CYCLOTOMIC FIELDS OF CLASS NUMBERS ONE AND TWO

DENNIS ACREMAN


CENTRE FOR NFLD. STUDIES
MAY 7 1979
MEMORIAL UNIVERSITY
OF NEWFOUNDLAND

CYCLOTOMIC FIELDS OF CLASS NUMBERS ONE AND TWO

BY

DENNIS ACREMAN (B.A., HONS.)

A THESIS

SUBMITTED IN PARTIAL

FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS, STATISTICS AND COMPUTER SCIENCE

MEMORIAL UNIVERSITY OF NEWFOUNDLAND

ST. JOHN'S, NEWFOUNDLAND

OCTOBER, 1977

NOTICE

The quality of this microfiche is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us a poor photocopy.

Previously copyrighted materials (journal articles, published tests, etc.) are not filmed.

Reproduction in full or in part of this film is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30. Please read the authorization forms which accompany this thesis.

THIS DISSERTATION
HAS BEEN MICROFILMED
EXACTLY AS RECEIVED

AVIS

La qualité de cette microfiche dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de mauvaise qualité.

Les documents qui font déjà l'objet d'un droit d'auteur (articles de revue, examens publiés, etc.) ne sont pas microfilmés.

La reproduction, même partielle, de ce microfilm est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30. Veuillez prendre connaissance des formules d'autorisation qui accompagnent cette thèse.

LA THÈSE A ÉTÉ
MICROFILMÉE TELLE QUE
NOUS L'AVONS REÇUE

TABLE OF CONTENTS

		PAGE
ABSTRACT		(ii)
ACKNOWLEDGEMENTS		(iii)
NOTATION		(v)
INTRODUCTION		1
CHAPTER I:	Class Number Formulas	2
	1. Fermat's Last Theorem, Unique Factorization and Class Number	3
	2. Preliminaries	8
	3. The Analytic Class Number Formula	9
	4. Calculation of $L(1, \chi)$	15
	5. The Arithmetic Class Number Formula	18
	6. Formulas for h_p^*	20
	7. An Important Formula for h_m^*	23
	8. Norms of Stickelberger Symbols	25
CHAPTER II:	Cyclotomic Fields of Class Number One	49
	1. Analytic Lemmas	50
	2. Kummer's Conjecture	62
	3. Divisibility Properties of h_m^*	64
	4. Determination of h_m^+	73
CHAPTER III:	Cyclotomic Fields of Class Number Two	82
	1. Cyclotomic Fields of Class Number Two	83
	2. Factorization in Algebraic Number Fields of Class Number Two	89
APPENDICES		92
BIBLIOGRAPHY		105

ACKNOWLEDGEMENTS

I wish to express my gratitude to my supervisor, Dr. Don Rideout, for his help, encouragement and the ideas he gave me in writing this thesis.

I would also like to thank Sandra Crane and Elaine Boone for their hard work in typing this thesis.

Dennis Acreman.

ABSTRACT

We find all fields of type $Q(\exp 2\pi i/m)$ with class number h_m equal to one or two. We derive various class number formulas and properties associated with these formulas and use these in determining class numbers of cyclotomic fields. The integer h_m decomposes as the product $h_m^* h_m^+$ of two integers where h_m^+ is the class number of $Q(\cos 2\pi/m)$. We find when $h_m^* = 1$ and show that for such m, $h_m^+ = 1$ also. There are 29 distinct full cyclotomic extensions of Q with class number one and $m = 90$ is the largest integer for which $h_m = 1$. We also find when $h_m^* = 2$ and show that for such m, $h_m^+ = 1$. There are 2 distinct full cyclotomic extensions of Q with class number two, namely, $m = 39$ and 56.

NOTATION

$\mathbb{N}$ - Natural numbers

$\mathbb{Z}$ - Integers

$\mathbb{R}$ - Reals

$\mathbb{Q}$ - Rationals

$\mathbb{P}$ - Set of all primes

ϕ_n - n-th cyclotomic polynomial

ϕ - Euler phi function

(a, b) - Greatest common divisor of a and b

$p \| b$ - p divides b but p^2 does not divide b.

INTRODUCTION

Let $Q_m = Q(\exp 2\pi i/m)$ be the m-th cyclotomic field over the rational numbers. The class number h_m^+ of $Q_m^+ = Q(\cos 2\pi/m)$, the maximal real subfield of Q_m, divides the class number h_m of Q_m. Therefore, $h_m = h_m^* h_m^+$ where the integer h_m^* is called the relative class number or sometimes the first factor of h_m. In general, the first factor is easier to compute because formulas for the second factor require information about the group of units U_m in Q_m^+. Chapter I describes the derivation of some of these formulas.

In connection with the last of these formulas, we determine that the norms of Stickelberger symbols belong to $\frac{1}{2p}\mathbb{Z}$. We see exactly when these norms have denominator 2, p or 2p and when they are even or odd integers. In Chapter I, we also discuss the connection between Fermat's Last Theorem and the class number of algebraic number fields.

Masley, assuming a conjecture of Kummer that $h_p^* > 1$ for primes $p > 19$, proved that there are exactly 29 different Q_m, with $h_m = 1$. Montgomery and later Uchida [25] via different methods proved Kummer's conjecture. Masley and Montgomery's paper [16] is a complete solution of the class number one problem for cyclotomic fields. In Chapter II, we examine this paper in detail.

Masley, using methods similar to the class number one case, has also solved the class number two problem for cyclotomic fields. In Chapter III, we examine his solution for this case. We also discuss a result of L. Carlitz concerning factorization in fields of class number less than or equal to two.

CHAPTER I

CLASS NUMBER FORMULAS

In this Chapter, we first discuss the connection between Fermat's Last Theorem and the class number of cyclotomic fields. We next make some preliminary remarks and then derive various class number formulas, in particular, those for cyclotomic fields. In connection with the last of these formulas, we discuss some properties of the norms of "Stickelberger" symbols. These properties will be used in Chapter 2 and 3, but also are of interest in their own right.

1.1 Fermat's Last Theorem, Unique Factorization and Class Number

Fermat's Last Theorem states that the equation

$$x^n + y^n = z^n$$

has no nonzero solutions in rational integers x, y, z when $n > 2$. It is clear that if this is true for some exponent n, then it is also true for all exponents which are multiples of n. Since any integer $n > 2$ is either divisible by 4 or by some odd prime, we may limit our consideration to the case $n = 4$ or n an odd prime. For $n = 4$, an elementary proof was given by Euler. We thus consider only

$$x^\ell + y^\ell = z^\ell \qquad (1.1)$$

where the exponent ℓ is an odd prime. We may clearly assume that the numbers x, y, z in (1.1) are relatively prime.

If ζ denotes a primitive ℓ-th root of unity, we have that

$$\zeta^{\ell-1} + \zeta^{\ell-2} + \ldots + 1 = 0$$

and hence, (1.1) may be written

$$\prod_{k=0}^{\ell-1} (x + \zeta^k y) = z^\ell \qquad (1.2)$$

The factors on the left side of (1.2) belong to the ring of integers of the ℓ-th cyclotomic field $Q(\zeta) = Q_\ell$. In 1835, Kummer "proved" Fermat's Last Theorem under the assumption that these rings of integers had unique factorization. (See Borevich-Shafarevich, [4], p. 156 f.f.) However, it was pointed out to him by Dirichlet that this assumption was false. In attempting to overcome this flow in his proof, Kummer and Dedekind developed the theory of "ideals" which showed that, although the arithmetic of algebraic numbers was radically different from the arithmetic of the rational number, it could be developed in great depth, allowing strong applications to number-theoretic problems.

We now sketch the basic ideas of the theory of divisors, which developed from the theory of "ideals" of Kummer and Dedekind (full details may be found in Borevich-Shafarevich [4], p. 168 f.f.). We let D be an arbitrary commutative ring (with unit element and without divisors of zero) and K be its quotient field. Then D may not have unique factorization, but it may have a theory of divisors. By a theory of divisors for the ring D, we shall mean the giving of some semigroup $\mathcal{D}$ with unique

factorization into prime elements along with a homomorphism $\alpha \to (\alpha)$ of the semigroup D^* (nonzero elements of D) into $\mathcal{D}$, satisfying the following conditions:

(1) An element $\alpha \in D^*$ is divisible by $\beta \in D^*$ in the ring D if and only if (α) is divisible by (β) in the semigroup $\mathcal{D}$.

(2) If α and β of D are divisible by $a \in \mathcal{D}$, (i.e. $a \mid (\alpha)$, $a \mid (\beta)$), then $\alpha \pm \beta$ are also divisible by a.

(3) If a and b are two elements of $\mathcal{D}$ and the set of all elements $\alpha \in D$ which are divisible by a coincides with the set of all elements $\beta \in D$ which are divisible by b, then $a = b$.

The elements of the semigroup $\mathcal{D}$ are called integral divisors of the ring D, and divisors of the form (α), $\alpha \in D^*$, are called principal integral divisors. Condition (1) clearly implies that the equality $(\alpha) = (\beta)$ holds if and only if α and β are associate in the ring D. We have that if a ring has a theory of divisors, then it is unique up to isomorphism. That is, if $\mathcal{D}'$ is also a theory of divisors for D, then there is an isomorphism $\mathcal{D} \cong \mathcal{D}'$ under which the principal divisors in $\mathcal{D}$ and $\mathcal{D}'$ which correspond to a given element $\alpha \in D^*$ are identified.

We now extend the theory of divisors of D to K. Let $p_1, \ldots, p_m$ be any finite system of prime divisors of D. An expression $p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ with integer exponents $k_1, \ldots, k_m$ (not necessarily positive) is called a divisor of the field K. If all the exponents k_i are nonnegative, then

the divisor is called integral (or an integral divisor of the ring D). Otherwise, it is called fractional. Since every nonzero $\gamma \in K$ is the quotient of two elements of D, we can associate to γ the principal divisor (γ) in the obvious way. When applied to elements of the ring D, the new concept of a principal divisor coincides with the previous one, and we have that the principal divisor (γ) will be integral if and only if γ belongs to D. We also have that $(\gamma) = (\eta)$ if and only if $\gamma = \eta\varepsilon$ where ε is a unit of the ring D. Under the obvious multiplication, the set of all divisors of the field K is an Abelian group. For divisors a and b (not necessarily integral), we say that a is divisible by b if there is an integral divisor c such that $a = bc$.

For an algebraic number field K, we have that the theory of divisors exists and is given by the set of all ideals of the field K, where an ideal of K (relative to D) is a subset $A \subset K$, containing at least one nonzero element, and satisfying:

(1) A is a group under the operation of addition.

(2) For any $\alpha \in A$ and any $\gamma \in D$, the product $\gamma\alpha$ lies in A.

(3) There is a nonzero element λ of the field K such that $\lambda A \subset D$.

If A and B are two ideals of the field K, then by their product AB, we mean the set of all elements $\gamma \in K$ which can be represented in the form $\gamma = \alpha_1\beta_1 + \ldots + \alpha_m\beta_m$ $(m \geq 1)$ $\alpha_i \in A$, $\beta_i \in B$ $(1 \leq i \leq m)$.

Under this multiplication, the set of all ideals of K becomes a group.

The ideal A is called integral if it is contained in D and otherwise, it is called fractional. An integral ideal in K is clearly just a nonzero ideal (in the usual sense) in D. The semigroup of all nonzero ideals of D has unique factorization into prime ideals and for any $\alpha \in D$, α is mapped into this semigroup via $\alpha \to (\alpha)$, the principal ideal of D generated by α. In general, for $\gamma \in K$, the principal ideal (γ) of K is the set $\{\beta \in K | \beta = \alpha\gamma$ where $\alpha \in D\}$.

We say two ideals of K are equivalent if they differ by a factor which is a principal ideal. We have that the number of ideal classes under this equivalence relation is finite and that the ideal classes form a group under the obvious multiplication. We call the (finite) order of the ideal class group the class number of K, and we write h_K. The class number is one if and only if every ideal is principal. But every ideal is principal if and only if the ring of integers has unique factorization. Hence, we see that Kummer's first approach to Fermat's Last Theorem worked only for prime cyclotomic fields of class number one. We shall see in Chapter 2 that this is true only for primes less than or equal to 19. (This was conjectured by Kummer.)

However, Kummer used the class number of cyclotomic fields to prove Fermat's Last Theorem for a much wider class of exponents. We call an odd prime which does not divide the class number of Q_ℓ a regular prime; otherwise, we call it irregular. Kummer proved Fermat's Last Theorem for regular primes. It is believed that there are infinitely many regular

primes, but this is as yet unproven. It has been proven that there are infinitely many irregular primes. The main basis for the above belief is that in every finite interval checked so far, regular primes have outnumbered irregular primes.

1.2 Preliminaries

Let K be an abelian number field of degree n over Q. Then the Kronecker-Weber Theorem in Class Field Theory states that $K \subseteq Q_f$ for some positive integer f (see Narkiewicz, [18], p. 263). The smallest such f is called the conductor of K. This very deep theorem, together with the connection of cyclotomic fields to Fermat's Last Theorem, has lead to the central role of cyclotomic fields in Algebraic Number Theory. The Galois group B of K over Q is a factor group of G_f, the Galois group of Q_f over Q. Specifically, $B = G_f / H$ where H is the subgroup of G_f that fixes K. If we let σ_a denote the automorphism of Q_f which sends $\zeta \to \zeta^a$ for each a relatively prime to f and each f-th root of unity ζ, then the map $\sigma_a \mapsto a \bmod f$ is an isomorphism of G_f onto $(\mathbb{Z} / f\mathbb{Z})^*$. Via this isomorphism, the characters of G_f are identified with residue class characters mod f. Since B is a factor group of G_f, the characters of B extend to the characters of G_f which are trivial on H. We denote by $\bar{X}$ the group of residue class characters mod f obtained from the characters of H, and we call $\bar{X}$ the characters or character group of K. The identify of $\bar{X}$ is called the principal character and is denoted by 1.

We associate to each $\chi \in \hat{X}$ its conductor $f(\chi)$ as residue class character. Then $f(\chi)$ is the smallest positive integer so that $\chi(a) = \chi(b)$ whenever $a \equiv b \pmod{f(\chi)}$. It is known that f is the least common multiple of the $f(\chi)$ for $\chi \in \hat{X}$ (see Hasse [9], p. 434).

Let J be the automorphism induced by complex conjugation σ_{-1}. We shall call the character $\chi \in \hat{X}$ even or odd according as $\chi(J) = \chi(-1)$ is equal to $+1$ or -1. (We write $\chi(J)$ using the identifications discussed above.) The field K is real if and only if J is the identity on K. But J is the identity on K if and only if all the characters of K are even. If K is imaginary, then $n = 2n_e$ as all automorphisms are complex-valued and occurring in conjugate pairs. Furthermore, K is of degree 2 over K^+ the maximal real subfield which is just the fixed field of the group $\{J, J^2 = 1\}$. The group $\hat{X}$ of n characters then splits into two cosets: X_e, the subgroup of n_e even characters which is just the character group of K^+, and X_0, the set of n_e odd characters. We note that for the m-th cyclotomic field Q_m, $Q_m^+ = Q(\zeta_m + \zeta_m^{-1}) = Q(\cos(\frac{2\pi}{m}))$ where ζ_m is a primitive m-th root of unity.

1.3 The Analytic Class Number Formula

In this Section and the next, full details may be found in Borevich-Shafarevich [4], Chapter 5, unless other references are given.

Let $h = H_K$ be the class number of K. The Dedekind Zeta function for K, $\zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_A N(A)^{-s} \qquad (1.3)$$

where A runs through all integral divisors of the field K, $N(A)$ denotes the norm of the divisor A, and s is real, positive. We shall show that the series on the right hand side of (1.3) converges for $1 < s < \infty$ and is a continuous function of the real variable s on this interval. Further, we shall obtain the formula

$$\lim_{s \to 1+0} (s - 1)\zeta_K(s) = hu \tag{1.4}$$

where u is a constant which depends on the field K in a simple manner, and which will be computed in the course of the discussion.

We break the series (1.3) into the sum of h series

$$\zeta_K(s) = \sum_C \left(\sum_{A \in C} \frac{1}{N(A)^s} \right)$$

where A runs through all integral divisors of the given divisor class C, and the exterior summation is taken over all h classes C. To prove that (1.3) converges, it suffices to show that each of the series

$$f_C(s) = \sum_{A \in C} \frac{1}{N(A)^s} \tag{1.5}$$

converges for $s > 1$. Further, if we show that for each class C, the limit

$$\lim_{s \to 1+0} (s - 1) f_C(s)$$

exists and has the same value u for each divisor class C, then we will have obtained Formula (1.4).

