Pzena, Howard Sheldon

THE EXPLICIT CONSTRUCTION OF RING CLASS FIELDS WITH APPLICATIONS TO QUADRATIC FORMS

City University of New York PH.D. 1983

THE EXPLICIT CONSTRUCTION OF RING CLASS FIELDS WITH APPLICATIONS TO QUADRATIC FORMS

by

HOWARD PZENA

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1983

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

7/20/83 — date

Harvey Cohn — Chairman, Examining Committee

7/20/83 — date

Executive Officer

Professor Harvey Cohn

Professor Burton Randol

Professor Alphonse Vasquez

Supervisory Committee

ACKNOWLEDGMENTS

I wish to thank my advisor, Professor Harvey Cohn, for his patience, guidance and constant encouragement.

I also wish to thank the other professors and students of the Mathematics Department for providing the right environment for doing research.

TABLE OF CONTENTS

Chapter 1 - Preliminaries

1.1 Algebraic Number Theory

Let K be a finite extension of $\mathbb{Q}$. We will call any finite extension field of $\mathbb{Q}$ a number field.

Definition: Let K be a number field. The ring of integers of K is the integral closure of $\mathbb{Z}$ in K. We will denote this ring by O_K.

Definition: A Dedekind domain D is an integral domain having the following three properties:

(1) D is integrally closed in its quotient field

(2) D is a Noetherian ring

(3) Every non-zero prime ideal P in D is a maximal ideal.

Theorem 1: Every ideal I in a Dedekind domain can be written uniquely as a product of prime ideals.

$$I = \prod_{i=1}^{n} P_i^{\alpha_i}$$

Theorem 2: Let K be a number field. Then O_K is a Dedekind domain.

Definition: If D is a domain and F its field of fractions, a fractional ideal I is a non-zero D - submodule of F such that $aI \subset D$ for some non-zero $a \in D$.

Note: Every ideal $I \subset D$ is a fractional ideal, which will sometimes be called an integral ideal. Let I_1 and I_2 be two fractional ideals of D. We define $I_1 I_2 = \{ \sum b_{1j} b_{2j} \mid b_{1j} \in I_1, b_{2j} \in I_2 \}$. This set is again a fractional ideal called the product of I_1 and I_2.

Theorem 3: The fractional ideals of a Dedekind domain constitute a group under multiplication with D as a unit. The inverse of a fractional ideal I is given by $J = \{ x \in F \mid xI \subset D \}$.

Notation: Let K be a number field. We denote by I(K) the group of fractional ideals and by P(K) the principal fractional ideals; i.e.

$P(K) = \{ I \mid I \in I(K) \text{ and } I = xO_K \text{ for some } x \in K \}$

Theorem 4: Let K be a number field. Then the group I(K)/P(K), which is called the class group of K, is a finite abelian group. The order of this group is denoted by h(K).

Besides the class group, which measures to what extent O_K fails to be a unique factorization domain (O_K is a unique factorization domain if and only if h(K)=1)

it will be important, for what follows, to associate to every number field another constant designed to measure a different phenomena.

Theorem 5: If K is a number field of degree n ($[K:\mathbb{Q}]=n$) then O_K, the ring of algebraic integers, is a free abelian group of rank n.

Definition: Any basis of the free abelian group O_K is called an integral basis of K.

The numerical invariant that we wish to attach to every number field K is given in the next definition.

Definition: Let K be a number field and let $\{x_1,\ldots,x_n\}$ be an integral basis of K. The discriminant of $K/\mathbb{Q}$ is defined to be $\text{discr}_{K/\mathbb{Q}}(x_1,\ldots,x_n) = \det(\text{Tr}_{K/\mathbb{Q}}(x_ix_j))$ that is, the determinant of the matrix whose (i.j) - entry is equal to $\text{Tr}_{K/\mathbb{Q}}(x_ix_j)$ (for $i,j = 1,\ldots,n$).

For this last definition to make sense it is necessary to show that if $\{y_1,\ldots,y_n\}$ is another integral basis of K then $\text{discr}_{K/\mathbb{Q}}(x_1,\ldots x_n) = \text{discr}_{K/\mathbb{Q}}(y_1,\ldots,y_n)$. Furthermore, it can be shown, without too much difficulty,

that d_K is a non-zero element of $\mathbb{Z}$. The significance of d_K will be revealed shortly; but first we must discuss, in general, how a prime ideal of O_K decomposes in the ring of integers of some field, of which K is a subfield.

Let L and K be number fields with $K \subset L$. Further, let $\mathfrak{p} \subset O_K$ be a prime ideal. The ideal $\mathfrak{p} O_L$ is not necessarily a prime ideal of O_L. Since O_L is a Dedekind domain $\mathfrak{p} O_L$ can be factored uniquely into a product of prime ideals, i.e. $\mathfrak{p} O_L = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g}$ with $\mathfrak{P}_i$, $i = 1$ to g, a prime ideal in O_L. When L/K is a Galois extension we have that $e_1 = \ldots = e_g$.

Definition: The integer e_i is called the ramification index of $\mathfrak{P}_i$ over K.

Definition: A prime ideal $\mathfrak{p}$ of O_K is said to ramify in L if any one of the ramification indices e_i is larger than one.

Theorem 6: Let p be a prime in $\mathbb{Z}$, and suppose (p) is ramified in a number field K. Then $p \mid d_K$. Conversely, if $p \mid d_K$ then (p) is ramified.

We would like to be able to handle the general case: Given the number fields K and L with $K \subset L$ find a necessary

and sufficient condition for a prime $\mathfrak{p}$ of O_K to ramify in L.

The relative case (L/K) is more difficult than the absolute case (K/$\mathbb{Q}$) due to the fact that O_L need not be a free O_K-module.

Definition: Let K and L be number fields with $K \subset L$. The discriminant (ideal) of L over K is the ideal of O_K generated by the discriminants of bases of L over K which are contained in O_L. It will be denoted $\mathfrak{D}_{L/K}$.

Theorem 7: A prime $\mathfrak{p}$ of O_K is ramified in L if and only if $\mathfrak{p} | \mathfrak{D}_{L/K}$.

Corollary: Let $K \subset L$ be two number fields. Only finitely many prime ideals $\mathfrak{p}$ of O_K ramify in L.

We next state two theorems concerning how primes decompose in larger fields.

Definition: Let L and K be number fields with $K \subset L$. A prime ideal $\mathfrak{p} \subset O_K$ is said to split completely from K to L if the ideal $\mathfrak{p} O_L = \mathfrak{P}_1 \cdots \mathfrak{P}_n$, where $n = [L:K]$.

Theorem 8: Let K be number field, and let L and M be two finite extensions of K. Let $\mathfrak{p}$ be a prime ideal in O_K. If $\mathfrak{p}$ splits completely in both L and M then $\mathfrak{p}$

splits completely in the compositum, LM. The converse is also true; namely, if $\mathfrak{p}$ splits completely in LM, it must split completely in both L and M.

Theorem 9: Let L/K be a Galois extension and let $S_{L/K}$ be the set of primes of K which split completely in L. If E is another extension of K then $S_{L/K} \subset S_{E/K}$ if and only if $E \subset L$.

Finally, we will have occasion to use the Dirichlet unit theorem, which provides a description of the unit group of O_K.

Theorem 10: Let K be number field and let $n = [K: \mathbb{Q}]$ Let r be the number of real embeddings of K into $\mathbb{C}$ and let 2s be the number of complex embeddings. $(n = r + 2s)$. Then U_K the group of units of O_K has the following structure: $U_K \approx W \times C_1 \times \ldots \times C_{r+s-1}$ where W is the cyclic group of finite order consisting of the roots of unity in K and each C_i is an infinite cyclic group.

1.2 Class Field Theory

The purpose of class field theory is to provide a complete description, for every number field K, of the abelian extensions of K. By suitably generalizing the notion of the class group of K it is possible to capture all the abelian extensions L/K. In addition, class field theory, through the Artin reciprocity laws, allows one to realize Gal (L/K) in terms of these generalized class groups, whenever Gal (L/K) is abelian. Finally, we also learn how a prime $\mathfrak{p}$ in K decomposes in L, for an abelian extension L of K.

Definition 10: A modulus for K is a formal product $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ taken over all primes $\mathfrak{p}$ of K in which $n(\mathfrak{p})$ is a nonnegative integer and $n(\mathfrak{p}) > 0$ for only a finite number of $\mathfrak{p}$. Furthermore $n(\mathfrak{p}) = 0$ or 1 when $\mathfrak{p}$ is a real infinite prime and $n(\mathfrak{p}) = 0$ when $\mathfrak{p}$ is a complex infinite prime. Let $\mathfrak{P}$ denote a real prime of K. Let $x \longrightarrow x_{\mathfrak{P}}$ denote the embedding of K into $K_{\mathfrak{P}}$. For elements α, β in K* we write $\alpha \equiv \beta \bmod \mathfrak{P}$ to mean $\alpha_{\mathfrak{P}}$ and $\beta_{\mathfrak{P}}$ have the same sign.

Now let $\mathfrak{p}$ be a finite prime, α, β elements in K* and suppose that $\alpha = \frac{a}{c}$, $\beta = \frac{b}{d}$ $a,b,c,d \in O_K$.

Then we write $\alpha \equiv \beta \mod^{x} \mathfrak{p}^{n}$ if $\frac{\alpha}{\beta} = \frac{ad}{bc}$ is in $(O_K)_{\mathfrak{p}}$ and this element is congruent to 1 modulo $\mathfrak{p}^{n}$; that is $\frac{ad-bc}{bc} \in \mathfrak{p}^{n}$.

Definition 11: For $\alpha, \beta \in K^*$ we write $\alpha \equiv \beta \mod^{x} \mathfrak{m}$ if $\alpha \equiv \beta \mod^{x} \mathfrak{p}^{n(\mathfrak{p})}$ for all primes with $n(\mathfrak{p}) > 0$.

We denote by $I(\mathfrak{m})$ the group of fractional ideals of K relatively prime to $\mathfrak{m}$. $P^{1}(\mathfrak{m})$ will denote the group of principal fractional ideals of K which have a generator $\alpha \equiv 1 \mod^{x} \mathfrak{m}$. The quotient group $I(\mathfrak{m})/P^{1}(\mathfrak{m})$ is called the ray class group mod $\mathfrak{m}$.

Theorem 10: For any modulus $\mathfrak{m}$, the ray class group mod $\mathfrak{m}$ is a finite group. Let $h(\mathfrak{m})$ denote the order of this group. Then $h(K) \mid h(\mathfrak{m})$.

A subgroup of H of I(K) is called a congruence subgroup if there exists a modulus $\mathfrak{m}$ such that $P^{1}(\mathfrak{m}) \subset H \subset I(\mathfrak{m})$. We will say that H is defined mod $\mathfrak{m}$ if H is a congruence subgroup and $P^{1}(\mathfrak{m}) \subset H \subset I(\mathfrak{m})$. Suppose $\mathfrak{n}$ is a modulus and $\mathfrak{n} \mid \mathfrak{m}$. Any ideal relatively prime to $\mathfrak{m}$ is also relatively prime to $\mathfrak{n}$ so $I(\mathfrak{m}) \subseteq I(\mathfrak{n})$. If there exists a congruence subgroup

$H_{\mathfrak{n}}$ defined mod $\mathfrak{n}$ such that $H = I(\mathfrak{m}) \cap H_{\mathfrak{n}}$ we say H is the restriction of $H_{\mathfrak{n}}$ to $I(\mathfrak{m})$.

<u>Theorem 11</u>: Let $\mathfrak{n} | \mathfrak{m}$ and $H_{\mathfrak{m}}, H_{\mathfrak{n}}$ be congruence subgroups defined mod $\mathfrak{m}$ and $\mathfrak{n}$. Suppose $H_{\mathfrak{m}} = I(\mathfrak{m}) \cap H_{\mathfrak{n}}$. Then

(a) $I(\mathfrak{m})/H \approx I(\mathfrak{n})/H_{\mathfrak{n}}$ (b) $H_{\mathfrak{n}} = H_{\mathfrak{m}} P^1(\mathfrak{m})$.

Let H_1 and H_2 be two congruence subgroups. If there exist a modulus $\mathfrak{m}$ such that $H_1 \cap I_{\mathfrak{m}} = H_2 \cap I_{\mathfrak{m}}$ we will write $H_1 \sim H_2$ and say H_1 is equivalent to H_2 ($\sim$ is an equivalence relation). An equivalence class of congruence subgroups H, is called a class group. It can be shown that there exists a unique modulus $\mathfrak{f}$ such that $H_{\mathfrak{f}} \in H$ and $H_{\mathfrak{m}} \in H$ implies $\mathfrak{f} | \mathfrak{m}$
This modulus is called the conductor of H.

Our next task is to discuss the Artin map, through which one establishes a one-to-one correspondence between abelian extensions L of K and class groups of K.

Let K and L be number fields with L a normal extension of K. Suppose $\mathfrak{p} \subset O_K$ is a prime ideal and let $\mathfrak{P} | \mathfrak{p} O_L$. We define two subgroups of $G = \mathrm{Gal}(L/K)$; the decomposition group $D(\mathfrak{P}|\mathfrak{p})$ and the inertia group $E(\mathfrak{P}|\mathfrak{p})$.

Definition: $D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \mid \sigma \in G \text{ and } \sigma\mathfrak{P} = \mathfrak{P}\}$ is called the decomposition group of $\mathfrak{P}$ over $\mathfrak{p}$.

Definition:

$E(\mathfrak{P}/\mathfrak{p}) = \{\sigma \mid \sigma \in G \text{ and } \sigma A \equiv A \bmod \mathfrak{P} \text{ for all } A \in O_L\}$ is the inertia group of $\mathfrak{P}$ over $\mathfrak{p}$.

It is easy to see that $E(\mathfrak{P}/\mathfrak{p}) \subset D(\mathfrak{P}/\mathfrak{p})$. If $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ then σ induces an automorphism $\bar{\sigma}$ of the field $O_L/\mathfrak{P}$ which leaves the subfield $O_K/\mathfrak{p}$ pointwise fixed. The map $\bar{\sigma}$ is given by $\bar{\sigma}(x + \mathfrak{P}) = \sigma x + \mathfrak{P}$. In what follows we will write D and E in place of $D(\mathfrak{P}/\mathfrak{p})$ and $E(\mathfrak{P}/\mathfrak{p})$, respectively.

Let $\bar{G} = \text{Gal}(O_L/\mathfrak{P} / O_K/\mathfrak{p})$. Then there is a group homomorphism of D to $\bar{G}$ which takes σ to $\bar{\sigma}$. The kernel of this homomorphism is E and the map $\sigma \longrightarrow \bar{\sigma}$ is onto $\bar{G}$ so $\bar{G} \approx D/E$. Since $O_L/\mathfrak{P}$ and $O_K/\mathfrak{p}$ are both finite fields $\bar{G}$ is a cyclic group generated by the map which sends $x + \mathfrak{P} \longrightarrow x^{N\mathfrak{p}} + \mathfrak{P}$. Assume now that $\mathfrak{p}$ is unramified in L. Then E is the trivial group so $\bar{G} \approx D$. This implies that for $\mathfrak{p}$ unramified in L there exists a unique element $D(\mathfrak{P}/\mathfrak{p})$ called the Frobenius automorphism ϕ of $\mathfrak{P}$ over $\mathfrak{p}$ which has the property that

$\phi(A) \equiv A^{N\mathfrak{p}} \pmod{\mathfrak{P}}$ for all $A \in O_L$. We will denote the Frobenius automorphism of $\mathfrak{P}$ over $\mathfrak{p}$ by $\left[\frac{L/K}{\mathfrak{P}}\right]$.

