INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600
Euclidean Systems

by

Stefan G. Treatman

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
1996

Doctoral Committee:

Professor James S. Milne, Chair
Associate Professor Jerry Blackstone
Assistant Professor Neil Dumigan
Associate Professor Tom Hales
Professor John Stembridge
To Mom and Dad
ACKNOWLEDGEMENTS

Thanks to my advisor James Milne for all his help and patience. To Neil Dummi-gan for his invaluable assistance without which this thesis would not have happened. Thanks also to Greg Martin for letting me bounce ideas around and for helping me to organize my ideas. I would like to thank my parents, my brothers and sisters Jack, Ethyl, Howard, and Jeremy, and the rest of my growing family for the uncondi-tional love and support they have shown throughout the years. To all my friends for life, you know who you are. You're the best. Finally, a special thanks to all my friends at Michigan who made graduate school survivable. I would especially like to acknowledge the Arts Chorale and the Rodents of Unusual Size for sustaining me throughout my five years in Ann Arbor.
# TABLE OF CONTENTS

DEDICATION ......................................................... ii  
ACKNOWLEDGEMENTS ................................................. iii  
LIST OF FIGURES ..................................................... v  

CHAPTER  
1. Introduction ..................................................... 1  
   1. Outline ....................................................... 1  
   2. Notations ..................................................... 1  
2. History ......................................................... 3  
3. Euclidean Systems ................................................ 7  
4. The Minimal Algorithm For A Euclidean Ideal Class ........... 22  
   1. Preliminaries ................................................ 22  
   2. Explicit Description of $\theta_c$ ............................ 28  

BIBLIOGRAPHY ....................................................... 42  

iv

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
LIST OF FIGURES

Figure

3.1 ................................................. 18
3.2 ................................................. 18
4.1 ................................................. 35
CHAPTER 1

Introduction

1. Outline

A Euclidean ring such as the integers is equipped with an algorithm for division with remainder. In non-Euclidean Dedekind domains with cyclic class group, Lenstra [5] generalized the notion of a Euclidean ring with his definition of a Euclidean ideal class. Let $K$ be a number field and let $S$ be a finite set of primes of $K$ which contains the infinite primes $S_{\infty}$. Then for any ring of $S$-integers of $K$, we define a Euclidean system, further generalizing the notion of a Euclidean ring. We show in Theorem 10 that for sufficiently large $S$, if we assume a generalized Riemann hypothesis, then a ring of $S$-integers has a Euclidean system, generalizing work of Weinberger [9] in which the class group is trivial. In the case that the class group is cyclic, we then know there is an algorithm for a generalized division with remainder. In Theorem 21, we discuss the minimal algorithm in this case, generalizing work of Lenstra [4] in which the class group is trivial.

2. Notations

We will use the following notations and conventions. Let $K$ be a number field, with $\mathcal{O}_K$ its ring of integers and $S$ a finite set of primes of $K$ containing $S_{\infty}$, the set
of infinite primes.

- \( R_S = \{ x \in K : \text{ord}_p x \geq 0 \text{ for all primes } p \not\in S \} \) is called the ring of \( S \)-integers of \( K \).

- The ideals of \( R_S \) are in one-to-one correspondence with the ideals of \( \mathcal{O}_K \) which are not divisible by any primes of \( S \).

- \( I^S = \{ \prod_{p \in S} p^{n(p)} \}, \text{ such that } n(p) \in \mathbb{Z} \text{ and } n(p) = 0 \text{ for all but finitely many primes } p \}. \text{ We identify } I^S \text{ with the group of all fractional ideals of } R_S. \)

- For an ideal \( b \) of \( \mathcal{O}_K \) with \( \text{ord}_p b = 0 \) for all \( p \in S \), \( I^{S,b} = \{ \prod_{p \in S} p^{n(p)} \text{ where } n(p) \in \mathbb{Z} \text{ and } n(p) = 0 \text{ for all but finitely many primes } p \}. \text{ We identify } I^{S,b} \text{ with the group of fractional ideals of } R_S \) generated by primes not dividing the ideal \( bR_S \).

- For an ideal \( b \) of \( \mathcal{O}_K \), \( K_{b,1} = \{ x \in K : (x) = \frac{(a)}{(b)} \}, \text{ where } ((a), b) = \mathcal{O}_K \text{ and } \text{ord}_p (x - 1) \geq m(p), \text{ where } b = \prod_{p \in \mathfrak{p}} p^{m(p)} \}.

- For an ideal \( b \) of \( \mathcal{O}_K \), \( I^b = \{ \prod_{p \in b} p^{n(p)} \}, \text{ with } n(p) \in \mathbb{Z} \text{ and } n(p) = 0 \text{ for all but finitely many } p \}.

- If \( p \) is a prime of \( \mathcal{O}_K \), then \( K_p \) is the completion at \( p \).

- For any \( n \), \( \zeta_n \) is a primitive \( n \)-th root of unity.

- \( I \) is the group of all fractional ideals of \( \mathcal{O}_K \) which we identify with \( \{ \prod_{\text{p prime}} p^{n(p)} \}, \text{ with } n(p) \in \mathbb{Z} \text{ and } n(p) = 0 \text{ for all but finitely many } p \}.

- \( i \) is the natural map of \( K^\times \) into \( I \).

- \( Cl_{R_S} \) is the ideal class group for the ring \( R_S \).
CHAPTER 2

History

Definition 1. A ring $R$ is said to be Euclidean if there is a function $\phi : R \rightarrow \mathbb{N}$ such that $\forall a, b \in R$, with $b \neq 0$, $\exists q, r \in R$ such that $a = bq + r$ with $\phi(r) < \phi(b)$. We say that $\phi$ is a Euclidean algorithm for $R$.

In 1979, Lenstra [5] generalized the notion of a Euclidean ring by defining a Euclidean ideal class. We give a version of that definition here. Let $R$ be a Dedekind domain with ideal class group $Cl_R$ and field of fractions $K$. Let $E = \{ b : b$ is a fractional ideal of $R$ and $b \supseteq R \}$.

Definition 2. Let $C$ be an ideal class of $Cl_R$ with $c \in C$. We say a function $\psi : E \rightarrow \mathbb{N}$ is a Euclidean algorithm for $C$ if $\forall b \in E$ and $\forall x \in bc \setminus c$, $\exists z \in x + c$ such that $\psi(bcz^{-1}) < \psi(b)$. In this situation, we call $C$ a Euclidean ideal class.

It is routine to check that this definition is independent of the choice of representative $c \in C$ and that $bcz^{-1} \in E$.

The notion of a Euclidean ideal class generalizes that of a Euclidean ring. This is seen in the following lemma originally stated by Lenstra [5].
Lemma 3. Let $R$ be a Dedekind domain. Then $R$ is a Euclidean ring if and only if $[R]$ is a Euclidean ideal class.

Proof. Assume $R$ is a Euclidean ring. Then $R$ is a principal ideal domain so that $Cl_R$ is trivial. Let $C = [R]$ and let $c = R$ be the representative. We show that $[R]$ is a Euclidean ideal class.

As $R$ is Euclidean, Samuel [8, p. 284] shows that there is a minimal Euclidean algorithm $φ$ for $R$ (in the classical sense) satisfying

\[(i) \quad \forall a, b \in R, \ ab \neq 0, \ φ(ab) \geq φ(b), \text{ with equality } \iff a \in R^x,\]

and \[(ii) \quad φ(a) = 1 \iff a \in R^x.\]

Since $R$ is a principal ideal domain, any fractional ideal $b$ of $R$ which contains $R$ can be written as $b = (\frac{1}{b}) = \{ t \frac{1}{b} : \ t \in R \}$ for some $b \in R$. Let $E = \{ b : b$ is a fractional ideal of $R$, and $b \supseteq R \}$. Define $ψ : E \rightarrow \mathbb{N}$ by $ψ(\frac{1}{b}) = φ(b) - 1$.

This is well-defined, for if we express $b = (\frac{1}{b}) = (\frac{1}{b'})$, then $b' = ab$, for some $a \in R^x$. Thus $φ(b') = φ(ab) = φ(b)$. Let $b = (\frac{1}{b})$ be given. Then for all $x \in bR \setminus R$, we must find $z \in x + R$ such that $ψ(bRz^{-1}) < ψ(b)$. Now any $x \in bR$ is of the form $x = \frac{t}{b}$ for some $t \in R$. Because $φ$ is a Euclidean algorithm for $R$, we can find $q, r \in R$ such that $t = bq + r$, with $φ(r) < φ(b)$. Note that as $x \in b \setminus R$, $r \neq 0$. Let $z = \frac{t}{b} - q = \frac{t - bq}{b} \in x + R$. Then

\[
ψ(\frac{1}{b})Rz^{-1}) = ψ(\frac{1}{b})(\frac{b}{t - bq}) = ψ(\frac{1}{t - bq}) = ψ(\frac{1}{r}) = φ(r) - 1 < φ(b) - 1 = ψ(\frac{1}{b}).
\]
Now assume that $[R]$ is a Euclidean ideal class with Euclidean algorithm $\psi$ and let $R$ represent the class $[R]$. Define $\phi : R \to \mathbb{N}$ by $\phi(b) = \psi(\frac{1}{b}) + 1$, if $b \neq 0$ and $\phi(0) = 0$. Given $a, b \in R$ with $b \neq 0$, we seek $q, r \in R$ such that $a = bq + r$ with $\phi(r) < \phi(b)$. Assume first that $b$ does not divide $a$. Let $b = \frac{1}{b}$ and consider $x = \frac{a}{b} \in bR \setminus R$. Then since $\psi$ is Euclidean for $[R]$, there is some $z = \frac{a}{b} + R$. say $z = \frac{a}{b} - q$, such that $\psi(bz^{-1}) < \psi(b)$. This implies

\[
\psi\left(\frac{1}{b}\left(\frac{b}{a - bq}\right)\right) < \psi\left(\frac{1}{b}\right),
\]

\[
\Rightarrow \psi\left(\frac{1}{a - bq}\right) < \psi\left(\frac{1}{b}\right),
\]

\[
\Rightarrow \phi(a - bq) - 1 < \phi(b) - 1,
\]

\[
\Rightarrow \phi(a - bq) < \phi(b).
\]

Thus if $b$ does not divide $a$, we may write $a = bq + r$, with $r = a - bq$ and $\phi(r) < \phi(b)$. If $b$ divides $a$, then we may write $a = bq$ for some $q \in R$. Thus $r = 0$ and $\phi(r) = 0 < 1 < 1 + \psi\left(\frac{1}{b}\right) = \phi(b)$. \hfill \Box

Now let $R$ be a ring of $S$-integers of a number field $K$. Let $N$ be the usual norm on $R$. That is, $N(x) = \#R/(x)$. If we extend $N$ to $\tilde{N} : K \to \mathbb{Q}$ by $\tilde{N}(\frac{a}{b}) = N(a)/N(b)$ and $N(0) = 0$, then it is routine to check that $N$ is a Euclidean algorithm for a ring $R$ if and only if $\forall x \in K, \exists y \in R$ such that $\tilde{N}(x - y) < 1$. The notion of a Euclidean ideal class becomes more accessible when the function $\psi$ is given by the norm by $\psi(b) = N(b^{-1})$. Here $N$ is defined on all integral ideals $a$ by $N(a) = \#R/a$ and extended by multiplicativity to all fractional ideals, with $N((0)) = 0$. Then $N$ is a Euclidean algorithm for a class $C$, with $c \in C$, if and only if $\forall x \in K, \exists y \in c$ such that $N((x - y)) < N(c)$. Note that when $C = [R]$ and $c = R$, then $N(c) = 1$. Thus, $N$ is a Euclidean algorithm for $R \iff \psi$ is a Euclidean algorithm for $[R]$. This we already knew from Lemma 3.
If one does not assume a generalized Riemann hypothesis, there are no known examples of number fields $K$ with full ring of integers $R$ for which $N$ is not a Euclidean algorithm, but some other function is. It is known that $N$ is not a Euclidean algorithm for $\mathbb{Z}[\sqrt{14}]$ and much has been done to find another function which makes $\mathbb{Z}[\sqrt{14}]$ Euclidean (see [6, 2]). If $R$ is the ring of integers in a quadratic extension of $\mathbb{Q}$, there are only a few rings [5, p. 123] with class number $> 1$ for which $N$ is a Euclidean algorithm for a non-principal class $C$.