We now transform the series (1.5) into a series over certain integers of the field K. In the inverse divisor class C^{-1} we choose an integral divisor A'. Then for any $A \in C$, the product AA' will be a principal divisor

$$AA' = (\alpha) \quad (\alpha \in K)$$

It is clear that the mapping

$$A \to (\alpha) \quad (A \in C)$$

establishes (for fixed A') a one-to-one correspondence between integral divisors A of the class C and principal divisors (α) divisible by A'. Using the equality

$$N(A)N(A') = N((\alpha)) = |N(\alpha)|$$

(see Borevich-Shafarevich [4], p. 217), we obtain

$$f_C(s) = N(A')^s \sum_{\substack{(\alpha) \\ \alpha \equiv 0 (\mathrm{mod}\ A')}} \frac{1}{|N(\alpha)|^s}, \qquad (1.6)$$

where the summation is taken over all principal divisors of the field K which are divisible by A'. Since two principal divisors (α_1) and (α_2) are equal if and only if the numbers α_1 and α_2 are associate, then we may consider that the summation in (1.6) is taken over a complete set of nonzero pairwise-nonassociate numbers of the field K which are divisible by A'.

To put the series (1.6) in a still more convenient form, we use the geometric representation of points of the field K by points in the n-dimensional space $\mathbb{R}^n$ (see Borevich-Shafarevich [4], p. 94 f.f.). Now, it is true that there exists a cone X in $\mathbb{R}^n$ such that in each class of associate numbers of the field K, there is one and only one number whose geometric representation lies in X (see Borevich-Shafarevich [4], p. 312). By a cone, we mean a subset of $\mathbb{R}^n$ such that whenever it contains any nonzero point x, it also contains the whole ray wx, $0 < w < \infty$. We denote by $x(\alpha)$ the image of $\alpha \in K$ in $\mathbb{R}^n$. If we denote by M the n-dimensional lattice in $\mathbb{R}^n$ which consists of all images $x(\alpha)$ where α is an integer of K divisible by A', then since

$$|N(\alpha)| = |N(x(\alpha))|$$

(see Borevich-Shafarevich [4], p. 98), we can write (1.6) in the form

$$f_C(s) = N(A') \sum_{x \in M \cap X} \frac{1}{|N(x)|^s}, \tag{1.7}$$

where the summation is taken over all points $x = x(\alpha)$ in the lattice M which are contained in X. Then, by a general result on series (see Borevich-Shafarevich [4], p. 321), in which the summation is carried out over all points of a lattice which lie in some cone, we find that the series (1.7) converges for $s > 1$ and

$$\lim_{s \to 1+0} (s-1) \sum_{x \in M \cap X} \frac{1}{|N(x)|^s} = \frac{V}{\Delta}$$

where Δ is the volume of the fundamental parallelepiped of the lattice M and V is the volume of the set T which consists of all points x of the fundamental domain X for which $|N(x)| < 1$. We have that Δ is given by

$$\Delta = \frac{1}{2^t} N(A) \sqrt{|D|} \tag{1.9}$$

where D is the discriminant of the field K, and that V is given by

$$V = \frac{2^r \pi^t R}{w} \tag{1.10}$$

where R is the regulator of K, w is the order of the group of roots of unity contained in K, r is the number of real embeddings of K, and $2t$ the number of complex embeddings. We note that $n = r + 2t$. It now easily follows that

$$\lim_{s \to 1+0} (s-1) f_C(s) = \frac{2^{r+t} \pi^t R}{w \sqrt{|D|}}.$$

Since $\zeta_K(s) = \sum_C f_C(s)$, we have that the series

$$\zeta_K(s) = \sum_A \frac{1}{N(A)^s}$$

converges for all $s > 1$. Further, we have the formulas

$$\lim_{s\to 1+0}(s-1)\zeta_K(s) = \begin{cases} \dfrac{2^{n-1}Rh}{\sqrt{|D|}} & K \text{ real} \\ \dfrac{(2\pi)^{n_e}Rh}{w\sqrt{|D|}} & K \text{ imaginary} \end{cases} \qquad (1.11)$$

For $s > 1$, the function $\zeta_K(s)$ can be represented as a convergent infinite product

$$\zeta_K(s) = \prod_P \frac{1}{1 - \frac{1}{N(P)^s}}, \qquad (1.12)$$

where P runs through all prime divisors of the field K. This representation is known as Euler's Identity. Using (1.12) and the known factorization of rational primes into prime divisors in the cyclotomic field Q_f, we obtain the formula

$$\zeta_K(s) = \prod_\chi L(s, \chi'), \quad (s > 1) \qquad (1.13)$$

where the product is taken over all $\chi \in \chi$, χ' denotes the primitive character (mod $f(\chi)$) that induces χ, and

$$L(s, \chi') = \prod_p \frac{1}{1 - \frac{\chi'(p)}{p^s}}$$

(p running over all rational primes and $\chi'(p)$ being zero for p dividing $f(\chi)$.) (For proof of (1.13), see Narkiewicz [18], p. 369 f.f.). We

observe that $L(s, 1')$ is $\zeta(s)$ the Riemann zeta function (see Borevich-Shafarevich [4], p. 330 noting that the m of that discussion is 1 by Apostol [2], p. 167) for which

$$\lim_{s\to 1+0} (s-1)\zeta(s) = 1$$

(see Borevich-Shafarevich [4], p. 321). Therefore, we have

$$\lim_{s\to 1+0} (s-1)\zeta_K(s) = \prod_{\chi\neq 1} L(1, \chi'). \tag{1.14}$$

Putting this together with (1.11), we obtain the analytic class number formula:

$$hR = \begin{cases} \dfrac{\sqrt{|D|}}{2^{n-1}} \displaystyle\prod_{\chi\neq 1} L(1, \chi') & K \text{ real} \\ \dfrac{w\sqrt{|D|}}{(2\pi)^{n_c}} \displaystyle\prod_{\chi\neq 1} L(1, \chi') & K \text{ imaginary} \end{cases} \tag{1.15}$$

1.4 Calculation of $L(1, \chi')$

In this section, we fix $\chi \in \underline{X}$ (and hence χ'), $\chi \neq 1$, and write f for $f(\chi)$ and ζ for $\exp 2\pi i/f$. We use $\sum_x$ (or $\sum_{x \bmod f}$ where ambiguity is possible) to denote summation over a prime residue system $\{x\} \bmod f$ (a set $\{x\}$ which is a complete system of representatives of the multiplicative group $(\mathbb{Z}/f\mathbb{Z})^*$), $\sum_{\pm x}$ (or $\sum_{\pm x \,(\mathrm{mod}\, f)}$) to denote

summation over a prime half residue system (a set $\{x\}$ where $\{\pm x\}$ is a prime residue system), and $\sum^{+}$ to denote that the residue system should consist of the smallest possible positive numbers.

For z a rational integer, we denote by $\tau_z(\chi')$ the Gauss sum

$$\tau_z(\chi') = \sum_x \chi'(x)\zeta^{xz} \tag{1.16}$$

If we put $\tau(\chi') = \tau_1(\chi')$ and if $(z, f) = 1$, then

$$\tau_z(\chi') = \overline{\chi'}(z)\tau(\chi').$$

But since χ' is primitive, then $\tau_z(\chi') = 0$ if $(z, f) \neq 1$ and so for any z

$$\tau_z(\chi') = \overline{\chi'}(z)\tau(\chi'). \tag{1.17}$$

Now for $s > 1$,

$$L(s, \chi') = \sum_{m=1}^{\infty} m^{-s}\chi'(m)$$

$$= \sum_x \chi'(x) \sum_{\substack{n\geq 1 \\ n\equiv x \pmod f}} n^{-s} = \sum_x \chi'(x) \sum_{n=1}^{\infty} n^{-s} f^{-1} \sum_{z=0}^{f-1} \zeta^{(x-n)z}$$

$$= f^{-1} \sum_{z=0}^{f-1} \left(\sum_x \chi'(x)\zeta^{xz}\right) \sum_{n=1}^{\infty} n^{-s}\zeta^{-nz},$$

and so

$$L(1, \chi') = f^{-1}\left(\sum_z \tau_z(\chi')\right) \sum_{n=1}^{\infty} n^{-1}\zeta^{-nz}$$

since $\tau_2(\chi') = 0$ for $(z, f) \neq 1$.

Further, we have,

$$\sum_{n=1}^{\infty} n^{-1}\zeta^{-nz} = -\log(1 - \zeta^{-z}) \qquad (1.18)$$

where we take the principal value of the logarithm (imaginary part between $-\pi i$ and πi).

Then by (1.17) and (1.18), we have

$$L(1, \chi') = \frac{-\tau(\chi')}{f} \sum_z \overline{\chi'}(z) \log(1 - \zeta^{-z}) \qquad (1.19)$$

Let $S(\chi') = \sum_z \overline{\chi'}(z) \log(1 - \zeta^{-z})$.

Interchanging z and $-z$, we obtain

$$S(\chi') = \sum_z \overline{\chi'}(z)\, \overline{\chi'}(-1) \log(1 - \zeta^{z}).$$

Therefore,

$$S(\chi') = \frac{1}{2} \sum_z \overline{\chi'}(z) \left[\log(1 - \zeta^{-z}) + \overline{\chi'}(-1) \log(1 - \zeta^{z})\right]. \qquad (1.20)$$

If we assume $\overline{\chi'}$ is even (and since $1 - \zeta^{z}$ and $1 - \zeta^{-z}$ are conjugates), then (1.20) becomes

$$S(\chi') = \frac{1}{2} \sum_z \overline{\chi'}(z) \log|1 - \zeta^{z}|^2$$

$$= \sum_z \overline{\chi'}(z) \log|1 - \zeta^{z}|$$

$$= 2 \sum_{\pm z} \overline{\chi'}(z) \log|1 - \zeta^{z}|.$$

Hence, (1.19) becomes

$$L(1, \chi') = \frac{2\tau(\chi')}{f} \sum_{\pm z \bmod f} (-\overline{\chi'}(z) \log|1 - \zeta^z|), \quad (\chi' \text{ even}) \qquad (1.21)$$

If χ' is odd, (1.20) becomes

$$S(\chi') = \frac{1}{2} \sum_z \overline{\chi'}(z) [\log(1 - \zeta^{-z}) - \log(1 - \zeta^z)]. \qquad (1.22)$$

Using trigonometric identities, it is easy to see that $1 - \zeta^{\pm z} = 2 \sin \frac{\pi z}{f} \exp[\pm \pi i (\frac{z}{f} - \frac{1}{2})]$. To obtain the principal value of the logarithm, we should take z to be in the smallest positive residue system. Then (1.22) becomes

$$S(\chi') = -\pi i \sum_z^+ \overline{\chi'}(z)(\frac{z}{f} - \frac{1}{2}) = \frac{\pi}{i} \frac{1}{f} \sum_z^+ \overline{\chi'}(z) z$$

(since $\sum_z^+ \overline{\chi'}(z) = 0$ as χ' is not the unit character) whence (1.19) becomes

$$L(1, \chi') = \frac{\pi}{i} \frac{\tau(\chi')}{f} \frac{1}{f} \sum_{z \bmod f}^+ \overline{\chi'}(z) z, \quad (\chi' \text{ odd}) \qquad (1.23)$$

1.5 The Arithmetic Class Number Formula

We can now substitute our calculations for $L(1, \chi')$ into (1.15) and use the product formulae for conductors and Gauss sums

$$\prod_\chi \tau(\chi) = \begin{cases} (\prod_\chi f(\chi))^{\frac{1}{2}} = |D|^{\frac{1}{2}} & K \text{ real} \\ i^{n_e} (\prod_\chi f(\chi))^{\frac{1}{2}} = i^{n_e} |D|^{\frac{1}{2}} & K \text{ imaginary} \end{cases} \qquad (1.24)$$

(see Hasse, [10], p. 8). (We note that $\chi = 1$ can be dropped from the above relations as $\tau(1) = 1$ and $f(1) = 1$) to obtain the following

$$hR = \prod_{\chi \neq 1} \sum_{\substack{\pm x \\ \bmod f(\chi)}} (-\chi(x) \log|1 - \zeta_{f(\chi)}^{x}| \quad K \text{ real} \qquad (1.25)$$

and

$$hR = -\prod_{\chi_e \neq 1} \sum_{\substack{\pm x \\ \bmod f(\chi_e)}} (-\chi_e(x) \log|1 - \zeta_{f(\chi_e)}^{x}|) \qquad (1.26)$$

$$\cdot \frac{w}{2} \prod_{\chi_o \in \overline{\chi}_o} \frac{1}{f(\chi_o)} \cdot \sum_{\substack{x \\ \bmod f(\chi_o)}}^{+} (-\chi_o(x)x)$$

for K imaginary. We note that the first factor in (1.26) is merely (1.25) for the field K^+ with class number h^+ and regulator R^+. The number E defined by the following formula

$$E = 2^{n_e - 1} R^+/R \qquad (1.27)$$

is analyzed in Hasse [10], where it is shown that E is always 1 or 2. For Q_f, we have $E = 1$ if and only if f is a prime power or twice a prime power (see Hasse [10], Satz 27, p. 71).

Putting (1.25), (1.26) and (1.27) together, we obtain the following arithmetic class number formula for abelian number fields

$$h = \frac{\prod_{\chi_e \neq 1} \sum_{\substack{x \\ \bmod f(\chi_e)}}^{+} (-\chi_e(x)) \log|1 - \zeta_{f(\chi_e)}^{x}|)}{R^+} \cdot Ew \prod_{\chi_o \in \underline{X}_o - \frac{1}{2f(\chi_o)}} \sum_{\substack{x \\ \bmod f(\chi_o)}}^{+} (-\chi_o(x)x) \tag{1.28}$$

The first factor in (1.28) is h^+. We denote the second factor by h^* and call it the relative class number of K/K^+, or more simply the relative class number of K.

$$h^* = Ew \prod_{\chi \text{ odd}} \frac{1}{2f(\chi)} \sum_{\substack{x \\ \bmod f(\chi)}}^{+} (-\chi(x)x) \tag{1.29}$$

We remark that we understand $h^* = h/h^+$ to be 1 when $K = K^+$, and there are no odd characters. We see immediately that h^* is rational but, in fact, h^* is an integer (see Hasse [10], Satz 10, p. 49)

1.6 Formulas for h_p^*

We derive various formulas for h_p^* which we shall use in Chapters two and three. For $K = Q_p$, we have $w = 2p$, $E = 1$, $n_e = \frac{p-1}{2}$ and from (1.27) $R = 2^{\frac{p-3}{2}} R^+$. Further, we have $\frac{p-1}{2}$ odd characters of conductor p, $\frac{p-3}{2}$ even characters of conductor p, and the unit character of conductor one. Hence, by (1.24), $d = p^{p-2}$ and $d^+ = p^{\frac{p-3}{2}}$ where d (respectively d^+) is the absolute value of the discriminant of Q_p (respectively Q_p^+).

If we plug these values in (1.15) applied to both Q_p and Q_p^+, we find that $h_p^* = h_p/h_p^+$ is given by

$$h_p^* = p^{\frac{p+3}{4} - (\frac{p-3}{2}) - (\frac{p-1}{2})} \pi \prod_{\chi \text{ odd}} L(1, \chi) \qquad (1.30)$$

If we denote by r a primitive root (mod p) and by r_k the least positive residue of r^k (mod p), then (1.29) can be written as

$$h_p^* = (-1)^s 2p \prod_{v=1}^{s} (2p)^{-1} \sum_{k=0}^{p-2} r_k \zeta^{(2v-1)k} \qquad (1.31)$$

where $s = \frac{1}{2}(p-1)$ and $\zeta = e^{2\pi i/(p-1)}$. To put this formula in another form, we first note that

$$(\zeta^{1-2v} - 1) \sum_{k=0}^{p-2} r_k \zeta^{(2v-1)k} = \sum_{k=0}^{p-2} (r_{k+1} - r_k)\zeta^{(2v-1)k} \qquad (1.32)$$

$$= 2 \sum_{k=0}^{s-1} (r_{k+1} - r_k)\zeta^{(2v-1)k}$$

Since ζ is a primitive $p-1$ root of unity and ζ^2 is a primitive $\frac{p-1}{2}$ root of unity, then

$$p - 1 = (1 - \zeta)(1 - \zeta^2)(1 - \zeta^3) \ldots (1 - \zeta^{p-2}),$$

$$\frac{p-1}{2} = (1 - \zeta^2)(1 - \zeta^4)(1 - \zeta^6) \ldots (1 - \zeta^{p-3}),$$

and so

$$\pm 2 = (\zeta - 1)(\zeta^3 - 1)(\zeta^5 - 1) \dots (\zeta^{p-2} - 1) \qquad (1.33)$$
$$= (\zeta^{-1} - 1)(\zeta^{-3} - 1) \dots (\zeta^{-(p-2)} - 1).$$

From (1.31), (1.32) and (1.33), we deduce that

$$h_p^* = \pm p^{1-s} \prod_{v=1}^{s} \sum_{k=0}^{s-1} (r_{k+1} - r_k)\zeta^{(2v-1)k} \qquad (1.34)$$

We now show that this result can be expressed in the form

$$h_p^* = \pm p^{1-s} \prod_{u|n} N_u(\alpha_u), \quad \alpha_u = \sum_{k=0}^{s-1} (r_{k+1} - r_k)\zeta^{uk} \qquad (1.35)$$

where N_u means the norm in the $2^c n/u$-th cyclotomic field $Q(e^{2\pi iu/(p-1)})$ and $p - 1 = 2^c n$, n odd. We recall that for y in this field

$$N_u(y) = \prod_{\substack{i=1 \\ (i, \frac{p-1}{u}) = 1}}^{\frac{p-1}{u}} \sigma_i(y) = \prod_{\substack{i=1 \\ (i, n/u) = 1,\ i \text{ odd}}}^{\frac{p-1}{u}} \sigma_i(y)$$

$$\text{Hence, } N_u(\alpha_u) = \prod_{\substack{i=1 \\ (i, n/u) = 1,\ i \text{ odd}}}^{\frac{p-1}{u}} \sum_{k=0}^{s-1} (r_{k+1} - r_k)\zeta^{uik}$$

It is easy to see that for all $u|n$, ui runs through all odds between 1 and $p - 2$ without repeats, which shows that (1.34) can be expressed in the form (1.35).