Theorem 12: Let L be a normal extension of K and let $\sigma \in \mathrm{Gal}(L/K)$. Then for any prime ideal $\mathfrak{P} \subset O_L$ we have $\left[\frac{L/K}{\sigma\mathfrak{P}}\right] = \sigma^{-1}\left[\frac{L/K}{\mathfrak{P}}\right]\sigma$.

Corollary: Let L be an abelian extension of K and let $\mathfrak{p}$ be a prime ideal of O_K which is unramified in L. Suppose $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are two prime ideals of O_L which divide $\mathfrak{p} O_L$. Then $\left[\frac{L/K}{\mathfrak{P}_1}\right] = \left[\frac{L/K}{\mathfrak{P}_2}\right]$

Proof: There exists a $\sigma \in \mathrm{Gal}(L/K)$ which sends $\mathfrak{P}_1$ to $\mathfrak{P}_2$, i.e. $\sigma\mathfrak{P}_1 = \mathfrak{P}_2$. By the preceding theorem we have $\left[\frac{L/K}{\mathfrak{P}_2}\right] = \left[\frac{L/K}{\mathfrak{P}_1}\right] = \sigma^{-1}\left[\frac{L/K}{\mathfrak{P}_1}\right]\sigma = \left[\frac{L/K}{\mathfrak{P}_1}\right]$ because $\mathrm{Gal}(L/K)$ is abelian.

Definition: For L/K abelian the common value $\left[\frac{L/K}{\mathfrak{P}}\right]$ for all $\mathfrak{P} \mid \mathfrak{p}$ is called the Artin symbol.

Thus for L/K abelian we have a way of associating to each prime ideal $\mathfrak{p} \subset O_K$, relatively prime to $\mathfrak{D}_{L/K}$, an element $\left[\frac{L/K}{\mathfrak{p}}\right]$ of G.

Definition: Let L/K be an abelian extension and let $\mathfrak{m}$ be any modulus divisible by all the finite primes of K which become ramified in L. Then by extending the definition

of the Artin symbol multiplicatively we get a homomorphism from $I(\mathfrak{m})$ to G = Gal L/K. More precisely, for $\mathfrak{a} \in I(\mathfrak{m})$ we define $\left[\frac{L/K}{\mathfrak{a}}\right]$ to be $\prod_{i=1}^{n}\left[\frac{L/K}{\mathfrak{p}_i}\right]^{\alpha_i}$ where $\mathfrak{a} = \prod_{i=1}^{n}\mathfrak{p}_i^{\alpha_i}$. This map from $I(\mathfrak{m})$ to G is called the Artin map.

We can now state the main theorems of class field theory, the first being a result due to Artin.

Theorem 13: (Artin Reciprocity Theorem) Let L/K be an extension with abelian Galois group G. Let $\mathfrak{m}$ be a modulus for K divisible at least by all primes which ramify in L and assume the exponents of the prime divisors of $\mathfrak{m}$ are sufficiently large. Then the Artin map $\left[\frac{L/K}{\ }\right]$ maps $I(\mathfrak{m})$ onto G and the kernel contains $P^1(\mathfrak{m})$. In fact the kernel is $N_{L/K}(I_L(\mathfrak{m}))P^1(\mathfrak{m})$. That is, $G \cong I(\mathfrak{m}) / N_{L/K}(I_L(\mathfrak{m}))P^1(\mathfrak{m})$. (Here $N_{L/K}$ denotes the relative norm and $N_{L/K}(I_L(\mathfrak{m}))$ denotes the group of ideals of K generated by the norms of ideals in L relatively prime to $\mathfrak{m}$). We say that the reciprocity law holds for the triple $(L,K,\mathfrak{m})$ if Gal L/K is abelian and

$$\text{Gal } L/K = I(\mathfrak{m}) / N_{L/K}(I_L(\mathfrak{m}))P^1(\mathfrak{m}).$$

Theorem 14: Let $\mathfrak{m}$ and $\mathfrak{n}$ be two moduli of K such that the reciprocity law holds for $(L,K,\mathfrak{m})$ and $(L,K,\mathfrak{n})$. That is assume

$$\mathrm{Gal}(L/K) \cong I(\mathfrak{m})/H_{\mathfrak{m}} \cong I(\mathfrak{n})/H_{\mathfrak{n}}$$

where $H_{\mathfrak{m}}$ and $H_{\mathfrak{n}}$ are congruence subgroups defined mod $\mathfrak{m}$ and mod $\mathfrak{n}$ respectively. Then $H_{\mathfrak{m}}$ and $H_{\mathfrak{n}}$ belong to the same ideal class group, which is denoted by H(L/K). Let $\mathfrak{f}(L/K)$ denote the conductor of H(L/K). Then the reciprocity law holds for $(L,K,\mathfrak{f}(L/K))$. Furthermore, if $\mathfrak{f}(L/K) \mid \mathfrak{m}$ then the reciprocity law holds for $(L,K,\mathfrak{m})$.

This last theorem combined with the one that follows establishes a one-to-one correspondence between all ideal class groups of K and all abelian extensions L of K.

Theorem 15: Let H be an ideal class group of K. Then there exists a unique abelian extension L of K such that H = H(L/K).

Theorem 16: Let L_1/K and L_2/K be two abelian extensions of conductors $\mathfrak{f}(L_1/K)$ and $\mathfrak{f}(L_2/K)$; so that the reciprocity law holds for $(L_1,K,\mathfrak{m})$ and $(L_2,K,\mathfrak{m})$. Finally, let H_1 and H_2 be the corresponding subgroups of $I(\mathfrak{m})$

then

$$H_1 \subset H_2 \text{ if and only if } L_1 \supset L_2$$

Theorem 17: A prime $\mathfrak{p}$ of K, ramifies in L, an abelian extension of K, if and only if $\mathfrak{p} \mid \mathfrak{f}(L/K)$.

Definition: Let K be a number field. We define the Hilbert class field of K, denoted by HCF(K), to be the maximal abelian unramified extension of K.

The conductor of this extension, by Theorem 17 is $\mathfrak{f}(HCF/K)=(1)$, since no prime of K ramifies. Furthermore, if this extension is to be the maximal abelian unramified extension we must have that the kernel under the Artin map is $P^1(1)$, which is just the group of principal fractional ideals. ($\alpha \equiv a \bmod {}^{\times}1$ imposes no restriction on α.) Consequently, by Artin reciprocity, we see that

$$\text{Gal}\ (HCF(K)/K) \approx I(K)/P(K)$$

Thus $[HCF(K):K] = h(K)$, the class number of K and the Galois group is isomorphic to the class group of K.

For L/K abelian, one can give a description of how a prime ideal $\mathfrak{p}$ of K decomposes in L based on the order of the image of $\mathfrak{p}$ under the Artin map. Since, in the applications that follow, we will be concerned only with primes $\mathfrak{p}$ which split completely in L the following theorem will be adequate.

Theorem 18: Let $\mathfrak{p}$ be a prime ideal of K which is unramified in L. Then $\mathfrak{p}$ splits completely from K to L if and only if $\left[\frac{L/K}{\mathfrak{p}}\right] = 1$

Proof: Suppose $\left[\frac{L/K}{\mathfrak{p}}\right] = 1$, then

$$A \equiv A^{N\mathfrak{p}} \bmod \mathfrak{p} O_L \quad \text{for every } A \in O_L$$

Let $\mathfrak{P} | \mathfrak{p}$ where $\mathfrak{P}$ is a prime ideal of O_L. It follows that

$$A \equiv A^{N\mathfrak{p}} \bmod \mathfrak{P}$$

For $A \notin \mathfrak{P}$ we get $A^{N\mathfrak{p}-1} \equiv 1 \bmod \mathfrak{P}$. But $(O_L/\mathfrak{P})^*$ is a cyclic group of order $N\mathfrak{P} - 1$ so we have $N\mathfrak{P} = N\mathfrak{p}$.

On the other hand,

$$N_{L/K}\mathfrak{P} = \mathfrak{p}^f \text{ where } f = \left[O_{L/\mathfrak{P}} : O_{K/\mathfrak{p}}\right]$$

Also,

$$N\mathfrak{P} = N(N_{L/K}\mathfrak{P}) = N\mathfrak{p}^f = (N\mathfrak{p})^f$$

This implies $f = 1$ for each prime ideal $\mathfrak{P}$ dividing $\mathfrak{p} O_L$. We next use the fact that if F/K is any finite extension of K then $\mathfrak{p}$ factors as

$$\mathfrak{p} O_F = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g} \text{ with } [F:K] = \sum_{i=1}^{g} e_i f_i$$

In our situation we have

$$\mathfrak{p} O_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$$

with $e_i = f_i = 1$ for all i. This implies $g = [L:K]$, i.e. $\mathfrak{p}$ splits completely from K to L.

Conversely, suppose $\mathfrak{p}$ splits completely, i.e. $\mathfrak{p}$ is unramified and

$$\mathfrak{p}\,O_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g \text{ where } \mathfrak{P}_i \neq \mathfrak{P}_j \text{ for } i \neq j,\ g = [L:K]$$

It follows, since we are assuming that $g = [L:K]$ that $f = 1$ so $N\mathfrak{P} = N\mathfrak{p}$.

But, then it follows that $A \equiv A^{N\mathfrak{p}} \bmod \mathfrak{p}$ or equivalently $\left[\frac{L/K}{\mathfrak{p}}\right] = 1$.

Applying this to the extension HCF(K)/K we see that a prime $\mathfrak{p}$ of K splits completely from K to HCF(K) if and only if $\mathfrak{p}$ is a principal ideal.

1.3 Quadratic Fields and Ring Class Fields

By a quadratic field we mean a finite extension of $\mathbb{Q}$ of degree 2. Every quadratic field k is of the form $\mathbb{Q}(\sqrt{D})$ where D is a square free integer. First we describe the ring of integers of k.

Theorem 19: Let $k = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Then O_k, the ring of integers of k, is given by

$$O_k = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}\left[\sqrt{D}\right] & \text{if } D \equiv 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z} \oplus \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \bmod 4 \end{cases}$$

Theorem 20: The discriminant $d_{k/\mathbb{Q}}$ is given by the following formula:

$$d_{k/\mathbb{Q}} = \begin{cases} 4D \text{ if } D \equiv 2 \text{ or } 3 \bmod 4 \\ D \text{ if } D \equiv 1 \bmod 4 \end{cases}$$

Note: The discriminant of a quadratic field is always congruent to 0 or 1 mod 4.

In order to describe how a prime $p \in \mathbb{Z}$ decomposes in $\mathbb{Q}(\sqrt{D})$, it is expedient to introduce the Kronecker symbol. We assume the reader is familiar with the Legendre symbol.

Definition: Let $d \equiv 0$ or $1 \bmod 4$, and suppose d is not a perfect square. Then $\left(\frac{d}{m}\right)$ is defined for all m by means of the following:

$$\left(\frac{d}{p}\right) = 0 \text{ if } p \mid d \text{ and } p \text{ is a prime}$$

$$\left(\frac{d}{2}\right) = \begin{cases} 1 & \text{if } d \equiv 1 \bmod 8 \\ -1 & \text{if } d \equiv 5 \bmod 8 \end{cases}$$

For p an odd prime and $p \nmid d$ $\left(\frac{d}{p}\right)$ = Legendre's symbol.

Finally $\left(\frac{d}{m}\right) = \prod_{r=1}^{n} \left(\frac{d}{p_r}\right)^{\alpha_r}$ for $m = \prod_{r=1}^{n} p_r^{\alpha_r}$

The next theorem provides information on how a prime $p \in \mathbb{Z}$ decomposes in k. We write d in place of $d_{k/\mathbb{Q}}$ whenever no confusion will result.

Theorem 21: Let $k = \mathbb{Q}(\sqrt{D})$ be a quadratic field of discriminant d, and let p be a prime in $\mathbb{Z}$. Then we have the following decomposition rules.

$$p\mathcal{O}_k = \mathfrak{p}_1 \mathfrak{p}_2 \quad \text{if} \quad \left(\frac{d}{p}\right) = 1 \qquad p \text{ splits}$$

$$p\mathcal{O}_k = \mathfrak{p} \quad \text{if} \quad \left(\frac{d}{p}\right) = 1 \qquad p \text{ is inert}$$

$$p = \mathfrak{p}^2 \quad \text{if} \quad \left(\frac{d}{p}\right) = 0 \qquad p \text{ ramifies}$$

Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field with $D > 0$. It follows from the Dirichlet unit theorem (Theorem 9) upon setting $n = 2$, $r = 2$ and $s = 0$ that the group of units $U_k \approx W \times C_1$ where $W = \{1, -1\}$ and C_1 is an infinite cyclic group.

In other words the unit group has the form $\langle \pm \varepsilon^k \rangle$ where ε is a generator of the infinite cyclic part of the unit group. It should be observed that ε , $-\varepsilon$, $\frac{1}{\varepsilon}$, and $\frac{-1}{\varepsilon}$ are also generators of this subgroup. Exactly one of these 4 numbers is greater than 1, say ε . Then ε is called the fundamental unit of k.

On the other hand for imaginary quadratic field, that is, those with $D < 0$ the unit group of a finite cyclic group. More precisely, we have

$$U_k = \begin{cases} \{-1,1\} \text{ for } D \neq -1 \text{ or } -3 \\ \{1,-1,\ i,-i\} \text{for } D = -1 \\ \{1,\rho,\rho^2,\ -\rho\ -\rho^2,\ -1\} \text{ for } D = -3 \end{cases}$$

Questions about the representation of primes by binary quadratic forms with rational integral coefficients can often be reduced to questions concerning the ring of integers of some quadratic field. We give some indication here of the connection between the quadratic number field $\mathbb{Q}(\sqrt{D})$ of discriminant d and the binary quadratic forms $Ax^2 + Bxy + Cy^2$ having discriminant $d = B^2 - 4AC$. The theory we are now about to describe is due to Gauss. For a more modern treatment of this subject we refer the reader to Cohn [4].

A form $F = aX^2+bXY+cY^2$ is said to be primitive if $(a,b,c) = 1$. Two forms F_1 and F_2 are said to be equivalent $F_1 \sim F_2$, when they are equal under a transformation in $SL(2,\mathbb{Z})$. If F_1 is a primitive form of discriminant $d = b^2 - 4ac$ then any form F_2, which is equivalent to F_1, is also primitive and has the same discriminant d. The number of equivalence classes of binary quadratic forms with the same discriminant d will be denoted by $h_+(d)$. This number $h_+(d)$ is closely related to the class number $h(D)$, of the field $\mathbb{Q}(\sqrt{D})$ where $d = f^2D$. Gauss' discovery was that one could put a group structure, called composition of forms, on the set of equivalence classes of forms of discriminant d (for $d < 0$ only positive definite forms are considered). For $d < 0$ and equal to the discriminant of the field $\mathbb{Q}(\sqrt{D})$ one has that $h(d) = h(D)$. In addition, this group is isomorphic to the class group of $\mathbb{Q}(\sqrt{D})$. For $d > 0$ there are complications if $N\varepsilon = +1$, where ε is the fundamental unit of $\mathbb{Q}(\sqrt{D})$. We need the following.

Definition: Two ideals $\mathcal{A}$ and $\mathcal{B}$ of the quadratic field $\mathbb{Q}(\sqrt{D})$ are called strictly equivalent if there exists a number $\alpha \neq 0$ of $\mathbb{Q}(\sqrt{D})$ such that $N(\alpha) > 0$ and $\mathcal{A} = (\alpha)\mathcal{B}$. Using this notion of equivalence one defines the strict class group.

Theorem 22: Let d be the discriminant of the field $\mathbb{Q}(\sqrt{D})$. Then there is an isomorphism between the strict class group of $\mathbb{Q}(\sqrt{D})$ and the equivalence classes of forms. of discriminant d under composition.