The main result proved by Lenstra [5] about Euclidean ideal classes is the following.

**Theorem 4 (Lenstra).** Let $R$ be a Dedekind domain with Euclidean ideal class $C$. Then $\text{Cl}_R$ is cyclic and is generated by $C$.

This generalizes the fact that if $R$ is a Euclidean ring, then $R$ is a principal ideal domain.
CHAPTER 3

Euclidean Systems

In the previous section, we saw that through the definition of a Euclidean ideal class, we can generalize the notion of a Euclidean ring to certain Dedekind domains with cyclic class group. In fact, we will see that for $\#S \geq 2$, assuming a generalized Riemann hypothesis, a ring of $S$-integers with cyclic class group has a Euclidean ideal class. Thus such a ring can be given an arithmetic structure which generalizes that of a Euclidean ring. We now explore more generally what can be said if the class group is any finite Abelian group.

**Definition 5.** Given a number field $K$ and a Dedekind domain $R$ whose field of fractions is $K$, let $\{C_1, \ldots, C_k\}$ be distinct classes in the ideal class group of $R$. Let $c_i \in C_i$ be a representative of each class with all $c_i$ pairwise co-prime. Let $E = \{b : b \supseteq R\}$ be the set of all fractional ideals of $R$ which contain $R$. Let $c = \bigcap_{i=1}^{k} c_i$. We say that $\{C_1, \ldots, C_k\}$ is a Euclidean system for $R$ if there is a function $\psi : E \to \mathbb{N}$ such that $\forall b \in E$ and $\forall x \in bc \setminus c$, there is some $c_j$ for which there exists $z \in x + c_j$ with $\psi(bc_jz^{-1}) < \psi(b)$. Such a function $\psi$ is said to be Euclidean for $\{C_1, \ldots, C_k\}$ or a Euclidean algorithm for $\{C_1, \ldots, C_k\}$ We call $\{C_1, \ldots, C_k\}$ a minimal Euclidean system for $R$ if no proper subset forms a Euclidean system.
We note that if $k = 1$, $\{C_1\}$ is a Euclidean system if and only if $C_1$ is a Euclidean ideal class. It is not hard to see that the definition is independent of the choice of representative for each class $C_i$.

**Lemma 6.** Let $\{C_1, ..., C_k\}$ be a Euclidean system for $R$ with function $\psi$. Then $\forall a, b \in E, \psi(ab) \geq \psi(b)$, with equality $\iff a = R$.

**Proof.** Fix $b \in E$. Choose $a' \in E$ such that $\psi(a'b)$ is minimal. Let $x \in a'c \setminus c$. Then $x \in a'bc \setminus c$ as well. Thus by definition, there is some $c_j$ and $z \in x + c_j$ with $\psi(a'bc_jz^{-1}) < \psi(a'b)$. But as $x \in a'c \subseteq a'c_j$, we see $z \in a'c_j + c_j \subseteq a'c_j$. Thus $z \in a'c_j$ so we have $a'c_jz^{-1} \in E$. This implies that $\psi((a'c_jz^{-1})b) < \psi(a'b)$ contradicts the minimality of $\psi(a'b)$. The only way to avoid this is for $a'c \setminus c$ to be empty. This occurs if and only if $a' = R$. Thus $\psi(ab)$ takes its minimal value if and only if $a = R$ in which case we have equality $\psi(ab) = \psi(b)$. This implies that for all $a \neq R$, $\psi(ab) > \psi(b)$. $\square$

**Corollary 7.** If $\{C_1, ..., C_k\}$ is a Euclidean system with function $\psi$, then $\psi(a)$ assumes its minimal value only when $a = R$.

**Proof.** Take $b = R$ in Lemma 6. $\square$

**Theorem 8.** Let $K$ be a number field with $R$ a Dedekind domain whose field of fractions is $K$. Let $\{C_1, ..., C_k\}$ be a Euclidean system with function $\psi$. Then $\{C_1, ..., C_k\}$ generates the ideal class group $Cl_R$.

**Proof.** We first prove the following lemma.
Lemma 9. Let \( \{C_1, \ldots, C_k\} \) be a Euclidean system with function \( \psi \). If \( b \in E \setminus \{R\} \), then \( b \in \prod_{i=1}^{k} C_i^{-n_i} \) with \( n_i \geq 0 \) and \( \sum_{i=1}^{k} n_i \leq \psi(b) \).

Proof of Lemma. Let \( c_i \in C_i \) and \( c = \bigcap_{i=1}^{k} c_i \). Let \( b \in E \setminus \{R\} \). Then \( bc \setminus c \) is non-empty so that we can find \( x \in bc \setminus c \). By definition, there is some \( c_j \) and \( z \in x + c_j \) such that \( \psi(bc_jz^{-1}) < \psi(b) \). If \( bc_jz^{-1} = R \), then \([b][c_j] = [R]\) which means \( b \in C_j^{-1} \) and by Corollary 7.1 \( 1 \leq \psi(b) \). (By Corollary 7.1, \( bc_jz^{-1} = R \) will always occur if \( \psi(b) \) is the minimal value taken by \( \psi \) on \( E \setminus \{R\} \).) Now assume the lemma is true for all \( a \in E \) with \( \psi(a) < \psi(b) \). Then if \( bc_jz^{-1} \neq R \) we have by assumption that \( bc_jz^{-1} \in \prod_{i=1}^{k} C_i^{-n_i} \) with \( \sum_{i=1}^{k} n_i \leq \psi(bc_jz^{-1}) \). Therefore, \( b \in C_j^{-1} \prod_{i=1}^{k} C_i^{-n_i'} = \prod_{i=1}^{k} C_i^{-n_i'} \) where \( n'_i = n_i \) for \( i \neq j \), and \( n'_j = n_j + 1 \). Thus, \( \sum_{i=1}^{k} n'_i = 1 + \sum_{i=1}^{k} n_i \leq 1 + \psi(bc_jz^{-1}) \leq \psi(b) \). \( \square \)

To prove the theorem, we note that \( Cl_R \) is generated by \( \{[b] : b \in E\} \). The lemma then shows that each generator can be written as \( [b] = \prod_{i=1}^{k} C_i^{-n_i} \) which shows that \( \{C_1, \ldots, C_k\} \) generate the class group.

Remark. It is of interest to note that if \( b \neq R \) is such that \( \psi(b) \) is the minimal value assumed by \( \psi \) on \( E \setminus \{R\} \), then for each \( x \in bc \setminus c \), there is exactly one \( c_j \) such that there is a \( z \in x + c_j \) with \( \psi(bc_jz^{-1}) < \psi(b) \). For suppose there are \( c_{j_1} \) and \( c_{j_2} \) for which this happens, with \( z_{j_1} \in x + c_{j_1} \) and \( z_{j_2} \in x + c_{j_2} \). Then by minimality, we must have 

\[
(bc_{j_1}z_{j_1}^{-1}) = R = (bc_{j_2}z_{j_2}^{-1}).
\]

This implies that \([c_{j_1}] = [c_{j_2}]\) which shows that \( j_1 = j_2 \) as the \( C_i \) are distinct classes.

We now come to our main result.
Theorem 10. Let $K$ be a number field and $\mathcal{O}_K$ be its ring of integers. Let $S$ be a finite set of primes including $S_\infty$ and let $R_S$ be the ring of $S$-integers. Suppose the class number of $R_S$ is $h$ and the ideal class group $\text{Cl}_{R_S} \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$, with this structure given uniquely by $d_1 \mid d_2 \mid \cdots \mid d_n$. Let $\{C_1, C_2, \ldots, C_n\}$ be generators of $\text{Cl}_{R_S}$ with the order of $C_i = d_i$. Suppose the rank of the unit group in $R_S$ is $s$. Suppose further that for every square-free integer $m$ and for every subset $S' \subset S$, the zeta-function for $K(\zeta_m, R_S^{1/m})$ satisfies the generalized Riemann hypothesis. Then if $s \geq \max\{1, n-1\}$, $\{C_1, \ldots, C_n\}$ is a minimal Euclidean system for $R_S$.

Note that as $\{C_1, \ldots, C_n\}$ is a minimal set of generators for $\text{Cl}_{R_S}$, Theorem 8 shows that if it is a Euclidean system, then it must be minimal.

Proof. The proof is constructive. Given a set of generators $\{C_1, \ldots, C_n\}$, we shall write down a function $\psi$ and show that it makes $\{C_1, \ldots, C_n\}$ into a Euclidean system.

For each class $C_i$, we choose a prime ideal $c$ of $R_S$ as a representative and write $c = \bigcap_{i=1}^{n} c_i$. Let $E = \{b : b \supseteq R_S\}$ be the set of all fractional ideals of $R_S$ which contain $R_S$. Here, we identify all fractional ideals of $R_S$ with divisors $b = \prod_{p \in R_S} p^{n(p)}$, with $n(p) \in \mathbb{Z}$ and $n(p) = 0$ for all but finitely many primes $p$. We define $\psi : E \rightarrow \mathbb{N}$ by,

$$\psi(b) = \sum_{p \text{ prime}} \text{ord}_p(b^{-1})n_p, \quad (3.1)$$

where if $p \in \prod_{i=1}^{n} C_i^{m_i}$ is written uniquely with $1 \leq m_1 \leq d_1$ and $0 \leq m_i \leq d_i - 1$ for $2 \leq i \leq n$, then

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
\[
\begin{align*}
\text{value of } n_p & \quad \text{class of } Cl_K \\
h + 1 = 17 & \quad C_1 \text{ with } R_s^x \rightarrow (R_S/p)^x \\
h + 2 = 18 & \quad C_1^2, C_1C_2, C_1C_3 \\
h + 3 = 19 & \quad C_1^2C_2, C_1^2C_3, C_1C_2C_3, C_1C_2^2, C_1 \text{ with } R_s^x \not\rightarrow (R_S/p)^x \\
h + 4 = 20 & \quad C_1^2C_3, C_1^2C_3^2, C_1C_2C_3, C_1C_3^3 \\
h + 5 = 21 & \quad C_1^2C_2C_3, C_1^2C_3^2, C_1C_3C_3^2 \\
h + 6 = 22 & \quad C_1^2C_2C_3^2 
\end{align*}
\]

In this example, note that for a prime \( p \in C_1 \) with \( R_s^x \rightarrow (R_S/p)^x \) not surjective, we have \( n_p = h + 3 = h + 1 + d_1 \) as \( d_1 = 2 \). Also note that principal primes \( p \) have \( n_p = h + 2 = h + d_1 \). More generally, a principal prime \( p \) will always have \( n_p = h + d_1 \).

If \( n > 1 \), the largest value assumed by any \( n_p \) is always \( h + (d_1 + \cdots + d_n) - (n - 1) \). This occurs when all the \( m_i \) are maximal. In the above example, \( h + (d_1 + \cdots + d_n) - (n - 1) = h + (2 + 2 + 4) - (3 - 1) = h + 6 \). If \( n = 1 \), the class group is cyclic and the largest value assumed by any \( n_p \) is \( h + d_1 + 1 = 2h + 1 \).