1.7 An Important Formula for h_m^*

Let v be the exponent of the group $\underline{X}$, that is, v is the least common multiple of the orders of all elements in $\underline{X}$.

Then $\chi \in \underline{X}$ takes values in Q_v and G_v acts on $\underline{X}$:

$$G_v \times \underline{X} \to \underline{X}$$
$$(\sigma_i, \chi) \mapsto \chi^{\sigma_i}$$

where $\chi^{\sigma_i} = \sigma_i(\chi(x)) = \chi^i(x)$ for all i such that $(i, v) = 1$ and all $x \in (\mathbb{Z}/f\mathbb{Z})^*$.

The orbit of $\chi = \{\chi^i \mid 1 \le i < v, \ (i, v) = 1\}$

$$= \{\chi^i \mid 1 \le i < n_\chi, \ (i, n_\chi) = 1\}$$

where n_χ is the order of χ in $\underline{X}$. Choose a system of representatives $\{\chi\}$ for the orbits of this action. Then the order n_χ of $\chi \in \underline{X}$, the conductor $f(\chi)$ and whether $\chi(-1) = 1$ or -1 are all invariants of an orbit. To see the first statement, we let m be the order of χ^i, i fixed, $(i, n_\chi) = 1$. Then $m \mid n_\chi$ since $(\chi^i)^{n_\chi} = (\chi^{n_\chi})^i = 1$. Also, $(\chi^i)^m = \chi^{im} = 1$. Therefore, $n_\chi \mid im$ but since $(i, n_\chi) = 1$, then $n_\chi \mid m$. Hence $m = n_\chi$.

To see the second statement, let $f(\chi^i)$ be the conductor of χ^i. Since $(i, n_\chi) = 1$, there exists $s, t \in \mathbb{Z}$ such that $is + n_\chi t = 1$. Then for $x \equiv y \bmod f(\chi^i)$, we have $\chi(x) = \chi^{is+n_\chi t}(x) = \chi^{is}(x) = \chi^{is}(y) = \chi^{is+n_\chi t}(y) = \chi(y)$. But since $f(\chi)$ is the conductor of χ, then $f(\chi) \le f(\chi^i)$. Now if $x \equiv y \bmod f(\chi)$, then $\chi^i(x) = \chi^i(y)$ since $\chi(x) = \chi(y)$.

Therefore, $f(\chi^i) \leq f(\chi)$ as $f(\chi^i)$ is the conductor of χ^i. Hence, $f(\chi^i) = f(\chi)$.

To see the third statement, if we let $\chi(-1) = +1$, then clearly $\forall\ i,\ (i, n_\chi) = 1,\ \chi^i(-1) = +1$. If $\chi(-1) = -1$, then $1 = \chi^{n_\chi}(-1) = (-1)^{n_\chi}$. Therefore, n_χ is even and since $(i, n_\chi) = 1$, then i is odd. Therefore, $\chi^i(-1) = (-1)^i = -1$.

We also have that two characters are in the same orbit if and only if they generate the same cyclic subgroup of $\underline{X}$. To see this, we first let χ^i, χ^j be in the same orbit. Again, there exists $s, t \in Z$ such that $js + n_\chi t = 1$. Therefore, $\chi^i = \chi^{i(js+n_\chi t)} = (\chi^j)^{is}$ which proves this direction. Then let $\langle\chi\rangle = \langle\psi\rangle$. Therefore, $\chi = \psi^i$. We must show $(i, n_\chi) = 1$. If $(i, n_\chi) = r$, then $\chi^{\frac{n_\chi}{r}} = \psi^{i\frac{n_\chi}{r}} = (\psi^{n_\chi})^{i/r} = 1$ (note $n_\chi = n_\psi$). Therefore, $r = 1$ and so χ and ψ are in the same orbit.

The $\phi(n_\psi)$ characters in the orbit of ψ are precisely the characters whose values are algebraically conjugate to those of ψ in Q_{n_ψ}, the field obtained by adjoining the values of ψ to Q. Hence, if we let

$$H_\psi = \frac{1}{2f(\psi)} \sum^{+}_{\bmod f(\psi)} \psi(x)x \qquad \text{(Stickelberger symbol)} \qquad (1.36)$$

and N_ψ be the norm map from Q_{n_ψ} to Q, then $N_\psi(H_\psi)$ is the product of factors H_{ψ^i} where the product is over all characters in the same orbit as ψ. Therefore, if we group the factors in (1.29) according to orbits, we get

$$h^* = E\, w \prod_{\psi \text{ odd}} N_\psi(H_\psi) \tag{1.37}$$

where the product is taken over a system of representatives $\{\psi\}$ for the orbits of odd characters.

1.8 Norms of Stickelberger Symbols

We prove the following properties of $N_\psi(H_\psi)$ (the proofs follow Hasse [10], p. 80-94):

Theorem 1.1 - Let ψ be a primitive character mod $f(\psi)$ with $\psi(-1) = -1$ and let n_ψ be the order of ψ.

(A) If $f(\psi)$ is divisible by more than one prime, then $N_\psi(H_\psi) \in \mathbb{Z}$.

(B) Suppose n_ψ is a power of 2:

(i) if at least three distinct primes divide $f(\psi)$ then $N_\psi(H_\psi) \in 2\mathbb{Z}$.

(ii) if only two distinct primes p, q, $p \neq 2$ divide $f(\psi)$, then $N_\psi(H_\psi)$ is an even or odd integer according as the quadratic residue symbol $(\frac{q}{p}) = 1$ or -1.

(C) If $f(\psi) = p^\alpha$, then $N_\psi(H_\psi) \in \frac{1}{2p}\mathbb{Z}$ and, more precisely, the denominator (in lowest terms):

(i) may be divisible by p if $p \neq 2$ and $n_\psi = \phi(p^\alpha)$;

(ii) is ± 4 for $f(\psi) = 4$ and ± 2 for $f(\psi) = 2^\alpha$, $\alpha \geq 3$;

(iii) is divisible by ± 2 if $n_\psi = 2^u$ (since $\psi(-1) = -1$, this occurs only for $2^u \| p - 1$ and, in addition, since $n_\psi = 2^u$, then α must be one);

(iv) is ± 1 in all other cases.

Proof of Theorem 1.1; A - Let $f(\psi) = f = f_1 f_2$ where $f_1, f_2 \neq 1$ and $(f_1, f_2) = 1$. We can then write $\psi = \psi_1 \psi_2$ where ψ_i is a primitive character mod f_i. Note that ψ_1 (say) is even, and ψ_2 is odd.

We shall rewrite the formula for $H_\psi = -\frac{1}{2f} \sum_{x \bmod f} x\psi(x)$ to eliminate the denominator $2f$. As x_i runs through the smallest positive residue system mod f_i with $(x_i, f_i) = 1$, then the x where

$$\frac{x}{f} = \frac{x_1}{f_1} + \frac{x_2}{x_2}$$

run through a complete system of representations for the elements of $(\mathbb{Z}/f\mathbb{Z})^*$. However, the numbers x are in the range $1 < x < 2f$. To prove this, we observe that if $(x_1, f_1) = (x_2, f_2) = 1$, then $(x, f) = 1$ and if $0 < x_1, y_1 < f_1$ and $0 < x_2, y_2 < f_2$, then $\frac{x_1}{f_1} + \frac{x_2}{f_2} = \frac{y_1}{f_1} + \frac{y_2}{f_2}$ if and only if $x_1 = y_1$ and $x_2 = y_2$. Hence, there are exactly $\phi(f_1)\phi(f_2) = \phi(f)$ distinct such x between 1 and $2f$ relatively prime to f. Further, no two are congruent mod f for if $x = x_1 f_2 + x_2 f_1 \equiv y = y_1 f_2 + y_2 f_1 \pmod f$ then $f \mid (x_1 - y_1) f_2$, $(x_2 - y_2) f_1$ which implies that $f_1 \mid (x_1 - y_1)$ and $f_2 \mid (x_2 - y_2)$. Thus, $x_1 = y_1$; $x_2 = y_2$ and so $x = y$.

We want to get a complete set of positive representatives of $(\mathbb{Z}/f\mathbb{Z})^*$ from numbers between 1 and f. We can do this by subtracting 1 from the fraction $\frac{x_1}{f_1} + \frac{x_2}{f_2} = \frac{x}{f}$ whenever $\frac{x_1}{f_1} + \frac{x_2}{f_2} > 1$. The resulting $\phi(f)$ numerators of f (either $x - f$ or x) will all be distinct, lie between

1 and f and be relatively prime to f. We now construct this set. We note that this construction will run through all the x_i of above and will subtract 1 where necessary. We restrict x_i to the range $1 \le x_i < \frac{f_i}{2}$; $i = 1, 2$. Then the numbers x_o, x_o', x_o'', x_o''' below give a complete system of distinct positive numbers between 0 and f and relatively prime to f:

$$\frac{x_o}{f} = \frac{x_1}{f_1} + \frac{x_2}{f_2}$$

$$\frac{x_o'}{f} = \frac{f_1 - x_1}{f_1} + \frac{x_2}{f_2} - \varepsilon(x_1, x_2)$$

$$\frac{x_o''}{f} = \frac{x_1}{f_1} + \frac{f_2 - x_2}{f_2} - (1 - \varepsilon(x_1, x_2))$$

$$\frac{x_o'''}{f} = \frac{f_1 - x_1}{f_1} + \frac{f_2 - x_2}{f_2} - 1$$

where $\varepsilon(x_1, x_2) = \begin{cases} 0 & \text{if } \frac{x_1}{f_1} > \frac{x_2}{f_2} \\ 1 & \text{if } \frac{x_1}{f_1} < \frac{x_2}{f_2} \end{cases}$

We note that $\psi(x_o) = \psi_1(x_o)\psi_2(x_o) = \psi_1(x_1f_2 + x_2f_1)\psi_2(x_1f_2 + x_2f_1)$

$$= \psi_1(x_1f_2)\psi_2(x_2f_1) = \psi_1(f_2)\psi_2(f_1)\psi_1(x_1)\psi_2(x_2)$$

and, hence, by similar expansions

$$\psi(x_o') = \psi(x_o); \quad \psi(x_o'') = -\psi(x_o); \quad \text{and} \quad \psi(x_o''') = -\psi(x_o).$$

Hence, $H_\psi = -\frac{1}{2f} \sum_{x \bmod f} x\psi(x) = +\frac{1}{2f} \sum_{x_o} - \psi(x_o)(x_o + x_o' - x_o'' - x_o''')$

$$= \psi_1(f_2)\psi_2(f_1) \sum_{\substack{\pm x_1 \\ (\mathrm{mod}\ f_1)}} \sum_{\substack{\pm x_2 \\ (\mathrm{mod}\ f_2)}} -\psi_1(x_1)\psi_2(x_2)\left[\frac{2x_2}{f_2} - \epsilon(x_1, x_2)\right].$$

We next recall that $\sum_{x \,(\mathrm{mod}\, f_1)} \psi_1(x) = 0$ since $\psi_1 \neq 1$ and also that $\psi_1(x) = \bar{\psi}_1(-x) = \psi_1(f_1 - x)$ since ψ_1 is even. Hence

$$\sum_{\pm x_1} \psi_1(x_1) = \frac{1}{2}\left(\sum_{x_1} \psi_1(x_1)\right) = 0.$$

Hence, $\sum_{\substack{0<x_i<\frac{f_i}{2} \\ (x_i,f_i)=1}} -\psi_1(x_1)\psi_2(x_2)\frac{2x_2}{f_2} = \sum_{\substack{\pm x_2 \\ (\mathrm{mod}\ f_2)}} -\psi_2(x_2)\frac{2x_2}{f_2}\left(\sum_{\substack{\pm x_1 \\ (\mathrm{mod}\ f_1)}} \psi_1(x_1)\right) = 0.$

Hence, $H_\psi = \psi_1(f_2)\psi_2(f_1) \sum_{\substack{0<x_i<\frac{f_i}{2} \\ (x_i,f_i)=1}} \psi_1(x_1)\psi_2(x_2)\epsilon(x_1, x_2)$

and so

$$H_\psi = \psi_1(f_2)\psi_2(f_1) \sum_{\substack{0<x_i<\frac{f_i}{2} \\ (x_i,f_i)=1 \\ \frac{x_1}{f_1}<\frac{x_2}{f_2}}} \psi_1(x_1)\psi_2(x_2) \qquad (1.38)$$

This last expression for H_ψ belongs to the ring of integers of Q_{n_ψ} and, hence, $N_\psi(H_\psi) \in Z$. //

To prove Theorem 1.1; B, we need the following Lemma:

Lemma 1.1 - Let m be a natural number $\neq 1, 2$, p an odd prime relatively prime to m and N the number of solutions (x, y) of the inequality $\frac{x}{m} < \frac{y}{p}$ where $0 < x < \frac{m}{2}$, $(x, m) = 1$ and $0 < y < \frac{p}{2}$, $(y, p) = 1$.

(1) If m is divisible by more than one prime, then N is even.

(2) If $m = q^{\gamma}$, q prime, then $(-1)^N = (\frac{q}{p})$.

Proof - For each of the solutions (x, y), we have that $0 < my - px < \frac{p}{2}m$. If we subdivide the interval $(0, \frac{p}{2}m)$ into $\frac{p+1}{2}$ subintervals $(0, \frac{1}{2}m)$; $(\frac{1}{2}m; \frac{3}{2}m)$; $(\frac{3}{2}m; \frac{5}{2}m)$; ...; $(\frac{p-2}{2}m, \frac{p}{2}m)$ where the zero-th subinterval has length $\frac{m}{2}$ and the others each have length m, then we have for N

$$N = N_0 + N_1 + \ldots + N_{\frac{p-1}{2}}$$

where N_k is the number of solutions (x, y) with $my - px$ in the kth subinterval. (We note that the endpoints of the subintervals have been omitted since $my - px$ cannot assume these values.)

We call an equation of the form

$$px = \pm x' + mz$$

where $z \in \mathbb{Z}$ and where x, x' belong to the collection $0 < x, x' < \frac{m}{2}$, $(xx', m) = 1$, a reduction. We note that $0 < z < \frac{p-1}{2}$. It is easy to check that there are exactly $\frac{\phi(m)}{2}$ such reductions. We let R_z be the numbers of such reductions with fixed z and U be the number of reductions with odd z.

Now, N_0 is the number of solutions (x, y) with $\frac{-m}{2} < px - my < 0$. These solutions correspond to the reductions with $-x'$ as residue, while $z \neq 0$. For $k = 1, 2, \ldots, \frac{p-1}{2}$, N_k is the number of solutions (x, y) with

$$\frac{-m}{2} - km < px - my < \frac{m}{2} - km.$$

Writing this in the form

$$\frac{-m}{2} < px - m(y - k) < \frac{m}{2},$$

we recognize that these solutions correspond to the reductions where $z = 0, 1, \ldots, \frac{p-1}{2} - k$. These reductions are obtained from $\frac{\phi(m)}{2}$ reductions by omitting the reductions with $z = \frac{p-1}{2} - (k - 1), \ldots, \frac{p-1}{2}$. Then

$$N_k = \frac{\phi(m)}{2} - (R_{\frac{p-1}{2}-(k-1)} + \ldots + R_{\frac{p-1}{2}}) \quad (k = 1, \ldots, \tfrac{p-1}{2}).$$

Thus,

$$N_1 + \ldots + N_{\frac{p-1}{2}} = \frac{p-1}{2} \cdot \frac{\phi(m)}{2} - (R_1 + 2R_2 + \ldots + \tfrac{p-1}{2} R_{\frac{p-1}{2}})$$

$$\equiv \frac{p-1}{2} \cdot \frac{\phi(m)}{2} - \sum_u R_u \pmod 2$$

where u runs through the odd numbers between 1 and $\frac{p-1}{2}$. Therefore,

$$N_1 + \ldots + N_{\frac{p-1}{2}} \equiv \frac{p-1}{2} \frac{\phi(m)}{2} + U \pmod 2.$$

We thus obtain the following congruence for N:

$$N \equiv \frac{p-1}{2}\frac{\phi(m)}{2} + N_o + U \pmod 2 \qquad (1.39)$$

where N_o is the number of reductions with negative residue and U the number of reductions with odd z.