The next theorem relates $h_+(f^2d)$ to $h_+(d)$, where it is assumed that d is a field discriminant.

Theorem 23: $h_+(f^2d) = \frac{h_+(d)f}{e_f} \prod_{p|f} (1 - (\frac{d}{p})\frac{1}{p})$, where $(\frac{d}{p})$ is the Kronecker symbol and e_f is the unit index which is defined to be $[O^*:O_f^*]$. (O_f is the order of conductor $f = [O:O_f]$).

The question of whether an integer a is represented by a binary quadratic F has never been answered in a completely satisfactory way. If a happens to be a prime then the situation is somewhat better. One can investigate for

which primes $p_1, p = F(X,Y)$ by using ring class fields. For the moment we restrict ourselves to forms F which represent 1 and whose discriminants are field discriminants. Any such form is called a principal form and is equivalent to the form

$$F_d(x_1y) = \begin{cases} X^2 + DY^2 & \text{if } D \equiv 2 \text{ or } 3 \bmod 4 \\ X^2 + XY + (\frac{1+D}{4})\, Y^2 & \text{if } D \equiv 1 \bmod 4 \end{cases}$$

Theorem 24 : Let $k = \mathbb{Q}(\sqrt{D})$. Then p is represented by $F_d(x,y)$ if and only if p splits completely from $\mathbb{Q}$ to HCF(k).

Proof: Suppose p splits completely from $\mathbb{Q}$ to HCF(k). Of necessity p must split from $\mathbb{Q}$ to k. That is $pO_k = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1\mathfrak{p}_2 \subset O_k$. It follows that $Ny_1 = p$. But $\mathfrak{p}_1$ splits completely from $\mathbb{Q}(\sqrt{D})$ to HCF(k) so $\mathfrak{p}_1$ must be a principal ideal, i.e. $\mathfrak{p}_1 = (\alpha), \alpha \in O_k$. Therefore $p = N(\alpha) = F_d(x,y)$ for suitable x,y integers. Now suppose $p = F_d(x,y)$ so $p = N\alpha$. It follows that p splits completely from $\mathbb{Q}$ to HCF(k). Our next task is to define ring class fields which will allow us to discuss primes p represented by $F_d(x,y)$ with d arbitrary.

Definition: Let $k = \mathbb{Q}(\sqrt{D})$ and suppose f is a positive integer.

The group $H(f) = \{(\alpha) \mid (\alpha, f) = 1$ and $\alpha \equiv z \bmod f$ where $z \in \mathbb{Z}\}$ is a congruence subgroup, i.e. $I(f) \supset H(f) \supset P^1(f)$. By class field theory, there exists a unique field of conductor f, denoted by RCF (f^2d), such that H(f) coincides with the kernel of the Artin map. RCF (f^2d) is called the ring class field of conductor f. Any subfield of RCF (f^2d) is called a ring class field. The quotient $I(f)/H(f)$ is called the ring class group.

Theorem 25: $p = F_d(x,y)$, p a prime if and only if p splits completely from $\mathbb{Q}$ to RCF f^2d. Let $k = \mathbb{Q}(\sqrt{d})$. Then HCF $(k) \subset$ RCF (f^2d). Furthermore

$[\text{RCF } f^2d : \mathbb{Q}(\sqrt{d})] = h_+(f^2d)$. When $d < 0$ $h_+(f^2d)$

$$= f \frac{h(d)}{e_f} \prod_{p \mid f} \left(1 - \left(\frac{d}{p}\right) \frac{1}{p}\right).$$

See [Deuring] for details.

When $d = -m$, m a prime congruent to 1 mod 4 and $f = 2^t$ the above formula gives us that

$[RCF : \mathbb{Q}(\sqrt{m})] = 2^t$ h(-4m) since 2 divides the discriminant - 4m.

Theorem 26: Let m be a prime congruent to 1 mod 4. Then the class number of $\mathbb{Q}(\sqrt{m})$ is odd.

Theorem 27: Let $k = \mathbb{Q}(\sqrt{D})$ be a quadratic field and suppose the discriminant d is divisible by precisely t distinct primes. Then the class group is isomorphic to $C(2^{r_1}) \times \ldots \times C(2^{r_{t-1}}) \times C(p_2^{n_2}) \ldots \times C(p_s^{r_s})$.

1.4 The Explicit Construction of Ring Class Fields

For k a quadratic imaginary field it is possible to obtain the ring class field of conductor f by adjoining to k, special values of a certain modular function. After stating the theorems of complex multiplication we will then construct some ring class fields using techniques developed long ago but only utilized recently, Cohn [5].

Definition : A function $f(\tau)$ defined on the upper half plane H, is called a modular function if

1) f is meromorphic on H

2) $f(\gamma(\tau)) = f(\tau)$ for $\gamma \in SL(2,\mathbb{Z})$

3) If $|f(\tau)| < e^{A y}$ for some positive constant A when $y = \mathrm{Im}(z) \to \infty$.

Definition: For $\tau \in H$ we set $g_2(\tau) = 60 \sum_{\substack{m,n = -\infty \\ (m,n) = 0,0)}}^{\infty} ((\frac{1}{m+n\tau})4$ and

$$g_3(\tau) = 140 \sum_{\substack{m,n = -\infty \\ (m,n) = (0,0)}}^{\infty} \frac{1}{(m\tau+n)^6}.$$

Definition : For $\tau \in H$ we set $\Delta = g_2^3 - 27 g_3^2$.

Finally $j(\tau) = \frac{1728 g_2^3(\tau)}{\Delta(\tau)}$

Theorem 28: For $\tau \in \mathbb{Q}(\sqrt{d}), d < 0$, $j(\tau)$ is an algebraic integer. Let $k = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field of discriminant d. For a natural number f, O_f denotes the order of conductor f in k, i.e. the ring of all algebraic integers belonging to k which are congruent modulo f to a rational integer. Let M be a full module, i.e. $M = \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ with α and β linearly independent over $\mathbb{Q}$ and $\alpha, \beta \in k$. The coefficient ring of a full module M is the ring $R = \{\lambda \mid \lambda \in O_k, \lambda m \in M \text{ for all } m \in M\}$. The coefficient ring coincides with some order O_f. By an ideal belonging to O_f we mean a full module with coefficient ring O_f. The set of ideals belonging to O_f forms a group under multiplication. The quotient of this group by the subgroup of principal ideals $H_f = \{\lambda O_f \mid \lambda \in k - \{0\}\}$ is called the ideal class group of O_f. The order h_f of this group G_f is connected to the order h of the class group of k by the formula $h_f = \frac{hf}{e_f} \prod_{p \mid f} (1 - (\frac{d}{p})\frac{1}{p})$. An ideal $\mathfrak{a}_f$ belonging

to O_f is said to be regular if for some $\xi \in O_f, (\xi, f) = 1$ we have $\xi \mathfrak{a}_f + fO = O_f$. In every ideal class of G_f there is a regular ideal. If $\mathfrak{a}$ is an ideal of k for which $(\mathfrak{a}, f) = 1$ then $\mathfrak{a} \cap O_f$ is a regular ideal of O_f. The ideal class group of O_f is isomorphic to the ring class group I(f)/J(f) via the map

$$\mathfrak{a} \; H(f) \longrightarrow \mathfrak{a}_f H_f$$

Let $T \in G_f$, the ideal class group of O_f. Further let $\mathfrak{a}_f = [\alpha, \beta]$ be an ideal belonging to O_f such that $\mathfrak{a}_f H_f = T$. One defines the class variant j(T) to be

$$j(T) = j(\mathfrak{a}_f) = j\left(\frac{\beta}{\alpha}\right) \text{ where } \frac{\beta}{\alpha} \in H$$

It can be shown that j (T) depends only on T, not on the choice of $\mathfrak{a}_f$ nor on the basis selected.

Theorem 29: The ring class field $RCF\{f^2 d\} = K(\sqrt{d}, j(T))$ where $T \in G_f$.

We will use Theorem 29 together with the next result, which can be found in Cohn [5] to compute some examples.

Theorem 30: There exists a modular function for the group $\Gamma_0(2)$ such that

$$j(\tau) = \frac{64(\eta(\tau)+3)^3}{(\eta(\tau)-1)^2}$$

Furthermore by solving for η one has that

$$\mathbb{Q}(j(2\tau)) = \mathbb{Q}(j(\tau), \sqrt{\eta})$$

$$\mathbb{Q}(j(4\tau)) = \mathbb{Q}(j(2\tau), \sqrt{\xi}) \text{ where } \xi = \frac{1+\sqrt{\eta}}{2}$$

$$\mathbb{Q}(j(8\tau)) = \mathbb{Q}(j(4\tau), \sqrt[4]{\xi})$$

$$\mathbb{Q}(j(16\tau)) = \mathbb{Q}(j(8\tau), \sqrt[8]{1+\quad})$$

Example 1: $RCF\{-256\} = \mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$

First, using only the definition one can see that $j(\sqrt{-1}) = 1728$. Let $\tau = \sqrt{-1}$. The equation

$$1728 = \frac{64(\eta+3)^3}{(\eta-1)^2}$$

has $\eta = 0$ as a root. By Theorem 30 one has

$RCF\{-16\} = \mathbb{Q}(\sqrt{-1})$ $\quad f=2,\ d=4$

$RCF\{-64\} = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ $f=4, d=4, \quad = \frac{1}{2}$.

$RCF\{-256\} = \mathbb{Q}(\sqrt{-1}, \sqrt[4]{2})$ $f=8,\ d=4$

Example 2: $RCF\{-128\} = \mathbb{Q}(\sqrt{-2}, \sqrt{1+\sqrt{2}})$

Since $\mathbb{Q}(\sqrt{-2})$ has class number 1, $j(\sqrt{-2})$ is a

rational integer. For this reason one can use the q - expansion for j given by

$$j(\tau) = \frac{1}{q} + 744 + 196844q + \ldots, q = e^{2\pi i\tau}$$

to determine $j(\sqrt{-2})$. Doing this one gets that $j(\sqrt{-2}) = 8000$. The equation

$$8000 = \frac{64\ (\eta+3)^3}{(\eta-1)^2}$$

has $\eta = 2$ as a root. By Theorem 30 it follows that

$$\text{RCF}\{-32\} = \mathbb{Q}(\sqrt{-2}, \sqrt{2}) \quad f = 2,\ d = -8$$

and $$\text{RCF}\{-128\} = \mathbb{Q}\left(\sqrt{-2}, \sqrt{\frac{1+\sqrt{2}}{2}}\right)\ f = 4, d = -8$$

Therefore $\text{RCF}\{-128\} = (\sqrt{-2},\ 1+\sqrt{2})$.

Chapter 2. Applications to Quadratic Forms

2.1 Introduction

In this part we apply the theory of ring class fields to prove two new results on binary quadratic forms. In an earlier paper Barrucand & Cohn [1], the authors prove some interesting results about prime p of the form $p = A^2 + 32B^2$. Among other things they show that $p = A^2+32B^2$ if and only if $(\frac{\varepsilon 2}{p})=1$ (see below for definition). Our first result shows that for suitable binary quadratic forms F_1 and F_2, if a prime p is represented by both of these forms it is is necessarily of the type A^2+32B^2.

In a series of papers, Lehmer develops properties of special quadratic and quartic symbols. In Lehmer [13] the author makes several conjectures about these symbols. Our second result, which is slightly more general, settles the conjecture 4 of this paper, in the affirmative.

We will state the first of these results now, since this will help to motivate the considerations that follow.

Main Theorem: Let m be a prime congruent to 1 mod 4. Also let p be a prime and suppose $p = X^2 + 16mY^2 = U^2 + 32mV^2$ for some integers X,Y, U and V. Then $p = A^2 + 32B^2$ where $A, B \in \mathbb{Z}$.

We first show how to translate this question into one about ring class fields so that we can employ theorems from algebraic number theory and class field theory.

As we have seen it is possible to give necessary and sufficient conditions for a prime p to be represented by a principal quadratic form. We recall that a prime p is represented by the principal form F, of discriminant f^2d, if and only if p splits completely from $\mathbb{Q}$ to $RCF\{f^2d\}$. Suppose $p = X^2 + 32mY^2 = U^2 + 16mV^2$. Then p splits completely from $\mathbb{Q}$ to $RCF\{-128m\}$ and from $\mathbb{Q}$ to $RCF\{-64m\}$. By Theorem 8 , p must necessarily split completely from $\mathbb{Q}$ to compositum of these two ring class fields, which we denote by $RCF\{-64m\} \cdot RCF\{-128m\}$. Suppose the theorem stated above is true and let $p = X^2 + 32mY^2 = U^2 + 16mV^2$. Then $p = A^2 + 32B^2$, so p splits completely from $\mathbb{Q}$ to $RCF\{-128\}$. Thus, if p splits

completely from $\mathbb{Q}$ to $K = RCF\{-64m\ \ RCF\{-128m$ then p splits completely from $\mathbb{Q}$ to $RCF\{-128\}$. By Theorem 9 since K is a normal extension of $\mathbb{Q}$, this entails that $RCF\{-128\} \subset RCF\{-64m\} \times RCF\{-128m\}$.

On the other hand suppose we knew that $RCF\{-128\} \subset RCF\{-64m\} \times RCF\{-128m\}$. Let $p = X^2 + 32mY^2 = U^2 + 16mV^2$. But this means p splits from $\mathbb{Q}$ to $RCF\{-64m\} \times RCF\{-128m\}$. However, this allows us to conclude that p splits from $\mathbb{Q}$ to $RCF\{-128\}$ since we are assuming this latter field is contained in the compositum of the ring class fields. Finally we can conclude that $p = A^2 + 32B^2$ because p splits completely from $\mathbb{Q}$ to $RCF\{-128\}$.

The above argument shows that the Main Theorem is equivalent to the following result:

Theorem 31: $RCF\{-128\} \subset RCF\{-64m\} \times RCF\{-128m\}$ for m a prime, $m \equiv 1 \bmod 4$

As we have seen, the field

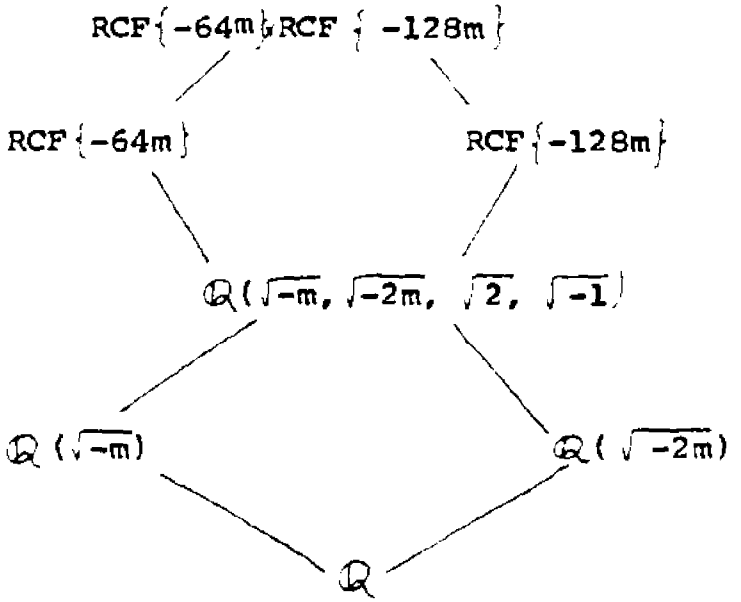
$RCF\{-128\} = \mathbb{Q}(\sqrt{-2}, \sqrt{1+\sqrt{2}})$, $\varepsilon_2 = 1+\sqrt{2}$ the fundamental unit in the field $\mathbb{Q}(\sqrt{2})$.