In any case, the maximal value of \( n_p \leq 2h + 1 \). (3.2)
Having now defined our function $\psi : E \to \mathbb{N}$ in (3.1), we must show that it is Euclidean for $\{C_1, ..., C_n\}$. Let $E' = \{b : b$ is an integral ideal of $R_S\}$. Define a function $\tilde{\psi} : I^S \to \mathbb{Z}$ by:

$$
\tilde{\psi}(a) = \sum_{\text{prime } p \in R_S} \text{ord}_p(a)n_p,
$$

where $n_p$ is defined as above. Note that if $a$ is an integral ideal or a fractional ideal containing $R_S$, we have the following relationship:

$$
\tilde{\psi}(a) = \begin{cases} 
\psi(a), & \text{if } a \in E. \\
\psi(a^{-1}) = -\tilde{\psi}(a^{-1}), & \text{if } a \in E'. 
\end{cases}
$$

Let $a \in E'$ (so $a^{-1} \in E$). To show $\psi$ is Euclidean, for all $x \in a^{-1}c \setminus c$, we need to find some $c_j$ and $z \in x + c_j$ such that $\psi(a^{-1}c_jz^{-1}) < \psi(a^{-1})$, or equivalently, $\tilde{\psi}(ac_j^{-1}z) < \tilde{\psi}(a)$. Since $\tilde{\psi}$ is a homomorphism from $I^S \to (\mathbb{Z}, +)$, we see that $\psi$ is Euclidean if $\forall a \in E'$ and $\forall x \in a^{-1}c \setminus c$, $\exists c_j$ and $z \in x + c_j$ such that

$$
\tilde{\psi}(a) + \tilde{\psi}(c_j^{-1}) + \tilde{\psi}((z)) < \tilde{\psi}(a),
$$

i.e.

$$
\tilde{\psi}((z)) < -\tilde{\psi}(c_j^{-1}),
$$

i.e.

$$
\tilde{\psi}((z)) < \tilde{\psi}(c_j).
$$

This formulation is now independent of $a$. Note that $K = \bigcup_{a \in E'} a^{-1}c$. Thus in proving that $\psi$ is Euclidean, it suffices to show that

$$
\forall x \in K \setminus c$, there is some $c_j$ and $z \in x + c_j$ with $\tilde{\psi}((z)) < \tilde{\psi}(c_j). \quad (3.3)
$$

To prove (3.3), we begin with $x \in K \setminus c$. For any $1 \leq i \leq n$, consider the fractional ideal $(x)_{c_i}$ of $R_S$ and write $(x)_{c_i} = \frac{a_i}{b_i}$, with $a_i$ and $b_i$ uniquely written as co-prime integral ideals of $R_S$. Let $F_i$ be the $S$-ray class field for the modulus $b_i$ so that

$$
I^{b_i}/\hat{H}_i \cong \text{Gal}(F_i/K), \quad (3.4)
$$
where $\tilde{H}_i$ is the subgroup $i(K_{b_{1,i}})$, ($p \in S$) of $I^b$. (Note that $I^b/\tilde{H}_i \cong I^{S,b_i}/(i'(K_{b_{1,i}}))$, where if $\Pi$ is the projection of $I^b$ onto $I^{S,b_i}$, then $i' = \Pi \circ i$). As $(a_i, b_i) = R_S$, we have $a_i \in I^{S,b_i}$ and thus under the Artin reciprocity map [3, p. 197], $a_i$ corresponds to some $\tau \in Gal(F_i/K)$. In fact, there are infinitely many integral ideals $a'_i \in I^{S,b_i}$ such that $(a'_i, F_i/K) = \tau$. For any such $a'_i$, it follows that $a'_i \equiv a_i$ in $I^{S,b_i}/(i'(K_{b_{1,i}}))$. That is, $a'_i = (\gamma)a_i$ for some $\gamma \in K_{b_{1,i}}$. We may write

$$\gamma = 1 + t$$

with $ord_{4}(t) \geq n(q)$, where $b_i = \prod q^{n(q)}$. \hspace{1cm} (3.5)

Let $z = x\gamma = x(1 + t) = x + xt$. We now show that $xt \in c_i$ so that $z \in x + c_i$. Since $a_i(\gamma) = a'_i$ is an integral ideal in $R_S$, we have that for all $a \in a_i$, $a\gamma \in R_S$. This implies that $a + at \in R_S$ which in turn shows that $at \in R_S$. This shows that $a_i(t)$ is an integral ideal. We consider $\psi((z)) = \frac{a_i(c_i(t))}{b_i} = \frac{c_i}{b_i}a_i(t)$. By (3.5), $b_i$ divides the integral ideal $a_i(t)$ so that $\psi((z)) = c_i\tau$ for some integral ideal $\tau$. This implies that $\psi((z)) \equiv c_i \tau$ and that $z \in x + c_i$. So for any $x \in K \setminus c$, we have found $z \in x + c_i$ such that,

$$\tilde{\psi}(z) = \tilde{\psi}(x\gamma) = \tilde{\psi}\left[\frac{a_i(c_i(y))}{b_i}\right] = \tilde{\psi}\left[\frac{c_i a_i'}{b_i}\right]$$

$$= \tilde{\psi}(c_i) + \tilde{\psi}(a'_i) - \tilde{\psi}(b_i).$$

If we can choose $a'_i$ so that $\tilde{\psi}(a'_i) < \tilde{\psi}(b_i)$, then the above shows that $\tilde{\psi}(z) < \tilde{\psi}(c_i)$, satisfying (3.3). We therefore complete the proof of the theorem by showing that for at least one $i$, $1 \leq i \leq n$, we can find some $a'_i \in I^{S,b_i}$ with $a'_i \equiv a_i$ in $I^{S,b_i}/i'(K_{b_{1,i}})$ and $\tilde{\psi}(a'_i) < \tilde{\psi}(b_i)$.

If any $b_i$ is not prime then we are done. For by definition of $n_p$, if $b_i$ is not prime, then $\tilde{\psi}(b_i) \geq 2h + 2$. Now the Chebotarev density theorem [3, p. 169] guarantees that there are infinitely many primes $p \equiv a_i$ in $I^{S,b_i}/i'(K_{b_{1,i}})$. Choose any such $p$. Then by (3.2), $\tilde{\psi}(p) \leq 2h + 1$. Hence we may take $a'_i = p$ so that
$\tilde{\psi}(a_i') \leq 2h + 1 < 2h + 2 \leq \tilde{\psi}(b_i)$ as required. Henceforth, when writing $\frac{(x)}{c_i} = \frac{a_i}{b_i}$, we may assume that all $b_i$ are primes of $R_S$.

**Lemma 11.** Let \( \{C_1, \ldots, C_n\} \) be as above with prime \( c_i \in C_i \) and \( c = \prod_{i=1}^n c_i \). Let \( x \in K \setminus c \) be given and for each \( i \), write $\frac{(x)}{c_i} = \frac{a_i}{b_i}$ with all \( b_i \) primes of \( R_S \). Assume $b_1 \neq c_1$. Then for all \( i \), \( b_i = b_1 \). Write $b_1 \in C_1^{m_1}C_2^{m_2} \cdots C_n^{m_n}$, with this uniquely defined by $1 \leq m_1 \leq d_1$, $0 \leq m_i \leq d_i - 1$ for $2 \leq i \leq n$. Then for all \( i \), \( a_i \in C_1^{m_1}C_2^{m_2} \cdots C_i^{m_i-1} \cdots C_n^{m_n}$.

**Proof.** Since $\frac{(x)}{c_i} = \frac{a_1}{b_1}$, it is clear that $a_1 \in C_1^{m_1-1}C_2^{m_2} \cdots C_n^{m_n}$. Now for any \( i \neq 1 \),

$$\frac{(x)}{c_i} = \frac{(x)}{c_1} \frac{c_1}{c_i} = \frac{a_1}{b_1} \frac{c_1}{c_i} = \frac{a_i}{b_i},$$

As \( b_i \) is prime, it must be that $\frac{a_1}{b_1} \frac{c_1}{c_i}$ is not in lowest terms. But \( a_1 \) and \( b_1 \) are co-prime and by assumption, \( b_1 \neq c_1 \). Since all the \( c_i \) are distinct primes, we must have that \( c_i \) divides \( a_1 \). Hence, $\frac{a_1}{b_1} = \frac{a_1}{b_1} \frac{c_1}{c_i}$, where $a_1 = a_1/c_i$. It now follows that $b_i = b_1$ and that $a_i \in C_1^{m_1}C_2^{m_2} \cdots C_i^{m_i-1} \cdots C_n^{m_n}$. \[\square\]

We now complete the proof by considering the three possibilities for the prime \( b_1 \). Let $b_1 \in C_1^{m_1}C_2^{m_2} \cdots C_n^{m_n}$.

**Case 1:** $b_1 \in C_1$.

If the projection $R_S^\times \rightarrow (R_S/b_1)^\times$ is not surjective, then by definition of \( n_p \), $\tilde{\psi}(b_1) = h + 1 + d_1$. Clearly in this case, \( a_1 \) is principal. In the comments proceeding (3.2), we saw that any principal prime \( p \) has $\tilde{\psi}(p) = h + d_1$. Since $Cl_{R_S}$ is a quotient of the $S$-ray class group, any prime $p \equiv a_1$ in $I^{S,b_1}/I'(K_{b_1,1})$ will also be equivalent to
Theorem 4.4.2.18 (Continued)

Thus we take \( \alpha_i' = p \) for any \( p \equiv a_i \) in \( I^{S_{b_1}}/i'(K_{b_1,1}) \). Then \( p \) is principal and \( \varphi(\alpha_i') = \varphi(p) = h + d_i < h + d_i + 1 = \varphi(b_1) \).

If the projection \( R_S^x \rightarrow (R_S/b_1)^x \) is surjective, then by definition, \( \varphi(b_1) = h + 1 \).

Again \( a_i = (a_1) \) is principal with \( \alpha_i \in (R_S/b_1)^x \). It follows that \( (a_1) \equiv R_S \) in \( I^{S_{b_1}}/i'(K_{b_1,1}) \). Hence, we may choose \( \alpha_i' = R_S \) so that \( \varphi(\alpha_i') = \varphi(R_S) = 0 < h + 1 = \varphi(b_1) \).

Case 2: \( b_1 \not\in C_1, \; \varphi(b_1) > h + 2 \).

We know by definition that since \( \varphi(b_1) > h + 2 \) we have \( \sum_{i=1}^n m_i > 2 \). This leaves three possibilities: i) \( m_1 > 2 \), ii) for at least one \( i \in \{2, \ldots, n\} \) we have \( m_i \geq 2 \), or

iii) for some \( i_1, i_2 \in \{2, \ldots, n\} \), \( m_{i_1} \geq 1 \) and \( m_{i_2} \geq 1 \). In the case that \( m_1 > 2 \), we consider \( \frac{x}{c_1} = \frac{a_1}{b_1} \). It follows that \( a_1 \in C_1^{m_1-1}C_2^{m_2} \cdots C_n^{m_n} \). By definition of \( n_p \), any prime \( p \in C_1^{m_1-1}C_2^{m_2} \cdots C_n^{m_n} \) will have \( \varphi(p) = h + ((m_1 - 1) + m_2 + \cdots + m_n) = \varphi(b_1) - 1 \).

So take \( \alpha_i' = p \) where \( p \) is any prime of \( R_S \) and such that \( p \equiv a_1 \) in \( I^{S_{b_1}}/i'(K_{b_1,1}) \).

(The Chebotarev density theorem implies there are infinitely many such \( p \).) Then \( p \equiv a_1 \) in \( Cl_{R_S} \) too and we have found \( \alpha_i' \) such that \( \varphi(\alpha_i') = \varphi(p) = \varphi(b_1) - 1 < \varphi(b_1) \) as required.