For the remainder of the proof, we have to distinguish some cases for m. We first examine the cases where m is odd. If we multiply all the reductions together, then we obtain the congruence

$$p^{\frac{1}{2}\phi(m)} \equiv (-1)^{N_o} \pmod m. \qquad (1.40)$$

Further, since $\sum z \equiv U \mod 2$ where the sum is over z from all the reductions, and since m is odd, the addition of all reductions results in the congruence

$$U \equiv 0 \pmod 2.$$

If m is divisible by more than one prime, then we have

$$p^{\frac{1}{2}\phi(m)} \equiv 1 \pmod m$$

(see Apostol [2], p. 211) and hence by (1.40), $N_o \equiv 0 \pmod 2$. Also, $\frac{\phi(m)}{2} \equiv 0 \mod 2$ and hence, it follows that

$$N \equiv 0 \pmod 2 \qquad (1.41)$$

If m is a prime power, say $m = q^\gamma$, q odd prime, $\gamma \geq 1$, then we claim that $p^{\frac{1}{2}\phi(m)} \equiv \left(\frac{p}{q}\right) \pmod m$. To see this, we first apply the Euler-Fermat Theorem (see Apostol [2], p. 113) to obtain

$$p^{\frac{\phi(m)}{2}} \equiv 1 \pmod{2m}. \tag{1.44}$$

To see this, we let $m = 2^{\alpha}n$, n odd. If $\alpha > 2$, then $p^{\frac{\phi(2^{\alpha+1})}{2}} \equiv 1 \pmod{2^{\alpha+1}}$ (see Apostol [2], p. 206) and if n is composite, then $p^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}$. (see Apostol [2], p. 211.) Hence, $p^{\frac{\phi(m)}{2}} = p^{\frac{\phi(2m)}{4}} = \left(p^{\frac{\phi(2^{\alpha+1})}{2}}\right)^{\frac{\phi(n)}{2}} \equiv 1 \pmod{2^{\alpha+1}n}$ since $(2^{\alpha+1}, n) = 1$.

If $\alpha = 1$, n composite, then $p^{\frac{\phi(2^{1+1})}{2}} = p \equiv \pm 1 \pmod{2^{1+1}}$ and $p^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}$. But $\frac{\phi(n)}{2}$ is even and so $p^{\frac{\phi(m)}{2}} = p^{\frac{\phi(2m)}{4}} = \left(p^{\frac{\phi(2^2)}{2}}\right)^{\frac{\phi(n)}{2}} \equiv 1 \pmod{2m}$.

If $\alpha \geq 2$ and $n = q^{\gamma}$ then $p^{\frac{\phi(n)}{2}} \equiv \pm 1 \pmod{n}$ and, as above, $p^{\frac{\phi(2^{\alpha+1})}{2}} \equiv 1 \pmod{2^{\alpha+1}}$. But $\frac{\phi(2^{\alpha+1})}{2}$ is even and so $p^{\frac{\phi(m)}{2}} = \left(p^{\frac{\phi(n)}{2}}\right)^{\frac{\phi(2^{\alpha+1})}{2}} \equiv 1 \pmod{2m}$, and so we have our claim. But then, it follows easily from (1.43) and (1.44) that $N_o \equiv 0 \pmod 2$ and $U \equiv 0 \pmod 2$. Furthermore, $\frac{\phi(m)}{2} \equiv 0 \pmod 2$ and so by (1.39), we get

$$N \equiv 0 \pmod 2. \tag{1.45}$$

If $m = 2q^{\gamma}$, then, since $p \equiv (-1)^{\frac{p-1}{2}} \pmod 4$, we have $p^{\frac{\phi(m)}{2}} \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod 4$. Hence by (1.43), we obtain $N_o + U \equiv \frac{p-1}{2}\cdot\frac{q-1}{2} \pmod 2$. But we also have that $\frac{\phi(m)}{2} \equiv \frac{q-1}{2} \pmod 2$ and so

$$q^{\gamma} \| p^{\phi(m)} - 1 = (p^{\frac{1}{2}\phi(m)} - 1)(p^{\frac{1}{2}\phi(m)} + 1)$$

and hence $q^{\gamma} \mid (p^{\frac{1}{2}\phi(m)} - 1)$ or $q^{\gamma} \mid (p^{\frac{1}{2}\phi(m)} + 1)$. If the former case then, $p^{\frac{1}{2}\phi(m)} \equiv +1 \pmod{q^{\gamma}}$ and hence $(p^{\frac{q-1}{2}})^{q^{\gamma-1}} \equiv +1 \pmod{q}$. But then since $p^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}$ and since $q^{\gamma-1}$ is odd, then $p^{\frac{q-1}{2}} \equiv +1 \pmod{q}$. But then by the Euler Criterion (see Apostol [2], p. 180) $(\frac{p}{q}) \equiv +1 \pmod{q}$ and hence $(\frac{p}{q}) = +1$. But then $p^{\frac{1}{2}\phi(m)} \equiv (\frac{p}{q}) \pmod{m}$. The argument for the second case is the same so we have our claim.

Hence, by (1.40), we have $(-1)^{N_o} = (\frac{p}{q})$. Furthermore, $\frac{1}{2}\phi(m) \equiv \frac{1}{2}(q-1) \pmod{2}$. Thus by (1.39) and the quadratic reciprocity law

$$(-1)^{N} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} (\frac{p}{q}) = (\frac{q}{p}). \qquad (1.42)$$

We now examine the cases where m is even. Here the x's are odd and, hence, from the reduction $px = \pm x' + mz$, we get the congruence $px \equiv \pm x'(1 + m)^{z} \pmod{2m}$. (This follows since $\pm x'(1 + m)^{z} \equiv \pm x'(1 + mz) \pmod{2m}$ and since $\pm x'mz \equiv mz \pmod{2m}$.). The multiplication of all reductions then gives

$$p^{\frac{\phi(m)}{2}} \equiv (-1)^{N_o}(1 + m)^{U} \pmod{2m} \qquad (1.43)$$

since $(1 + m)^{z} \equiv 1 \pmod{2m}$ if z is even and $(1 + m)^{z} \equiv 1 + m \pmod{2m}$ if z is odd.

If m is divisible by more than one prime but not of the form $2q^{\gamma}$, q odd prime, then we claim that

it follows from (1.39) that

$$N \equiv 0 \pmod 2 \tag{1.46}$$

The first case we must consider is when $m = 2^\gamma$ $(\gamma \geq 2)$. We note that $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}$ (see Apostol [2], p. 180). Further, by an easy induction argument on γ for $\gamma \geq 2$, we have

$$\alpha_p^{\frac{\phi(m)}{2}} \equiv (-1)^{\frac{p-1}{2}\cdot\frac{\phi(m)}{2}} (1+m)^{\frac{p^2-1}{8}} \pmod{2m}.$$

Therefore, by (1.43), we have

$$N_o \equiv \frac{p-1}{2}\,\frac{\phi(m)}{2} \pmod 2; \quad U \equiv \frac{p^2-1}{8} \pmod 2.$$

Therefore, by (1.39), we have

$$(-1)^N = \left(\frac{2}{p}\right). \tag{1.47}$$

Through the assertions (1.41), (1.42), (1.45), (1.46) and (1.47), the lemma in each of the five different cases has been proven. //

We now prove Theorem 1.1; B.

Proof of Theorem 1.1; B - If $n = 2^u$, $u > 1$, then $\psi(x) = \zeta_{2^u}^i \equiv 1 \pmod Z$ where Z is the only prime ideal factor of 2 in the field $Q(\zeta_{2^u})$ and ζ_{2^u} is a primitive 2^u-th root of unity (see Samuel [22], p. 72). It now follows by the above and by (1.38) that if $f(\psi)$ is divisible by more than one prime, then

$$H_\psi \equiv N(f_1, f_2) \pmod{Z}$$

where $f = f_1 \cdot f_2$, $(f_1, f_2) = 1$ and where $N(f_1, f_2)$ is the number of solutions of $\frac{x_1}{f_1} \leq \frac{x_2}{f_2}$ where x_1, x_2 are defined as before:

$1 \leq x_i \leq \frac{f_i}{2}$, $(x_i, f_i) = 1$.

By forming the norm, we get

$$N_\psi(H_\psi) \equiv N(f_1, f_2) \pmod{2} \tag{1.48}$$

We recall that in (1.38) f_1 corresponds to ψ_1 where ψ_1 is even and f_2 corresponds to ψ_2 where ψ_2 is odd. We note that if ψ_1 were odd and ψ_2 were even, then instead of (1.38), we would obtain

$$H_\psi = -\psi_1(f_2)\psi_2(f_1) \sum_{\substack{0<x_i<\frac{f_i}{2} \\ (x_i,f_i)=1 \\ \frac{x_1}{f_1} < \frac{x_2}{f_2}}} \psi_1(x_1)\psi_2(x_2)$$

and hence $H_\psi = -N(f_1, f_2) \pmod{Z}$. However, this would not affect (1.48) as a change of sign makes no difference modulo 2. Hence in (1.48), it doesn't matter whether f_1 (or f_2) corresponds to an even or an odd character.

If we assume that $p \mid f(\psi)$, $p \neq 2$, then $p^i \nmid f(\psi)$, $i > 1$. For if $f(\psi) = p^i k$, $(p, k) = 1$, $i \geq 1$, then $\psi = \psi_1\psi_2$ where ψ_1 is

primitive $(\mathrm{mod}\ p^i)$ and ψ_2 is primitive $(\mathrm{mod}\ k)$. Further ψ_1 is of order 2^ℓ, $\ell \geq 1$, as ψ is of order $n_\psi = 2^u$, $u \geq 2$. Thus, as will be seen in the proof of the next theorem, $i = 1$. (We note that this does not involve any circular reasoning.) Hence, we can assume that the decomposition $f = f_1 f_2$ is of the form mp where $(p, m) = 1$. (We note that the character ψ_2 associated with $f_2 = p$ could be odd or even.) Therefore, by (1.48) and by Lemma 1.1, we have:

If $f(\psi)$ has at least three distinct prime factors, then

$$N_\psi(H_\psi) \equiv 0 \pmod 2.$$

If, however, there are only two distinct prime factors p, q in $f(\psi)$ where $p \neq 2$, then

$$N_\psi(H_\psi) \equiv 0 \text{ or } 1 \pmod 2$$

depending on whether $(\frac{q}{p}) = 1$ or -1.

(We note that if both q, p are odd, then using the quadratic reciprocity law and the fact that $n_\psi = 2^u$, it is easy to see that $(\frac{q}{p}) = (\frac{p}{q})$. //

To prove Theorem 1.1; C, we first consider characters with odd prime power conductors.

Proof of Theorem 1.1; C

Case I - We let ψ be a primitive character with conductor $f = p^\gamma$, $p \neq 2$, $\gamma \geq 1$. Let g be a primitive root $(\mathrm{mod}\ p)$ which is also a

primitive root $(\mathrm{mod}\ p^\gamma)$ for all $\gamma \geq 2$ (see Apostol [2], p. 209). Then $g = (g')^{p^{\gamma-1}}$ has order $p - 1$ $(\mathrm{mod}\ p^\gamma)$ for all $\gamma \geq 2$ and is still primitive $(\mathrm{mod}\ p)$. By induction on t, $t \geq 1$, it is easily seen that $(1 + p)^{p^t} \equiv 1 \ (\mathrm{mod}\ p^{t+1})$ but $(1 + p)^{p^t} \not\equiv 1 \ (\mathrm{mod}\ p^{t+2})$. From this, it easily follows that the order of $(1 + p)$ $(\mathrm{mod}\ p^\gamma)$, for $\gamma \geq 1$, is $p^{\gamma-1}$. Hence, there are $\phi(p^\gamma)$ numbers $g^\alpha(1 + p)^\beta$, $0 \leq \alpha < p - 1$, $0 \leq \beta < p^{\gamma-1}$ which are all incongruent $(\mathrm{mod}\ p^\gamma)$ and hence form a complete set of representatives of the group $(\mathbb{Z}/p^\gamma\mathbb{Z})^*$.

If $x \equiv g^\alpha(1 + p)^\beta \ (\mathrm{mod}\ p^\gamma)$ and if ψ' is a character $(\mathrm{mod}\ p^\gamma)$, then ψ' is given by

$$\psi'(x) = \zeta^{-\alpha} z^{-\beta} \tag{1.49}$$

where ζ is a primitive m-th root of unity, with $m | p - 1$, and z is a primitive s-th root of unity, with $s | p^{\gamma-1}$. (The negative sign in the exponents is convenient in later calculations.) But if ψ is a primitive character $(\mathrm{mod}\ p^\gamma)$, we claim that z is a primitive $p^{\gamma-1}$-st root of unity, i.e. $s = p^{\gamma-1}$. To see this, we assume that $s = p^{\gamma-i}$, $i > 1$. Now if $x \equiv g^\alpha(1 + p)^\beta \ (\mathrm{mod}\ p^\gamma)$, $x' \equiv g^{\alpha'}(1 + p)^{\beta'} \ (\mathrm{mod}\ p^\gamma)$ and if $g^\alpha(1 + p)^\beta \equiv g^{\alpha'}(1 + p)^{\beta'} \ (\mathrm{mod}\ p^{\gamma-i+1})$, then $g^\alpha \equiv g^{\alpha'} \ (\mathrm{mod}\ p)$ and so $p - 1 | \alpha - \alpha'$. Thus $(1 + p)^\beta \equiv (1 + p)^{\beta'} \ (\mathrm{mod}\ p^{\gamma-i+1})$ and so $(1 + p)^{\beta-\beta'} \equiv 1 \ (\mathrm{mod}\ p^{\gamma-i+1})$. Therefore, $p^{\gamma-i} | \beta - \beta'$ as $1 + p$ has order $p^{\gamma-i}$ $(\mathrm{mod}\ p^{\gamma-i+1})$. But then $\psi(x) = \zeta^{-\alpha} z^{-\beta} = \zeta^{-\alpha'} z^{-\beta'} = \psi(x')$, which is a contradiction as ψ is primitive. (see Apostol [2], Theorem 8.16).

Hence, for ψ primitive (mod p^γ), z is a primitive $p^{\gamma-1}$-st root of unity and so $n_\psi = mp^{\gamma-1}$. We note that this last statement implies that if ψ is a primitive character (mod p^γ) with $n_\psi = 2^u$, then $\gamma = 1$. Since $\psi(-1) = -1$, then $p-1/m$ must be odd (i.e. the 2-part of $p-1$ must be in m). This follows as $g^{\frac{p-1}{2}} \equiv -1 \pmod{p^\gamma}$ and so $-1 = \psi(-1) = \psi\left(g^{\frac{p-1}{2}}\right) = \zeta^{\frac{p-1}{2}} = \left(\zeta^{\frac{m}{2}}\right)^{\frac{p-1}{m}} = \left(\frac{}{-1}\right)^{\frac{p-1}{m}}$ where we note that $2|m$. We also note that the field $Q_{n_\psi} = Q(\zeta z)$ is composed of Q_m and $Q_{p^{\gamma-1}}$ which are distinct and have degrees $\phi(m)$, $\phi(p^{\gamma-1})$, respectively.

A relatively prime half-system (mod p^γ) is obtained if one restricts the basis representation $x \equiv g^\alpha(1+p)^\beta \pmod{p^\gamma}$ to $0 \le \alpha \le \frac{p-1}{2} - 1$ (since $g^{\frac{p-1}{2}} \equiv -1 \pmod{p^\gamma}$) while β is not restricted. We recall formula (1.36)

$$H_\psi = \frac{1}{2f} \sum_{x \bmod f}^{+} -\psi(x)x = \frac{1}{2f}\left[\sum_{\pm x \bmod f}^{+} -\psi(x)x + \sum_{\pm x \bmod f}^{+} -\psi(f-x)(f-x)\right]$$

$$= \frac{1}{2f}\left[2 \sum_{\pm x \bmod f}^{+} -\psi(x)x + f \sum_{\pm x \bmod f}^{+} \psi(x)\right]$$

$$= \frac{1}{2} \sum_{\pm x \bmod f}^{+} \psi(x) + \frac{1}{f} \sum_{\pm x \bmod f}^{+} -\psi(x)x$$

(We recall that ψ is assumed to be odd.) If we let $A(\psi) = \sum_{\pm x \bmod f}^{+} \psi(x)$, $B(\psi) = \sum_{\pm x \bmod f}^{+} -\psi(x)x$, then

$$H_\psi = \frac{1}{2} A(\psi) + \frac{1}{f} B(\psi). \qquad (1.50)$$

We recall that $\sum_{\pm x \bmod f}$ means the summation is over any half system (mod f). Since $\psi(-1) = -1$, then $A(\psi) = \sum^{+}_{\pm x \bmod f} \equiv \sum_{\pm x \bmod f} \psi(x) \pmod 2$ and $B(\psi) = \sum^{+}_{\pm x \bmod f} \psi(x)x \equiv \sum_{\pm x \bmod f} \psi(x)x \pmod f$.

