ and $b = v\beta_1 \cdots \beta_n$, one can show

$$a = (vv^{-1})(u)(\prod_{i=1}^{n} x_i\beta_i)(\prod_{j=n+1}^{m} \alpha_{\phi(j)}) = (b)(uv^{-1}\prod_{i=1}^{n} x_i \prod_{j=n+1}^{m} \alpha_{\phi(j)}),$$

and hence $b \mid a$. □

Remark 1.29. In Lemma 1.28, if we suppose $a = u\alpha_1^{p_1} \cdots \alpha_m^{p_m}$ and $b = v\beta_1^{q_1} \cdots \beta_n^{q_n}$ for some distinct irreducibles $\alpha_j, \beta_i \in R$, $p_j, q_i \in \mathbb{N}$, and $u, v \in [1]$, then one can similarly show that $b \mid a$ if and only if $n \leq m$, and there exists a permutation ϕ of $\{1, \ldots, m\}$ such that $[\beta_i] = [\alpha_{\phi(i)}]$ and $q_i \leq p_{\phi(i)}$ for all i.

Proposition 1.30. *In a unique factorization domain, every irreducible element is prime.*

Proof. Let R be a UFD. Let $\pi \in R$ with π irreducible. Suppose $\pi \mid ab$ for some non-zero, non-unit $a, b \in R$. Then $a = u\alpha_1 \cdots \alpha_m$ and $b = v\beta_1 \cdots \beta_n$ for some irreducibles $\alpha_j, \beta_i \in R$ and $u, v \in [1]$. Let $\alpha_{m+i} = \beta_i$ for all i. Substituting, we have

$$ab = (u\alpha_1 \cdots \alpha_m)(v\beta_1 \cdots \beta_n) = (uv)(\alpha_1 \cdots \alpha_{m+n}).$$

By Lemma 1.19, $uv \in [1]$. We have $\pi = 1 \cdot \pi$. Then $[\pi] = [\alpha_k]$ for some $k \in \{1, \ldots, m+n\}$ by Lemma 1.28. Thus, $[\pi] = [\alpha_j]$ for some j or $[\pi] = [\beta_i]$ for some i. Without loss of generality, suppose $[\pi] = [\alpha_j]$. Then $\pi \mid \alpha_j$ by Lemma 1.16. Since $\alpha_j \mid a$, by Lemma 1.9, $\pi \mid a$. Suppose either $a \in [1]$ or $b \in [1]$. One can show by similar logic that $\pi \mid a$ or $\pi \mid b$. Note a and b cannot both be units. Otherwise,

applying Lemma 1.19, we have $ab = r\pi \in [1]$, and so $\pi \in [1]$. By definition, π is prime. □

Definition 1.31. Let R be an integral domain. Let $a, b \in R$ with $a \neq 0$. A *greatest common divisor* (GCD) of a and b in R is some $g \neq 0 \in R$ such that for all $r \in R$, $r \mid a$ and $r \mid b$ if and only if $r \mid g$. The set of all GCDs of a and b in R is denoted $\gcd_R(a, b)$, or simply $\gcd(a, b)$.

Observation 1.32. Let R be an integral domain. Let $a, b \in R$ with $a \neq 0$. If $g \in \gcd(a, b)$, then $g \neq 0$. Thus $g \mid g$, so g is a common divisor of a and b, or $g \mid a$ and $g \mid b$, by Definition 1.31.

Lemma 1.33. *Let R be an integral domain. Let $a, b \in R$ with $a \neq 0$. Then $g_0 \in \gcd(a, b)$ if and only if $[g_0] = \gcd(a, b)$.*

Proof. Suppose $g_0 \in \gcd(a, b)$. If $g_1 \in \gcd(a, b)$, then $g_0 \mid g_1$ and $g_1 \mid g_0$ since both are common divisors of a and b. By Lemma 1.16, $g_1 \in [g_0]$. Thus, $\gcd(a, b) \subset [g_0]$. Suppose $\gamma \in [g_0]$. By Lemma 1.16, $\gamma \mid g_0$ and $g_0 \mid \gamma$. Let $r_0 \neq 0 \in R$ such that $r_0 \mid a$ and $r_0 \mid b$. By Definition 1.31, $r_0 \mid g_0$. By Lemma 1.9, $r_0 \mid \gamma$. Suppose $r_1 \neq 0 \in R$ such that $r_1 \mid \gamma$. By Lemma 1.9, $r_1 \mid g_0$. By Definition 1.31, $r_1 \mid a$ and $r_1 \mid b$. By Definition 1.31, $\gamma \in \gcd(a, b)$. Thus, $[g_0] \subset \gcd(a, b)$, so $[g_0] = \gcd(a, b)$. If $[g_0] = \gcd(a, b)$, then $g_0 \in \gcd(a, b)$ trivially. □