To prove Theorem 31 we will first show, that for m a prime congruent to 1 mod 4, $\sqrt{\varepsilon}_m \in \mathrm{RCF}\{-64m\}$ and $\sqrt{\varepsilon}_{2m} \in \mathrm{RCF}\{-128m\}$. Once this has been established, the result will follow from the fact that

$$\varepsilon_2 \varepsilon_m \varepsilon_{2m} = \eta^2 \text{ where } \eta \in \mathrm{RCF}\{-64m\}\mathrm{RCF}\{-128m\}$$

The proof given below for the fact that $\sqrt{\varepsilon}_m \in \mathrm{RCF}\{-64m\}$ differs from the proof $\sqrt{\varepsilon}_{2m} \in \mathrm{RCF}\{-128m\}$. As we shall see the proof of the former requires no class field theory, only algebraic number theory. Although a unified proof is possible, it is felt that it is advantageous, in the sense that additional information is provided to give separate arguments.

We first demonstrate that the diagram below is correct



Later on, we will show, in fact, that

$$RCF\{-64m\} \cap RCF\{-128m\} = \mathbb{Q}(\sqrt{-m}, \sqrt{-2m}, \sqrt{2}, \sqrt{-1})$$

Lemma $\sqrt{-1} \in HCF(K)$, $k = \mathbb{Q}(\sqrt{-m})$

Proof: Since HCF(k) is a normal extension of $\mathbb{Q}$ we can use Theorem 8 to show that $\mathbb{Q}(\sqrt{-1}) \subseteq HCF(K)$, by indicating why a prime p which splits completely from $\mathbb{Q}$ to HCF(k) must also split completely from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{-1})$. First, recall that

$p \in S_{HCF(k)/\mathbb{Q}}$ if and only if $p = X^2 + mY^2$

Since $M \equiv 1 \bmod 4$ it follows that $p \equiv 1 \bmod 4$. But $p \equiv 1 \bmod 4$ if and only if $p \in S_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}$

Here we are using Theorem 21 and the fact that $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. Thus, we conclude, since $S_{HCF(k)/\mathbb{Q}} \subset S_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}$ that $\mathbb{Q}(\sqrt{-1}) \subset RCF\{-16m\}$.

Lemma $\sqrt{2} \in RCF\{-64m\}$

Proof: We employ virtually the same argument used to prove the preceding lemma. A prime p splits completely from to $RCF\{-64m\}$ if and only if $p = x^2 + 16my^2$. Since p is a prime x must be odd, but this implies $p \equiv$ mod 8. But, by Theorem 21 and the fact that $(\frac{2}{p}) = (-1)^{\frac{p-1}{8}}$ it follows that p splits completely in $\mathbb{Q}(\sqrt{2})$. Hence by Theorem 9, $\mathbb{Q}(\sqrt{2}) \subset RCF\{-64m\}$

Lemma : Let $K = \mathbb{Q}(\sqrt{-2m})$. Then $\sqrt{-2} \in HCF(K)$

Proof: If p splits completely from $\mathbb{Q}$ to HCF(K) then

$$p = x^2 + 2my^2$$

First we remark that $(\frac{p}{m}) = 1$ because if we reduce the above equation modulo m we get

$$p \equiv x^2 \bmod m \Rightarrow (\frac{p}{m}) = 1.$$

By quadratic reciprocity ($m \equiv 1 \bmod 4$) it follows that

$$(\frac{m}{p}) = (\frac{p}{m})(-1)^{(\frac{p-1}{2})(\frac{m-1}{2})} = 1$$

Next, upon reducing $p = x^2 + 2my^2$ modulo m we obtain

$$0 \equiv X^2 + 2mY^2 \bmod p$$

$$-2mY^2 \equiv X^2 \bmod p$$

$$-2m \equiv \left(\frac{X}{Y}\right)^2 \bmod p \text{ (Note } p \nmid Y \text{) for otherwise}$$

$p \mid x$ too, which implies $p = \pm 1$)

Therefore $\left(\frac{-2m}{p}\right) = 1$

But $\left(\frac{-2m}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{-2}{p}\right)$

Consequently, $\left(\frac{-2}{p}\right) = 1$ so p splits completely from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{-2})$.

Hence, by Theorem 8 again, we have $\mathbb{Q}(\sqrt{-2}) \subset HCF(K)$.

Lemma : $\mathbb{Q}(\sqrt{-1}) \subset RCF(-32m)$

Proof: Step by step the same as Lemma .

Theorem 32: Let $K_1 = \mathbb{Q}(\sqrt{d_1})$ and $K_2 = \mathbb{Q}(\sqrt{d_2})$ be two distinct quadratic fields and let K be a ring class field over K_1 and K_2. Then K is a field of the composite quadratic type: $K = \mathbb{Q}(\sqrt{r_1}, \ldots, \sqrt{r_t}) \supset \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.

Proof: Since K is a ring class field over $\mathbb{Q}(\sqrt{d_1})$ there exists an $S_1 \in Gal(K/\mathbb{Q})$ such that $S_1^2 = 1$, $S_1 T S_1 = T^{-1}$ for all $T \in Gal(K/\mathbb{Q}(\sqrt{d_1}))$.

In fact can $S_1 \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{d_2}))$. Likewise there exists S_2 with $S_2^2 = 1$, $S_2 \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{d_1})$ and $S_2 T S_2 = T^{-1}$ for $T \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{d_2}))$. Let $U \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}))$ then

$$S_1 U S_1 = U^{-1}$$

and $S_1 U S_1 = U$

Therefore $U^2 = 1$ which implies that $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}))$ $\simeq C(2)^g$. Since every element of $\mathrm{Gal}(K/\mathbb{Q})$ can be expressed as $S_2 T$ with $T \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{d_2}))$ it follows that element is of order 2. But then the group is abelian so we are done.

2.2 Ring Class Fields of Conductor 4

In this section we prove that $\sqrt{\varepsilon_m} \in RCF\{-64m\}$ and $\varepsilon_{2m} \in RCF\{-128m\}$ for m a prime congruent to 1 mod 4.

Lemma 1: $\sqrt{2} \notin RCF\{-16m\}$, $m \equiv 1 \bmod 4$

Proof: Assume $\mathbb{Q}(\sqrt{2}, i) \subset RCF\{-16m\}$ and let p be a prime belonging to $S_{RCF\{-16m\}/\mathbb{Q}}$. Then $p \in S_{\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}}$ since $\mathbb{Q}(\sqrt{2}, i) \subset RCF\{-16m\}$. But, this means $p \equiv 1 \bmod 8$. But a prime p splits in $RCF\{-16m\}$ if and only if $p = X^2 + 4mY^2$. To derive a contradiction we must show that the form $X^2 + 4mY^2$ represents primes which are not congruent to 1 mod 8.

If $p = X^2 + 4mY^2$ and $p \equiv 1 \bmod 8$ then Y must be even. Since p is an odd prime X must be odd. Consequently,

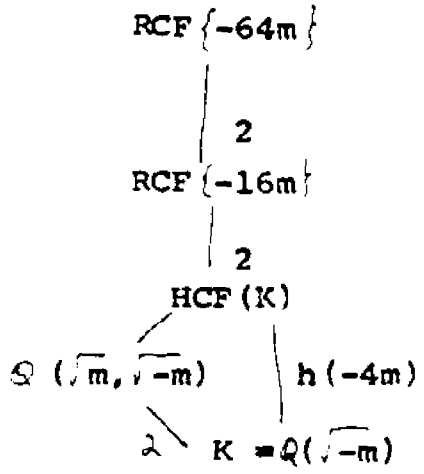
$$p \equiv 1 + 4mY^2 \bmod 8$$

Therefore $8 \mid 4mY^2$ which implies that $2 \mid Y$.

Thus $p = X^2 + 4m(2Y')^2 = X^2 + 16mY'^2$, so p splits completely from $\mathbb{Q}$ to $RCF\{-64m\}$. If every prime representable by the form $X^2 + 4mY^2$ were congruent to 1 mod 8 we would $RCF\{-16m\} = RCF\{-64m\}$. However, $[RCF\{-64m\} : RCF\{-16m\}] = 2$. by Theorem 29, contradiction.

Lemma 2: $\left[RCF\{-16m\} : \mathbb{Q}(\sqrt{m}, \sqrt{-m}) \right] = h(-4m)$, the class number of the field $\mathbb{Q}(\sqrt{-m})$.

Proof: We already know that this diagram is correct:



Since $\sqrt{m} \in HCF\{-4m\}$ we have $\left[RCF\{-16m\} : \mathbb{Q}(\sqrt{m}, \sqrt{-m}) \right] = h(-4m)$

Note: The above diagram shows that $2 \mid h(-4m)$.

Lemma 3: There exists a field $K \subset RCF\{-16m\}$ which is normal over $\mathbb{Q}$ of degree 8 and which contains the field $\mathbb{Q}(\sqrt{m}, \sqrt{-m})$

Proof: Since $G = Gal\left[RCF\{-16m\} / \mathbb{Q}(\sqrt{m}, \sqrt{-m}) \right]$ is an abelian group, we have, by the Fundamental Theorem of Abelian Groups that

$$G \cong C(2^{t_1}) \times \ldots \times C(2^{t_m}) \times C(P_1^{m_1}) \ldots \times C(P_n^{m_n}).$$

Consequently, by Galois Theory, there is an extension K of $\mathbb{Q}(\sqrt{m},\sqrt{-m})$ such that $[K:\mathbb{Q}(\sqrt{m},\sqrt{-m})]=2$ and $K \subset RCF\{-16m\}$

Let $K=\mathbb{Q}(\sqrt{m},\sqrt{-m},\alpha)$ where $\alpha=\sqrt{a+b\sqrt{-1}+c\sqrt{m}+d\sqrt{-m}}$ a,b,c and $d\in\mathbb{Q}$.

Case I $\alpha=\sqrt{a+b\sqrt{-1}}$. Since $RCF\{-16m\}/\mathbb{Q}$ is a normal extension $\sqrt{a+b\sqrt{-1}} \in RCF\{-16m\}$ implies $\sqrt{a-b\sqrt{m}} \in RCF\{-16m\}$, therefore $\sqrt{a+b\sqrt{-1}}\sqrt{a-b\sqrt{-1}}=\sqrt{a^2+b^2} \in RCF\{-16m\}$. But this means $\sqrt{a^2+b^2} \in \mathbb{Q}(\sqrt{m},\sqrt{-m})$ (since $\sqrt{2} \notin K$ and $\sqrt{a^2+b^2}$ has degree at most 2 over $\mathbb{Q}$). Hence $\sqrt{a-b\sqrt{m}} \in K$ also, so K is normal.

Case II $\alpha=\sqrt{a+c\sqrt{m}}$, same as case I

Case III $\alpha=\sqrt{a+d\sqrt{-m}}$, same as case I

Case IV $\alpha=\sqrt{a+b\sqrt{-1}+c\sqrt{m}+d\sqrt{-m}}$ (at least 3 of the 4 coefficients differ from zero).

Since RCF$\{-16m\}/\mathbb{Q}$ is a normal extension, RCF $\{-16m\}$ contains

$$\alpha_2 = \sqrt{a-b\sqrt{-1}-c\sqrt{m}+d\sqrt{-m}}$$

$$\alpha_3 = \sqrt{a-b\sqrt{-1}+c\sqrt{m}-d\sqrt{-m}}$$

and $$\alpha_4 = \sqrt{a+b\sqrt{-1}-c\sqrt{m}-d\sqrt{-m}}$$

We write $\alpha\alpha_2 = \sqrt{A+B\sqrt{-m}}$ $A, B \in \mathbb{Q}$

$\alpha\alpha_3 = \sqrt{C+D\sqrt{m}}$ $C, D \in \mathbb{Q}$

$\alpha\alpha_4 = \sqrt{E+F\sqrt{-1}}$ $E, F \in \mathbb{Q}$

If $\alpha\alpha_2, \alpha\alpha_3$ and $\alpha\alpha_4 \in \mathbb{Q}(\sqrt{m}, \sqrt{-m})$ then K is a normal extension of $\mathbb{Q}$. On the other hand, if one of these products say, $\alpha\alpha_2 \notin \mathbb{Q}(\sqrt{m}, \sqrt{-m})$ then we can replace K by the normal extension $\mathbb{Q}(\sqrt{m}, \sqrt{-m}, \alpha\alpha_2)$ of $\mathbb{Q}$ of degree 8 containing $\mathbb{Q}(\sqrt{m}, \sqrt{-m})$.

Lemma 4: Let K be a subfield of RCF$\{-16m$ containing $\mathbb{Q}(\sqrt{m}, \sqrt{-m})$ which is normal over $\mathbb{Q}$ of degree 8. Then

$$K = \mathbb{Q}(\sqrt{-m}, \sqrt{a+b\sqrt{m}}) \quad a, b \in \mathbb{Q}$$

Proof: Since $K/\mathbb{Q}$ is a normal extension $Gal(K/\mathbb{Q}) \approx D_8$, the dihedral group of order 8. This is because K is a ring class field, so $Gal(K/\mathbb{Q})$ is either $C(2)\times C(2)\times C(2)$ or D_8.

The first group is ruled out by the fact that $RCF_{\{}-16m$, hence K also, has only 3 subfields of degree 2 over $\mathbb{Q}$.

Note: by Lemma $\sqrt{2} \notin RCF\{-16m\}$

Also $Gal(K/\mathbb{Q}(\sqrt{m}))$ must be C(4), which means that $Gal(K/\mathbb{Q}(\sqrt{m})) \cong C(2) \times C(2)$. But then $K = \mathbb{Q}(\sqrt{m}, \sqrt{-m}, \sqrt{r})$ where $r \in \mathbb{Q}(\sqrt{m})$. Since $\mathbb{Q}(\sqrt{m}, \sqrt{-m})$ is the maximal subfield of $RCF\{-16m\}$ which is abelian over $\mathbb{Q}$, $r \notin \mathbb{Q}$. Therefore $r = a+b\sqrt{m}$.

Lemma 5: $a^2 - b^2m = t^2$ where $t \in \mathbb{Q}$

Proof: We eliminate all the other possibilities.

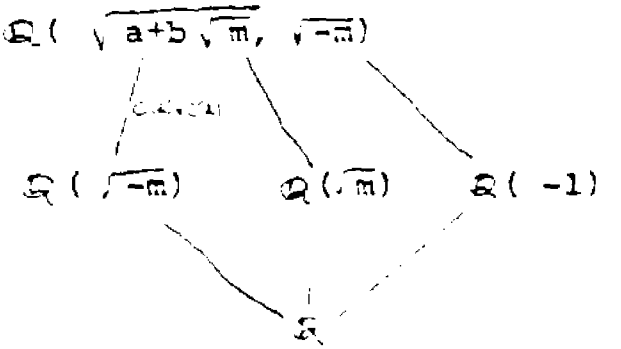
Case I $a^2 - b^2m = t^2$ $t \in \mathbb{Q}$

Let $\tau \in Gal\left[\mathbb{Q}(\sqrt{a+b\sqrt{m}}, \sqrt{-m})/\mathbb{Q}(\sqrt{-m})\right]$ such that

$\tau(\sqrt{a+b\sqrt{m}}) = \sqrt{a-b\sqrt{m}}$. τ leaves $\sqrt{a+b\sqrt{m}}\sqrt{a-b\sqrt{m}} = t$ fixed. Now we calculate $\sqrt{a+b\sqrt{m}}\sqrt{a-b\sqrt{m}} = \tau(\sqrt{a+b\sqrt{m}}\sqrt{a-b\sqrt{m}}) = \sqrt{a-b\sqrt{m}}\,\tau(\sqrt{a-b\sqrt{m}})$ so $\tau(\sqrt{a-b\sqrt{m}}) = \sqrt{a+b\sqrt{m}}$ i.e.