We now calculate the congruence values of $A(\psi) \pmod 2$ and $B(\psi) \pmod{p^\gamma}$:

Calculation of $A(\psi) \pmod 2$

From (1.49), we obtain

$$A(\psi) \equiv \sum_{\pm x \bmod p^\gamma} \psi(x) \equiv \sum_{\substack{\pm\alpha \\ (\bmod p)}} \zeta^{-\alpha} \sum_{\beta=0}^{p^{\gamma-1}-1} z^{-\beta} \pmod 2 \qquad (1.51)$$

$$\equiv \sum^{+}_{\pm\alpha} \zeta^{-\alpha} \sum_{\beta=0}^{p^{\gamma-1}-1} z^{-\beta} \pmod 2$$

But

$$\sum^{+}_{\pm\alpha} \zeta^{-\alpha} = \frac{\zeta^{-\frac{p-1}{2}} - 1}{\zeta^{-1} - 1} = \frac{-\zeta(2)}{1-\zeta} \qquad (1.52)$$

since $\zeta^{-\frac{p-1}{2}} = \left(\frac{-m}{2}\right)^{\frac{p-1}{m}} = (-1)^{\frac{p-1}{m}} = -1$. If $m = 2^u \cdot n$, n odd, $n > 1$, then we claim that $1 - \zeta$ is a unit in Q_m and so by (1.52), we have

$$\sum^{+}_{\pm\alpha} \zeta^{-\alpha} \equiv 0 \pmod 2 \quad \text{for } m \neq 2^u. \qquad (1.53)$$

$1 - \zeta$ is a unit since $N_{Q_m}(1 - \zeta) = \prod_{(i,m)=1} (1 - \zeta^i) = \Phi_m(1)$. But

$$\Phi_m(x) \cdot \prod_{d|2^u} \Phi_d(x) \cdot \prod_{\substack{d|n \\ d\neq 1}} \Phi_d(x) \cdot \prod_{d|2^u n \atop d\neq 1, d\neq m, d\nmid 2^u, d\nmid n} \Phi_d(x) = (x^{2^u})^n - 1 =$$

$$(x^{2^u} - 1)(x^{2^u(n-1)} + x^{2^u(n-2)} + \ldots + x^{2^u} + 1)$$

and so after cancelling $\prod_{d|2^u} \Phi_d(x)$ and $x^{2^u} - 1$, we obtain that $\Phi_m(1) | 1$ since $\prod_{d|n, d\neq 1} \Phi_d(1) = n$. Therefore, $\Phi_m(1) = \pm 1$ and so $N_{Q_m}(1 - \zeta) = \pm 1$ which implies that $(1 - \zeta)$ is a unit in Q_m.

If, however, $m = 2^u$, then, as remarked in the proof of Theorem 1.1;B, $\mathfrak{Z} = 1 - \zeta$ is the only prime divisor of 2 in $Q_m = Q_{2^u}$ and from (1.52), it follows that

$$\sum_{\pm\alpha}^{+} \zeta^{-\alpha} \equiv 0 \pmod{\frac{2}{\mathfrak{Z}}}, \text{ but not } \pmod{\mathfrak{Z}}, \text{ for } m = 2^u \tag{1.54}$$

Furthermore, we have

$$\sum_{\beta=0}^{p^{\gamma-1}-1} z^{-\beta} = \begin{cases} 1 & \text{if } \gamma = 1 \\ 0 & \text{if } \gamma \geq 2. \end{cases} \tag{1.55}$$

We put (1.53), (1.54) and (1.55) into (1.51) to obtain

$$A(\psi) \equiv 0 \begin{cases} \pmod 2 & \text{for } n_\psi \neq 2^u \\ \pmod{\frac{2}{\mathfrak{Z}}}, \text{ but not } \pmod 2, & \text{for } n_\psi = 2^u. \end{cases} \tag{1.56}$$

We note that if $n_\psi = 2^u$, then $\gamma = 1$ as $n_\psi = mp^{\gamma-1}$. From (1.56), it follows by division of 2 that

$$\frac{1}{2} A(\psi) \equiv \begin{cases} 0 \pmod{+1} \text{ for } n_\psi \neq 2^u \\ \frac{+1}{2} \pmod{+1}, \text{ but not } \pmod{+1}, \text{ for } n_\psi = 2^u. \end{cases} \tag{1.57}$$

Calculation of $B(\psi) \pmod{p^\gamma}$.

From (1.49), we obtain

$$B(\psi) \equiv \sum_{\pm x \bmod p^\gamma} \psi(x) x \equiv -\sum_{\pm\alpha} \zeta^{-\alpha} g^\alpha \sum_{\beta=0}^{p^{\gamma-1}-1} z^{-\beta} (1+p)^\beta \pmod{p^\gamma} \tag{1.58}$$

We also have

$$-\sum_{\pm\alpha}^{+} \zeta^{-\alpha} g^\alpha = -\frac{(\zeta^{-1} g)^{\frac{p-1}{2}} - 1}{\zeta^{-1} g - 1} = \zeta \frac{g^{\frac{p-1}{2}} + 1}{g - \zeta}. \tag{1.59}$$

For $m \neq p-1$, $g - \zeta$ is prime to p for if not, then $p \mid N_{Q_m}(q - \zeta) = \Phi_m(g) \mid g^m - 1$ which contradicts g being a primitive root $\pmod p$. Also, $g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p^\gamma}$ and so by (1.59)

$$-\sum_{\pm\alpha} \zeta^{-\alpha} g^\alpha \equiv 0 \pmod{p^\gamma} \text{ for } m \neq p-1. \tag{1.60}$$

If $m = p-1$, we first note the equality

$$x^n - y^n = \prod_{i=0}^{n-1} (x - \xi^i y) \text{ where } \xi \text{ is a primitive } n\text{-th root of unity.}$$

Hence

$$g^{\frac{p-1}{2}} + 1 = g^{\frac{p-1}{2}} - \zeta_{p-1}^{\frac{p-1}{2}} = \prod_{0\le i<\frac{p-1}{2}} (g - \zeta_{p-1}^{2i}\,\zeta_{p-1}) = \prod_{0\le i<\frac{p-1}{2}} (g - \zeta_{p-1}^{2i+1}).$$

Hence, we have

$$-\sum_{\pm\alpha}^{+} \zeta^{-\alpha} g^{\alpha} = \frac{g^{\frac{p-1}{2}} + 1}{g - \zeta} = \zeta \prod_{u} (g - \zeta^{u}) \qquad (1.61)$$

where u runs through all odd numbers in the range $1 < u < p-1$.

Now, $N_{Q_m}(g - \zeta) = \Phi_m(g)$ and $\prod_{d|m} \Phi_d(g) = g^m - 1 = p^{\gamma} \cdot$ integer since $m = p - 1$. But $\Phi_d(g) \mid g^d - 1$ and so for $d < m$, $p \nmid \Phi_d(g)$. Hence, $p^{\gamma} \mid N_{Q_m}(g - \zeta)$. We let D denote the ring of integers of Q_m. Then $pD = pp'p'' \ldots$ (a product of $\phi(p-1)$ prime divisors) (see Ribenboim [20], p. 269) and so $\prod_{(u,m)=1} (g - \zeta^u)\, D = p^{\gamma}p'^{\gamma}p''^{\gamma} \ldots I$ where I is an ideal of D prime to pD. If $p \mid (g - \zeta^u)D$ and $(g - \zeta^v)D$ for $u \neq v$, then $p \mid \zeta^u(1 - \zeta^{v-u})D$, i.e. $p\,(1 - \zeta^{v-u})D$. But $1 - \zeta^{v-u}$ is a unit in $Q_m = Q_{p-1}$ unless $p - 1$ is a power of 2 (We saw this while calculating $A(\psi)$, in which case $(1 - \zeta^{v-u})D = (1 - \zeta)D$ is the unique prime ideal above 2 in D. Thus $p \nmid (1 - \zeta^{v-u})D$ since $p \neq 2$. Thus, since p (say) divides $(g - \zeta)D$ then, in fact, $p^{\gamma} \mid (g - \zeta)D$. The $\phi(p-1)$ elements of the Galois group of Q_m permute the $p, p', p'', \ldots$ and send $(g - \zeta)D$ into $(g - \zeta^u)D$ for $(u, p-1) = 1$. Hence, each ideal $(g - \zeta^u)D$, $(u, p-1) = 1$ is divisible by the γ-th power of one of $p, p', p'', \ldots$ but is relatively prime to the remaining

$\phi(p-1)-1$ prime ideals. Further, if u is odd and $(u, p-1) = d \neq 1$, then $(\frac{u}{d}, \frac{p-1}{d}) = 1$ and so $(g - \zeta^u) = g - \left(\zeta^d\right)^{\frac{u}{d}} = g - \zeta^{\frac{u}{d}}_{\frac{p-1}{d}}$. Therefore, $N_{Q_{\frac{p-1}{d}}}\left(g - \zeta^{\frac{u}{d}}_{\frac{p-1}{d}}\right) = \phi_{\frac{p-1}{d}}(g)$ which divides $g^{\frac{p-1}{d}} - 1$. Hence, $g - \zeta^u$ is prime to p since $g^{\frac{p-1}{d}} - 1$ is prime to p. Therefore, it follows from (1.61) that

$$-\sum_{\pm\alpha} \zeta^{-\alpha} g^{\alpha} \equiv 0 \mod p'^{\gamma} p''^{\gamma} \ldots, \text{ but prime to } p \text{ for } m = p-1. \tag{1.62}$$

In the special case $p = 3$, since $\frac{p-1}{m}$ is odd (because $\psi(-1) = -1$), it follows that $m = p - 1 = 2$. Then $Q_{p-1} = Q$ and hence $p = p$ is the only prime divisor of p. Hence (1.62) implies that

$$-\sum_{\pm\alpha} \zeta^{-\alpha} g^{\alpha} \text{ prime to } p \text{ for } p = 3. \tag{1.63}$$

(This is also clear without (1.62) because the sum is reduced to a single term 1.)

For $p \neq 3$, p has several prime divisors $p, p', \ldots$ in Q_{p-1}, and we shall see that the additional statement contained in (1.62) (that the sum considered is prime to p) will not be useful to us because we can conclude from it that the norm of the sum on the left hand side is only divisible by the norm of $p'^{\gamma} p''^{\gamma} \ldots$, that means only by $p^{\gamma(\phi(p-1)-1)}$.

Now for $\gamma \geq 2$, we have

$$\sum_{\beta=0}^{p^{\gamma-1}-1} z^{-\beta}(1+p)^{\beta} = \frac{(z^{-1}(1+p)^{p^{\gamma-1}}-1}{z^{-1}(1+p)-1} = z\left[\frac{(1+p)^{p^{\gamma-1}}-1}{1+p-z}\right]. \quad (1.64)$$

As was seen earlier in this proof, the numerator of this last expression is divisible by p^{γ} but not by $p^{\gamma+1}$. The denominator is divisible by the only prime divisor p of p (represented by $1 - z$) in the field $Q_{p^{\gamma-1}}$ but not by p^2. Thus the numerator equals kp^{γ} where $(k, p) = 1$ and the denominator as an ideal in $Q_{p^{\gamma-1}}$ equals $p \cdot J$ where J is an integral ideal of $Q_{p^{\gamma-1}}$ which is prime to p (and hence to p). Therefore, since the left hand side of (1.64) and $\frac{p^{\gamma}}{p}$ are both integral ideals, then $J|K$ and so we have

$$\sum_{\beta=0}^{p^{\gamma-1}-1} z^{-\beta}(1+p)^{\beta} \equiv 0 \pmod{\frac{p^{\gamma}}{p}} \text{ but not } \pmod{p^{\gamma}}. \quad (1.65)$$

For $\gamma = 1$, (1.65) holds trivially as the sum reduces to the single term 1 and $p = p$.

Putting (1.60), (1.62) and (1.65) into (1.58), we get

$$B(\psi) \equiv 0 \begin{cases} \pmod{p^{\gamma}} & \text{for } n_{\psi} \neq \phi(p^{\gamma}) \\ \pmod{\frac{p^{\gamma}}{p^*}} & \text{for } n_{\psi} = \phi(p^{\gamma}) \end{cases} \quad (1.66)$$

where p^* is the only prime divisor of p in $Q_{p-1}Q_{p^{\gamma-1}}$. We note that for $p = 3$, we have $B(\psi) \not\equiv 0 \pmod{p^{\gamma}}$ by (1.63) and (1.65), but for

$p \neq 3$ and $n_\psi = \phi(p^\gamma)$, $B(\psi)$ may or may not be congruent to 0 (mod p^γ). From (1.66), it follows by division by p^γ that

$$\frac{1}{p^\gamma} B(\psi) \equiv 0 \begin{cases} \pmod{+1} & \text{for } n_\psi \neq \phi(p^\gamma) \\ \pmod{+\frac{1}{p^*}}, \text{ but for } p = 3 \text{ not } \pmod{+1}, & \\ \text{for } n_\psi = \phi(p^\gamma). & \end{cases} \tag{1.67}$$

The results (1.57) and (1.67) yield by (1.50) a statement concerning the congruence values of H_ψ (mod +1) and, therefore, a statement on the denominator of H_ψ. Since in each case at most one prime divisor 2 of 2 and one prime divisor p^* of p is contained in this denominator, we obtain the following facts about the denominator of $N_\psi(H_\psi)$:

If ψ is a primitive character with odd prime power conductor $f(\psi) = p^\gamma$ $(p \neq 2)$, then $N_\psi(H_\psi)$ is a rational number whose denominator is at most $2p$.

The prime factor 2 occurs in the denominator precisely when ψ is of 2 power order $n_\psi = 2^u$; in this case, $\gamma = 1$ and 2^u is the highest power of 2 contained in $p - 1$.

The prime factor p occurs in the denominator at most in the case $n_\psi = \phi(p^\gamma)$; for $p = 3$, it really occurs.

Case II - We let ψ be a primitive character with conductor $f = f(\psi) = 2^\gamma$, $\gamma \geq 2$. (Note that the case $f = 2$ does not occur as the only character mod 2 is the unit character which has conductor 1). By induction on t,

easily seen to imply that $\psi(x + 2^{\gamma-1}) = -\psi(x)$. Thus the following quadruple

$$x,\ 2^{\gamma-1} - x,\ 2^{\gamma-1} + x,\ 2^{\gamma} - x$$

have corresponding character values

$$\psi(x),\ \psi(x),\ -\psi(x),\ -\psi(x).$$

As x runs through the smallest positive prime half system $\pmod{2^{\gamma-1}}$, this quadruple runs through the smallest positive prime system $\pmod{2^{\gamma}}$ and so by (1.36), we have

$$H_{\psi} = \frac{1}{2^{\gamma+1}} \sum_{\pm x \bmod 2^{\gamma-1}}^{+} (-\psi(x)[x + (2^{\gamma-1} - x) - (2^{\gamma-1} + x) - (2^{\gamma} - x)])$$

$$= \frac{1}{2} \sum_{\pm x \bmod 2^{\gamma-1}}^{+} \psi(x). \tag{1.70}$$

If, in the basis representation $x \equiv (-1)^{\alpha}(1 + 2^2)^{\beta} \pmod{2^{\gamma}}$, $0 \le \alpha < 2$, $0 \le \beta < 2^{\gamma-2}$, we restrict the domain of exponents to $\alpha = 0$ and $0 \le \beta < 2^{\gamma-3}$, then we obtain a quarter system $\pmod{2^{\gamma}}$. We then have

$$\sum_{\pm x \bmod 2^{\gamma-1}}^{+} \psi(x) \equiv \sum_{\beta=0}^{2^{\gamma-3}-1} \psi[(1 + 2^2)^{\beta}] \pmod{2}$$

and by (1.68)

$$\sum_{\beta=0}^{2^{\gamma-3}-1} \psi[(1 + 2^2)^{\beta}] = \sum_{\beta=0}^{2^{\gamma-3}-1} z^{\beta}.$$

it is easily seen that $(1 + 2^2)^{2^t} \equiv 1 \pmod{2^{t+2}}$ but $(1 + 2^2)^{2^t} \not\equiv 1 \pmod{2^{t+3}}$. From this, it easily follows that the order of $1 + 2^2$ is $2^{\gamma-2} \pmod{2^\gamma}$ for $\gamma \geq 2$. Then the $\phi(2^\gamma)$ numbers $(-1)^\alpha(1 + 2^2)^\beta$, $0 \leq \alpha < 2$, $0 \leq \beta < 2^{\gamma-2}$, are all incongruent $(\mathrm{mod}\ 2^\gamma)$ and, hence, form a complete set of representatives of the group $(\mathbb{Z}/2^\gamma\mathbb{Z})^*$.

If $x \equiv (-1)^\alpha(1 + 2^2)^\beta$ and if ψ is a primitive character $(\mathrm{mod}\ 2^\gamma)$ (we recall ψ is assumed to be odd), then ψ is given by

$$\psi(x) = (-1)^\alpha z^\beta \tag{1.68}$$

where z is a primitive $2^{\gamma-2}$-nd root of unity. (We note that a similar argument as for the odd prime power case shows z is a primitive $2^{\gamma-2}$-nd root of unity.)