Remark 1.34. Let R be an integral domain. Let $a, b \in R$ with $a \neq 0$. We write $[g] = \gcd(a, b)$ if g is a GCD of a and b following Lemma 1.33.

Lemma 1.35. *Let $a, b \in R$ with $a \neq 0$. Then $a \mid b$ if and only if $[a] = \gcd(a, b)$.*

Proof. Suppose $a \mid b$. Let $r_0 \neq 0 \in R$ such that $r_0 \mid a$. By Lemma 1.9, $r_0 \mid b$. Any element $r_1 \in R$ that divides a and b divides a. Then $[a] = \gcd(a, b)$ by Definition 1.13. Suppose $[a] = \gcd(a, b)$. Then a is a common divisor of a and b, so $a \mid b$. □

Observation 1.36. Let R be an integral domain. Let $a \in R$ and $u \in [1]$. Then $u \mid a$, so $\gcd(a, u) = [u] = [1]$ by Lemma 1.35. Let $b \neq 0 \in R$. Then $0 = 0 \cdot b$ by Lemma 1.3, so $b \mid 0$. Thus $\gcd(b, 0) = [b]$ by Lemma 1.35.

Proposition 1.37. *Let R be a UFD. Let $a, b \in R$ with $a \neq 0$. Then $\gcd(a, b) \neq \emptyset$.*

Proof. By Observation 1.36, we may assume $a, b \notin [1]$ and $b \neq 0$. Then $a = u\alpha_1^{p_1} \cdots \alpha_m^{p_m}$ and $b = v\beta_1^{q_1} \cdots \beta_n^{q_n}$ for some distinct irreducibles $\alpha_j, \beta_i \in R$, $p_j, q_i \in \mathbb{N}$, and $u, v \in [1]$. Let

$$G = \{\alpha_j \mid [\alpha_j] = [\beta_i] \text{ for some } i\}.$$

If $G \neq \emptyset$, we can assign the symbols $\gamma_1, \ldots, \gamma_x$, with $x \leq m$ and $x \leq n$, to every element in G. Then there exist permutations ψ of $\{1, \ldots, m\}$ and ω of $\{1, \ldots, n\}$ such that $[\gamma_y] = [\alpha_{\psi(y)}] = [\beta_{\omega(y)}]$ for all y. Define

$$z_y = \min(p_{\psi(y)}, q_{\omega(y)})$$

for all y, and let $g = \gamma_1^{z_1} \cdots \gamma_x^{z_x}$. Since $z_y \leq p_{\psi(y)}$ and $z_y \leq q_{\omega(y)}$, we have $g \mid a$ and $g \mid b$ by Remark 1.29. Thus, any divisor of g is a common divisor of a and b by Lemma 1.9.

Now suppose $r \neq 0 \in R$ such that $r \mid a$ and $r \mid b$. If $r \in [1]$, then we know $r \mid g$. Otherwise, $r = w\lambda_1^{s_1} \cdots \lambda_l^{s_l}$ for some distinct irreducibles $\lambda_k \in R$, $s_k \in \mathbb{N}$, and $w \in [1]$. By Remark 1.29, we have $l \leq m$, and there exists a permutation

ϕ of $\{1, \dots, m\}$ such that $[\lambda_k] = [\alpha_{\phi(k)}]$ with $s_k \leq p_{\phi(k)}$ for all k. We also have $l \leq n$, and there exists a permutation τ of $\{1, \dots, n\}$ such that $[\lambda_k] = [\beta_{\tau(k)}]$ with $s_k \leq q_{\tau(k)}$ for all k. Thus, $[\lambda_k] = [\alpha_{\phi(k)}] = [\beta_{\tau(k)}]$ and $s_k \leq \min(p_{\phi(k)}, q_{\tau(k)})$ for all k. This implies

$$[\lambda_k] = [\gamma_{\psi^{-1}(\phi(k))}] \text{ and } s_k \leq z_{\psi^{-1}(\phi(k))}$$

for all k. By Remark 1.29, $r \mid g$, and so $\gcd(a, b) = [g]$ by Definition 1.31.