$Gal\left(\mathbb{Q}(\sqrt{a+b\sqrt{m}}, \sqrt{-m})/\mathbb{Q}(\sqrt{-m})\right) \cong C(2) \times C(2)$.

But $Gal(K/\mathbb{Q}(\sqrt{-m})) \cong C(4)$ so $a^2 - b^2m \neq t^2$.



Case II $a^2 - b^2 m = m t^2$ $t \in \mathbb{Q}$

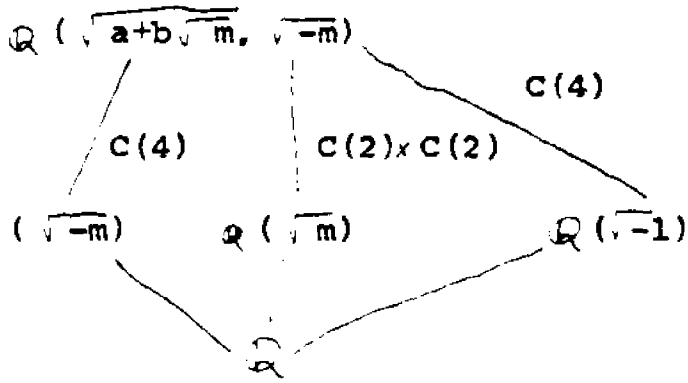
If $a^2 - b^2 m = m t^2$, $t \in \mathbb{Q}$ we get that Gal $(K/\mathbb{Q}(\sqrt{-1})) \approx C(4)$

For let $\tau \in$ Gal $(K/\mathbb{Q}(\sqrt{-1}))$ such that $\tau(a+b\sqrt{m}) = a-b\sqrt{m}$.

$\tau(\sqrt{a+b\sqrt{m}}\ \sqrt{a-b\sqrt{m}}) = \tau(t^2\sqrt{m}) = -t^2\sqrt{m}$

Therefore $\tau(\sqrt{a-b\sqrt{m}}) = -\sqrt{a+b\sqrt{m}}$ which implies $\tau^2 = 1$.

It follows that Gal$(K/\mathbb{Q}) \approx C(2) \times C(4)$, which contradicts the fact that Gal$(K/\mathbb{Q}) \approx D_8$



Case III $a^2 - b^2 m = -m t^2$

Let $\tau \in$ Gal$(K/\mathbb{Q}(\sqrt{-m}))$ with the property that

$$\tau(\sqrt{a+b\sqrt{m}}) = \sqrt{a-b\sqrt{m}}$$

Then $\tau(\sqrt{a+b\sqrt{m}}\ \sqrt{a-b\sqrt{m}}) = \tau(t\sqrt{-m}) = t\sqrt{-m}$. This means that $\tau(\sqrt{a-b\sqrt{m}}) = \sqrt{a+b\sqrt{m}}$ which in turn implies Gal$(K/\mathbb{Q}(\sqrt{-m})) \approx C(2) \times C(2)$. But Gal $K/\mathbb{Q}((\sqrt{-m}))$ must be C(4), so $a^2 - b^2 m \neq -m t^2$

We will need to use the following result from Kummer Theory, Hilbert 13 :

Theorem 33: Let k be a number field and let $\alpha \in k$. Then a prime ideal $\mathfrak{p} \subset O_k$, $\mathfrak{p} \nmid (2)$ which divides (α) to an odd power is ramified in $k(\sqrt{\alpha})$. Furthermore if $\mathfrak{p}$ is an odd prime and $\mathfrak{p}$ divides (α) to an even power then $\mathfrak{p}$ is unramified.

Theorem 34: Let m be a prime which is congruent to 1 mod 4. Then $\sqrt{\varepsilon_m}$, where ε_m denotes the fundamental unit of $\mathbb{Q}(\sqrt{m})$ is contained in the field $RCF\{-64m\}$.

Proof: By the previous lemma we have that

$$\sqrt{a+b\sqrt{m}} \in RCF\{-16m\} \subset RCF\{-64m\}, \text{ where } a^2-b^2m=t^2.$$

We may assume without loss of generality that a, b and t are integers and that m does not divide a or t. Let us write the principal ideal $(a+b\sqrt{m})$ as the product of prime ideals in $\mathbb{Q}(\sqrt{m})$

$$(a+b\sqrt{m}) = P_1^{n_1} \ldots P_r^{n_r}$$

where $P_1, \ldots, P_r$ are the prime ideals lying over the primes $p_1, \ldots p_s$, the prime divisors of t $(s < r)$.
First if $P_i^{n_i} \,||\, (a+b\sqrt{m})$ with P_i an odd prime (NP_i is odd)

then n_i is even because $K/\mathbb{Q}$ is unramified at p if $p \mid m$ or 2. We look at several cases:

Case I 2 is inert, i.e. $(2) = 2\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ is a prime ideal in $\mathbb{Q}(\sqrt{m})$. Let $(a+b\sqrt{m}) = (2)^r P_2^{n_2} \dots P_s^{n_s}$

Then $\left(\frac{a+b\sqrt{m}}{2^r}\right) = P_2^{n_2} \dots P_s^{n_s}$ so $\frac{a+b\sqrt{m}}{2^r}$ is an integer in $\mathbb{Q}(\sqrt{m})$.

Set $\tau = \frac{a+b\sqrt{m}}{2^r}$. Since $P_2^{n_2} \dots P_s^{n_s}$ is a principal ideal we know that $P_2^{\frac{n_2}{k}} \dots P_s^{\frac{n_s}{k}}$ is also a principal ideal. Indeed, the class number of $\mathbb{Q}(\sqrt{m})$ is odd; for m is a prime congruent to 1 mod 4 so the number of prime divisors of the discriminant of $\mathbb{Q}(\sqrt{m})$ is one. But $(P_2^{\frac{n_2}{k}} \dots P_s^{\frac{n_s}{k}})^2 = (\tau)$ is a principal ideal and $2 \nmid h(m)$ so $P_2^{\frac{n_2}{k}} \dots P_s^{\frac{n_s}{k}}$ is also principal. Let $(\beta) = P_2^{\frac{n_2}{k}} \dots P_s^{\frac{n_s}{k}}$. Then $(\beta)^2 = (\tau)$ so $\tau = (\beta^2)$ (unit) or $\sqrt{\tau} = \beta\sqrt{\text{unit}}$. This implies $\sqrt{\varepsilon_m} \in \text{RCF}\{-64m\}$ (We do not necessarily have $\sqrt{\varepsilon_m} \in \text{RCF}\{-16m\}$ for $\tau = \frac{a+b\sqrt{m}}{2^r}$ and r might be odd).

Case II Next, we assume that 2 splits, i.e. $(2) = Q_1 Q_2$ where Q_1 and Q_2 are prime ideals of $\mathbb{Q}(\sqrt{m})$ lying above 2. Let $(a+b\sqrt{m}) = Q_1^{r_1} Q_2^{r_2} P_1^{n_1} \dots P_s^{n_s}$

As before $n_1, \dots n_s$ must be even because the primes $P_1, \dots, P_s$ are unramified in RCF$\{-16m\}$. We also have that $(t^2) = Q_1^{r_1+r_2} Q_2^{r_1+r_2} P_1^{n_1} \dots P_s^{n_s} P_1^{-n_1} \dots P_s^{-n_s} = (2^{r_1+r_2}) P_1^{n_1} \dots P_s^{n_s}$.

It follows that

$$(t^2) = Q_1^{r_1+r_2} Q_2^{r_1+r_2} P_1^{n_1} \ldots P_s^{n_s} \bar{P}_1^{n_1} \ldots \bar{P}_s^{n_s}$$
$$= (2^{r+r}) P_1^{n_1} \ldots \bar{P}_s^{n_s}.$$

Now if $2 \mid t$ then 2^2 divides t^2 so $r_1 + r_2$ is even.

Replacing $a+b\sqrt{m}$ by $\frac{a+b\sqrt{m}}{r_2}$ we may proceed as before.

$$\left(\frac{a+b\sqrt{m}}{2^{r_2}}\right) = Q_1^{r_1 - r_2} P_1^{n_1} \ldots P_s^{n_s} \quad r_1 - r_2, n_1 \ldots n_s$$

all even.

We call attention to the following result which is an immediate consequence of this method of proof:

Corollary: Let m be a prime, $m \equiv 1 \bmod 4$ and let $k = \mathbb{Q}(\sqrt{-m})$. Suppose $4 \mid h(-m)$ the class number of k. Then either $\sqrt{\varepsilon_m}$ or $\sqrt{2\varepsilon_m}$ is contained in HCF(k).

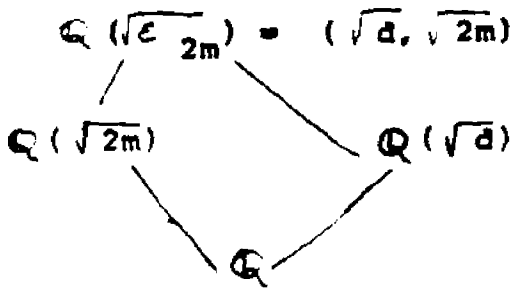
We cannot use the same argument to show that $\sqrt{\varepsilon_{2m}} \in \mathrm{RCF}\{-128m\}$ because $h(2m)$ is always even. Instead we must use class field theory. In all that follows we assume m is a prime congruent to 1 mod 4.

Lemma If $N\varepsilon_{2m} = 1$ then $\sqrt{\varepsilon_{2m}} \in \mathbb{Q}(\sqrt{m}, \sqrt{2m}) \subset \mathrm{RCF}\{-128m\}$

Proof: Let $\varepsilon_{2m} = a+b\sqrt{m}$. Since $N\varepsilon_{2m} = 1$ we have that

$\sqrt{a-b\sqrt{m}} \in \mathbb{Q}(\sqrt{\varepsilon_{2m}})$ and $\mathbb{Q}(\sqrt{\varepsilon_{2m}})/\mathbb{Q}$ is a normal extension of degree 4 having Galois group $C(2)\times C(2)$.

Consequently we have



Since $\mathbb{Q}(\sqrt{\varepsilon_{2m}})/\mathbb{Q}$ is necessarily unramified outside of $\{2,m\}$ (this is because ε_{2m} is a unit) d must be m or 2, so the lemma holds.

Theorem: 35 Let $k = \mathbb{Q}(\sqrt{D})$ with $D<0$. An abelian extension K of k is a ring class field if there exists a $T \in Gal(K/\mathbb{Q})$ such that $T^2=1$, $T(\sqrt{D}) = -\sqrt{D}$ and $TST^{-1} = S^{-1}$ for every $S \in Gal(K/k)$.

Proof: First we show that the kernel of the Artin Map $\left[\frac{K/k}{}\right]$ contains the group

$H = \{(\alpha) \mid \alpha \in \mathbb{Q}^* \ \alpha = p_1^{n_1} \ldots p_s^{n_s}$ and no p_i is unramified in $K\}$.

It suffices to show that for every $p \in \mathbb{Z} \cap H$ that $\left[\frac{K/k}{(p)}\right] = 1$, where $1 \in Gal(K/k)$ is the identity element.

Case I Let $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ where $\mathfrak{p}_i \subset O_k$

Let $S_1 = \left[\frac{K/k}{\mathfrak{p}_1}\right]$ and $S_2 = \left[\frac{K/k}{\mathfrak{p}_2}\right]$. Then we have

$$S_1 A \equiv A^p \bmod \mathfrak{p}_1 O_K \text{ for every } A \in O_K$$

Applying T to both sides of this congruence we get

$$TS_1(A) \equiv (A^p) \bmod \mathfrak{p}_2 O_K \text{ since } T(\mathfrak{p}_1 O_K) = (T\mathfrak{p}_1)O_K = \mathfrak{p}_2 O_K.$$

Therefore, $TS_1(A) \equiv T(A^p) \equiv (TA)^p \equiv S_2(TA) \bmod \mathfrak{p}_2 O_K$

for all $A \in O_K$. Equivalently, we have

$$T^{-1}S_2^{-1}TS_1(A) \equiv A \bmod \mathfrak{p}_2 O_K$$

Using the fact that $T^{-1}S_2^{-1}T = S_2$ we may rewrite this as

$$S_2 S_1(A) \equiv A \bmod \mathfrak{p}_2 O_K$$

We can conclude that $S_2 S_1 = 1$ since $\mathfrak{p}_2$ is unramified from k to K(If $\mathfrak{P} \subset O_K$ with $\mathfrak{P} | \mathfrak{p}_2 O_K$ then $S_1 S_2 \in E(\mathfrak{P}|\mathfrak{p}_2)$ = the trivial group because $\mathfrak{p}_2$ is unramified).

But $\left[\frac{K/k}{(p)}\right] = \left[\frac{K/k}{\mathfrak{p}_1}\right]\left[\frac{K/k}{\mathfrak{p}_2}\right] = S_1 S_2$ so (p) is in the kernel of the Artin map.

Case II Let $(p) = \mathfrak{p}$ where $\mathfrak{p} \subset O_k$, i.e. let p be inert.

We denote $\left[\frac{K/k}{\mathfrak{p}}\right] = \left[\frac{K/k}{(p)}\right]$ by R. Let $\mathfrak{P} | pO_K$ A and set $\left[\frac{K/\mathfrak{P}}{\mathfrak{p}}\right] = U$. We wish to express R in terms of U.

$$R(A) \equiv A^{N\mathfrak{p}} = A^{p^2} \bmod pO_K \quad \text{for all } A \in O_K$$

$$U(A) \equiv A^{N\mathfrak{p}} = A^p \bmod \mathfrak{P} \quad \text{for all } A \in O_K.$$

In place of the first congruence we may write instead

$$R(A) \equiv A^{p^2} \bmod \mathfrak{P}$$

But $U^2(A) \equiv A^{p^2} \bmod \mathfrak{P}$. Since $\mathfrak{P}$ is unramified over $\mathbb{Q}$ we get that $R = U^2$. Our next task is to show that $U \notin \mathrm{Gal}(K/k)$. This is accomplished by proving the existence of an element of $D(\mathfrak{P} \mid p)$ which does not belong to $\mathrm{Gal}(K/k)$. For this let

$$p\,O_K = \mathfrak{P}_1 \cdots \mathfrak{P}_g \text{ where } \mathfrak{P}_1 = \mathfrak{P}$$

and let $T\mathfrak{P}_1 = \mathfrak{P}_j$. $\mathrm{Gal}(K/k)$ acts transitively on the set $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$ because p is inert. It follows that for some $S \in \mathrm{Gal}(K/k)$ $S\mathfrak{P}_j = \mathfrak{P}_1$. But then $ST_1\mathfrak{P}_1 = S\mathfrak{P}_j = \mathfrak{P}_1$ and $ST_1 \notin \mathrm{Gal}(K/k)$. It follows now that $U = \left[\frac{K/\mathbb{Q}}{\mathfrak{P}}\right]$ the generator of $D(\mathfrak{P}\mid p)$ does not belong to $\mathrm{Gal}(K/k)$. Consequently $U=ST$ where $S \in \mathrm{Gal}(K/k)$. But then $U^2 = STST = S(TST) = SS^{-1} = 1$.

Recall that $\left[\frac{K/k}{(p)}\right] = R = U^2$ so $\left[\frac{K/k}{(p)}\right] = 1$.

It has now been shown that the kernel of the Artin map contains H. Let f be a rational integer which is divisible by $\mathfrak{f}(K/k)$, the conductor of K/k. Then the reciprocity law holds for (K,k,f) so the group $P_f^1 =$

$\{(\alpha) \mid (\alpha, f) = 1 \text{ and } \alpha \equiv 1 \bmod^{\times} f\}$ is in the kernel of

the Artin map defined on ideals $\mathcal{A}$ with $(\mathcal{A}, f) = 1$.