So for $\gamma = 2$, $\psi = (-1)^\alpha$, $Q_{n_\psi} = Q$ and by (1.50), we obtain

$$H_\psi = \frac{1}{2} - \frac{1}{2^2} = \frac{1}{2^2}.$$

Hence, also, we have

$$N_\psi(H_\psi) = \frac{1}{2^2}. \tag{1.69}$$

For $\gamma \geq 3$, the order of ψ is $n_\psi = 2^{\gamma-2}$ and the field Q_{n_ψ} is the field $Q_{2^{\gamma-2}}$ of degree $\phi(2^{\gamma-2}) = 2^{\gamma-3}$ over Q. Now the congruence $u^2 \equiv 1 \pmod{2^\gamma}$ has the solution $u \equiv 1 + 2^{\gamma-1} \pmod{2^\gamma}$ and hence, $\psi(1 + 2^{\gamma-1}) = \pm 1$. But $\psi(1 + 2^{\gamma-1}) = 1$ leads to a contradiction since ψ is primitive $(\mathrm{mod}\ 2^\gamma)$ and so $\psi(1 + 2^{\gamma-1}) = -1$. This in turn is

Hence by (1.70)

$$H_\psi \equiv \frac{1}{2} \sum_{\beta=0}^{2^{\gamma-3}-1} z^{-\beta} \pmod{+1}. \qquad (1.71)$$

But we have

$$\sum_{\beta=0}^{2^{\gamma-3}-1} z^{\beta} = \frac{z^{2^{\gamma-3}} - 1}{z - 1} = \frac{-1 - 1}{z - 1} = \frac{-1}{1 - z}$$

and so by (1.71)

$$H_\psi \equiv 0 \pmod{+\tfrac{1}{2}}, \text{ but not } \pmod{+1}, \qquad (1.72)$$

where 2 is the only prime divisor (represented by $1 - z$) of 2 in the field $Q_{2^{\gamma-2}}$. By forming the norm one gets from (1.72)

$$N_\psi(H_\psi) \equiv 0 \pmod{+\tfrac{1}{2}}, \text{ but not } \pmod{+1}. \qquad (1.73)$$

By means of (1.69) and (1.73), we have the following facts about the denominator of $N_\psi(H_\psi)$ when ψ is primitive $(\bmod 2^\gamma)$, $\gamma \geq 2$:

$N_\psi(H_\psi)$ is a rational number whose denominator for $\gamma = 2$ is precisely 2^2, for $\gamma \geq 3$ is precisely 2. This completes the proof of Theorem 1.1; C. //

CHAPTER II

CYCLOTOMIC FIELDS OF CLASS NUMBER ONE

In this chapter, we shall determine exactly which cyclotomic fields have class number one. We will follow the paper by Masley and Montgomery, "Cyclotomic Fields with Unique Factorization". [16] The statement of the result follows.

Theorem 2.1 - There are precisely twenty-nine distinct cyclotomic fields Q_m, $m > 2$, with class number $h_m = 1$. They are given by $m = 3,4,5,7,8,9,11,12,13,15,16,17,19,20,21,24,25,27,28,32,33,35,36,40,44,45,48,60,84$.

One should keep in mind that we are assuming $m \not\equiv 2 \pmod 4$, as there are fifteen additional m with $m \equiv 2 \pmod 4$ such that $h_m = 1$; the fields Q_m which arise in this way are listed above as Q_{2m}.

We observe that the above gives the following

Corollary 2.1 - (Kummer's Conjecture) The prime cyclotomic field Q_p has class number $h_p = 1$ if and only if $p < 19$.

2.1 Analytic Lemmas

We assume throughout this section that $p > 200$, we let

$$f(s) = \sum_{\chi(-1)=-1} \text{Log } L(s,\chi) \tag{2.1}$$

where the sum is over all characters $\chi \pmod p$ with $\chi(-1) = -1$, and we write $s = \sigma + it$. Clearly $f(s)$ is multiple-valued, but for $\sigma > 1$ $\text{Log}(s,\chi)$ is defined as follows

$$\text{Log } L(s,\chi) = \sum_{\substack{k\in N \\ q\in P}} \chi(q)^k / kq^{ks} \tag{2.2}$$

where the sum is absolutely convergent. (see Serre [24], p.71 and p.74). Hence $f(s)$ is single-valued for $\sigma > 1$. Further, from known zero-free regions (see Estermann [8], Theorems 39, 40, 46 and Davenport [7], p. 99 with $c_{27} = \frac{1}{6}$) we have by easy calculations that the $L(s,\chi)$ do not vanish for

$$|s-1| \leq .2p^{-3} \qquad (2.3)$$

Thus, as zero is the branch point of the complex logarithm, $f(s)$ is single-valued in the union of this disc and the half-plane $\sigma > 1$. Our goal is to estimate $f(1)$. To this end we establish the following lemmas.

Lemma 2.1 - If $\sigma > 1$, then

$$f(\sigma) = \left(\frac{p-1}{2}\right) \sum_{n\equiv 1(p)}^{\infty} \frac{\Lambda(n)}{\log n} n^{-\sigma} - \left(\frac{p-1}{2}\right) \sum_{n\equiv -1(p)}^{\infty} \frac{\Lambda(n)}{\log n} n^{-\sigma}$$

where $\Lambda(n) = \log q$ if $n = q^t$, q prime, $t \geq 1$

$= 0$ otherwise.

Proof - By (2.2), we have that

$$f(\sigma) = \sum_{\chi(-1)=-1} \sum_{k,q} \chi(q)^k / kq^{k\sigma}$$

$$= \sum_{\chi(-1)=-1} \sum_{k,q} (\chi(q^k) \log q / \log (q^k) (q^k)^{\sigma})$$

$$= \sum_{\chi(-1)=-1} \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{(\log n) n^{\sigma}} = \sum_{n=1}^{\infty} \frac{\left[\sum_{\chi(-1)=-1} \chi(n)\right]\Lambda(n)}{(\log n) n^{\sigma}}$$

Thus, to finish the proof, it suffices to show that

$$\sum_{\chi(-1)=-1} \chi(k) = 0, \quad k \not\equiv \pm 1 \pmod{p} \tag{2.4}$$

$$= -\left(\frac{p-1}{2}\right), \quad k \equiv -1 \pmod{p}$$

$$= +\left(\frac{p-1}{2}\right), \quad k \equiv +1 \pmod{p}$$

Let χ_1 be the generator for the group of characters (mod p) and let g generate the group of non-zero, positive residues (mod p). Then $\chi_1(g) = \zeta$ where ζ is a primitive p-1 st root of unity. In addition, $\chi_1(-1) = -1$, for if $\chi_1(-1) = 1$ then the order of χ_1 would be $\frac{p-1}{2}$. We then have

$$\sum_{\chi(-1)=-1} \chi(k) = \sum_{m=1}^{\frac{p-1}{2}} \chi_1^{2m-1}(k) = \sum_{m=1}^{\frac{p-1}{2}} \chi_1^{2m-1}(g^r) \text{ (for some } r)$$

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

But since

$$\sum_{i=0}^{\frac{p-1}{2}-1} (\zeta^{2r})^i = \begin{cases} 0 & \text{if } \zeta^{2r} \neq 1 \\ \frac{p-1}{2} & \text{if } \zeta^{2r} = 1 \end{cases},$$

then

$$\sum_{\chi(-1)=-1} \chi(k) = \sum_{i=0}^{p-2} \zeta^{ri} = \begin{cases} 0 & \text{if } \zeta^{2r} \neq 1 \\ \frac{p-1}{2} & \text{if } \zeta^{2r} = 1 \end{cases}$$

$$= \begin{cases} 0 & \text{if } \zeta^r \neq 1 \\ p-1 & \text{if } \zeta^r = 1 \end{cases} - \begin{cases} 0 & \text{if } \zeta^{2r} \neq 1 \\ \frac{p-1}{2} & \text{if } \zeta^{2r} = 1 \end{cases}$$

$$= \begin{cases} 0 & \text{if } \zeta^r \neq 1 \\ p-1 - \left(\frac{p-1}{2}\right) & \text{if } \zeta^{2r} = 1 \text{ and } \zeta^r = 1 \\ 0 - \left(\frac{p-1}{2}\right) & \text{if } \zeta^{2r} = 1 \text{ and } \zeta^r = -1 \end{cases}.$$

But we have

(i) $1 \neq \zeta^{2r} = \chi_1^2(k) \iff k \not\equiv \pm 1 \pmod p$

(ii) $1 = \zeta^r = \chi_1(k) \iff k \equiv +1 \pmod p$

and (iii) $-1 = \zeta^r = \chi_1(k) \iff k \equiv -1 \pmod p$

and so we have (2.4). //

Lemma 2.2 - If $1 < \sigma \leq 2.5$ then $|f(\sigma)| \leq 3 + \log\left(\frac{p}{\sigma-1}\right)$.

Proof - By Lemma 2.1, we have that

$$f(\sigma) = \left(\frac{p-1}{2}\right) \sum_{\substack{n=1 \\ n\equiv 1(p)}}^{\infty} \frac{\Lambda(n)}{\log n} n^{-\sigma} - \left(\frac{p-1}{2}\right) \sum_{\substack{n=1 \\ n\equiv -1(p)}}^{\infty} \frac{\Lambda(n)}{\log n} n^{-\sigma}$$

$$= T_1 - T_2 \quad \text{(say)}$$

and so $-T_2 \leq f(\sigma) \leq T_1$. We bound T_2 and note that our argument may be modified to provide the same bound for T_1.

We will need the following result (see Montgomery and Vaughan [17], Theorem 2 with "x" of their notation equal to ½, say): if $x > p$ then

$$\pi(x;p,a) < \frac{2x}{(p-1)\log(\frac{x}{p})} \qquad (2.5)$$

where $\pi(x;p,a)$ equals the number of primes $q \leq x$ with $q \equiv a \pmod p$.

We first show that

$$\frac{p-1}{2} \sum_{q\equiv -1(p)} q^{-\sigma} = \frac{p-1}{2} \cdot \sigma \int_{pe^{2/3}}^{\infty} \frac{\pi(x;p,-1)}{x^{\sigma+1}}\, dx \qquad (2.6)$$

By labelling the ith prime congruent to -1 (p) by q_i, we get

$$\frac{1}{\sigma}\left(\frac{p-1}{2}\right) \sum_{q\equiv -1(p)} q^{-\sigma} = \frac{1}{\sigma}\left(\frac{p-1}{2}\right) \sum_{i=1}^{\infty} q_i^{-\sigma} \text{ and } \pi(q_i;p,-1) = i. \text{ Hence}$$

$$\frac{1}{\sigma}\left(\frac{p-1}{2}\right) \sum_{q\equiv -1(p)} q^{-\sigma} = \frac{1}{\sigma}\left(\frac{p-1}{2}\right) \left[\sum_{i=2}^{\infty} \left\{\frac{\pi(q_i;p,-1) - \pi(q_{i-1};p,-1)}{q_i^{\sigma}}\right\} + \frac{\pi(q_1;p,-1)}{q_1^{\sigma}}\right]$$

$$= \frac{1}{\sigma} \cdot \frac{p-1}{2} \sum_{i=1}^{\infty} \left\{\frac{\pi(q_i;p,-1)}{q_i^{\sigma}} - \frac{\pi(q_i;p,-1)}{q_{i+1}^{\sigma}}\right\}$$

$$= \frac{p-1}{2} \int_{q_1}^{\infty} \frac{\pi(x;p,-1)}{x^{\sigma+1}}\, dx \qquad \text{(by partial summation)}$$

$$= \frac{p-1}{2} \int_{pe^{2/3}}^{\infty} \frac{\pi(x;p,-1)}{x^{\sigma+1}}\, dx \qquad \text{(since } pe^{2/3} < q_1\text{)}$$

and so we have (2.6). But then by (2.5) and (2.6)

$$\frac{p-1}{2} \sum_{q\equiv -1(p)} q^{-\sigma} < \frac{p-1}{2} \cdot \sigma \int_{pe^{2/3}}^{\infty} \frac{2x}{(p-1)\log(\frac{x}{p})x^{\sigma+1}}\,dx$$

$$= \sigma p^{1-\sigma} \int_{e^{2/3}}^{\infty} \frac{1}{y^{\sigma}\log y}\,dy \qquad \text{(letting } y = \frac{x}{p}\text{)}$$

$$< \int_{2/3\,(\sigma-1)}^{\infty} \frac{e^{-w}}{w}\,dw \qquad \text{(letting } w = \log y^{\sigma-1}\text{; and}$$

observing that $\sigma p^{1-\sigma} < 1$)

$$< \int_{2/3\,(\sigma-1)}^{1} w^{-1}dw + \int_{1}^{\infty} e^{-w}\,dw \quad \text{(we note that } 0 < \tfrac{2}{3}(\sigma-1) \le 1\text{)}$$

$$= e^{-1} + \log \frac{3}{2(\sigma-1)}$$

Hence we have

$$\frac{p-1}{2} \sum_{q\equiv -1(p)} q^{-\sigma} < e^{-1} + \log \frac{3}{2(\sigma-1)} \qquad (2.7)$$

We will use (2.7) in combination with the following to obtain the lemma.

We let

$$\pi(x;q,a) = \sum_{\substack{n\le x \\ n\equiv a(q)}} \frac{\Lambda(n)}{\log n}$$

and we first show that

$$\Pi(x;p,a) - \pi(x;p,a) < \sum_{2\le k\le \log_2 x} \left(\frac{x}{p}^{1/k} + 1\right)(k,p-1)k^{-1} \qquad (2.8)$$

Now,

$$\Pi(x;p,a) - \pi(x;p,a) = \sum_{\substack{n\le x \\ n\equiv a(p)}} \frac{\Lambda(n)}{\log n} - \sum_{\substack{q\le x \\ q\equiv a(p) \\ q \text{ prime}}} 1$$

$$= \sum_{\substack{q^k<x, \\ q^k\equiv a(p) \\ q \text{ prime} \\ k>1}} \frac{1}{k} < \sum_{2\le k\le \log_2 x} \frac{v}{k}$$

where v is the number of primes q such that $q^k \equiv a\ (p)$ and $q^k \le x$ for a fixed k. We will establish an upper bound for v.

We let g be a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ and $q_1, \ldots, q_v$ be the primes satisfying the conditions:

$$q^k \equiv a \pmod p \quad \text{and} \quad q^k \le x, \quad \text{for a fixed } k.$$

Then there exists s_i, $0 \le s_i \le p-2$ such that $q_i \equiv g^{s_i} \pmod p$. To bound v, we shall "count" the number of s_i, $1 \le i \le v$. We first note that $q_i^k \equiv g^{s_i k} \equiv a \pmod p$, $\forall i$. Therefore $g^{s_i k} \equiv g^{s_j k} \pmod p$, $\forall i, j$ and so $ks_i \equiv ks_j \pmod{p-1}$, $\forall i, j$, i.e. $p-1 \mid (s_i - s_j)k$, $\forall i,j$.

If we let $d = (k, p-1)$ then $\frac{p-1}{d} \mid (s_i - s_j)$. Further, if we let $0 \le s_{i_1} < s_{i_2} \ldots < s_{i_r} < p-1$ be the distinct s_i's then

$$p-1 > r \min.(s_{i_\ell} - s_{i_{\ell-1}}) \geq r\left(\frac{p-1}{d}\right)$$

and hence $r < d$. We now see how many times each of the distinct s_i's can occur. We let $s = s_\ell$ be fixed and let t be the number of s_i's in the list $s_1, s_2, \ldots, s_v$ that are equal to s. We note that $s_i = s_j$ if and only if $q_i \equiv q_j \pmod p$ and so if we let q be the smallest prime in the list $q_1, \ldots q_v$ such that $q \equiv g^s \pmod p$ then $q, q+p, q+2p, \ldots, q+(m-1)p$ are the total number of possibilities for the q's congruent to $g^s \pmod p$, where $q+(m-1)p \leq x^{1/k}$ and $q+mp > x^{1/k}$.

Thus $m \leq \frac{x^{1/k}}{p} - \frac{q}{p} + 1 < \frac{x^{1/k}}{p} + 1$ and so $t \leq m < \frac{x^{1/k}}{p} + 1$. This upper bound for t is independent of the choice of subscript ℓ. Hence $v \leq r \cdot \max. t < d\left(\frac{x^{1/k}}{p} + 1\right) = (p-1,k)\left(\frac{x^{1/k}}{p} + 1\right)$ and so we have (2.8).