If $G = \emptyset$, then $[a_j] \neq [b_i]$ for all i, j. Thus, for any $r \neq 0 \in R$ such that $r \mid a$ and $r \mid b$, we have $r \in [1]$. Thus, $r \mid 1$. It follows that $\gcd(a, b) = [1]$ since any unit divides a and b. □

Definition 1.38. Let R be a UFD. Let $a, b \in R$ such that $a \neq 0$. We say that a and b are *co-prime* if $\gcd(a, b) = [1]$.

Lemma 1.39. *Let R be a UFD. Let $\alpha_1, \alpha_2 \in R$ be non-zero, non-unit, and co-prime. Suppose $[\alpha_1 \cdot \alpha_2] = [\beta^n]$ for some non-zero, non-unit $\beta \in R$ and $n \in \mathbb{N}$. Then, $[\alpha_1] = [x^n]$ and $[\alpha_2] = [y^n]$ for some $x, y \in R$.*

Proof. We have $\beta = u\pi_1^{e_1} \cdots \pi_m^{e_m}$, $\alpha_1 = v\theta_1^{p_1} \cdots \theta_r^{p_r}$, and $\alpha_2 = w\rho_1^{q_1} \cdots \rho_s^{q_s}$ for some distinct irreducibles $\pi_i, \theta_j, \rho_k \in R$, $e_i, p_j, q_k \in \mathbb{N}$, and $u, v, w \in [1]$. Let $E_i = ne_i$ for all i so that

$$\begin{aligned} \beta^n &= (u\pi_1^{e_1} \cdots \pi_m^{e_m})^n \\ &= (u^n)(\pi_1^{ne_1} \cdots \pi_m^{ne_m}) \\ &= (u^n)(\pi_1^{E_1} \cdots \pi_m^{E_m}), \end{aligned}$$

and let $\theta_{r+k} = \rho_k$ and $p_{r+k} = q_k$ for all k so that

$$\begin{aligned} \alpha_1 \cdot \alpha_2 &= (v\theta_1^{p_1} \cdots \theta_r^{p_r})(w\rho_1^{q_1} \cdots \rho_s^{p_s}) \\ &= (vw)(\theta_1^{p_1} \cdots \theta_{r+s}^{p_{r+s}}). \end{aligned}$$

We have $z(\alpha_1 \cdot \alpha_2) = \beta^n$ for some $z \in [1]$. Then we can obtain

$$(zvw)(\theta_1^{p_1} \cdots \theta_{r+s}^{p_{r+s}}) = (u^n)(\pi_1^{E_1} \cdots \pi_m^{E_m})$$

by substituting from above. By Lemma 1.19, $u^n \in [1]$ and $(vwz) \in [1]$. We have $\gcd(\alpha_1, \alpha_2) = [1]$ since α_1 and α_2 are co-prime. By Proposition 1.37, $[\theta_j] \neq [\rho_k]$ for all j, k. Then, by uniqueness, $m = r + s$, and there exists a permutation ϕ of $\{1 \dots, m\}$ such that $[\pi_{\phi(j)}] = [\theta_j]$ and $E_{\phi(j)} = ne_{\phi(j)} = p_j$ for all j. Thus,

$$\alpha_1 = v\theta_1^{ne_{\phi(1)}} \cdots \theta_r^{ne_{\phi(r)}} = (v)(\theta_1^{e_{\phi(1)}} \cdots \theta_r^{e_{\phi(r)}})^n.$$

Then $[\alpha_1] = [x^n]$ where $x = \theta_1^{e_{\phi(1)}} \cdots \theta_r^{e_{\phi(r)}}$. Similarly $[\alpha_2] = [y^n]$, where $y = \rho_1^{e_{\phi(r+1)}} \cdots \rho_s^{e_{\phi(r+s)}}$. □

Observation 1.40. In Lemma 1.39, if instead $[\beta^n] = [\alpha_1 \cdots \alpha_w]$ for some non-zero, non-unit, and pairwise co-prime $\alpha_z \in R$, then it can be shown inductively for all z that $[\alpha_z] = [x^n]$ for some $x \in R$.