But now it is easy to show that the group

$H(f) = \{ (\alpha) \mid (\alpha, f) = 1$ and $\alpha \equiv z \bmod^{\times} f$, with z a rational integer$\}$

is also in the kernel of the Artin map. Let $(\alpha) \in H(f)$.

Then $(\frac{\alpha}{z}) \in P^1_f$ so

$$\left[\frac{K/k}{(\alpha)}\right] = 1.$$

But this implies $\left[\frac{K/k}{(\alpha)}\right] = \left[\frac{K/k}{(z)}\right] = 1$

Thus K is a ring class field as required.

Lemma: $Gal(\mathbb{Q}(\sqrt{-2m}, \sqrt{\varepsilon_{2m}})/\mathbb{Q} \approx D_8$ and

$Gal(\mathbb{Q}(\sqrt{-2m}, \sqrt{\varepsilon_{2m}})/\mathbb{Q}(\sqrt{-2m})) \approx C(4)$ if $N\varepsilon_{2m} = -1$.

Proof: Let $K = \mathbb{Q}(\sqrt{-2m}, \sqrt{\varepsilon_{2m}})$ and $k(\sqrt{-2m})$. First note that $K/\mathbb{Q}$ is a normal extension for $\sqrt{\bar{\varepsilon}_{2m}} = \frac{i}{\sqrt{\varepsilon_{2m}}}$ and $i \in K$. Suppose $\tau \in Gal(K/k)$ such that $\tau(\sqrt{\varepsilon_{2m}}) = \sqrt{\bar{\varepsilon}_{2m}}$. Then $\tau(\sqrt{2m}) = -\sqrt{2m}$ so $\tau(i) = -i$ because $\tau \in Gal(K/k)$ and hence leaves $\sqrt{-m}$ fixed. To determine τ^2 compute as follows:

$-i = \tau(i) = \tau(\sqrt{\varepsilon_{2m}}\sqrt{\bar{\varepsilon}_{2m}}) = \sqrt{\bar{\varepsilon}_{2m}}\,\tau(\sqrt{\bar{\varepsilon}_{2m}}) = \sqrt{\bar{\varepsilon}_{2m}}\,\tau^2(\sqrt{\varepsilon_{2m}})$

Therefore $\tau^2(\sqrt{\varepsilon_{2m}}) = -\sqrt{\varepsilon_{2m}}$ so $\mathrm{Gal}(K/k) \approx C(4)$

Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\sigma(\sqrt{-2m}) = -\sqrt{-2m}$$

$$\sigma(\sqrt{\varepsilon_{2m}}) = \sqrt{\varepsilon_{2m}}$$

Since σ leaves $\sqrt{2m}$ fixed but sends $\sqrt{-2m}$ to $-\sqrt{-2m}$ it follows that $\sigma(i) = -i$. But $i = \sqrt{\varepsilon_{2m}}\sqrt{\bar{\varepsilon}_{2m}}$ so on applying σ we get $-i = \sigma(i) = \sigma(\sqrt{\varepsilon_{2m}}\sqrt{\bar{\varepsilon}_{2m}}) = \sqrt{\varepsilon_{2m}}\,\sigma(\sqrt{\bar{\varepsilon}_{2m}})$

Therefore, $\sigma(\sqrt{\bar{\varepsilon}_{2m}}) = -\sqrt{\bar{\varepsilon}_{2m}}$.

The proof is completed by showing that

$$\sigma\tau\sigma = \tau^{-1}$$

But $\sigma\tau\sigma(\sqrt{\varepsilon_{2m}}) = \sigma\tau(\sqrt{\varepsilon_{2m}}) = \sigma(\sqrt{\bar{\varepsilon}_{2m}}) = -\sqrt{\bar{\varepsilon}_{2m}} = \tau^{-1}(\sqrt{\varepsilon_{2m}})$

$\sigma\tau\sigma(\sqrt{-2m}) = \sqrt{-2m} = \tau^{-1}(\sqrt{-2m})$

So we are done.

All the conditions of Theorem 35 are met so we have the following

<u>Lemma:</u> $\mathbb{Q}(\sqrt{-2m}, \sqrt{\varepsilon_{2m}}) / \mathbb{Q}(\sqrt{-2m})$ is a ring class field

<u>Lemma:</u> $\mathbb{Q}(\sqrt{-2m}, \sqrt{\varepsilon_{2m}}) / \mathbb{Q}(\sqrt{-2m})$ is unramified except at 2_1, the prime ideal lying above (2).

Proof: $\mathcal{E}_{2m}$ is a unit so there are no prime ideals which divide $\mathcal{E}_{2m}$. Consequently if $\mathfrak{p}$ is odd prime then $\mathfrak{p}$ is unramified. The question of whether 2_1 ramifies is a more delicate matter. We note that if $2_1 \nmid \mathcal{D}_{K/k}$ then K/k is unramified and abelian. This forces K to be a subfield of HCF(k) because HCF(k) is the maximal abelian unramified extension. Certainly a precondition for $\sqrt{\mathcal{E}_{2m}} \in$ HCF(k) is that $\sqrt{2m}$ belong to HCF(k). If $\sqrt{\mathcal{E}_{2m}} \in$ HCF(k) then $\mathbb{Q}(\sqrt{-1}) \subset$ HCF(k). From this last inclusion we would derive the fact that every prime which splits completely from k to HCF(k), i.e. every prime of the form

$$p = X^2 + 2mY^2$$

is congruent to 1 mod 4. However, this requires that for every such p $2 \mid Y$ since $p \equiv 1 + 2Y^2 \bmod 4$ and for Y odd, p would instead satisfy $p \equiv 3 \bmod 4$. As before this leads to a contradiction since $\mathrm{RCF}\{-32m\} \neq \mathrm{HCF}(k)$. Thus 2_1 ramifies in K. It is useful to record the following result.

Lemma: $\mathbb{Q}(\sqrt{-2m}, \sqrt{\varepsilon_{2m}}) \subset \mathrm{RCF}\{-2^{2t}, 8m\}$ for some t.

Proof: $\mathbb{Q}(\sqrt{-2m}, \sqrt{\varepsilon_{2m}})$ is a ring class field and the only prime which ramifies from $\mathbb{Q}(\sqrt{-2m})$ to $\mathbb{Q}(\sqrt{-2m}, \sqrt{\varepsilon_{2m}})$ is 2_1 the prime above (2). But every prime which divides the conductor $f(K/k)$ ramifies. It follows that $f = 2^t$ for some t.

Lemma: $\mathrm{Gal}\left[\mathrm{RCF}\{-2^{2t}, 8m\} / \mathrm{HCF}(k)\right] \approx C(2^t)$

Proof: Under the Artin map HCF(k) corresponds to the group

$P(f) = \{(\alpha) \mid (\alpha, f) = 1\}$ and

$H = \{(\alpha) \mid (\alpha, f) = 1 \text{ and } \alpha \equiv z \bmod 2^t \; z \in \mathbb{Z}\}$

corresponds to $\mathrm{RCF}\{-2^{2t}, 8m\}$. Thus

$\mathrm{Gal}(\mathrm{HCF}(k)/k) \approx I(f)/P(f)$ and

$\mathrm{Gal}\left[\mathrm{RCF}\{-2^{2t}, 8m\}/k\right] \approx I(f)/H$. By Galois theory

$\dfrac{\mathrm{Gal}(\mathrm{RCF}\{-2^{2t}, 8m/k;\})}{\mathrm{Gal}\ (\mathrm{RCF}\{-2^{2t}, 8m\}/\mathrm{HCF}(k)} \approx \mathrm{Gal}\ (\mathrm{HCF}(k)/k)$. Furthermore

$\mathrm{Gal}(\mathrm{HCF}(k)/k) \approx I(f)/P(f) \approx \dfrac{I(f)/H}{P(f)/H}$. It follows that

$$\left|\mathrm{Gal}(\mathrm{RCF}\{-2^{2t}, 8m\}/\mathrm{HCF}(k))\right| = \left|P(f)/H\right|.$$

For the remainder of the proof let $L = \mathrm{RCF}\{-2^{2t}, 8m\}$ and $K = \mathrm{HCF}(k)$.

Claim: The Artin map $\left[\dfrac{L/k}{}\right]$ maps P(f) to Gal(L/K)

Indeed, let $\mathfrak{p}$ be a prime ideal of k such that $(\mathfrak{p}, f) = 1$ and suppose $\mathfrak{p} \in P(f)$. Then $\left[\frac{K/k}{\mathfrak{p}}\right] = 1$, that is $A \equiv A^N \bmod \mathfrak{p}\, O_K$ for all $A \in O_K$. Further let $S = \left[\frac{L/k}{\mathfrak{P}}\right]$ so $SA \equiv A^N \bmod O_L$ for all $A \in O_L$. It follows that $SA \equiv A^{N\mathfrak{p}} \bmod \mathfrak{P}\, O_K$ for all $A \in O_K$ (Note $SA - A^{N\mathfrak{p}} \in \mathfrak{P} O_L \cap O_K = \mathfrak{p} O_K$). This means that $SA \equiv A^{N\mathfrak{p}} \bmod \mathfrak{p} O_K$ for all $A \in O_K$ where S restricted to K is trivial for $\mathfrak{p}$ is unramified. Therefore $S \in \mathrm{Gal}(L/K)$. Given an arbitrary ideal $\mathfrak{a}$ of O_K such that $\mathfrak{a} \in P(f)$ there there exists

$$\mathfrak{p} \in P(f) \text{ such that } \left[\frac{L/K}{\mathfrak{a}}\right] = \left[\frac{L/K}{\mathfrak{p}}\right] \in \mathrm{Gal}(L/K)$$

It follows that $P(f)/H$ is isomorphic to a subgroup of $\mathrm{Gal}(L/K)$. But $|P(f)/H| = |\mathrm{Gal}(L/K)|$ so the map is onto and $P(f)H \approx \mathrm{Gal}(L/K)$. As a result it suffices to show that $P(f)/H \approx C(2^t)$ where $f = 2^t$. Since $\left[RCF\left[-2^{2t}, 8m\right] : HCF(k)\right] = 2^t$. it suffices to find an ideal (α) such that $(\alpha) \in P(f)_1$ $(\alpha)^{2^t} \in H$ and $(\alpha)^{2^r} \notin H$ for $r < t$. Let $(\alpha) = (1 + \sqrt{-2m})$. Since $(1+\sqrt{-2m})^{2r} = x + 2^r Y\sqrt{-2m}$ where X and Y are odd it follows that $(1+\sqrt{-2m})^{2^t} \in H$ but $(1+\sqrt{-2m})^{2^r} \notin H$ for $r < t$.

Theorem 36: $\sqrt{\varepsilon_{2m}} \in RCF\{-128m\}$

Proof: $\sqrt{\varepsilon_{2m}} \in RCF\{-2^{2t} \cdot 8m\}$ for some t. Furthermore $Gal(HCF(k)[\sqrt{\varepsilon_{2m}}] / HCF(k)) \approx C(4)$. It follows that $\sqrt{\varepsilon_{2m}} \in RCF\{-128m\}$ for otherwise for some t the group $Gal(RCF\{-2^{2t} \cdot 8m\} / HCF(k))$ would contain two subgroups of the same order which is impossible because of the preceding lemma. In order to complete the proof of the Main Theorem we must show that $\varepsilon_2 \varepsilon_m \varepsilon_{2m}$ is a square in the field $RCF\{-64m\} \times RCF\{-128m\}$.

It is necessary to first give a brief discussion of the Anti-Pellian equation:

$$X^2 - dY^2 = -4, \text{ for d a positive square free integer.}$$

A necessary condition for the existence of a solution (X,Y) is that $d \not\equiv 3 \bmod 4$. When d is a prime $P \equiv 1 \bmod 4$ the equation always has a solution. The condition that $d \equiv 1$ however, does not guarantee a solution. For example, if $D = 221$ the equation is unsolvable. Likewise for $d = 2p$ where p is a prime congruent to 1 mod 4 the Anti-Pellian equation may or may not have a solution, e.g. $X^2 - 34Y^2 = -4$ has no solution. It is easy to see that

this equation has a solution if and only if ε_d the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm - 1.

Before continuing with the proof that $\varepsilon_2 \varepsilon_m \varepsilon_{2m}$ is a square in the composition field $RCF\{-64m\} \times RCF\{-128m\}$ it is necessary to state some more basic results from algebraic number theory.

Theorem 37: Let ε_d be the fundamental unit of $K = \mathbb{Q}(\sqrt{d})$ and suppose $N\varepsilon = -1$. Then if $\mathcal{P}_1, \ldots, \mathcal{P}_t$ are some of the prime ideals dividing d the ideal $\mathcal{P}_1 \ldots \mathcal{P}_t$ is not principal unless $\mathcal{P}_1 \ldots \mathcal{P}_t = (\sqrt{d})$.

Proof: Suppose $\mathcal{P}_1 \ldots \mathcal{P}_t$ is a principal ideal, that is suppose

$$\mathcal{P}_1 \ldots \mathcal{P}_t = (a+b\sqrt{d})$$

Then $\mathcal{P}_1^2 \ldots \mathcal{P}_t^2 = (a+b\sqrt{d})^2 = (p_1 \ldots p_t)\, O_K$. It follows that $(a+b\sqrt{d})^2 = \varepsilon p_1 \ldots p_t$ for some unit ε in $\mathbb{Q}(\sqrt{d})$. If $p_1 \ldots p_t \neq d$ then ε cannot be a square. Indeed if $\varepsilon = (\quad 1)^2$ we get

$$\frac{(a+b\sqrt{d})^2}{1} = p_1 \ldots p_t = \sqrt{p_1 \ldots p_t} \in \mathbb{Q}(\sqrt{d}),$$ which is false. It follows that $N\varepsilon = -1$ since $\varepsilon = \pm \varepsilon_d^s$ where s is

an odd integer. Upon taking the norms of both sides we get

$$N\left[(a+b\sqrt{d})^2\right] = (N\,\varepsilon)\; N(p_1 \ldots p_t)$$

or $(N\,[a+b\sqrt{d}])^2 = N\varepsilon\; p_1^2 \ldots p_t^2$ which means $N\varepsilon = +1$. This contradiction forces us to conclude that $\mathfrak{P}_1 \ldots \mathfrak{P}_t$ is not principal unless $\mathfrak{P}_1 \ldots \mathfrak{P}_t = (\ d)$.

Theorem 38: Let K be a number field, and let L and M be two extensions of K. Fix a prime $\mathfrak{p}$ of K. If $\mathfrak{p}$ is unramified in both L and M, then $\mathfrak{p}$ is unramified in the composite field LM.

Proof: For a proof see Marcus 19 pg. 107.

Theorem (Hilbert's Theorem 90): Let L be a normal extension of K with Gal(L/K) a cyclic group generated by S. Then an element a in L has norm 1 if and only if it has the form $a = \frac{b}{(Sb)}$ for some $b \neq 0$ in L.

In Scholz 20 the author gives a proof of the next proposition which avoids any use of the Dedekind Zeta function ζ_K.

Theorem 39 : Let p_1 and p_2 be primes, either both congruent to 1 mod 4 or $p_1 = 2$. If $\varepsilon = \varepsilon_{p_1p_2}$ the fundamental unit of $k = \mathbb{Q}(\sqrt{p_1p_2})$ has norm -1 then

$\mathfrak{p}_1\mathfrak{p}_2$ is $G(\overline{\mathfrak{p}_1}, \overline{\mathfrak{p}_2})$ where $\mathfrak{f}_1 = f\mathfrak{p}_1$ and $\mathfrak{f}_2 = f\mathfrak{p}_2$.