In ii), we may assume that for some \( i \neq 1, \; m_i \geq 2 \). Then consider \( \frac{x}{c_i} = \frac{a_i}{b_i} \). By Lemma 11, we have \( b_i = b_1 \) and \( a_i \in C_1^{m_1}C_2^{m_2} \cdots C_i^{m_i-1} \cdots C_n^{m_n} \). Note that by definition of \( n_p \), any prime \( p \) in the same class as \( a_i \) will have \( \varphi(p) = h + (m_1 + m_2 + \cdots + (m_i - 1) + \cdots + m_n) = \varphi(b_1) - 1 \). By Chebotarev, we can find a prime \( p \in R_S \) with \( p \equiv a_i \) in \( I^{S_{b_1}}/i'(K_{b_1,1}) \). Then \( p \equiv a_i \) in \( Cl_{R_S} \) as well. We may take \( \alpha_i' = p \) so that \( \varphi(\alpha_i') = \varphi(p) = \varphi(b_i) - 1 < \varphi(b_i) \), as required.
In $iii)$, we have $i_1$ and $i_2$ such that $m_{i_1} \geq 1$ and $m_{i_2} \geq 1$. As in $ii)$, we consider
\[
\frac{x}{c_{i_1}} = \frac{a_{i_1}}{b_{i_1}}.
\]
Again by Lemma 11, we have $b_{i_1} = b_1$ and $a_{i_1} \in C_{i_1}^{m_1} C_{i_2}^{m_2} \cdots C_{i_{i_1 - 1}}^{m_{i_1 - 1}} \cdots C_{n}^{m_n}$. So by definition of $n_p$, any prime $p$ in the same class as $a_{i_1}$ will have $\bar{\psi}(p) = h + (m_1 + m_2 + \cdots + (m_{i_1} - 1) + \cdots + m_{i_2} + \cdots + m_n) = \bar{\psi}(b_1) - 1$. So by Chebotarev, we can find a prime $p \in R_S$ such that $p \equiv a_{i_1}$ in $I^{S,b_1}/i'(K_{b_1,1})$. Then $p \equiv a_{i_1}$ in $Cl_{R_S}$ as well. We may take $a'_{i_1} = p$ so that $\bar{\psi}(a'_{i_1}) = \bar{\psi}(p) = \bar{\psi}(b_1) - 1 < \bar{\psi}(b_{i_1})$, as required.

Case 3: $b_1 \notin C_i$. $\bar{\psi}(b_1) = h + 2$.

By definition, $b_1 \in C_i C_j$ for some $j \in \{1, 2, \ldots, n\}$. To mimic the above arguments, we need to find a class of $Cl_{R_S}$ in which primes $p$ will have $\bar{\psi}(p) = h + 1$. This can only happen if $p \in C_i$ and $R_S^p \longrightarrow (R_S/p)^X$ is surjective. Hence we consider
\[
\frac{x}{c_j} = \frac{a_j}{b_j}.
\]
By Lemma 11, $b_j = b_1$ and $a_j \in C_i$. Let $\tau = (a_j, F_1/K)$. We seek a prime $p \in R_S$ such that $p \equiv a_j$ in $I^{S,b_1}/i'(K_{b_1,1})$ with $R_S^p \longrightarrow (R_S/p)^X$. This is equivalent to finding $p$ such that $(p, F_1/K) = \tau$ and $R_S^p \longrightarrow (R_S/p)^X$, where $F_1$ is the $S$-ray class field for the modulus $b_1$.

To find such $p$, we apply a theorem of Lenstra [4, (4.8) p. 208]. We consider the special case of this theorem in which $F_1$ is the $S$-ray class field for the modulus $b_1$, $C = \{\tau\}$, $W = R_S^p$, and $k = 1$. We assume that for every subset $S' \subset S$ and for every square-free integer $m$ that the zeta-function for $K(\zeta_m, R_S^{1/m})$ satisfies the generalized Riemann hypothesis. Then the theorem says that the set of primes $p$, for which $(p, F_1/K) = \tau$ and $R_S^p \longrightarrow (R_S/p)^X$ is surjective, is infinite if and only if there is no prime $l$ for which there is a field $L_l = K(\zeta_l, R_S^{1/\ell})$ such that $K \subset L_l \subseteq F_1$ and $\tau \in Gal(F_1/L_l)$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
If we can show no such field $L_1$ exists with $K \subset L_1 \subsetneq F_1$ and $\tau \in \text{Gal}(F_1/L_1)$, then we can always find a suitable prime $p \in R_\mathcal{S}$ with $\bar{\psi}(p) = h + 1 < h + 2 = \bar{\psi}(b_1)$. In this event, we take $\alpha' = p$ and then $\bar{\psi}(\alpha') < \bar{\psi}(b)$ as required. Thus we complete the proof of Theorem 10 if we can show there is no such $L_1$ as above. Henceforth, we suppose such an $L_1$ exists as above, and derive a contradiction.

**Lemma 12.** With the current definitions, if there is an $L_1$ with $K \subset L_1 \subsetneq F_1$ and $\tau \in \text{Gal}(F_1/L_1)$, then $\zeta_1 \in K$.

**Proof.** By class field theory, $F_1/K$ is an Abelian (Galois) extension. Hence any intermediate field must be Abelian over $K$ as well. In particular, let $u$ be any unit of $R_\mathcal{S}$ which is not an $l$-th power, for instance, any fundamental unit. Let $K' = K(u^{1/l}) \subset L_1$, so $[K' : K] = l$. Then $K'$ is Abelian over $K$ and must be the splitting field of $x^l - u$ over $K$. This implies that $K' = K(\zeta_1, u^{1/l})$. Clearly we have $K \subseteq K(\zeta_1) \subseteq K'$. But note that $[K(\zeta_1) : K] \leq l - 1$ and divides $[K' : K] = l$ so that $[K(\zeta_1) : K]$ must be 1. Therefore $\zeta_1 \in K$. □

Next, we note that since $\text{Cl}_{R_\mathcal{S}}$ is a quotient of $I^S_{\mathcal{H}_1}/i'(K_{b_1,1})$, the S-Hilbert class field $H$ of $K$ is a subfield of $F_1$. This produces the tower of fields in Figure 3.1.

We consider the field $H \cap L_1$. We have $\tau \in \text{Gal}(F_1/K)$ such that $\tau$ fixes $L_1$. But recall that $\tau = (\alpha_j, F_1/K)$ and $\alpha_j \in \mathcal{C}_1$. This means that $\tau|_H = \sigma_1$, where $\sigma_1$ corresponds to $\mathcal{C}_1$ under the isomorphism $\text{Cl}_{R_\mathcal{S}} \cong \text{Gal}(H/K)$. Therefore, $\sigma_1$ generates a subgroup of $\text{Gal}(H/K)$ of order $d_1$. It follows that if $H'$ denotes the fixed field of $\sigma_1$, then

$$\text{Gal}(H'/K) \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}. \quad (3.6)$$

Since $\tau$ fixes $L_1$, it must be that $L_1 \cap H \subsetneq H'$. We now have a tower as shown in Figure 3.2. Further, by Galois theory, we know that
Figure 3.1:

Figure 3.2:
[L_l : H \cap L_l] divides [F_1 : H]. \hspace{1cm} (3.7)

To determine [F_1 : H], we examine the exact sequence

$$0 \longrightarrow (R_S/b_1)^X / \pi(R_S^X) \longrightarrow I^{S,b_1,i}(K_{b_1,1}) \longrightarrow Cl_{R_S} \longrightarrow 0,$$

where $\pi : R_S^X \longrightarrow (R_S/b_1)^X$ is the natural projection. To see why this is exact, we recognize that the $S$-ray class group $I^{S,b_1,i}(K_{b_1,1})$ projects naturally onto $Cl_{R_S} = I^S/i'(K^X)$. We determine that the kernel of this projection consists of those fractional ideals of $I^{S,b_1,i}(K_{b_1,1})$ which are principal. These are of the form $\left(\frac{a}{b}\right)$ for some $a, b \in (R_S/b_1)^X$. Now, if $\bar{b} \in R_S$ represents a multiplicative inverse of $b$ in $(R_S/b_1)^X$.

then we see that

$$\left(\frac{a}{b}\right) \equiv (a\bar{b}) \text{ in } I^{S,b_1,i}(K_{b_1,1}).$$

Thus every principal fractional ideal of $I^{S,b_1}$ can be represented in $I^{S,b_1,i}(K_{b_1,1})$ by an integral ideal $(a\bar{b})$ where $a\bar{b} \in (R_S/b_1)^X$. But we must consider that for any unit $u \in R_S^X$. and for any $x \in (R_S/b_1)^X$, we have $(x) = (xu)$. Thus the kernel is given by $i((R_S/b_1)^X / \pi(R_S^X))$ and the above sequence is exact. Thus $\#(I^{S,b_1,i}(K_{b_1,1})) = \#Cl_{R_S} \cdot \#((R_S/b_1)^X / \pi(R_S^X))$. This yields

$$[F_1 : K] = h \cdot \#((R_S/b_1)^X / \pi(R_S^X)), \hspace{1cm} (3.4)$$

by (3.4). As $[H : K] = h$, we have determined that

$$[F_1 : H] = \#((R_S/b_1)^X / \pi(R_S^X)). \hspace{1cm} (3.8)$$

To determine $[L_l : H \cap L_l]$, we note that by Lemma 12. $L_l$ is a Kummer extension [7, p.15] of $K$. In fact, if $\{u_1, \ldots, u_s\}$ form a system of fundamental units of $R_S^X$, then $L_l = K(u_1^{1/l}, \ldots, u_s^{1/l}, \zeta_r^{1/l})$, where $r \geq 1$ is maximal such that $\zeta_r \in K$. Hence, $[L_l : K] = l^{s+1}$ and $Gal(L_l/K) \cong \mathbb{Z}/l\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/l\mathbb{Z}$, where there
are \( s + 1 \) copies. Because \( \text{Gal}(H \cap L_i/K) \) is a quotient of \( \text{Gal}(L_i/K) \), we have 
\[
\text{Gal}(H \cap L_i/K) \cong \Z/l\Z \oplus \cdots \oplus \Z/l\Z,
\]
with the number of copies equal to some \( t \leq s + 1 \). But \( \text{Gal}(H \cap L_i/K) \) must also be a quotient of \( \text{Gal}(H'/K) \), so by (3.6), 
\( t \leq n - 1 \). By assumption, \( s \geq \max\{1, n - 1\} \) so that \( s + 1 \geq \max\{2, n\} \). It follows that \( t < s + 1 \) and 
\[
[L_i : H \cap L_i] = l^{s+1-t} \tag{3.9}
\]

As a result, there is some unit \( u \in \{u_1, \ldots, u_s, \zeta_r\} \) such that \( K(u^{1/l}) \not\subset H \cap L_i \). Let 
\( K' = K(u^{1/l}) \). Because \( K' \not\subset H \) and \( H \) is the maximal unramified Abelian extension of \( K \), \( K'/K \) is ramified at some prime \( l \) of \( R_S \). In fact, since the minimal polynomial for \( u^{1/l} \) over \( K \) is \( f(x) = x^l - u \), we have 
\[
\text{Disc}(f(x)) = \text{Disc}(x^l - u) = \pm Nm_{K'/K}(u^{1/l})^{l-1} = \pm l^t u^{l-1}.
\]

So \( \text{Disc}(f(x)) = (l)^t \) which shows that \( \text{Disc}(K'/K) \) divides \( (l)^t \). Thus, \( l \) must be a prime of \( R_S \) lying over \( l \). On the other hand, \( K' \subset F_l \) and the only primes of \( R_S \) which ramify in \( F_l \) are those dividing the modulus \( b_1 \). However, \( b_1 \) is prime and we conclude that \( b_1 = l \) and thus \( R_S/b_1 \) has characteristic \( l \). From (3.8), we see now that \( [F_l : H] \) divides \( l^f - 1 \), for some \( f \geq 1 \). But we have already established in (3.9) that \( [L_i : H \cap L_i] = l^{k} \), for some \( k \geq 1 \). This contradicts (3.7). Thus there can be no such \( L_i \) with \( K \subset L_i \subset F_l \) and \( \tau \in \text{Gal}(F_l/L_i) \). This completes the proof of the theorem. \( \square \)

**Conclusion:** Recall that if a ring \( R \) is Euclidean with a multiplicative function \( \psi \) which is extended to \( \bar{\psi} : K \rightarrow \Q \) by \( \bar{\psi}(\frac{a}{b}) = \psi(a)/\psi(b) \) and \( \psi(0) = 0 \), then the
division algorithm can be stated as: \( \forall x \in K, \exists y \in R \) such that \( \tilde{\psi}(x - y) < 1 \). A Euclidean system generalizes this in the following way. Because \( \tilde{\psi} \) is a homomorphism, we have that \( \forall x \in K \setminus c \), there is some \( c \), such that \( \exists y \in c \), such that \( \tilde{\psi}((x - y)) < \tilde{\psi}(c) \).