But

$$\sum_{2\leq k\leq \log_2 x}\left(\frac{x^{1/k}}{p} + 1\right)(p-1,k)\,k^{-1} \leq \sum_{2\leq k\leq \log_2 x}\left(\frac{x^{1/k}}{p} + 1\right)$$

$$\leq \frac{4\sqrt{x}}{p} + \log_2 x \qquad \text{(we show below that } \sum_{2\leq k\leq \log_2 x} x^{1/k} < 4\sqrt{x}\text{)}$$

$$< 4\frac{\sqrt{x}}{p} + 2\log x.$$

We note that

$$\sum_{2\le k\le \log_2 x} x^{1/k} = \sqrt{x} + \sqrt[3]{x} + \sqrt[4]{x} + \ldots,$$

$$< \sqrt{x} + \sqrt[3]{x}\ (\log_2 x - 2)$$

$$= \sqrt{x} + \sqrt{x}\left(\frac{\log_2 x - 2}{\sqrt[6]{x}}\right)$$

$$< \sqrt{x} + 3\sqrt{x}\ \left(\text{as max. } f(x) = \frac{\log_2 x - 2}{\sqrt[6]{x}} < 3\right)$$

$$= 4\sqrt{x}$$

Therefore, we have

$$\Pi(x;p,a) - \pi(x;p,a) < \frac{4\sqrt{x}}{p} + 2\log x. \qquad (2.9)$$

We recall formula (2.6)

$$\left(\frac{p-1}{2}\right)\sigma\int_p^\infty \frac{\pi(x;p,-1)}{x^{\sigma+1}}\,dx = \left(\frac{p-1}{2}\right)\sum_{q\equiv -1(p)} q^{-\sigma}$$

In a similar manner, we have

$$\left(\frac{p-1}{2}\right)\sigma\int_p^\infty \frac{\Pi(x;p,-1)}{x^{\sigma+1}}\,dx = \left(\frac{p-1}{2}\right)\sum_{\substack{n=1\\ n\equiv -1(p)}}^{\infty} \frac{\Lambda(n)}{\log n}\, n^{-\sigma}$$

Therefore we have

$$\frac{p-1}{2}\sum_{\substack{n=1\\ n\equiv -1(p)}}^{\infty} \frac{\Lambda(n)}{\log n}\, n^{-\sigma} < \frac{p-1}{2}\sum_{q\equiv -1(p)} q^{\sigma}$$

$$= \sigma \frac{p-1}{2} \int_p^\infty \frac{\pi(x;p,-1) - \pi(x;p,-1)}{x^{\sigma+1}} \, dx$$

$$< \frac{p-1}{2} \int_p^\infty (4\sqrt{x}\, p^{-1} + 2 \log x) x^{-2} dx \qquad \text{(by (2.9) and since}$$

$$\frac{\sigma}{x^{\sigma+1}} < \frac{1}{x^2} \text{ for } \sigma > 1)$$

$$< p \int_p^\infty (2\sqrt{x}\, p^{-1} + \log x) x^{-2} dx$$

$$< \frac{7}{5} + \log p.$$

But then by (2.7)

$$T_2 - (e^{-1} + \log \frac{3}{2(\sigma-1)}) < \frac{7}{5} + \log p$$

and so $$T_2 < 3 + \log \frac{p}{\sigma-1}.$$

Hence the proof of the lemma is complete. //

Lemma 2.3 - Let $\sigma_0 = 1 + p^{-3}$. Then $\operatorname{Re} f(s) < \frac{1}{2} p \log p$ for

$$|s - \sigma_0| \leq 2 p^{-3} \qquad (2.10)$$

Proof - It is easily seen by partial summation that for $\sigma > 0$

$$L(s,\chi) = s \int_1^\infty S(u) u^{-s-1} du$$

where $S(u) = \sum_{n \le u} \chi(n)$. Now $S(u)$ reduces to a sum of at most $\frac{p-1}{2}$ p-th roots of unity since χ is odd and since $\sum_{\substack{n=r \\ r \equiv 1 (p)}}^{r+p-2} \chi(n) = 0$. (See Borevich and Shafarevich [4], p. 418).

Therefore

$$|S(u)| \le \frac{p-1}{2} < \frac{p}{2}$$

and so

$$|L(s,\chi)| \le |s| \int_1^\infty |S(u)| \, |u^{-s-1}| \, du$$

$$< \frac{1}{2} p \, |s| \int_1^\infty |u^{-s-1}| \, du = \frac{1}{2} p \, |s| \int_1^\infty u^{-\sigma-1} \, du$$

$$= \frac{p|s|}{2\sigma}$$

Now, in the disc under consideration, $\frac{|s|}{2\sigma} < 1$ and so

$$|L(s,\chi)| < p$$

in this disc.

Hence $\operatorname{Re} \operatorname{Log} L(s,\chi) < \log p$ and therefore

$$\operatorname{Re} f(s) = \sum_{\chi(-1)=-1} \operatorname{Re}(\log L(s,\chi)) \le \sum_{\chi(-1)=-1} \log p \le \frac{1}{2} p \log p. \quad //$$

Lemma 2.4 - With σ_0 as above, if $1 \le \sigma \le \sigma_0$ then $|f'(\sigma)| \le 4p^4 \log p$

Proof - The disc (2.10) lies in the union of the disc (2,3) and the half-plane $\sigma > 1$, so $g(s) = f(s) - f(\sigma_0)$ is regular for s satisfying (2.10). Now, assuming s does satisfy 2.10, we have

$$\begin{aligned} \operatorname{Re} g(s) &= \operatorname{Re} f(s) - \operatorname{Re} f(\sigma_0) \\ &\leq \tfrac{1}{2}p \log p + 3 + \log \frac{p}{\sigma_0 - 1} \quad \text{(by lemma (2.2) and (2.3))} \\ &= \tfrac{1}{2}p \log p + 3 + 4 \log p \leq p \log p. \end{aligned}$$

We need the following result:

Let $r > S$, $k(z) = \sum_{n=1}^{\infty} b_n \left(\frac{z-a}{S}\right)^n$ for $|z-a| < r$, and $\operatorname{Re} k(z) \leq M$ for $|z-a| = S$.

Then $|b_n| \leq 2M$ $(n = 1,2,3,\ldots)$.

(The proof of this result is essentially the same as the proof of Theorem 7, Estermann [8]).

We use this result to show that if $h(z)$ is regular in a domain containing the disc $|z-a| \leq R$, if $h(a) = 0$, and if $\operatorname{Re} h(z) \leq M$ in the disc then $|h'(z)| \leq \frac{8M}{R}$ in $|z-a| \leq \frac{1}{2}R$.

Since $h(z)$ is regular in a domain containing the disc $|z-a| \leq R$, then in this domain we may write

$$h(z) = \sum_{n=0}^{\infty} c_n (z-a)^n$$

where $c_0 = h(a) = 0$. (see Churchill [6], p. 129). But then

$$h(z) = \sum_{n=1}^{\infty} b_n \left(\frac{z-a}{R}\right)^n$$

where $c_n = \frac{b_n}{R^n}$. Here we have $\operatorname{Re} h(z) \leq M$ for $|z-a| = R$ and so, by the above, $|b_n| \leq 2M$ $(n = 1,2,3,\ldots)$.

But $h'(z) = \sum_{n=1}^{\infty} n b_n \left(\frac{z-a}{R}\right)^{n-1} \frac{1}{R}$

$$\therefore \quad |h'(z)| \leq \sum_{n=1}^{\infty} 2Mn\,(\tfrac{1}{2})^{n-1} \frac{1}{R} \quad \text{for } |z-a| \leq \tfrac{1}{2}R$$

$$= \frac{4M}{R}\left(\sum_{n=1}^{\infty} \frac{n}{2^n}\right) = \frac{8M}{R}.$$

Applied to $g(s)$, this gives $|g'(s)| \leq 4p^4 \log p$ for $|s-\sigma_0| \leq p^{-3}$. But $f'(s) = g'(s)$ and $|\sigma-\sigma_0| \leq p^{-3}$, so we are done. //

2.2 Kummer's Conjecture

We now use the formula

$$h_p^* = p^{\frac{p+3}{4}} 2^{\frac{p-3}{2}} \prod^{\frac{p-1}{2}} \prod_{\chi(-1)=-1} L(1,\chi)$$

to estimate h_p^*. From this formula and the lemmas of the previous section we derive

Theorem (2.2) - If $p > 200$ then

$$\log h_p^* = \frac{p}{4}\log p - \frac{p}{2}\log 2\pi + (\frac{3}{4} + 7\theta)\log p,$$

where $-1 < \theta < 1$.

Proof - By (1.30),

$$\log h_p^* = \frac{p+3}{4}\log p - \frac{p-3}{2}\log 2 - \frac{p-1}{2}\log\pi + f(1)$$

where $f(s)$ is given by (2.1).

We are finished if we show,

$$|\frac{3}{2}\log 2 + \frac{1}{2}\log\pi + f(1)| < 7\log p$$

we actually show the stronger inequality,

$$\frac{3}{2}\log 2 + \frac{1}{2}\log\pi + |f(1)| < 7\log p$$

By the mean value theorem,

$$f(1) = f(\sigma) - f'(\gamma)(\sigma-1)$$

fow some γ, $1 < \gamma < \sigma$; so that if $\sigma \leq \sigma_0$ then

$$|f(1)| \leq 3 + \log\frac{p}{\sigma-1} + 4(\sigma-1)p^4\log p,$$

by Lemmas (2.2) and (2.4). We take $\sigma = 1 + p^{-5}$, and the desired result follows, since for $\sigma = 1 + p^{-5}$

$$|f(1)| \leq 3 + 6\log p + \frac{4\log p}{p}$$

and $\frac{3}{2}\log 2 + \frac{1}{2}\log \pi + 3 + \frac{4\log p}{p} < \log p$ for $p > 200$. //

Corollary (2.2) - We have $h_p^* = 1$ if and only if $p \leq 19$. Moreover, $h_p^* \leq 10^{20}$ if and only if $p \leq 131$.

Proof - The least prime $p > 200$ is $p = 211$ and from Theorem (2.2) we see that $h_p^* > 10^{20}$ for $p \geq 211$. The numbers h_p^*, $3 \leq p \leq 200$ have been calculated independently by Schrutka [23] and M. Newman [19]. (see Table 1 in Appendix A) and in shorter ranges by Kummer [13], [13'] and Hasse [10]. (It has been found that three values given by Kummer are incorrect; see [19].) From the table, we find that $h_p^* = 1$ precisely when $p \leq 19$ and that $h_p^* < 10^{20}$ precisely when $p \leq 131$.

2.3 Divisibility Properties of h_m^* -

In this section we establish some divisibility properties of h_m^* and use then to determine those m for which $h_m^* = 1$.

We restate formula (1.37) for h_m^*. Let $\overline{X}$ be the group of characters mod m. For each cyclic subgroup of $\overline{X}$ choose a generator χ, let $\psi \pmod{f(\psi)}$ be the primitive character which induces χ, and let n_ψ be the order of ψ. Let $\mathcal{P}$ be the set of such ψ with $\psi(-1) = -1$. Let N_ψ be the norm map $N_\psi : \mathbb{Q}_{n_\psi} \to \mathbb{Q}$, and put

$$H_\psi = \frac{-1}{2f(\psi)} \sum_{x \pmod{f(\psi)}} x\psi(x)$$

Then

$$h_m^* = Ew \prod_{\psi G \chi} N_\psi(H_\psi) \qquad (1.37)$$

where $E = 1$ if m is a prime power and $E = 2$ otherwise, and w is the number of roots of unity in Q_m, $w = 2m$ if m is odd, $w = m$ if m is even. We shall also use the properties of the $N_\psi(H_\psi)$ which we proved in Section (1.8).

Lemma (2.5) - If $m|n$ then $h_m^*|h_n^*$

Proof - It clearly suffices to prove that for $(p,m) = 1$ we have $h_m^*|h_{mp}^*$ and $h_{mp^\alpha}^*|h_{mp^{\alpha+1}}^*$ for $\alpha \geq 1$. Let $h_b^* = (Ew)_b \Pi_b$ be a shorthand notation for (1.37). Then

$$\frac{h_{mp}^*}{h_m^*} = \frac{(Ew)_{mp}\,\Pi_{mp}}{(Ew)_m\,\Pi_m} \qquad (2.11)$$

If m is a prime power, $\frac{(Ew)_{mp}}{(Ew)_m} = 2p$ by calculation. It is also clear by the construction that $\frac{\Pi_{mp}}{\Pi_m} = \prod_{p|f_\psi} N_\psi(H_\psi)$. Hence (2.11) becomes $2p \prod_{p|f(\psi)} N_\psi(H_\psi)$ which belongs to Z by Theorem 1, parts (A) and (C).

If at least two distinct primes q and r divide m, then $\frac{(Ew)_{mp}}{(Ew)_m} = p$ by calculation. Further, we again have

$\frac{\Pi_{mp}}{\Pi_m} = \prod_{p|f(\psi)} N_\psi(H_\psi)$ but in this product we have a factor where p, q and r divide f_ψ and n_ψ is a power of 2. That is, ψ is a character of type B)i) in Theorem 1.1. Such a ψ is given for example by $\psi(z) = \gamma_p(z)\gamma_q(z)\gamma_r(z)$ for $(z,pqr) = 1$ where γ_2 is the quadratic character mod 4 and $\gamma_t = \chi_t^{\frac{t-1}{2u}}$ with χ_t a generator of the group of characters mod t, $2^u \| t-1$ if t is an odd prime. We note that ψ is a primitive character (mod pqr) as it is the product of primitive characters of moduli p, q and r. It is immediate that $\psi(-1) = -1$ and that n_ψ is a power of 2.

Hence (2.11) becomes

$$\frac{h^*_{mp}}{h^*_m} = p \prod_{p|f(\psi)} N_\psi(H_\psi)$$

$$= p \text{ (element of } \frac{1}{2p}\mathbb{Z}) \text{ (element of } 2\mathbb{Z})$$

by Theorem 1.1, parts A), B)i) and C), and hence belongs to $\mathbb{Z}$.

We now consider

$$\frac{h^*_{mp^{\alpha+1}}}{h^*_{mp^\alpha}} = \frac{(Ew)_{mp^{\alpha+1}} \Pi_{mp^{\alpha+1}}}{(Ew)_{mp^\alpha} \Pi_{mp^\alpha}} \qquad (2.12)$$

For p odd, or $\alpha > 1$, $\dfrac{(Ew)_{mp^{\alpha+1}}}{(Ew)_{mp^{\alpha}}} = p$ and by construction

$$\frac{\Pi_{mp^{\alpha+1}}}{\Pi_{mp^{\alpha}}} = \prod_{p^{\alpha+1} \mid f(\psi)} N_{\psi}(H_{\psi}).$$

When p is odd, this product is an element of $\frac{1}{p}\mathbb{Z}$ by Theorem 1.1, parts A), C)i) and C)iii). When $p = 2$, the product is an element of $\frac{1}{2}\mathbb{Z}$ by Theorem 1.1, parts A) and C)ii).

Hence (2.12) becomes

$$p \text{ (element of } \tfrac{1}{p}\mathbb{Z}),$$

which belongs to $\mathbb{Z}$.

If $p^{\alpha} = 2$ and m is a prime power, we first note that

$$\frac{h^*_{4m}}{h^*_{2m}} = \frac{h^*_{4m}}{h^*_{m}} \text{ since } h^*_{m} = h^*_{2m} \text{ as } m \text{ is odd. Now, } \frac{(Ew)_{4m}}{(Ew)_{m}} = 4 \text{ and}$$

$$\frac{\Pi_{4m}}{\Pi_{m}} = \prod_{4 \mid f(\psi)} N_{\psi}(H_{\psi}) \text{ belongs to } \tfrac{1}{4}\mathbb{Z} \text{ by Theorem 1.1, parts A) and C)ii).}$$

Hence (2.12) becomes

$$4 \text{ (element of } \tfrac{1}{4}\mathbb{Z}).$$

If $p^\alpha = 2$ and m is not a prime power, then $\frac{(Ew)_{4m}}{(Ew)_m} = 2$ and

$\frac{\Pi_{4m}}{\Pi_m} = \prod_{4|f(\psi)} N_\psi(H_\psi)$. In this product we get a factor where ψ is of type B)i), as described above, and so (2.12) becomes

$$= 2 \text{ (element of } \tfrac{1}{4}\mathbb{Z}) \prod_{\substack{4|f(\psi) \\ \psi \neq \gamma_2}} N_\psi(H_\psi)$$

$$= \tfrac{1}{2} \text{ (element of } 2\mathbb{Z}) \text{ by Theorem 1.1, parts A), B)i)}$$

and C)ii) and hence belongs to $\mathbb{Z}$. //

We note that it is known that $m|n$ implies $h_m^+|h_n^+$, and also $h_m|h_n$. [See Ankeny, Hasse, Chowla [1], Theorem 2].

Lemma 2.6 - If four distinct primes divide m, then $4|h_m^*$.