Proof: We will use the following notation throughout the proof: $K = G(\overline{\mathfrak{p}_1}, \overline{\mathfrak{p}_2})$, $k_1 = G(\overline{\mathfrak{p}_1})$ $k_2 = G(\overline{\mathfrak{p}_2})$ and $k = G(\overline{\mathfrak{p}_1\mathfrak{p}_2})$. In addition, let $\mathrm{Gal}(K/k_1) = \langle S \rangle$. In order to use the last theorem we observe that $\mathrm{Gal}(K/k_1)$ is cyclic and that $N_{K/k_1}\mathfrak{f}_2 = 1$. It is also rewarding to notice that $\frac{\mathfrak{p}_2}{S\mathfrak{p}_2} = -1$. It follows, by Hilbert's Theorem 90, that $\mathfrak{f}_2 = \frac{\alpha}{S\alpha}$. Without loss of generality, we may assume that $\alpha \in O_K$. It follows that (α) is an ideal which is left fixed by S. As it will be shown below the proof can be completed if $\mathfrak{f}_2 = \frac{\varepsilon\alpha}{S\alpha}$ for some unit ε of K.

Lemma: If $\mathfrak{a}$ is an ideal of k, and $\mathfrak{a}O_K = (\alpha)$ then $\mathfrak{a}$ is a principal ideal in k_1.

Proof: Let $\mathfrak{a} \subset O_{k_1}$ and suppose $\mathfrak{a}O_K = (\alpha)$. Taking the norm of both sides we get $\mathfrak{a}^2 = (N\alpha)$. Consequently $\mathfrak{a}^2$ is a principal ideal. But $2 \nmid h(\mathfrak{p}_1)$ since $\mathfrak{p}_1$ is prime and congruent to 1 mod 4. It follows

that $\mathfrak{a}$ is principal.

Let (α) be an ideal of O_K which is invariant under S. Further let $(\alpha) = \mathfrak{p}_1^{n_1} \ldots \mathfrak{p}_t^{n_t}$

Since $S(\alpha) = (\alpha)$ we have that $(\alpha) = \mathfrak{P}_1^{n_1} \ldots \mathfrak{P}_s^{n_s} \ldots \mathfrak{p}_{s+1}^{n_{s+1}} \ldots \mathfrak{p}_t^{n_t}$ where $\mathfrak{P}_1 = \mathfrak{p}_1 \cap O_{k_1}, \ldots, \mathfrak{P}_s = \mathfrak{p}_s \cap O_{k_1}$ are primes of O_{k_1} which either split or are inert and $\mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_t$ are the ramified primes. Since $(2) \subset \mathbb{Z}$ is unramified in $k_1 = \mathbb{Q}(\sqrt{p_1})$ and $k_2 = \mathbb{Q}(\sqrt{p_2})$ it follows that (2) is unramified in the compositum K. Therefore, the prime ideals $\mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_t$ are divisors of p_2. Since (α) is a principal ideal the relative norm of (α) with respect to k is again principle. $N\varepsilon = -1$ it follows that $\mathfrak{p}_{s+1}^{n_{s+1}} \ldots \mathfrak{p}_t^{n_t} = (\sqrt{p_2})^i$ as in the proof of the lemma. Thus

$$\left(\frac{\alpha}{(\sqrt{p_2})^i}\right) = \mathfrak{P}_1^{n_1} \ldots \mathfrak{P}_n^{n_s} O_K \text{ is a principal ideal.}$$

Since $\left(\frac{\alpha}{(\sqrt{p_2})^i}\right)$ is a principal ideal it follows that $\mathfrak{P}_1^{n_1} \ldots \mathfrak{P}_s^{n_s}$ is a principal ideal. Letting $(\alpha_1) = \mathfrak{P}_1^{n_1} \ldots \mathfrak{P}_s^{n_s}$ we see that $(\alpha) = (\alpha_1)(\sqrt{p_2})^i$ where $\alpha_1 \in k_1$

Now

$$\varepsilon\varepsilon_2 = \frac{\alpha}{S\alpha_1} = \frac{\alpha_1 (\sqrt{p_2})^i \text{ (unit)}}{S\alpha_1 \, S(\sqrt{p_2})^i \, S(\text{unit})} = \frac{\alpha_1}{\alpha_1} (-1)^i \frac{\text{unit}}{S(\text{unit})} = \pm \frac{\eta}{S\eta}$$

The unit η ($S\eta$) is invariant under S which means that $\eta(S\eta) \in k_1$. Therefore $\eta(S\eta) = \pm \varepsilon_1^t$

$$\frac{\eta}{S\eta} = \frac{\eta(S\eta)}{(S\eta)^2} = \frac{\pm \varepsilon_1^t}{(S\eta)^2}$$

If t were even then $\pm \varepsilon\varepsilon_2$ would be a square. However

$$N_{K/k_1}(\varepsilon\varepsilon_2) = (\varepsilon\varepsilon_2) \, S(\varepsilon\varepsilon_2) = (-1)\varepsilon_2^2$$

This implies that -1 is square in $K = Q(\sqrt{p_1}, \sqrt{p_2})$. But K is real so t must be odd.

If $\frac{\varepsilon_1^t}{(S\eta)^2} = \varepsilon\varepsilon_2$ then $\frac{\varepsilon_1^{t+1}}{(S\eta)^2} = \varepsilon\varepsilon_1\varepsilon_2 \Rightarrow \frac{\varepsilon_1^{\frac{t+1}{2}}}{(S\eta)} = \sqrt{\varepsilon\varepsilon_1\varepsilon_2}$.

Remark: When $p \equiv 5 \bmod 8$ the norm of the fundamental unit is -1. To complete the proof of the main theorem the case $N\varepsilon_{2p} = 1$ must be investigated. For this part the reader is assumed to be familiar with biquadratic reciprocity.

Definition: Let q be a prime with $q \equiv 1 \bmod 8$. Then $X^2 \equiv 2 \bmod q$ has a solution. We define the symbol $(\frac{\varepsilon_2}{q})$ as follows:

Let $J^2 \equiv$ mod q. Then

$$(\frac{\varepsilon 2}{q}) = (\frac{1+J}{q}),$$ the ordinary Legendre symbol.

It should be noted that $(\frac{\varepsilon 2}{q})$ is well defined i.e. does not depend on the choice of J. The following theorem will be used a few times in the subsequent developments. This result is Theorem 118 of Hecke [12]

Theorem 40: Let k be a number field which contains the ℓth roots of unity where ℓ is a prime. Let μ be an element of k. Let $K = k(\sqrt[\ell]{\mu})$. Assume that M is not the ℓ th power of a number in k so that $[K:k] = \ell$. Let $\wp$ be an ideal which does not divide ℓ or μ. Then $\wp$ decomposes into a product of ℓ distinct prime ideals in K provided the congruence

$$\mu \equiv x^{\ell} \pmod{\wp}$$

can be solved for x an integer in k. On the other hand $\wp$ remains a prime ideal in K if this congruence cannot be solved.

Theorem 41 : $(\frac{\varepsilon 2}{q}) = 1$ if and only if $q = A^2+32B^2$.

Proof: Suppose $q = A^2+32B^2$. Then q splits from $\mathbb{Q}$ to RCF $\sqrt{-128}$. Recall that

RCF - 128 = $\mathbb{Q}(\sqrt{-2}, \sqrt{1+\sqrt{2}})$ and $\varepsilon_2 = 1+\sqrt{2}$.

Let $q = Q_1 Q_2$ be the decomposition of q in $\mathbb{Q}(\sqrt{2})$. Since both Q_1 and Q_2 split from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{1+\sqrt{2}})$, we can solve the congruences $x_1^2 \equiv \varepsilon_2 \bmod Q_1$

and $x_2 \equiv \varepsilon_2 \bmod Q_2$

using the Chinese Remainder Theorem we find that $x^2 \equiv \varepsilon_2 \bmod q$ is solvable (here $x = a+b\sqrt{2}$). It follows that $(\frac{\varepsilon_2}{q}) = 1$. Next let $(\frac{\varepsilon_2}{q}) = 1$. We wish to show that $q = A^2 + 32B^2$. Let

$J^2 \equiv \bmod q$. We are assuming that

$x^2 \equiv 1 + J \bmod q$ has a solution.

It follows that $Y^2 \equiv 1 - J \bmod q$ is also solvable.

Let $Q = (a+b\sqrt{2})(a-b\sqrt{2})$. Since $q \mid J^2 - 2$ we get that either $a+b\sqrt{2} \mid J+\sqrt{2}$ or $a+b\sqrt{2} \mid J-\sqrt{2}$ (This is true because $\mathbb{Z}(\sqrt{2})$ is a unique factorization domain). Without loss of generality we may assume $a+b\sqrt{2} \mid J-\sqrt{2}$.

Let $X = r+s\,J$ so $(r+s\,J)^2 \equiv 1 + J \bmod q$

$(r+s\,J)^2 \equiv 1 + J \bmod (a+b\sqrt{2})$

$(r+s\sqrt{2})^2 \equiv 1 + J \bmod (a+b\sqrt{2})$

Let $Y = u+v\,J$ so $(u+v\,J)^2 \equiv 1 - J \bmod q$

$(u+v\,J)^2 \equiv 1 - J \bmod (a-b\sqrt{2})$

$(u-v\sqrt{2})^2 \equiv 1+ 2 \bmod (a-b\sqrt{2})$

Therefore $(a+b\sqrt{2})$ splits from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(1+\sqrt{2})$. Similarly $(a-b\sqrt{2})$ splits from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{1+\sqrt{2}})$. Consequently q splits from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{1+\sqrt{2}})$. Also q splits from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{-2})$. Therefore q splits from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{2}, \sqrt{1+\sqrt{2}}) = \mathrm{RCF}(-128)$. But this implies $q = A^2+32B^2$.

<u>Theorem 42:</u> Let Q be a prime, $q \equiv 1 \bmod 8$. Then

$$\left(\frac{2}{q}\right)_4 (-1)^{\frac{q-1}{8}} = \left(\frac{Q}{q}\right)$$

Proof: We will need the following facts

(1) $\left(\frac{2}{q}\right)_4 = 1$ if and only if $q = X^2 + 64Y^2$. For a proof of this the reader can use Example 1 of Section 1.4. It has been shown moreover, that $q = X^2 + 64Y^2$ if and only if q splits completely from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt[4]{2}, i)$

(2) $q \equiv 1 \bmod 16$ if and only if q splits completely in the field containing the 16th roots of unity.

$\mathbb{Q}(\zeta_{16}) = \mathbb{Q}(\sqrt{-1}, \sqrt{2-\sqrt{2}})$

Using the identity

$$\sqrt{2-\sqrt{2}}\,\sqrt{1+\sqrt{2}} = \sqrt[4]{2}$$

one observes that the compositum of any two of the following three fields contain the third:

$$\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{-2}),\ \mathbb{Q}(\sqrt[4]{2}, \sqrt{-1}) \text{ and } \mathbb{Q}(\sqrt{2-\sqrt{2}}, \sqrt{-1})$$

On the basis of this observation it is readily seen that if $(\frac{2}{q})_4 = (\frac{-1}{q})_8 = 1$ then $(\frac{\varepsilon 2}{q}) = 1$ also. Note $(\frac{-1}{q})_8 = 1$ if and only if $q \equiv 1 \bmod 16$. By symmetry it follows that whenever any two of the symbols $(\frac{2}{q})_4$, $(\frac{-1}{q})_8$, or $(\frac{\varepsilon 2}{q})$ are positive the third is positive as well. Perhaps it should be pointed out that we are using the fact if q splits completely in $L_1/\mathbb{Q}$ and $L_2/\mathbb{Q}$ then q splits completely in $L_1 L_2/\mathbb{Q}$ and in $F/\mathbb{Q}$ where F is any subfield of $L_1 L_2$.

Now suppose $(\frac{2}{q})_4 = (\frac{-1}{q})_8 = -1$. Since $q \equiv 1 \bmod 8$, q splits completely in $\mathbb{Q}(\sqrt{J}_8)/\mathbb{Q}$. But $[\mathbb{Q}(\sqrt{\ }_8) : \mathbb{Q}] = 4$ so we have

$$(q) = \mathfrak{Q}_1, \mathfrak{Q}_2, \mathfrak{Q}_3, \mathfrak{Q}_4$$

Since q does not split completely in $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ at least one of the ideals $\mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3$ or $\mathfrak{Q}_4$ remains inert in

$K(\sqrt[4]{2}, i)/K(\sqrt{8})$. But $K(\sqrt[4]{2}, i)/Q(\sqrt{8})$ is a normal extension so Q_1, Q_2, Q_3 and Q_4 must remain inert. This says that the congruences

$$x^2 \equiv \sqrt{2} \bmod Q_i \text{ for } i = 1 \text{ to } 4$$

has no solution with x an integer in $k = K(\sqrt{8})$. Likewise since q does not split completely from $K(\sqrt{16})/Q$ it follows by the same reasoning provided above that the congruences

$$x^2 \equiv 2 - \sqrt{2} \bmod Q_i \text{ for } i = 1 \text{ to } 4$$

also have no solutions in O_k. Since $(O_k/Q_i)^*$ $i=1,\ldots,4$ is a cyclic group it follows that for each $i = 1,\ldots,4$ the congruence

$$x^2 \equiv 1 + \sqrt{2} \bmod Q_i \text{ is solvable.}$$

This implies that each Q_i splits completely from $K(\sqrt{8})$ to RCF (-128). Therefore q splits in RCF $(-128)/Q$ so $(\frac{\pm 2}{q}) = 1$. Next suppose $(\frac{2}{q})_4 = 1$ but $(\frac{-1}{q})_8 = -1$. Then the congruence

$$x^2 \equiv 1 + \sqrt{2} \bmod Q_i \text{ is unsolvable}$$

so q does not split in RCF $(-128)/Q$. Therefore $(\frac{\pm 2}{q}) = -1$.

There are a few more cases to consider but as each is similar to one of those already discussed we may regard the proof as complete.

Definition : Let p and q be primes congruent to 1 mod 4. Further let $(\frac{p}{q}) = 1$. Then if $J^2 \equiv p \bmod q$ we define $(\frac{\varepsilon p}{q})$ to be equal to the Legendre symbol $(\frac{a+bJ}{q})$ if $\varepsilon p = a+b\sqrt{p}$. Since $N\varepsilon_p = -1$ and $(\frac{-1}{q})=1$ there is no ambiguity. The next two theorems are from Lehmer [17]. The proofs given are hers; we present them only as a convenience to the reader.

Theorem 43: $(\frac{\varepsilon p}{q}) = (\frac{p}{q})_4 \quad (\frac{q}{p})_4$

Proof: We use the following class number formula which can be found in Hasse [13]:

$$\varepsilon_q^h = (\frac{2}{q}) \frac{\prod (\zeta^n - \zeta^{-n})}{(\zeta^r - \zeta^{-r})} = (\frac{2}{q}) \frac{N}{R}$$

where r runs over the quadratic residues and n over the non-residues of q less than $(\frac{q}{2})$ where ζ is a primitive q-th root of unity and h is the class number of the field $\mathbb{Q}(\sqrt{q})$. Since $\sqrt{q} = \prod_{v=1}^{\frac{q-1}{2}} (\zeta^v - \zeta^{-v}) = NR$ it follows that

$$\sqrt{q}^{\,h} \varepsilon_q^h = (\frac{2}{q}) \quad N^2$$

We next introduce the cyclotomic periods of order 4:

$\eta_i = \sum \zeta^{g^{4m+i}}$ $(i = 0,1,2,3)$ where g is a primitive root of q. N can be rewritten as

$$N = \prod_{\substack{k \\ 1<g^{2k+1}_{red}<p-1}} (\zeta^{g^{2k+1}} - \zeta^{-g^{2k+1}})$$

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ which sends $\zeta \to \zeta^g$.