**Remark:** In the special case of Theorem 10 in which \( n = 1 \), \( d_1 \geq 1 \). \( R_S \) has a cyclic class group of order \( h = d_1 \). The theorem then says that \( \{C_1\} \) is a minimal Euclidean system which is equivalent to saying that \( C_1 \) is a Euclidean ideal class. This proves a theorem originally stated by Lenstra [5, p. 127]. The algorithm is then given by

\[
n_p = \begin{cases} 
  h + 1, & \text{if } p \in C_1 \text{ and } R_S^x \rightarrow (R_S/p)^x \text{ is surjective.} \\
  h + 2, & \text{if } p \in C_1^2. \\
  \vdots & \vdots \\
  2h, & \text{if } p \in C_1^h, \text{ i.e., } p \text{ is principal.} \\
  2h + 1, & \text{if } p \in C_1, \text{ } R_S^x \rightarrow (R_S/p)^x \text{ is not surjective.}
\end{cases}
\]

This is not the minimal possible algorithm. The minimal algorithm is discussed in the next section.

**Remark:** If we take the special case of Theorem 10 in which \( n = 1 \) and \( d_1 = 1 \), then \( Cl_{R_S} \) is trivial and thus \( Cl_{R_S} = \{[R_S]\} \). The theorem then says that if \( R_S \) is a PID and the number of units is infinite, then assuming a generalized Riemann hypothesis, \( \{[R_S]\} \) is a Euclidean system. Equivalently, \( [R_S] \) is a Euclidean ideal class and thus \( R_S \) is a Euclidean ring, by Lemma 3. In this case the algorithm is given by:

\[
n_p = \begin{cases} 
  2, & \text{if the projection } R_S^x \rightarrow (R_S/p)^x \text{ is surjective.} \\
  3, & \text{otherwise.}
\end{cases}
\]

This is precisely the algorithm given by Weinberger [9] in his proof that for any ring \( R_S \) with infinitely many units and \( S = S_\infty \), assuming a generalized Riemann hypothesis, \( R_S \) is a PID \( \iff \) \( R_S \) is Euclidean.
CHAPTER 4

The Minimal Algorithm For A Euclidean Ideal
Class

1. Preliminaries

Let $K$ be a number field with $S$ a finite set of primes containing $S_{\infty}$ and $\#S \geq 2$. Let $R_S$ be the ring of $S$-integers and suppose the ideal class group $Cl_{R_S}$ is cyclic of order $h$. Let $C$ be any class which generates the class group. In the previous section, we saw that assuming a generalized Riemann hypothesis, $C$ must be a Euclidean ideal class. In this chapter, we determine the minimal algorithm, $\theta_C$, for $C$. As before, let $E = \{b : b \text{ is a fractional ideal of } R_S \text{ and } b \supseteq R_S\}$.

**Definition 13.** The map $\theta_C : E \to \mathbb{N}$ defined by

$$\theta_C(b) = \min\{\psi(b) : \psi \text{ is a Euclidean algorithm for } C\}$$

is called the minimal algorithm for $C$.

We readily verify that $\theta_C$ is an algorithm for $C$. Let $c \in C$ represent the class and let $b \in E$. Choose some algorithm $\psi$ for $C$ such that $\theta_C(b) = \psi(b)$. Take any $x \in bc \setminus c$. We seek $z \in x + c$ such that $\theta_C(bcz^{-1}) < \theta_C(b)$. Since $\psi$ is an algorithm for
we know there exists $z \in x + c$ with $\psi(bc^{-1}) < \psi(b) = \theta_c(b)$. But by definition, this yields $\theta_c(bc^{-1}) \leq \psi(bc^{-1}) < \theta_c(b)$, as required.

The minimal algorithm $\theta_c$ satisfies properties similar to those satisfied by the minimal algorithm for a Euclidean ring [8]. In what follows, Lemmas 14, 18, 19 20 were originally stated by Lenstra [5]. We begin with a fact which holds for any Euclidean algorithm for $C$.

**Lemma 14.** Let $\psi$ be a Euclidean algorithm for $C$ with $c \in C$. Then,

$$\text{for } a, b \in E, \psi(ab) \geq \psi(b), \text{ with equality } \iff a = R_S.$$  

**Proof.** For a fixed $b$, choose $a \in E$ such that $\psi(ab)$ is minimal. Let $x \in ac \setminus c$. Then $x \in abc \setminus c$ as well and by definition, $\exists z \in x + c$ such that $\psi(abcz^{-1}) < \psi(ab)$. Since $x \in ac$, we see that $z \in x + c \subseteq ac$. Thus, $z \in ac$ which means $acz^{-1} \in E$. Therefore $\psi((acz^{-1})b) < \psi(ab)$ contradicts the minimality of $\psi(ab)$. The only resolution is that $ac \setminus c$ must be empty. That is, $a = R_S$. Therefore, $\psi(ab)$ takes its minimal value if and only if $a = R_S$ in which case we have equality $\psi(ab) = \psi(b)$. This implies that for all $a \neq R_S$, $\psi(ab) > \psi(b)$. \hfill \Box

**Lemma 15.** If $\theta_c$ is the minimal algorithm for $C$, then for every $a \in E \setminus \{R_S\}$, $\exists x \in ac \setminus c$ such that:

(i) $\forall z \in x + c, \theta_c(acz^{-1}) \geq \theta_c(a) - 1$,

(ii) with equality for some $z_0 \in x + c$.

**Proof.** Any algorithm $\theta_c$ must satisfy the condition:

$$\forall a \in E \text{ and } \forall x \in ac \setminus c, \exists z \in x + c \text{ s.t. } \theta_c(acz^{-1}) < \theta_c(a).$$
(⋆) Suppose in contradiction to (i) that there is some \( a \in E \setminus \{R_S\} \) such that for all \( x \in ac \setminus c \), one can find \( z \in x + c \) s.t. \( \theta_c(acz^{-1}) \leq N - 2 \), where \( \theta_c(a) = N \).

We can then reassign the value of \( \theta_c(a) \) by \( \theta_{c_{\text{new}}}(a) = N - 1 \). This is so because (⋆) ensures that the definition which makes \( \theta_c \) an algorithm is still satisfied since

a) For any \( x \in ac \setminus c \), we can always find \( z \) s.t. \( \theta_c(acz^{-1}) \leq N - 2 < N - 1 = \theta_{c_{\text{new}}}(a) \).

and

b) If \( a = a'cz^{-1} \) for some other \( a' \). (i.e. \( a \) occurs as the "remainder" from a fractional ideal \( a' \) of larger size), then if \( \theta_c(a) = N < \theta_c(a') \) is true, then \( \theta_{c_{\text{new}}}(a) = N - 1 < \theta_c(a') \) will be true as well.

This shows that \( \theta_c \) will still be a Euclidean algorithm for \( C \) if the value of \( \theta_c(a) \) is changed from \( N \) to \( N - 1 \). This contradicts the minimality of \( \theta_c \). This proves (i). Since \( \theta_c \) is a Euclidean algorithm for \( C \) and (i) holds, this implies that (ii) must hold as well. \( \square \)

**Lemma 16.** Let \( \theta_c \) be the minimal algorithm for \( C \). Then for all \( a \in E \), \( \theta_c(a) = 0 \iff a = R_S \).

*Proof.* Every algorithm \( \psi \) for \( C \) maps from \( E \rightarrow \{0, 1, 2, \ldots\} \). By Lemma 14, with \( b = R_S \), we see that \( \psi(a) \geq \psi(R_S) \) for all \( a \in E \). In particular \( \theta_c(a) \geq \theta_c(R_S) \) for all \( a \). By minimality of \( \theta_c \), we then must have \( \theta_c(R_S) = 0 \). Conversely, if \( a \neq R_S \), then by definition, one can find a suitable \( z \) such that \( \theta_c(acz^{-1}) < \theta_c(a) \). As the range of \( \theta_c \) is \( \{0, 1, 2, \ldots\} \), this implies that \( \theta_c(a) \neq 0 \). \( \square \)
Lemma 17. Let $\theta_C$ be the minimal algorithm for $C$. Then for all $a, b \in E$, $\theta_C(ab) - \theta_C(a) \geq 0$.

Proof. Since $\theta_C$ is an algorithm for $C$, this follows from Lemma 14. □

The following property is directly analogous to a property satisfied by the minimal algorithm for a Euclidean ring:

Lemma 18. Let $\theta_C$ be the minimal algorithm for $C$. Then for all $a, b \in E$, $\theta_C(ab) \geq \theta_C(a) + \theta_C(b)$.

Proof. Fix any $b \in E$. We show that $a = R_S$ is the only ideal in $E$ satisfying:

(i) $\theta_C(ab) - \theta_C(a) = k$, with $k$ minimal.

(ii) Among those $a$ satisfying (i), $\theta_C(a)$ is minimal.

Suppose $a \neq R_S$ satisfies (i) and (ii), then by Lemma 15, $\exists x \in ac \setminus c$ s.t. $\forall z \in x + c$.

$$\theta_C(acz^{-1}) \geq \theta_C(a) - 1. \quad (4.1)$$

Since $x$ belongs to $abc \setminus c$ as well, $\exists y \in x + c$ s.t. $\theta_C(abcy^{-1}) < \theta_C(ab)$ or

$$\theta_C(abcy^{-1}) \leq \theta_C(ab) - 1. \quad (4.2)$$

As $x \in ac$ this implies $y \in ac$ too. Since $y \in x + c$, we have:

$$\theta_C(acy^{-1}) \geq \theta_C(a) - 1. \quad \text{by (4.1)}$$
Case 1: If \( \theta_c(ac^{-1}) = \theta_c(a) - 1 \), then
\[
\theta_c(abcy^{-1}) - \theta_c(ac^{-1}) \leq \theta_c(ab) - 1 - \theta_c(acy^{-1}) \quad \text{by (4.2)}
\]
\[= \theta_c(ab) - 1 - (\theta_c(a) - 1)
\]
\[= \theta_c(ab) - \theta_c(a)
\]
\[= k.
\]
Hence \( ac^{-1} \) satisfies (i). However, \( \theta_c(ac^{-1}) < \theta_c(a) \), contradicting (ii).

Case 2: If \( \theta_c(ac^{-1}) > \theta_c(a) - 1 \), then
\[
\theta_c(abcy^{-1}) - \theta_c(ac^{-1}) \leq \theta_c(ab) - 1 - \theta_c(acy^{-1}) \quad \text{by (4.2)}
\]
\[< \theta_c(ab) - 1 + 1 - \theta_c(a)
\]
\[= k,
\]
contradicting (i). So for no \( a \neq R_S \) can both (i) and (ii) hold. Therefore, \( \theta_c(R_Sb) - \theta_c(R_S) = \theta_c(b) - 0 = \theta_c(b) \) is minimal. This implies that \( \forall a \in E \), \( \theta_c(ab) - \theta_c(a) \geq \theta_c(b) \).

Lemma 19. Let \( \theta_C \) be the minimal algorithm for \( C \). Then for any \( b \in E \), \( b \in C^{-\theta_C(b)} \).

Proof. If \( \theta_C(b) = 0 \), then \( b = R_S \) and so \( b \in C^0 = [R_S] \). If \( \theta_C(b) = 1 \), then \( \exists z \) such that \( \theta_C(bcz^{-1}) < 1 \). This implies that \( \theta_C(bcz^{-1}) = 0 \) which means \( bcz^{-1} = R_S \). Thus \( [b]C = [R_S] \) which implies \( [b] = C^{-1} \). Assume that if \( \theta_C(b) \leq N \) then \( b \in C^{-\theta_C(b)} \).

Let \( \theta_C(b) = N + 1 \). By Lemma 15, \( \exists x \in bc \setminus c \) such that \( \exists z_0 \in x + c \) with \( \theta_C(bcz_0^{-1}) = \theta_C(b) - 1 = N \). By induction, we have \( bcz_0^{-1} \in C^{-N} \). Therefore, \( [b]C = C^{-N} \), which implies \( b \in C^{-(N+1)} = C^{-\theta_C(b)} \).
Lemma 20. Let $\theta_C$ be the minimal algorithm for $C$. Then for $b \in E$, $\theta_C(b) = 1 \iff b^{-1} = p$, where $p$ is a prime of $R_S$, $p \in C$, and the natural projection $R_S^x \rightarrow (R/p)^x$ is surjective.