Definition 1.41. A *Euclidean Domain* (R, d) is an integral domain R with a *degree* function $d : R \setminus \{0\} \longrightarrow \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$, and either $r = 0$, or $d(r) < d(b)$.

Lemma 1.42. *Let R be an integral domain. Let $a, b \in R$ with $b \neq 0$. Suppose there exist $q, r \in R$ such that $a = qb + r$. Then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Suppose there exists some $g_0 \in R$ such that $[g_0] = \gcd(a, b)$. Let $s \neq 0 \in R$ such that $s \mid b$ and $s \mid r$. Then $s \mid qb$ by Lemma 1.9, so $s \mid a$ by Lemma 1.8. Thus $s \mid g_0$ by Definition 1.31. If $t \neq 0 \in R$ such that $t \mid g_0$, then $t \mid a$ and $t \mid b$ by Definition 1.31. We have $a = qb + r$, and thus $r = a - qb$. By Lemma 1.8, $t \mid r$, so $[g_0] = \gcd(b, r)$ by Definition 1.13. By similar logic, if there exists some $g_1 \in R$ such that $[g_1] = \gcd(b, r)$, then $[g_1] = \gcd(a, b)$. Otherwise, $\gcd(a, b) = \gcd(b, r) = \emptyset$. □

Proposition 1.43. *Let (R, d) be an Euclidean Domain. Let $a, b \in R$ with $b \neq 0$. Then $\gcd(a, b) \neq \emptyset$. Moreover, there exist $m, n \in R$ such that $\gcd(a, b) = [ma + nb]$.*

Proof. We have:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ &\vdots \\ r_{i-2} &= q_i r_{i-1} + r_i \end{aligned}$$

for some $q_i, r_i \in R$ such that $d(r_{i+1}) < d(r_i)$, where $b = r_0$. The sequence of natural numbers $d(r_0) > \ldots > d(r_i)$ cannot be infinite by the well-ordering principle. In particular, there exists $n \in \mathbb{N}$ such that $r_n = 0$ and $r_{n-2} = q_n r_{n-1}$. Thus, $\gcd(r_{n-1}, r_{n-2}) = [r_{n-1}]$ by Lemma 1.35. By Lemma 1.42, we have $\gcd(a, b) = [r_{n-1}]$. Rearranging, we obtain:

$$\begin{aligned} r_1 &= a - q_1 b \\ r_2 &= b - q_2 r_1 \\ &\vdots \\ r_{n-1} &= r_{n-3} - q_{n-1} r_{n-2}. \end{aligned}$$

Substituting recursively, we have $r_{n-1} = ma + nb$ for some $m, n \in R$. □

Proposition 1.44. *Let (R, d) be a Euclidean Domain. Then every irreducible element in R is prime.*

Proof. Let $\pi \in R$ be irreducible. Suppose $\pi \mid ab$ for some non-zero $a, b \in R$, but π does not divide a. We first show $\gcd(\pi, a) = [1]$. Suppose $r \neq 0 \in R$ such that $r \mid \pi$ and $r \mid a$. Then $\pi = sr$ for some $s \in R$. If $r \notin [1]$, then $[s] \in [1]$ since π is irreducible. Then π and r are associates, so $\pi \mid r$ by Lemma 1.16. Then $\pi \mid a$ by Lemma 1.9, and hence a contradiction, so $r \in [1]$. Thus, $r \mid 1$. It follows that $\gcd(\pi, a) = [1]$ since any unit divides π and a. Now by Proposition 1.43, there exist $m, n \in R$ such that $m\pi + na = 1$. Multiplying by b, we obtain $m\pi b + nab = b$. Then $\pi \mid b$ by Lemma 1.8, so π is prime by Definition 1.21. This proof follows from one given in Chapter 1 of [3]. □

Lemma 1.45. *Let (R, d) be an Euclidean Domain. Let $a \neq 0 \in R$. If $a = bc$ for some $b, c \in R$ with $c \notin [1]$, then there exists some $\beta \in [b]$ such that $d(\beta) < d(a)$.*