Then $\sigma(N) = \prod (\zeta^{g^{2m+1}} - \zeta^{-g^{2m+1}})$

$$= (-1)^{\mu} \prod_r (\zeta^r - \zeta^{-r})$$

where r ranges over the residues mod q which lie between 1 and $\frac{q-1}{2}$.

$$\sigma^2(N) = (-1)^{\mu} (-1)^{\gamma} \prod (\zeta^n - \zeta^{-n})$$

By Gauss' Lemma $\mu + \gamma$ is odd since g is a primitive root. Therefore $\sigma^2(N) = -N$. It is easy to see that N can be expressed as

$$N = \sum a_i \zeta^i \quad \text{where } a_i \in \mathbb{Z}$$

We can also write $N = \sum a_i \zeta^{g^i}$. Since $\sigma^4 = 1$ we have $N = \sigma^4(N) = \sum a_i \zeta^{g^{i+4}}$. Since $\{1, \zeta, \ldots, \zeta^{q-1}\}$ is a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$ it must be the case that $a_i = a_{i+4}$.

By taking i = 0 it is seen that $a_0 = a_4 = a_8 = \ldots$

Therefore one can write

$$N = C_0 \zeta_0 + C_1 \zeta_1 + C_2 \zeta_2 + C_3 \zeta_3.$$

Further since $\sigma^2(N) = -N$ we see that $C_0 = -C_2$ and $C_1 = -C_3$. Thus $N = \pi(\varepsilon^n - \varepsilon^{-n}) = C_0(\zeta_0 - \zeta_2) + C_1(\zeta_1 - \zeta_3)$ where C_0 and C_1 are integers. We now introduce the prime p and recall that

$$\zeta_i^p \equiv \zeta_{i+r} \bmod p$$

More explicitly

$$\zeta_i^p = (\sum \zeta^{g^{4m+i}})^p \equiv \sum_{m=1}^{\frac{p-1}{4}} \zeta^{pg^{4m+i}} \bmod p$$

If $(\frac{p}{q})_4 = 1$ then $\zeta_i^p \equiv \zeta_i \bmod p \quad r = 0$

If $(\frac{p}{q})_4 = -1$ then $\zeta_i^p \equiv \zeta_{i+2} \bmod p \quad r = 2$

(Note $(\frac{p}{q}) = 1$ so r = 0 or 2)

$$N^p \equiv C_0(\zeta_r - \zeta_{r+2}) + C_1(\zeta_{r+1} - \zeta_{r+3}) \bmod p$$

These calculations show that

$$N^p \equiv \begin{cases} N \bmod p & \text{if } r = 0 \\ -N \bmod p & \text{if } r = 2 \end{cases}$$

Using this one can verify that

$$(\frac{N^2}{p}) \equiv (N^2)^{\frac{p-1}{2}} \equiv (\frac{p}{q})_4 \bmod p$$

Since h is odd it follows from

$$\sqrt{q}^{\,h} \equiv \left(\frac{2}{q}\right) N \pmod{q}$$

that $$\left(\frac{\sqrt{q}}{p}\right)\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{N}{p}\right)$$

or $$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{q}{p}\right)_4 \left(\frac{p}{q}\right)_4$$

Theorem 44: Let $p = c^2 + 8q\,d^2$. Then

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^d \left(\frac{\varepsilon_2}{p}\right)$$

Here q is a prime congruent to 1 mod 4.

Proof: We first remark that c must be odd and $p \equiv 1 \pmod 8$.

Then $\left(\frac{2}{c}\right) = (-1)^{\frac{c^2-1}{8}} = (-1)^{\frac{p-1}{8}} (-1)^d$ where $\left(\frac{2}{c}\right)$

is a Jacobi symbol.

By reducing $p = c^2 + 8qd^2$ modulo q we get

$$p \equiv c^2 \pmod q$$

Hence $$\left(\frac{p}{q}\right)_4 = \left(\frac{c}{q}\right)$$

Also $$\left(\frac{q}{p}\right)_4 = \left(\frac{2}{p}\right)\left(\frac{cd}{p}\right)$$

because $c^2 + 8qd^2 \equiv 0 \pmod 8$

$$\text{so } q \equiv \frac{-c^2}{8d^2} \pmod p$$

and $\left(\frac{-1}{p}\right)_4 = 1$ for $p \equiv 1 \pmod 8$

If δ is the largest odd factor of d then $(\frac{\delta}{p}) = 1$; for let r be any prime divisor of δ. Since $p = c^2+8qd^2 = c^2 +8qr^2t^2$ we have $(\frac{p}{r}) = 1$. But $p \equiv 1 \bmod 8$ so $(\frac{p}{r}) = (\frac{r}{p})$. This implies that $(\frac{\delta}{p}) = 1$.

It follows that $(\frac{d}{p}) = 1$. Let $r \mid c$, r a prime.

Since

$$p = c^2+8qd^2$$

we get $p \equiv 8qd^2 \bmod r$. Therefore

$$(\frac{r}{p}) = (\frac{p}{r}) = (\frac{8}{r}) \quad (\frac{q}{r}) = (\frac{2}{r}) \quad (\frac{r}{q})$$

This implies that $(\frac{c}{q}) = (\frac{2}{c}) \ (\frac{c}{q})$. We know from before that $(\frac{2}{q})_4 \ (-1)^{\frac{q-1}{8}} = (\frac{\varepsilon_2}{q})$. Consequently,

$$(\frac{\varepsilon_q}{p}) = (\frac{p}{q})_4 \ (\frac{q}{p})_4 = (\frac{c}{q}) \ (\frac{2}{p})_4 \ (\frac{2}{c}) \ (\frac{c}{q})$$

$$= (\frac{2}{p})_4 \ (\frac{2}{c}) = (\frac{2}{p})_4 \ (-1)^{\frac{p-1}{8}} (-1)^d = (\frac{\varepsilon_2}{p}) \ (-1)^d.$$

We now apply this to show that $\varepsilon_2 \ \varepsilon_m \ \varepsilon_{2m} = \eta^2$ with $\eta \in RCF(-64m) \times RCF(-128m)$ or equivalently that

$$RCF(-128) \subseteq RCF(-64m) \times RCF(-128m).$$

Proof: Let $p = X^2 +16mY^2 = U^2 +32mV^2$; i.e. Suppose p splits completely from $\mathbb{Q}$ to $RCF(-64m) \times RCF(-128m)$.

Since ε_m belongs to RCF $\{-64m\}$, RCF $\{-128m\}$ it follows that p splits completely from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{\varepsilon_m})$. Suppose $p = P_1P_2$ where P_1 and P_2 are the prime ideals of $\mathbb{Q}(\sqrt{m})$ which lie over p. Then we can solve the congruences

$$X_1^2 \equiv \varepsilon_m \mod P_1$$

and $X_2^2 \equiv \varepsilon_m \mod P_2$, X_1, X_2 integers in $\mathbb{Q}(\sqrt{m})$.

By the Chinese Remainder Theorem we can solve the congruence

$X^2 \equiv \varepsilon_m \mod (p)$ where X is an integer in $\mathbb{Q}(\sqrt{m})$.

This means $(\frac{\varepsilon_m}{p}) = 1$. Now since $p = X^2+32mY^2$, the previous theorem shows that $(\frac{\varepsilon_m}{p}) = (-1)^2\ (\frac{\varepsilon}{p}) = (\frac{\varepsilon_2}{p})$.

Therefore $(\frac{\varepsilon_2}{p}) = 1$ so p splits completely from $\mathbb{Q}$ to RCF $\{-128\}$. Since p was an arbitrary prime contained in $S_{\text{RCF}\{-64m\}, \text{RCF}\{-128m\}}$ we get that RCF $\{-128\} \subset$ RCF $\{-64m\}$, RCF $\{-128m\}$. This completes the proof of the main theorem.

2.3 On Lehmer's Conjecture

In this part we shall show that Conjecture 4 of Lehmer [8] is true by using the same techniques developed earlier. A key step in the proof is to show that for m a prime congruent to 1 mod 4, $4\sqrt{2+m} \subseteq RCF(-256\ m)$

As a first step in this direction we prove the

Lemma : Let $m \equiv 1 \bmod 4$, m a prime and let $k = \mathbb{Q}(\sqrt{m})$.

Then $G = Gal(RCF(-2^{2t}\cdot 4m)/HCF(k)) \simeq C(2)\cdot C(2^{t-1})$

Proof: As in the proof of an earlier lemma all that is required is to produce two subgroups of G both of which are cyclic of order 2^{t-1}. Let $\alpha = 2+\sqrt{-m}$ and $\beta = 1+2\sqrt{-m}$. Then the principal ideals (α) and (β) are both relatively prime to the conductor $f = 2^t$.

Denote by H(f) the group

$\{(\tau)\ |\ (\tau, f)=1\ \tau \equiv z \bmod f,\ z \in \mathbb{Z}\}$. Then $(\alpha)^{2^{t-1}} \in H(f)$ and $(\beta)^{2^{t-1}} \in H(f)$ with no smaller powers doing the trick.

Since $G = 2^t$ we are done.

Lemma : $\mathbb{Q}(\sqrt[4]{2\varepsilon_m}, \sqrt{-m})/\mathbb{Q}(\sqrt{-m})$ is a ring class field.

Proof: Let $K = \mathbb{Q}(\sqrt[4]{2\varepsilon_m}, \sqrt{-m})$ and $k = \mathbb{Q}(\sqrt{-m})$.

Let $\tau \in \mathrm{Gal}(K/k)$ such that $\tau(\sqrt[4]{2\varepsilon_m})(\sqrt[4]{2\varepsilon_m}) = i\sqrt{2}$ and $\tau(\sqrt{m}) = -\sqrt{m}$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{m}))$ such that $\sigma(\sqrt{-m}) = \sqrt{-m}$ and $\sigma(\sqrt[4]{2\varepsilon_m}) = \sqrt[4]{2\varepsilon_m}$

Then $\langle\tau\rangle$ is a cyclic group of order 8, $\sigma^2 = 1$ and $\sigma\tau\sigma = \tau^{-1}$. This proves that $K/\mathbb{Q}(\sqrt{-m})$ is a ring class field.

Lemma : $\mathbb{Q}(\sqrt[4]{2\varepsilon_m}, \sqrt{-m}) \subset \mathrm{RCF}\cdot -2^{2t}\cdot 4m$ for some t

Proof: ε_m is a unit so $\mathbb{Q}(\sqrt[4]{2\varepsilon_m}, \sqrt{-m})/\mathbb{Q}(\sqrt{-m})$ is unramified outside of 2.

From these three lemmas it follows that

$\sqrt[4]{2\varepsilon_m} \in \mathrm{RCF}\cdot -256$

Next we state Lehmer's conjecture.

Theorem 45: If $p \equiv 1 \bmod 8$ and if $q = 5, 13$, and 37 then $(\frac{\pm q}{p})_4 = (-1)^{b+d}$ where $p = a^2+16b^2 = c^2+16qd^2$

Proof: It can be shown that for q assuming these values

and $p \equiv 1 \bmod 4$ such that $(\frac{p}{q}) = 1$, one has $(\frac{\varepsilon_q}{p}) = 1$ if and only if $p = c^2+4qd^2$. If it is further assumed that $p \equiv 1 \bmod 8$ then one can in fact write

$p = a^2+16b^2 = c^2+16qd^2$

Case I $p = a^2+64(b')^2 = c^2+64q(d')^2$

In this situation p splits completely from $\mathbb{Q}$ to the compositum field $K = RCF\{-256\} \times RCF\{-256q\}$. Since $\sqrt[4]{2} \in RCF\{-256\}$ and $\sqrt[4]{2\varepsilon_q} \in RCF\{-256q\}$ it follows that $\sqrt[4]{\varepsilon_q} \in K$. But p splits from $\mathbb{Q}$ to K so one has for any prime $\mathfrak{p}$ of $RCF\{-64\} \times RCF\{-64q\}$ with $\mathfrak{p} \mid p$, that the congruence

$$X^2 \equiv \sqrt{\varepsilon_q} \bmod \mathfrak{p}$$

is solvable.

It follows that one can also write $(\frac{\varepsilon_q}{p})_4 = 1$

Case II b odd, d even

In this case one has that

$X^2 \equiv \sqrt{2\varepsilon_q} \bmod$ is solvable

and $X^2 \equiv \sqrt{2} \bmod$ has no solutions.

It follows that $X^2 \equiv \varepsilon q$ has no solutions. Therefore $(\frac{\varepsilon q}{p})_4 = -1$ (Note: $\mathbb{Z}/p\mathbb{Z} \subset O_k/\wp_k$

$= RCF(-64) \setminus RCF(-64q)$ since p splits from $\mathbb{Q}$ to k)

Case III: b odd, d odd

Here both the congruences

$$X^2 \equiv 2\varepsilon q \bmod \wp$$

and $$X^2 \equiv 2 \bmod \wp$$

are unsolvable. It follows that

$$X^2 \equiv \varepsilon q \bmod \wp$$

has solutions. Therefore $(\frac{\varepsilon q}{p})_4 = 1$

This completes the proof. For $q \equiv 1 \bmod 4$, q otherwise arbitrary the following statement still holds:

$(\frac{\varepsilon q}{p})_4 = 1$ whenever $p = a^2+64b^2 = c^2+64qd^2$.

BIBLIOGRAPHY

1. Barrucand, P., and Cohn, H., Note on Primes of Type $x^2 + 32y^2$, J. Reine Angew. Math. 238 (1969), pp. 67-70

2. Borevich, Z.I. and Shafarevich, I.R., Number Theory, Academic Press, New York (1966)

3. Cassels, J.W.S., and Frohlich, A.,(ed.) Algebraic Number Theory, (Symposium) Thompson Book Co., Wash., D.C. (1967)

4. Cohn, H., A Second Course in Number Theory, John Wiley, New York (1962)

5. _____, Iterated Ring Class Fields and the Icosahedron, Math. Ann 255, pp. 107-122 (1981)

6. _____, A Classical Invitation to Algebraic Numbers and Class Fields, Springer-Verlag, New York,(1978)

7. Deuring, M., Die Klassenkorper der komplexen Multiplikation, Enzykl. d. math. Wiss. 1/2, 2. Aufl., Heft 10, Stuttgart, (1958)

8. Fricke, R., Lehrbuch der Algebra III (Algebraische Zahlen) Braunschweig, (1928)

9. Halter-Koch, Franz, Arithmetische Theorie der Normal Korper von 2 - Potenzgrad mit Diedergruppe, J. Number Theory 4 (1971), pp. 412-443

10. Hasse, H., Klassenkorpertheorie, Lect. Notes, Marburg,(1933)

11. _____, Vorlesungen uber Zahlentheorie, Springer Berlin, (1950)

12. Hecke, E., Algebraische Zahlen, Chelsea Publishing Co., New York, (1970)

13. Hilbert, D., Uber die Theorie des relativquadratischen Zahlkorpers, Math., Ann. 51 (1899) pp. 1-127

14. Janusz, G. J., Algebraic Number Fields, Academic Press, New York, (1973)

15. Kubota, T., Uber die Beziehung der Klasserzahl der Unterkorper des bizyklischen biquadratischen Zahlkorpers, Nagoya Math. J., (1950) pp. 1-10

16. Lehmer, E., On the Quadratic Character of Some Quadratic Surds, J. Reine Angew. Math. 250 (1971) pp. 42-48

17. _____, On Some Special Quartic Reciprocity Laws, Acta Arithmetica XXI, (1972), pp. 367-377

18. _____, On the Quartic Character of Quadratic Units, Math. 268/269 (1974), pp.294-301

19. Marcus, D. Number Fields, Springer Verlag, New York, 1977

20. Scholz, A., Uber die Losharkeit der Gleichung $t^2 - Du^2 = 4$, Math Zeitschr. 39 (1935) pp. 95-111