Proof. $\iff$: Suppose $b \in E$, where $b^{-1} = p$, $p \in C$ is a prime of $R_S$, and the natural projection $R_S^x \rightarrow (R_S/p)^x$ is surjective. In the definition of $\theta_C$, take $c = p$ as the representative for the Euclidean ideal class $C$. So the expression $bc \backslash c$ in the definition becomes $bb^{-1} \backslash p$ or $R_S \backslash p$. For any $x \in R_S \backslash p$, it can be shown that there exists $z \in x + p$ such that $\theta_C(R_Sz^{-1}) = \theta_C((z^{-1})) = 0$. For by Lemma 16, this is equivalent to showing that $\forall x \in R_S \backslash p$, $\exists$ a unit $z \in x + p$. Now if $x \in R_S \backslash p$, then $x \neq 0$ in $R_S/p$. By the surjectivity of $R_S^x \rightarrow (R_S/p)^x$, we can find a unit $z$ s.t. $z \equiv x \mod p$. That is, $z \in x + p$ as desired. By the minimality of $\theta_C$ and Lemma 15, this shows that $\theta_C(b) = 1$.

$\Rightarrow$: If $\theta_C(b) = 1$, then by Lemma 19, $b \in C^{-1}$ or $b^{-1} \in C$. I claim $b^{-1} = p$ is prime. If not, then write $p = gh$, with $g, h \neq R_S$. Then by Lemma 18, $\theta_C(b) \geq \theta_C(g^{-1}) + \theta_C(h^{-1}) \geq 2$. This contradicts that $\theta_C(b) = 1$. It remains to show that the natural map $R_S^x \rightarrow (R_S/p)^x$ is surjective. We may take $c = p$ in the definition of $\theta_C$. Then $bc \backslash c$ becomes $p^{-1}p \backslash p$ or $R_S \backslash p$. Since $\theta_C(b) = 1$ and by the definition of $\theta_C$, for every $x \in R_S \backslash p$, there is $z \in x + p$ such that $\theta_C(p^{-1}pxz^{-1}) = \theta_C(Rz^{-1}) = \theta_C(z^{-1}) < 1$. That is, $\theta_C(z^{-1}) = 0$. But by Lemma 16, this occurs if and only if $z$ is a unit. Hence, $\forall x \in R_S \backslash p$, $\exists$ a unit $z \in x + p$. This is equivalent to saying that $R_S^x \rightarrow (R_S/p)^x$ is surjective.

\[\square\]
Remark: At this point, we are able to give an alternate proof to the following well known fact. The rings of integers in the number fields \( \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}) \), and \( \mathbb{Q}(\sqrt{-163}) \) are all principal ideal domains for which there is no Euclidean algorithm. We prove this for \( K = \mathbb{Q}(\sqrt{-19}) \). If there were a Euclidean algorithm, \( \psi \) for \( R = \mathcal{O}_K \), then by Lemma 3, \([R]\) would be a Euclidean ideal class. Thus there must be a minimal Euclidean algorithm, \( \theta \), for \([R]\). For such a minimal algorithm, \( \theta \) must assume the value 1. That is, there must be some \( b \in E \) with \( \theta(b) = 1 \). By Lemma 20, \( \theta(b) = 1 \iff b^{-1} = p \) for some prime \( p \) with the natural projection \( R^* \rightarrow (R/p)^* \) surjective. Now \( R^* = \{1, -1\} \), so \( R^* \rightarrow (R/p)^* \) can only be surjective if \( #(R/p)^* = 1 \) or 2. This can only happen if \( p \) lies over (2) or (3). It is routine to check that (2) remains prime in \( R \) so that if \( p \) lies over (2), then the residue field degree of \( p \) over (2) is 2, i.e., \( #(R/p) = 4 \) so that \( #(R/p)^* = 3 \). Similarly, (3) stays prime in \( R \) as well and if \( p \) lies over (3), then \( #(R/p)^* = 3 \). In either case, \( #(R/p)^* \) is too large so that in \( R \), there are no primes \( p \) with \( R^* \rightarrow (R/p)^* \) surjective. Hence there can be no minimal Euclidean algorithm for \([R]\) and thus \( R \) is not a Euclidean ring.

2. Explicit Description of \( \theta_C \)

Theorem 21. Let \( K \) be a number field and let \( S \) be a finite set of primes containing \( S_{\infty} \) with \( \#S \geq 2 \). Let \( R_S \) be the ring of \( S \)-integers and suppose the class group of \( R_S \) is cyclic of order \( h \neq 2 \). Assume that for all square-free integers \( m \), and for every subset \( S' \subset S \), the \( \zeta \)-function for \( K(\zeta_m, R_{S'}^{1/m}) \) satisfies the generalized Riemann hypothesis. Let \( C \) be any class that generates the class group of \( R_S \) and set \( E = \{ b : b \) is a fractional ideal of \( R_S \) and \( b \supseteq R_S \} \). Then for all but at most one generating class \( C \), the minimal algorithm, \( \theta_C \), for \( C \) is given by:
\[ \theta_C(b) = \sum_{p \in R_S \text{ prime}} \text{ord}_p(b^{-1})n_p, \]

where

\[ n_p = \begin{cases} 
1. & \text{if } p \in C \text{ and the natural map } R_S^\times \to (R/p)^\times \text{ is surjective.} \\
2. & \text{if } p \in C^2. \\
\vdots & \vdots \\
n. & \text{if } p \in C^n, \text{ for } n \leq h. \\
\vdots & \vdots \\
h. & \text{if } p \in C^h \text{ i.e., } p \text{ is principal.} \\
h + 1. & \text{if } p \in C \text{ but } R_S^\times \to (R/p)^\times \text{ is not surjective.} 
\end{cases} \]

Specifically, we have the following:

(a) If \( K/\mathbb{Q} \) is Galois, then for all generating classes \( C \), \( \theta_C \) is given as above.

(b) Let \( [K : \mathbb{Q}] = n, r \) be the number of real embeddings of \( K \) and \( S_f \) be the set of finite primes of \( S \). If \( n < r + 2\#S_f \), then \( \theta_C \) as given above is the minimal algorithm for all generating classes \( C \).

(c) If \( h = 1 \), then there is only one class \( C = [R_S] \) and \( \theta_C \) is given as above.

(d) If \( h > 2 \), then of the \( \phi(h) \) classes, \( C \), which generate \( Cl_{R_S} \), for at least \( \phi(h) - 1 \) classes, \( \theta_C \) is given as above.

Here, \( \phi \) is the Euler phi-function. We note that we identify the fractional ideals \( b \) of \( R_S \) with those divisors \( b \in I^S = \prod_{p \in R_S} p^{n(p)}, \) with \( n(p) \in \mathbb{Z} \) and \( n(p) = 0 \) for all but finitely many \( p \).
Proof. If $h = 1$, then $R_S$ is a principal ideal domain. From Lemma 3, we know the trivial class $C = [R_S]$ is a Euclidean ideal class if and only $R_S$ is a Euclidean ring. Lenstra [4] gives the minimal Euclidean algorithm, $\theta$, for a principal ideal domain and this coincides with $\theta_C$ above. This proves part (c) of Theorem 21.

Henceforth, we may assume that $h > 2$. \hfill (4.3)

Consider $\theta_C$ as defined above. We first show that if $\theta_C$ is an algorithm for $C$, then it must be the minimal one.

Lemma 22. If the function $\theta_C$ as above is a Euclidean algorithm for $C$, then it must be the minimal one.

Proof. Let $\theta_C'$ be any minimal Euclidean algorithm for $C$ and let $b \in E$. Then by Lemma 20, $\theta_C'(b) = 1 \iff b^{-1} = p$ for some prime $p \in C$ such that the map $R^\times_S \to (R_S/p)^\times$ is surjective. Hence in this case, $\theta_C'(b) = 1 = n_p = \theta_C(b)$. Now let $q$ be any prime of $R_S$ (so $q^{-1} \in E$). By Lemma 19, $\theta_C'(q^{-1}) = n_q + hk$ for some $k \in \mathbb{N}$. Now for any $b \in E$, Lemma 18 implies that

\[
\theta_C'(b) \geq \sum_{p \in R_S} \text{ord}_p(b^{-1})\theta_C'(p^{-1}) \\
= \sum_{p \in R_S} \text{ord}_p(b^{-1})(n_p + hk) \\
\geq \sum_{p \in R_S} \text{ord}_p(b^{-1})n_p \\
= \theta_C(b).
\]

Thus if $\theta_C$ is Euclidean algorithm for $C$, it must be the minimal algorithm. \hfill \square

It now remains to show that $\theta_C$ is a Euclidean algorithm for $C$, for at least $\phi(h) - 1$ classes $C$. Let $E' = \{ b : b$ is an integral ideal of $R_S \}$. Define a function $\psi_C : I^S \to \mathbb{Z}$
by:

\[ \psi_C(a) = \sum_{\substack{p \in \mathcal{R}_S \text{ prime} \atop p \mid a}} \text{ord}_p(a) n_p. \]

with \( n_p \) as above. Note that if \( a \in E \) or \( a \in E' \), we have the following relationship:

\[
\psi_C(a) = \begin{cases} 
-\theta_C(a), & \text{if } a \in E, \\
\theta_C(a^{-1}) = -\psi_C(a^{-1}), & \text{if } a \in E'. 
\end{cases}
\]

Choose a representative \( c \) of \( C \) and let \( x \in K \setminus c \). As \( K = \bigcup_{a \in E'} a^{-1} c \), we must have \( x \in a^{-1} c \setminus c \) for some integral ideal \( a \). Then \( \theta_C \) is a Euclidean algorithm for \( C \) only if \( \exists z \in x + c \) such that \( \theta_C(a^{-1}cz^{-1}) = \theta_C(a^{-1}) \) or equivalently, \( \psi_C(ac^{-1}z) < \psi_C(a) \). Since \( \psi_C \) is a homomorphism from \( I^S \rightarrow (\mathbb{Z}, +) \), we see that \( \theta_C \) is a Euclidean algorithm only if

\[
\psi_C(a) + \psi_C(c^{-1}) + \psi_C((z)) < \psi_C(a) \\
\text{i.e.} \quad \psi_C((z)) < -\psi_C(c^{-1}) \\
\text{i.e.} \quad \psi_C((z)) < \psi_C(c).
\]

Because this formulation is now independent of \( a \), to prove that \( \theta_C \) is a Euclidean algorithm for \( C \), it suffices to show that:

\[
\forall x \in K \setminus c. \exists z \in x + c \text{ such that } \psi_C((z)) < \psi_C(c). \tag{4.4}
\]

To prove (4.4), we begin with \( x \in K \setminus c \). Consider the fractional ideal \( \frac{\langle x \rangle}{c} \) of \( \mathcal{R}_S \) and write \( \frac{\langle x \rangle}{c} = \frac{a}{b} \), with \( a \) and \( b \) uniquely written as co-prime integral ideals of \( \mathcal{R}_S \).

Let \( F \) be the S-ray class field for the modulus \( b \) so that

\[ I^b / \hat{H} \cong \text{Gal}(F/K'), \]

where \( \hat{H} \) is the subgroup \( \iota(K_{b,1}) \cdot \langle p \in S \rangle \) of \( I^b \). (Here, we use that \( I^b / \hat{H} \cong I^{S,b} / i'(K_{b,1}) \), where if \( \Pi \) is the projection of \( I^b \) onto \( I^{S,b} \), then \( i' = \Pi \circ i \) ) As \( (a, b) = R_S \), we have that \( a \in I^{S,b} \) and thus under the Artin reciprocity map, \( a \)
corresponds to some $\tau \in \text{Gal}(F/K)$. In fact, there are infinitely many integral ideals $\mathfrak{a}'$ such that $(\mathfrak{a}', F/K) = \tau$. For any such $\mathfrak{a}'$, it follows that $\mathfrak{a}' \equiv \mathfrak{a}$ in $I^{S,b}/i'(K_{b,1})$. That is, $\mathfrak{a}' = (\gamma)\mathfrak{a}$ for some $\gamma \in K_{b,1}$. We may write

$$\gamma = 1 + t \text{ with } t \in K^\times \text{ and } \text{ord}_q(t) \geq n(q), \text{ where } b = \prod q^{n(q)}.$$  \hspace{1cm} (4.5)

Let $z = x\gamma = x(1 + t) = x + xt$. We now show that $xt \in c$ so that $z \in x + c$. Since $a(\gamma) = a'$ is an integral ideal, we have that for all $a \in a$, $a\gamma \in R_S$. This implies that $a + at \in R_S$ which in turn shows that $at \in R_S$. This shows that $a(t)$ is an integral ideal. We consider $(xt) = \frac{ac}{b}(t) = \frac{c}{b}a(t)$. By (4.5), $b$ divides the integral ideal $a(t)$ so that $(xt) = \tau t$ for some integral ideal $\tau$. This implies that $xt \in c$ and that $z \in x + c$.