Proof. We have:

$$\begin{aligned} b &= q_1 a + r_1 \\ a &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \end{aligned}$$

for some $q_i, r_i \in R$ such that $d(r_{i+1}) < d(r_i)$, where $a = r_0$, $r_n = 0$, and $\gcd(a, b) = [r_{n-1}]$ as in Proposition 1.43. We have $b \mid a$ since $b \neq 0$, or else $a = 0$ by Lemma 1.3. Then $\gcd(a, b) = [b]$ by Lemma 1.35, so $r_{n-1} \in [b]$. If $n = 1$, then $b = q_1 a$, so $a \mid b$. We have $b \mid a$. By Lemma 1.16, a and b are associates, so $c \in [1]$, and hence a contradiction. Then $n > 1$, so $d(r_{n-1}) < d(a)$. □

Corollary 1.46. *Let (R, d) be a Euclidean Domain. Let $r \in R$ be non-zero, non-unit. Suppose $r = a_1 \cdots a_n$ for some non-zero, non-unit $a_i \in R$. Then $n \leq d(r)$.*

Proof. Let $k \in \{1, \ldots, n-1\}$. Then $\prod_{m=1}^{n-(k-1)} a_l = (\prod_{m=1}^{n-k} a_l)(a_{n-(k-1)})$. Since $a_{n-(k-1)} \notin [1]$, we have $d(r) = d(a_1 \cdots a_n) > d(\alpha_1) > \ldots > d(\alpha_{n-1}) \geq 1$ for some $\alpha_k \in [\prod_{m=1}^{n-k} a_l]$ by Lemma 1.45. Thus, $n \leq d(r)$. □

Proposition 1.47. *Let (R, d) be a Euclidean Domain. Then R is a UFD.*

Proof. Let $r \in R$ be non-zero, non-unit. We show r can be expressed as a product of a unit and some irreducibles in R. If r is irreducible, we have $r = 1 \cdot r$, and we are done. If not, then $r = ab$ for some non-unit $a, b \in R$. Consider the set $S = \{n \in \mathbb{N} \setminus \{1\} \mid \text{there are some non-zero, non-unit } a_1, \ldots, a_n \in R \text{ and } r = a_1 \cdots a_n\}$. We have $S \neq \emptyset$. By Corollary 1.46, for every $s \in S$, $s \leq d(r)$. Thus, there exists some $m \in S$ such that for every $s \in S$, $s \leq m$. We have $r = a_1 \cdots a_m = 1 \cdot a_1 \cdots a_m$ for some $a_i \in R$. Then each a_i is irreducible, or else for some i, we have $a_i = bc$ for some non-unit $b, c \in R$. It follows that there exists some $l \in S$ with $m < l$, and hence a contradiction. □

2. Imaginary Quadratic Domains

Definition 2.1. An *imaginary quadratic domain* is an integral domain $\mathbb{Z}[D] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ such that D is a square-free integer and $D < 0$.

Definition 2.2. The map $N : \mathbb{Z}[D] \longrightarrow \mathbb{N}$, $N(a + b\sqrt{D}) = a^2 - Db^2$ is called the *norm* map on $\mathbb{Z}[D]$.

Lemma 2.3. *The norm map on $\mathbb{Z}[D]$ is multiplicative, i.e., for any $a = \alpha_1 + \alpha_2\sqrt{D}, b = \beta_1 + \beta_2\sqrt{D} \in \mathbb{Z}[D]$, we have $N(ab) = N(a)N(b)$.*

Proof. We have

$$\begin{aligned} ab &= (\alpha_1 + \alpha_2\sqrt{D})(\beta_1 + \beta_2\sqrt{D}) \\ &= (\alpha_1\beta_1 + D\alpha_2\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)\sqrt{D} \end{aligned}$$

and so

$$\begin{aligned} N(ab) &= (\alpha_1\beta_1 + D\alpha_2\beta_2)^2 - D(\alpha_1\beta_2 + \alpha_2\beta_1)^2 \\ &= ((\alpha_1\beta_1)^2 + 2D\alpha_1\alpha_2\alpha_2\beta_2 + (D\alpha_2\beta_2)^2) \\ &\quad - D((\alpha_1\beta_2)^2 + 2\alpha_1\beta_2\alpha_2\beta_1 + (\alpha_2\beta_1)^2) \\ &= (\alpha_1\alpha_2)^2 - D(\alpha_1\beta_2)^2 - D(\alpha_2\beta_1)^2 + (D\alpha_2\beta_2)^2 \\ &= (\alpha_1^2 - D\alpha_2^2)(\beta_1^2 - D\beta_2^2) = N(a)N(b). \end{aligned}$$

by definition. □

Definition 2.4. Let $x = y_1 + y_2\sqrt{D} \in \mathbb{Z}[D]$. The *complex conjugate* of x, denoted $\overline{x}$, is given by $\overline{x} = y_1 - y_2\sqrt{D}$.

Lemma 2.5. *Let $x = y_1 + y_2\sqrt{D} \in \mathbb{Z}[D]$. Then $N(x) = N(\overline{x}) = x\overline{x}$.*

Proof. By definition, $x\overline{x} = (y_1 + y_2\sqrt{D})(y_1 - y_2\sqrt{D}) = y_1^2 - Dy_2^2$ and $N(\overline{x}) = y_1^2 - D(-y_2)^2 = y_1^2 - Dy_2^2$. Then $N(x) = y_1^2 - Dy_2^2 = N(\overline{x}) = x\overline{x}$ by definition. □

Lemma 2.6. *Let $u \in \mathbb{Z}[D]$. Then $u \in [1]$ if and only if $N(u) = 1$.*

Proof. Suppose $u \in \mathbb{Z}[D]$ is a unit. Then there exists $u^{-1} \in \mathbb{Z}[D]$ such that $uu^{-1} = 1$. By Lemma 2.3, we have $N(u)N(u^{-1}) = N(uu^{-1}) = N(1) = 1$, so $N(u) = 1$. Suppose $N(u) = 1$. By Lemma 2.5, $N(u) = u\overline{u} = 1$, so $u \in [1]$. □

Lemma 2.7. *In $\mathbb{Z}[D]$, 2 is irreducible if $D \leq -3$.*

Proof. Suppose $2 = ab$ for some $a, b \in \mathbb{Z}[D]$. By Lemma 2.3, $N(a)N(b) = N(ab) = N(2) = 4$. Thus, either $N(a) = N(b) = 2$, $N(a) = 1$ and $N(b) = 4$, or $N(a) = 1$ and $N(b) = 4$. In the last two cases, either a or b is a unit by Lemma 2.6. Suppose $N(a) = N(b) = 2$. We have $a = \alpha_1 + \alpha_1\sqrt{D}$ for some $\alpha_1, \alpha_2 \in \mathbb{Z}$. Then $N(a) = N(\alpha_1 + \alpha_2\sqrt{D}) = \alpha_1^2 - D\alpha_2^2 = 2$. Since $D \leq -3$, we have $\alpha_2 = 0$, or else $2 < -D\alpha_2^2$, and so $2 < N(a)$. Thus, $N(a) = \alpha_1^2 = 2$, but 2 is not a square, and hence a contradiction. Then either a or b is a unit, so 2 is irreducible. □

Remark 2.8. Let $D \in \mathbb{Z}$ such that D is square-free. Then one can show the product $a\sqrt{D}$ for some $a \in \mathbb{Z}$ is not contained in $\mathbb{Z}$ unless $a = 0$.

Lemma 2.9. *In $\mathbb{Z}[D]$, 2 does not divide $\sqrt{D}$, $1 + \sqrt{D}$, nor $1 - \sqrt{D}$.*