So for any $x \in K \setminus c$, we have found $z \in x + c$ such that,

$$\psi_c((z)) = \psi_c((x\gamma)) = \psi_c[\frac{ac}{b}(\gamma)] = \psi_c(\frac{ca'}{b})$$

$$= \psi_c(c) + \psi_c(a') - \psi_c(b).$$

If we can choose $a'$ so that $\psi_c(a') < \psi_c(b)$, then the above shows that $\psi_c((z)) < \psi_c(c)$. Thus if we can always find such an $a'$, we will have shown that $\theta_C$ is the minimal algorithm for $C$. We proceed to show that for $\phi(h) - 1$ of the generating classes $C$, we can always find such an ideal $a'$.

Because $\frac{(x)}{c}$ is written uniquely as $\frac{a}{b}$, we discuss cases based on $\psi_c(b)$.

**Case 1:** $\psi_c(b) = 0$.

Since $b$ is an integral ideal, the definition of $\psi_c$ shows this occurs only when $b = R_S$. Thus

$$\frac{(x)}{c} = \frac{a}{R_S} \text{ which implies } (x) = ac.$$
This implies that $x \in c$ so this case cannot occur as $x \in K \setminus c$.

**Case 2:** $\psi_c(b) = 1$.

In this case, the definition of $\psi_c$ and the fact that $b$ is an integral ideal imply that $b$ must be a prime ideal with $n_p = 1$. That is, $b \in C$ and the natural projection $R^\times_S \to (R_S/b)^\times$ is surjective. Because $\left(\frac{x}{c}\right) = \frac{a}{b}$ and $b, c \in C$, we see that $a = (a)$ is a principal ideal. Further, as $a$ and $b$ are co-prime, we must have that $\bar{a} \in (R_S/b)^\times$.

Because the units of $R_S$ map surjectively onto $(R_S/b)^\times$, this means that $a \equiv u \pmod{b}$ for some unit $u$. Equivalently, $\frac{a}{u} \equiv 1 \pmod{b}$, which means $\frac{a}{u} \in K_{b,1}$. As ideals, $(a) = \left(\frac{a}{u}\right)$, so this gives that $(a) \in i'(K_{b,1})$. Therefore, in $I^{S,b}/i'(K_{b,1})$, $a \equiv R_S$. Hence we may choose $a' = R_S$ so that $\psi_c(a') = \psi_c(R_S) = 0 < 1 = \psi_c(b)$ as desired.

**Case 3:** $\psi_c(b) \geq 3$.

Let $b \in C^N$ with $3 \leq N \leq h + 2$, where $h$ is the class number. Then by Lemma 19 and the definition of $\psi_c$, $\psi_c(b) = N + kh$. For some non-negative integer $k$. As before, since $\left(\frac{x}{c}\right) = \frac{a}{b}$, we have $a \in C^{N-1}$. By the Chebotarev density theorem, there are infinitely many primes $p$ such that $(p, F/K) = (a, F/K) = \tau$. Now any such prime is equivalent to $a$ in $I^{S,b}/i'(K_{b,1})$ and is also equivalent to $a$ in $Cl_{R_S}$. Hence any of these infinitely many primes also belongs to $C^{N-1}$. So by definition, we have two possibilities. If $3 \leq N \leq h + 1$ then take $a' = p$ so that

$$2 \leq \psi_c(p) = N - 1 < N \leq \psi_c(b).$$
If $N = h + 2$, then $p \in C$ so that by definition, $\psi_c(p) = 1$ or $h + 1$. In either case, we may take $a' = p$ and

$$\psi_c(p) \leq h + 1 < h + 2 \leq \psi_c(b).$$

**Case 4: $\psi_c(b) = 2.$**

In this case, $b \in C^2$. The above argument does not carry through for although we can find infinitely many primes $p \in C^1$ equivalent to $a$ in $I^{S_b, l'}(K_{b, l})$, $\psi_c(p) = 1$ requires the extra condition that the projection $R_S^x \rightarrow (R_S / p)^x$ be surjective. We should be able to find such primes because Lenstra’s theorem on page 16 says that the set $M = \{p : (p, F/K) = \tau \text{ and } R_S^x \rightarrow (R_S / p)^x \text{ is surjective}\}$ is infinite if and only if there is no prime integer $l$ such that $K \subseteq L_l \subseteq F$ and $\tau \in \text{Gal}(F/L_l)$. Here, $L_l = K(\zeta_l, R_S^{x_1})$. If no such $L_l$ exists, then $M$ is infinite and we find a prime $p \in M$, $p \in R_S$. We set $a' = p$ so that $\psi_c(a') = 1 < 2 = \psi_c(b)$.

Thus $\theta_c$ is the minimal algorithm for $C$ if no such $L_l$ exists. So let us assume that there is some such $L_l$ and attempt to find a contradiction.

First note that the existence of such an intermediate field $L_l$ implies that $\zeta_l \in K$. We see this as follows. By class field theory, $F/K$ is an Abelian (Galois) extension. Hence any intermediate field must be Abelian over $K$ as well. In particular, let $u$ be any unit of $R_S^x$ which is not an $l$-th power, for instance, any fundamental unit. Let $K' = K(u^{1/l}) \subseteq L_l$, so $[K' : K] = l$. Then $K'$ is Abelian over $K$ and must be the splitting field of $x^l - u$ over $K$. This implies that $K' = K(\zeta_l, u^{1/l})$. Clearly we have $K \subseteq K(\zeta_l) \subseteq K'$. But note that $[K(\zeta_l) : K] \leq l - 1$ and divides $[K' : K] = l$ so that $[K' : K]$ must be 1. Therefore $\zeta_l \in K$. 

---

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Figure 4.1:

Next, we note that since the Hilbert class field $H$ of $K$ is a subfield of $F$, we have the extensions of fields given in Figure 4.1.

Since $\psi_C(b) = 2$, we know that $b \in C^2$. By $\frac{a}{b} = \frac{\alpha}{b}$, we deduce that $a \in C$. Note that $(a, H/K) = \sigma$ generates the cyclic group $Gal(H/K)$ because $C$ was assumed to be a generator of the class group and $Gal(H/K) \cong CL_{R_S}$ under the Artin map. From this we may conclude that $\tau|_H = \sigma$. We notice that this implies

$$L_l \cap H = K$$

(4.6)

because $\tau|_H$ is a generator for $Gal(H/K)$ whereas $\tau$ fixes $L_l$. Hence as any elements of $H$ which are fixed by $\tau$ must lie in $K$, we see that (4.6) must hold.

Now (4.6) implies that $L_l$ is ramified over $K$ since $H$ is the maximal Abelian. unramified extension of $K$. In fact it can only ramify at primes dividing $(l)$. However, the only primes of $R_S$ which may ramify from $K$ up to $F$ are the primes dividing $b$.

So the existence of $L_l \subseteq F$ implies that there is a prime $l$ of $R_S$, such that

$$ord_l(l) > 0 \text{ and } ord_l b > 0.$$  

(4.7)

Now since $\psi_C(b) = 2$, the definition of $\psi_C$ implies there are three possible factorizations of $b$ into primes:
1. \( b = l \), with \( n_l = 2 \), or
2. \( b = l \cdot q \), with \( n_l = n_q = 1 \) and \( l \neq q \), or
3. \( b = l^2 \), with \( n_l = 1 \).

Before analyzing these cases, we make two important observations. First, since \( \zeta_l \in K \), \( L_l \) is a Kummer extension [7, p.15] of \( K \) and

\[
[L_l : K] = l^i, \quad \text{for some integer } i \geq 1. \tag{4.8}
\]

Second, as on page 19, the following series is exact:

\[
0 \longrightarrow (R_S/b)^x/\pi(R_S^x) \longrightarrow I^{S,b}/i'(K_{b,1}) \longrightarrow I^S/i'(K^x) \longrightarrow 0.
\]

where \( \pi : R_S^x \longrightarrow (R_S/b)^x \) is the natural projection. Thus

\[
\#I^{S,b}/i'(K_{b,1}) = \#I^S/i'(K^x) \cdot \#((R_S/b)^x/\pi(R_S^x)).
\]

This yields

\[
[F : K] = h \cdot \#((R_S/b)^x/\pi(R_S^x)), \tag{4.9}
\]

because \( \text{Gal}(F/K) \cong I^b/\hat{H} \cong I^{S,b}/i'(K_{b,1}) \).

Consider the case that \( b = l \) with \( n_l = 2 \). Let \( d = \#((R_S/b)^x/\pi(R_S^x)) \). As \( l|(l) \), the characteristic of \( R_S/b \) is \( l \). This implies that \( d \) divides \( l^f - 1 \), for some \( f \). Consider the composite \( H \cdot L_l \). By (4.6) and (4.8), \( [H \cdot L_l : K] = h \cdot l^i \). Since \( H \cdot L_l \subseteq F \), we have \( h \cdot l^i|h \cdot d \). This implies that \( l^i|d \) which in turn yields \( l|d \). This means \( l|(l)^f - 1 \) which is impossible, so this first case can never occur.

Next consider the possibility that \( b = l \cdot q \) with \( n_l = n_q = 1 \) and \( l \neq q \). Here, \( (R_S/b)^x \cong (R_S/l)^x \oplus (R_S/q)^x \). Because \( n_q = 1 \), the subgroup \( \pi(R_S^x) \) of \( (R_S/b)^x \) projects onto the second term of the direct sum. This implies that \( \#((R_S/b)^x/\pi(R_S^x)) \)
divides $\#(R_S/l)^*$. That is, $d$ divides $l^d - 1$. Proceeding as above, we derive a contradiction so this possibility never occurs.

Last we consider the case that $b = l^2$ with $n_t = 1$. Recall $L_l = K(\zeta_l, R_S^{2 \zeta_l})$. Let $u$ be a unit of $R_S$ which is not an $l$-th power in $K^\times$. Let $\alpha = u^{1/l}$ and consider the field $K' = K(\alpha)$. Then $K \subset K' \subset L_l$ and $[K' : K] = l$. As $K'$ is contained in $F$, $K'/K$ is an Abelian (Galois) extension and is the splitting field for $f(x) = x^l - u$ over $K$. Further, we know that if $R'$ is the ring of integers in $K'$ and $S'$ is the set of primes lying over those prime of $S$, then

$$Disc(R_S[\alpha]/R_S) = Disc(R'_S/R_S) \cdot ([R'_S : R_S[\alpha]])^2. \quad (4.10)$$

where $[R'_S : R_S[\alpha]]$ is the $R_S$-module index of $R_S[\alpha]$ in $R'_S$. This is determined locally by $[R'_S : R_S[\alpha]]_p = [R'_S : R_{S_p}[\alpha]]$, for all primes $p$. We compute that

$$Disc(R_S[\alpha]/R_S) = Disc(f(x))$$

$$= Disc(x^l - u)$$

$$= \pm Nm_{K'/K}(l \cdot \alpha^{l-1})$$

$$= \pm l^d u^{l-1}.$$  

So as ideals of $R_S$,

$$(Disc(R_S[\alpha]/R_S)) = (l)^l. \quad (4.11)$$

Consider the ideal $(l)$ of $R_S$. We know $l|(l)$, so write $(l) = l^{e_i} \prod_{i=2}^{m} q_i^{e_i}$, where $e_i$ is the ramification index of each prime of $R_S$ lying over $(l)$. Since $\zeta_l \in K$, $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_l) \subseteq K$.