Proof. Suppose $2 \mid \sqrt{D}$. Then $\sqrt{D} = 2a$ for some $a \in \mathbb{Z}[D]$. We have $a = \alpha_1 + \alpha_2\sqrt{D}$ for some $\alpha_1, \alpha_2 \in \mathbb{Z}$. Then $\sqrt{D} = 2(\alpha_1 + \alpha_2\sqrt{D}) = 2\alpha_1 + 2\alpha_2\sqrt{D}$. Rearranging, we obtain $\sqrt{D}(1 - 2\alpha_2) = 2\alpha_1$. We have $2\alpha_1 \in \mathbb{Z}$. However, $\sqrt{D}(1 - 2\alpha_2) \notin \mathbb{Z}$ unless $0 = 1 - 2\alpha_2$ by Remark 2.8. Then $1 = 2\alpha_2$, so $2 \in [1]$. However, $N(2) = 4 \neq 1$, and hence a contradiction to Lemma 2.6. Suppose $2 \mid (1 + \sqrt{D})$. Then $1 + \sqrt{D} = 2b$ for some $b \in \mathbb{Z}[D]$. We have $b = \beta_1 + \beta_2\sqrt{D}$ for some $\beta_1, \beta_2 \in \mathbb{Z}$. Then $1 + \sqrt{D} = 2(\beta_1 + \beta_2\sqrt{D}) = 2\beta_1 + 2\beta_2\sqrt{D}$. Rearranging, we obtain $\sqrt{D}(2\beta_2 - 1) = 1 - 2\beta_1$. We have $1 - 2\beta_1 \in \mathbb{Z}$. However, $\sqrt{D}(2\beta_2 - 1) \notin \mathbb{Z}$ unless $0 = 2\beta_2 - 1$ by Remark 2.8. Then $1 = 2\beta_2$, so $2 \in [1]$, but we know this is a contradiction. By similar logic, 2 does not divide $1 - \sqrt{D}$. □

Theorem 2.10. *If $(\mathbb{Z}[D], N)$ is a Euclidean Domain, then $D \geq -2$.*

Proof. Suppose $(\mathbb{Z}[D], N)$ is a Euclidean Domain and $D \leq -3$. By Proposition 1.47, $\mathbb{Z}[D]$ is a UFD. By Lemma 2.7, 2 is irreducible, so 2 is prime by Proposition 1.30. If D is even, then 2 divides $D = \sqrt{D} \cdot \sqrt{D}$, but 2 does not divide $\sqrt{D}$ by Lemma 2.9, and hence a contradiction to Definition 1.21. If D is odd, then 2 divides $1 - D = (1 + \sqrt{D})(1 - \sqrt{D})$, but 2 does not divide $1 + \sqrt{D}$ nor $1 - \sqrt{D}$ by Lemma 2.9, and hence a contradiction to Definition 1.21. This proof follows from one given by Chris Eagle at [1] □

Lemma 2.11. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $|r| \leq \frac{1}{2}|b|$.*

Proof. Suppose $0 \leq a$ and $0 < b$. Consider the set $S = \{n \in \mathbb{Z} \mid 0 \leq a - nb\}$. We have $S \neq \emptyset$ because $a - 0 \cdot b = a - 0 = a \geq 0$. Since $\mathbb{N} \cup \{0\}$ is well-ordered, S has a least element, or there exists $q_0 \in \mathbb{Z}$ such that $0 \leq a - q_0 b < s$ for any $s \in S$. Suppose $b \leq a - q_0 b$. Then $0 \leq a - (q_0 + 1)b < a - q_0 b$ given $0 < b$, and hence a contradiction since $a - (q_0 + 1)b \in S$. If $a - q_0 b \leq \frac{1}{2}b$, choose $q = q_0$ and $r = a - q_0 b$. Otherwise, we have $\frac{1}{2}b < a - q_0 b < b$. Subtracting b, we obtain $-\frac{1}{2}b < a - (q_0 + 1)b < 0$, so $|a - (q_0 + 1)b| < \frac{1}{2}b$. Then choose $q = q_0 + 1$ and $r = a - (q_0 + 1)b$. If $a < 0$ and $0 < b$, then we have shown there exist $q_1, r_1 \in \mathbb{Z}$ such that $-a = q_1 b + r_1$ and $|r_1| \leq \frac{1}{2}b$. Then choose $q = -q_1$ and $r = -r_1$. If $0 \leq a$ and $b < 0$, then similarly there exist $q_2, r_2 \in \mathbb{Z}$ such that $a = q_2(-b) + r_2$ and $|r_2| \leq \frac{1}{2}(-b) = \frac{1}{2}|b|$. Then choose $q = -q_2$ and $r = r_2$. If $a < 0$ and $b < 0$, then there exist $q_3, r_3 \in \mathbb{Z}$ such that $-a = q_3(-b) + r_3$ and $|r_3| \leq \frac{1}{2}(-b) = \frac{1}{2}|b|$. Then choose $q = q_3$ and $r = -r_3$. One can check via direct computation that these choices are satisfactory, or $a = qb + r$ and $|r| \leq \frac{1}{2}b$. □