Now in $\mathbb{Z}(\zeta_l)$. $(l) = (1 - \zeta_l)^{l-1}$. This implies $(l - 1)|e_i$ for $1 \leq i \leq m$. Hence in $R_S$,

$$(l) = l^{e_1(l-1)} \prod_{i=2}^{m} q_i^{e_i(l-1)}. \quad (4.12)$$
for some integers \( k_i \).

Let us now reconsider (4.8). Let \( S_f \subset S \) be the set of finite primes of \( S \). Let \( r \) be the number of real embeddings of \( K \) and let \( s \) be the number of pairs of complex conjugate embeddings. Then the rank of \( R_S^x \) is \( r + s + \#S_f - 1 \). Since the torsion subgroup of \( R_S^x \) is always cyclic, let \( \zeta_g \) be any generator. If we let \( \{ \zeta_1, \ldots, \zeta_r + s + \#S_f - 1 \} \) be a set of fundamental units, then \( L_t = K(\zeta_1^{1/l}, \zeta_1^{1/l}, \ldots, \zeta_1^{1/l}, \zeta_1^{1/l}, \ldots, \zeta_1^{1/l}) \). We conclude from Kummer theory [7, p. 15] that

\[
[L_t : K] = l^{r + s + \#S_f}. \tag{4.13}
\]

Because of (4.6), Galois theory tells us that

\[
[L_t : K] \text{ divides } [F : H]. \tag{4.14}
\]

We next consider \( [F : H] \). Since \( [H : K] = h \), (4.9) tells us that \( [F : H] = \#((R_S/b)^x)/\pi(R_S^x)) \). As \( l \mid (l) \), \( R_S/l \) has characteristic \( l \). Thus for some \( f \), \( \#(R_S/l)^x = l^f - 1 \). It follows that since \( b = l^2 \), \( \#(R_S/b)^x = l^f(l^f - 1) \). We conclude that

the \( l \)-component of \( [F : H] \) divides \( l^f \). \tag{4.15}

Let \( [K : \mathbb{Q}] = n \). We know from above that the residue field degree of \( l \over (l) \) is \( f \). Thus \( f \cdot k_1(l - 1) \leq n \). From (4.13), (4.14), and (4.15), we now have

\[
\frac{n}{2} + \frac{r}{2} + \#S_f = r + s + \#S_f \leq f \leq \frac{n}{k_1(l - 1)},
\]

since \( n = r + 2s \). This implies

\[
k_1(l - 1) \leq \frac{2n}{n + r + 2\#S_f} \leq 2. \tag{4.16}
\]

If \( n < r + 2\#S_f \), then we have \( k_1(l - 1) < 1 \) which is impossible since \( l \mid (l) \).

Thus there is no such \( L_t \) in this case and \( \theta_c \) is the minimal algorithm for \( C \) for all generating classes \( C \). This proves part \( b \) of the theorem.
If $k_1(l - 1) = 2$, we have equality throughout and $(l) = \mathfrak{f}^{(l-1)} = \mathfrak{f}^2$. This occurs in two situations. In the first, $k_1 = 1$ and $l = 3$. We conclude that $(3) = \mathfrak{f}^2$. But recall that in the subfield $\mathbb{Q}(\zeta_3)$ of $K$, we have $(3) = (1 - \zeta_3)^2$. Thus $l = (1 - \zeta_3)$ is a principal ideal. But since $l \in C$, which generates the class group, this implies that $h = 1$. We may ignore this case by (4.3). In the second situation, $k_1 = 2$ and $l = 2$. Here, we have $(2) = \mathfrak{f}^2$. This implies $h = 1$ or $2$ so by (4.3), we may ignore this case as well.

We are left with the possibility that $k_1(l - 1) = 1$. This occurs if and only if $k_1 = 1$ and $l = 2$. We see that $\theta_C$ can only fail to be the minimal algorithm for $C$ if $K \subset L_2 \subset F$ and $\tau \in \text{Gal}(F/L_2)$. Assume for the moment that this is the case and consider any of the other $\phi(h) - 1$ generators $C'$ for $C|_{R_K}$. Note that as $h \geq 3$, there is at least one generator distinct from $C$. Proceeding exactly as we did for $C$, we see that $\theta_{C'}$ is the minimal algorithm for $C'$ unless the following occurs. There is some prime $m \in C'$ with $R_S^\times \to (R_S/m)^\times$ surjective and some ideal $b' = m^{2}$. Further, if $F'$ is the $S$-ray class field for the modulus $b'$, then $\theta_{C'}$ fails to be the minimal algorithm for $C'$ only if there is some $L_{r'} \subset F'$ and some $r' \in \text{Gal}(F'/L_{r'})$ with $r'|_H = (m, H/K)$. As in (4.12), we write $(l') = m^{i(l'-1)} \prod_{i=2}^{m} p_i^{(l'-1)}$. Then as before, such $L_{r'}$ can only exist if $j_1(l' - 1) \leq 2$. If $j_1 = 1$, $l' = 3$, then as before, $h = 1$, so we may ignore this case. If $j_1 = 2, l' = 2$, then as above, $h = 1$ or $2$, so we ignore this case as well. This leaves only the possibility that $j_1 = 1, l' = 2$. Then $\theta_{C'}$ fails to be the minimal algorithm only if $K \subset L_2 \subset F'$. Recall we have assumed that $L_2 \subset F$, so consider the intersection of the two ray class fields $F$ and $F'$. Since $F$ can only ramify at the prime $l$ and $F'$ can only ramify at the prime $m$, the fact that $l \neq m$ tells us that $F \cap F' = H$. But by (4.6), $H \cap L_2 = K$. We conclude that if $L_2 \subset F$, then $L_2 \subset F'$ and $\theta_{C'}$ is the minimal algorithm for $C'$. This holds for any
of the \( \phi(h) - 1 \) generators \( C' \) distinct from \( C \). This proves part \((d)\) of Theorem 21.

We next prove \((a)\) of Theorem 21. Assume \( K/Q \) is a Galois extension of degree \( n \). Above, we showed that for any generating class \( C, \theta_C \) fails to be the minimal algorithm for \( C \) only if \( K \subset L_2 \subset F \) and \( \tau \in \text{Gal}(F/L_2) \). In this case, we saw that the only remaining possibility for which \( \theta_C \) may fail occurs when \( k_1 = 1, l = 2 \). Then \( (l) = (2) = l \cdot \prod_{i=1}^{\infty} q_i^{k(l-1)} = l \cdot \prod_{i=1}^{\infty} q_i^{k_i} \). Since \( K/Q \) is Galois, we must have \( k_i = 1 \) for all \( i \). Thus \( (2) \) is unramified in \( R_S \). Let \( u \in R_S^2 \setminus R_S^{x^2} \) and set \( K' = K(\sqrt{u}) \). Let \( K' \)
be the completion of \( K \) at \( \mathfrak{l} \) and for any prime \( \mathfrak{L} \) of \( K' \) lying over \( \mathfrak{l} \), let \( K'_{\mathfrak{L}} \) be the completion of \( K' \) at \( \mathfrak{L} \). Let \( f \) be the residue field degree of any prime of \( K' \) lying over \( (2) \). Then after replacing \( u \) by \( u^{2f-1} \in R_S^2 \setminus R_S^{x^2} \), we may assume \( u \equiv 1 \pmod{l} \). By an extension of a result which can be found in Fröhlich and Taylor [1, eqn. (3.11) p.141], since \( l \) is unramified over \( (2) \) we have

\[
\begin{align*}
  i) & \quad \text{ord}_l(u - 1) \geq 3 \quad \text{iff} \quad K'_{\mathfrak{L}} = K_{\mathfrak{l}}. \\
  ii) & \quad \text{ord}_l(u - 1) = 2 \quad \text{iff} \quad K'_{\mathfrak{L}} \neq K_{\mathfrak{l}} \quad \text{is unramified over} \quad K_{\mathfrak{l}}. \\
  iii) & \quad \text{ord}_l(u - 1) = 1 \quad \text{iff} \quad K'_{\mathfrak{L}} \quad \text{is totally ramified over} \quad K_{\mathfrak{l}}.
\end{align*}
\]

In fact this holds for the completions at any prime lying over \( (2) \) which is unramified.

In our present situation, this means it holds for all \( q_i \) as \( (2) \) is unramified.

Since \( K' \cap H = K \). \( K' \) must be ramified over \( K \) and thus can only ramify at \( \mathfrak{l} \) since \( K' \subset F \). Thus \( K'_{\mathfrak{L}} \) is totally ramified over \( K_{\mathfrak{l}} \). This means that \( \text{ord}_{\mathfrak{l}}(u - 1) = 1 \).

In the expression \( (2) = l \cdot \prod_{i=1}^{\infty} q_i^{f_i} \), assume for the moment that \( m \geq 1 \). That is, assume there is at least one prime other than \( \mathfrak{l} \) which lies over \( (2) \). Because \( K/Q \) is Galois, there is some \( \iota \in \text{Gal}(K/Q) \) such that \( \iota(\mathfrak{l}) = q_1 \). Then it follows that \( \text{ord}_{q_1}(\iota(u) - 1) = 1 \). Let \( u'' = \iota(u) \) and let \( K'' = K(\sqrt{u''}) \neq K \). Then we have \( K''_{\mathfrak{Q}_1} \)

is ramified over \( K_{q_1} \), where \( Q_1 \) is a prime of \( K'' \) lying over \( q_1 \). This in turn says that \( q_1 \) ramifies from \( K \) up to \( K'' \subset L_2 \subset F \). This contradicts the fact that only \( \mathfrak{l} \) may
ramify in $F$. This tells us that if $K/Q$ is Galois, then $L_2 \subseteq F$ and $\tau \in Gal(F/L_2)$ imply that $(2) = 1$. But this means that $f$ is principal and thus as $f \in C$, which generates the class group, we see that $R_S$ has $\hat{h} = 1$. Thus if $h > 2$ this case can not occur and so $\theta_C$ is the minimal algorithm for $C$ for every class $C$ which generates the class group. This completes the proof of Theorem 21. \hfill \square

**Conclusion:** The theorem tells us that there is always at least one class $C$ for which $\theta_C$ is the correct minimal algorithm. Since $\psi_C$ is a homomorphism in this case, we discover the arithmetic structure of $R_S$. Namely, $\forall x \in K \setminus C, \exists y \in c$ such that $\psi_C((x - y)) < \psi_C(c)$. This directly generalizes the Euclidean algorithm $\psi$ for a Euclidean ring $R$ in which case we have that $\forall x \in K. \exists y \in R$ such that $\tilde{\psi}(x - y) < 1$. if $\psi$ is multiplicative and is extend to $\tilde{\psi} : K \to \mathbb{Q}$ by $\tilde{\psi}(\frac{a}{b}) = \psi(a)/\psi(b)$ and $\psi(0) = 0$.

**Remark:** There is the practical matter of determining for which classes $C$ is $\theta_C$ the correct minimal algorithm. In general, we know this will be so for all but at most one generating class. Given any class $C$, recall the factorization of $(2) = l \cdot \prod q_i^{e_i}$. Then $\theta_C$ can only fail to be the correct minimal algorithm if for some prime $p$, which equals $l$ or one of the $q_i$ for which $e_i = 1$, we have

1) $p \in C$ with $R_S^\times \to (R_S/p)^\times$.

2) $L_2 \subseteq F$ where $F$ is the $S$-ray class field for $b = p^2$, and

3) there is some $\tau \in Gal(F/K)$ such that $\tau|_{L_2} = id$ and $\tau|_H = (p, H/K)$ where $H$ is the $S$-Hilbert class field.

There are only finitely many primes to check and finitely many $S$-ray class fields to compute. If it turns out that 1), 2), and 3) hold, then immediately we know that for all generating classes $C'$ other than $C$, $\theta_{C'}$ is the correct minimal algorithm. $\theta_C$ may still work for $C$ in this situation, although this has not been proved.
BIBLIOGRAPHY
BIBLIOGRAPHY