Proposition 2.12. *$(\mathbb{Z}[D], N)$ is a Euclidean Domain if $D = -1$ or $D = -2$.*

Proof. Let $a, b \in \mathbb{Z}[D]$ with $b \neq 0$. We have $a = \alpha_1 + \alpha_2\sqrt{D}$ and $b = \beta_1 + \beta_2\sqrt{D}$ for some $\alpha_i, \beta_i \in \mathbb{Z}$. Then

$$\begin{aligned} a\bar{b} &= (\alpha_1 + \alpha_2\sqrt{D})(\beta_1 - \beta_2\sqrt{D}) \\ &= (\alpha_1\beta_1 - D\alpha_2\beta_2) + (\alpha_2\beta_1 - \alpha_1\beta_2)\sqrt{D}. \end{aligned}$$

Since $N(b) \in \mathbb{Z}$, there exist by Lemma 2.11 $q_1, r_1 \in \mathbb{Z}$ such that

$$\alpha_1\beta_1 - D\alpha_2\beta_2 = q_1(N(b)) + r_1 \text{ and } |r_1| \leq \frac{1}{2}N(b),$$

and there exist q_2, r_2 such that

$$\alpha_2\beta_1 - \alpha_1\beta_2 = q_2(N(b)) + r_2 \text{ and } |r_2| \leq \frac{1}{2}N(b).$$

Thus, we have, by substituting and rearranging,

$$a\bar{b} = (q_1 + q_2\sqrt{D})N(b) + (r_1 + r_2\sqrt{D}).$$

By Lemma 2.5, $N(b) = b\bar{b}$. Then $\bar{b}$ divides $a\bar{b}$ and $N(b)$, so it divides $r_1 + r_2\sqrt{D}$ by Lemma 1.8. Then there exists $r \in \mathbb{Z}[D]$ such that $r_1 + r_2\sqrt{D} = r\bar{b}$. Thus,

$$a\bar{b} = (q_1 + q_2\sqrt{D})(b\bar{b}) + r\bar{b} = ((q_1 + q_2\sqrt{D})(b) + r)\bar{b}.$$

Since $\bar{b} \neq 0$, we have $a = (q_1 + q_2\sqrt{D})b + r$ by Lemma 1.9. By Lemma 2.3 and Lemma 2.5,

$$\begin{aligned} N(r\bar{b}) &= N(r)N(\bar{b}) \\ &= N(r)N(b) \end{aligned}$$

and by substitution,

$$\begin{aligned} N(r\bar{b}) &= N(r_1 + r_2\sqrt{D}) \\ &= r_1^2 - Dr_2^2 \\ &\leq (\frac{1}{2}N(b))^2 - D(\frac{1}{2}N(b))^2 \end{aligned}$$

by the inequalities above. Therefore,

$$N(r)N(b) \leq (\frac{1}{2}N(b))^2 - D(\frac{1}{2}N(b))^2.$$

Dividing by $N(b)$ and simplifying, we have

$$N(r) \leq \frac{1}{4}N(b) - D\frac{1}{4}N(b).$$

If $D = -1$, then $N(r) \leq \frac{1}{2}N(b)$. If $D = -2$, then $N(r) \leq \frac{3}{4}N(b)$. Thus for $D = -1$ or $D = -2$, there exist $q = q_1 + q_2\sqrt{D}, r \in \mathbb{Z}[D]$ such that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$. This proof follows from one by Tim Ratigan at [2]. □

3. Acknowledgements

It is a pleasure to thank my mentor, Zana Tran, for her guidance in the process of writing this paper. Through lectures and conversations, Zana's insight truly helped clarify and illuminate various concepts discussed here. I also thank Professor J. Peter May and fellow REU participant Oliver Bock for helping me revise and edit this paper.

4. Bibliography

References

[1] https://math.stackexchange.com/questions/70976/why-is-mathbbz-sqrt-n-n-ge-3-not-a-ufd?noredirect=1lq=1

[2] https://math.stackexchange.com/questions/600424/prove-that-the-gaussian-integers-ring-is-a-euclidean-domain

[3] Stillwell, John. Algebraic Number Theory for Beginners: Following a Path from Euclid to Noether. Cambridge University Press, 2022.