Proof - By Lemma 2.5 it suffices to show that h^*_{pqrs} and h^*_{4pqr} are divisible by 4 for distinct odd peimes p, q, r and s. For $m = pqrs$, $w = 2pqrs$ and by Theorem 1.1, part C), the product of the non-integral factors in Π_m has denominator (in lowest terms) at most $2p \cdot 2q \cdot 2r \cdot 2s = 8w$. For $m = 4pqr$, $w = 4pqr$ and by Theorem 1.1, part C), the product of the non-integral factors in Π_m has denominator (in lowest terms) at most $2p \cdot 2q \cdot 2r \cdot 4 = 8w$. The factor w is cancelled

automatically in $h_m^* = (Ew)_m \Pi_m$. Now for each divisor of m which consists of exactly three primes a, b, c we have the character $\psi = \gamma_a\gamma_b\gamma_c$ of type B)i). (See proof of Lemma 2.5 above). Hence the integral part of Π_m for $m = pqrs$ or $m = 4pqr$ has at least $\binom{4}{3} = 4$ factors of 2. Since $E = 2$ for both cases, then $h_m^* = (Qw)_m \Pi_m$ is divisible by 4. //

We now determine when $h_m^* = 1$.

Lemma 2.7 - If $h_{p^\alpha}^* = 1$ and $\alpha > 1$ then $p^\alpha = 2^2, 2^3, 2^4, 2^5, 3^2, 3^3,$ or 5^2.

Proof - By Lemma 2.5 and Corollary 2.2, we may restrict our attention to $p \leq 19$. In the tables of h_m^* (see Appendix A), we find that $h_m^* = 1$ for the values of m listed above and that $h_m^* > 1$ for $m = 2^6, 3^4, 5^3, 7^2$ and 13^2. As in Masley [14], we complete the proof by showing that $h^*_{17^2}$ and $h^*_{19^2}$ are not 1.

We first show that $h^*_{17^2} \neq 1$. Since $h^*_{17} = 1$, then

$$h^*_{17^2} = \frac{h^*_{17^2}}{h^*_{17}} = 17 \prod_{\substack{17^2 \mid f(\psi) \\ \psi(-1)=-1}} N_\psi(H_\psi) = 17 \prod_{\substack{f(\psi)=17^2 \\ \psi(-1)=-1}} N_\psi(H_\psi)$$

where the product is over the generators ψ of each cyclic subgroup of $\overline{X}$ (the group of characters (mod 17^2)) with ψ odd and of

conductor 17^2. Now the group of characters of $(\mathbb{Z}/17^2\mathbb{Z})^*$ is cyclic since $(\mathbb{Z}/17^2\mathbb{Z})^*$ is cyclic (see Apostol [2], p. 209). Therefore, a generator ψ_1 of the group of characters of $(\mathbb{Z}/17^2\mathbb{Z})^*$ must necessarily have conductor 17^2 since its order is $16 \cdot 17$. Further, ψ_1 is odd since Q_{17^2} is complex. Now, it is straightforward to show that any other odd primitive character with conductor 17^2 is in the same orbit as ψ_1. Hence, we have

$$h^*_{17^2} = 17 N_\psi(H_\psi) \tag{2.13}$$

where ψ is a representative of the orbit of the odd characters of order $16 \cdot 17$ and conductor 17^2.

We let ζ be a primitive 17-th root of unity. Then

$$\begin{aligned} N_\psi(1 - \zeta) &= N_{Q_{16\cdot 17}}(1 - \zeta)) \\ &= N_{Q_{17}/Q}(N_{Q_{16\cdot 17}/Q_{17}}(1 - \zeta)) \\ &= N_{Q_{17}/Q}((1 - \zeta)^{[Q_{16\cdot 17}:Q_{17}]}) \\ &= N_{Q_{17}/Q}((1 - \zeta)^8) = 17^8. \end{aligned}$$

But then by (2.13)

$$N_\psi((1 - \zeta)H_\psi) = N_\psi(1 - \zeta)N_\psi(H_\psi) = 17^8 \frac{h^*_{17^2}}{17} = 17^7 h^*_{17^2}.$$

Now in Appendix B, we see that

$$N_\psi((1 - \zeta)H_\psi) \equiv 5 \pmod 7$$

Therefore, since $17^7 \equiv 3 \pmod 7$, we have

$$3h^*_{17^2} \equiv 5 \pmod 7$$

and so $h^*_{17^2} \neq 1$.

Now we show that $h^*_{19^2} \neq 1$. We will simplify our computations by using the result that if $K \subset L \subset Q_{p^2}$, then $h^*_K | h^*_L$ (see Uchida [25], Lemma 9). The Galois group of Q_{19^2}/Q is cyclic of order $19 \cdot 18$ and, hence, there exists a unique subgroup H of $(Z/19^2Z)^*$ of order 9. Its fixed field K is of order $\frac{19 \cdot 18}{9} = 38$ over Q. Now since $K \subset Q_{19^2}$ then, by the above, $h^*_K | h^*_{19^2}$. Hence, it suffices to show that $h^*_K \neq 1$.

We let χ be a generator of the cyclic group of characters of $(Z/19^2Z)^*$. Then χ must be odd with conductor 19^2 and so χ^9 has order 38 and is also odd. Further, using the fact that $(9, 19^2) = 1$, we can easily show that the conductor of χ^9 is 19^2. Now χ^9 is trivial on the subgroup H since H is of order 9, and so χ^9 is a character of K. But χ^9 is of order 38 and so it generates the cyclic group of characters of K. So we have that there are only two odd orbits of the character group of K; namely, the orbit with representative χ^9 ($= \psi$, say) and the orbit with representative ψ^{19}. Hence, by formula (1.37)

$$h^*_K = Ew(N_\psi(H_\psi)) \cdot (N_{\psi^{19}}(H_{\psi^{19}})).$$

But K is imaginary of conductor 19^2 and hence $E = 1$ (see Hasse [10], p. 68, Satz 23). We next show that $w = 2$. Any root of unity in K must be contained in Q_{19^2}. Therefore, any root of 1 in K must be contained in Q_{19^2}. Therefore, any root of 1 in K is a 19^2-th root of 1 or the negative of a 19^2-th root of 1, fixed by H. We let g be a primitive root (mod 19) which is also a primitive root (mod 19^2) (see Apostol [2], p. 209). Then the Galois group of Q_{19^2}/Q equals $\{\sigma_{g_i} | 0 \leq i \leq 19 \cdot 18 - 1\}$ where $\sigma_{g_i} : \zeta_{19^2} \to \zeta_{19^2}^{g^i}$. Therefore, $H = \{\sigma_{g^{38i}} | 0 \leq i \leq 8\}$, the group generated by $\sigma_{g^{38}}$, and so for any 19^2-th root of unity in K, $\zeta_{19^2}^n$ say, we have

$$\sigma_{g^{38}}(\zeta_{19^2}^n) = \zeta_{19^2}^n$$

$$\text{i.e. } \zeta_{19^2}^{g^{38}n} = \zeta_{19^2}^n \quad \text{i.e. } \zeta_{19^2}^{n(g^{38}-1)} = 1.$$

Therefore, $19^2 | n(g^{38} - 1)$. But $g^{38} \not\equiv 1 \pmod{19}$ and so $19^2 \nmid g^{38} - 1$. Therefore, $19^2 | n$ and so $\zeta_{19^2}^{g^{38}n} = \zeta_{19^2}^n = 1$. Thus, the only roots of 1 in K are ± 1 and so $w = 2$.

Now in Appendix B, we see that $N_\psi(H_\psi) \equiv 6 \pmod{11}$ (we note that in the computations for $N_\psi(H_\psi)$, we actually used $\psi' = \chi^{9 \cdot 17}$ which is in the same orbit as ψ) and that $N_{\psi_{19}}(H_{\psi_{19}}) = \frac{1}{2}$. Therefore, $h_K^* \equiv 6 \pmod{11}$ so $h_K^* \neq 1$ and hence $h_{19^2}^* \neq 1$. //

Theorem 2.3 - Suppose that $m \not\equiv 2 \pmod 4$. Then $h_m^* = 1$ if and only if $m = 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60,$ or 84.

Proof - Corollary 2.2, Lemma 2.5 and Lemma 2.6 show that if $h_m^* = 1$, then $m = p_1^{a_1} p_2^{a_2} p_3^{a_3}$ where p_1, p_2, p_3 are primes ≤ 19 and a_1, a_2, a_3 are non-negative integers. Further, Lemma 2.7 shows that $p_i^{a_i} \leq 32$, $i = 1, 2, 3$. Now for m of this type with $\phi(m) \leq 256$, we can use the tables of Schrutka [23] or Appendix A (if $m \leq 200$) to find h_m^*. Other possible cases for m with $\phi(m) > 256$ can be handled by using formula (1.37) and Theorem 1.1. (See, for example, the calculations for $h_{17\cdot 19}^*$ in the proof of Theorem 3.2.) By this process, we have our result. //

2.4 Determination of h_m^+

In this section, we determine those cyclotomic fields with class number one by showing that $h_m^+ = 1$ whenever $h_m^* = 1$.

We shall need the following Lemmas:

Lemma 2.8 - Let K be a finite algebraic number field and L/K a Galois extension of degree a power of a prime p. Suppose that exactly one prime of K is ramified in L. Then $p|h_L$ only if $p|h_K$, where h_K and h_L are the class numbers of K and L, respectively.

This is the content of Theorem 3 and 4 of Yokoyama [27]. Iwasawa [12] established the special case of Lemma 2.8 in which L/K is a cyclic extension and the ramified prime is fully ramified. We omit the proof of this Lemma as the methods used by Yokoyama are beyond the scope of this report.

Lemma 2.9 - Let p be an odd prime, L/K an abelian extension of type (2, 2) and h_L and h_K the class numbers of L and K, respectively. Then $p|h_L$ implies that p divides the class number of at least one of the three proper intermediate fields between L and K.

Proof - Let $G = \{1, \sigma, \tau, \sigma\tau\}$ be the Galois group of L/K and let L_t be the fixed field of $\{1, t\}$ for $t = \sigma, \tau, \sigma\tau$. For any field F, let S_p denote the p-Sylow subgroup of C_F, the ideal class group of F.

Assume first that $p|h_K$. We shall show that then $p|h_{L_t}$ for $t = \sigma, \tau, \sigma\tau$. $p|h_K$ implies that the class of some K-ideal a has order p in C_K (see Rotman [21], p. 85). Now $p \nmid h_{L_t}$ implies that there exists $S, q \in \mathbb{Z}$ such that $pS + h_{L_t} q = 1$. Then, letting D_{L_t} be the ring of integers of L_t, we have

$$(aD_{L_t})^1 = (aD_{L_t})^{pS}(aD_{L_t})^{qh_{L_t}}$$

$$= (a^p D_{L_t})^S (aD_{L_t})^{h_{L_t} q}$$

and so clearly, a is principal as an L_t-ideal. Since L_t/K is of degree 2, we have $N(aD_{L_t}) = a^2$ and so a^2 is equivalent to a principal K-ideal as aD_{L_t} is principal. That is, the class of a has order 2 in C_K which is a contradiction since the class of a was assumed to have order p. Hence $p|h_{L_t}$ for $t = \sigma, \tau, \sigma\tau$.

Hence, we may assume that $p \mid h_K$. G acts on C_L and on S_L in the natural way (for $\sigma \in G$ and an ideal a, $\sigma(a) = \{\sigma(\alpha) \mid \alpha \in a\}$). Squaring is an automorphism of the abelian group S_L since S_L has odd order. Consequently, $x^2 = b$ has a unique solution $x = b^{\frac{1}{2}}$ for any $b \in S_L$ and we may extend the action of G on S_L linearly to an action of $D = (\mathbb{Z}[\frac{1}{2}])[G]$ on S_L. We write this action exponentially. For example, for $b \in S_L$, $b^{\frac{1+\sigma}{2}} = b^{\frac{1}{2}} \cdot b^{\frac{\sigma}{2}}$ where $b^{\frac{\sigma}{2}}$ is the solution of $x^2 = b^{\sigma}$ in S_L.

Let $2\varepsilon_t^{\pm} = 1 \pm t$ for $t = \sigma, \tau, \sigma\tau$. Then $\varepsilon_t^{\pm} \in D$. For a subgroup H of S_L, $\alpha \in D$, let $H^{\alpha} = \{h \in H \mid h^{\alpha} = h\}$ be the subgroup of H fixed by α. Since $1 = \varepsilon_\sigma^+ + \varepsilon_\sigma^-$ is a decomposition of 1 into orthogonal idempotents, $S_L = S_L^{\varepsilon_\sigma^+} \times S_L^{\varepsilon_\sigma^-}$ is a direct product decomposition of S_L. In a similar manner, using $1 = \varepsilon_\tau^+ + \varepsilon_\tau^-$, we decompose the subgroups $S_L^{\varepsilon_\sigma^+}$ and $S_L^{\varepsilon_\sigma^-}$ and get

$$S_L = S_L^{+,+} \times S_L^{+,-} \times S_L^{-,+} \times S_L^{-,-} \tag{2.14}$$

where, for example, $S_L^{+,-} = \{b \in S_L \mid b^{\varepsilon_\sigma^+} = b^{\varepsilon_\tau^-} = b\}$. The norm map of C_L to C_{L_σ}, say, restricts to

$$N_{L/L_\sigma} : S_L^{+,-} \to S_{L_\sigma} \subset C_{L_\sigma}.$$

Now for $b \in S_L^{+,-}$, $N_{L/L_\sigma}(b) = b \cdot b^{\sigma} \in C_{L_\sigma}$ where $b \cdot b^{\sigma} D_{L_\sigma} = 1(b) \cdot \sigma(b) = b^{1+\sigma} = b^{2\varepsilon_\sigma^+} = b^2$ since $b^2 \in S_L^{+,-}$. Now if b is in the principal class

in C_{L_σ}, then $b^{D_L} = b^2$ is principal in $S_L^{+,-}$. But $S_L^{+,-}$ has odd order and so b is principal in $S_L^{+,-}$. Hence, this restriction is a monomorphism. In a similar manner, we obtain embeddings

$$N_{L/K} : S_L^{+,+} \to C_K,$$

$$N_{L/L_\tau} : S_L^{-,+} \to C_{L_\tau},$$

and $$N_{L/L_{\sigma\tau}} : S_L^{-,-} \to C_{L_{\sigma\tau}},$$

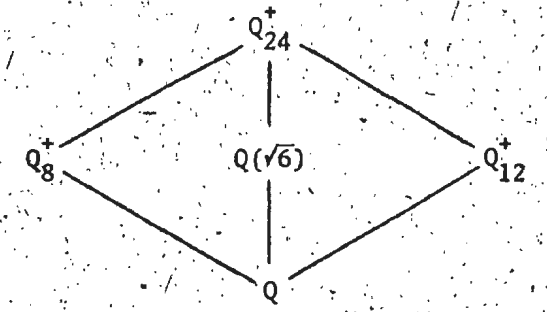
where we observe that $\varepsilon_\sigma^- \varepsilon_\tau^- = \varepsilon_{\sigma\tau}^+ \varepsilon_\tau^- = \varepsilon_{\sigma\tau}^+ \varepsilon_\sigma^-$. The group C_K has order h_K prime to p by assumption so $S_L^{+,+}$ must be trivial. By hypothesis, S_L is non-trivial so by (2.14), at least one of $S_L^{+,-}$, $S_L^{-,+}$, and $S_L^{-,-}$ is non-trivial. This provides an element of order p in at least one of C_{L_σ}, C_{L_τ}, or $C_{L_{\sigma\tau}}$ so p divides the class number of at least one of L_σ, L_τ, or $L_{\sigma\tau}$. //

We are now ready to prove the main result which we restate.

Theorem 2.1 - Suppose that $m \not\equiv 2 \pmod 4$. Then Q_m has class number one if and only if $m = 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60,$ or 84.

Proof - Since $h_m = h_m^* h_m^+$, we may restrict to those m for which $h_m^* = 1$. These are precisely the m mentioned above, so we have only to show that $h_m^+ = 1$ for these m.

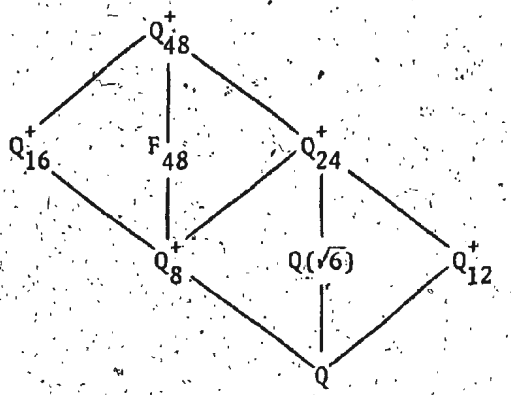
When Q_m^+ is cyclic, we find that $h_m^+ = 1$ from computations of Bauer [3] (see Appendix C). The Galois group G of Q_m is $(Z/mZ)^*$ and that of Q_m^+ is G/H where H is the subgroup consisting of $\{\bar{1}, -\bar{1}\}$. Now G (and hence G/H) is cyclic for $m = 1, 2, 4, p^\alpha, 2p^\alpha$ (p odd prime, $\alpha \geq 1$) (see Apostol [2], p. 204.ff.). Now, it is easy to see that for m not of this form that Q_m^+ is cyclic if and only if there exists $\bar{g} \in (Z/mZ)^*$ such that $\bar{g}$ has order $\frac{\phi(m)}{2}$ (mod m) but $\bar{g}^{\frac{\phi(m)}{4}} \neq -1$ (mod m). Using this, we see, for example, that for $m = 33$, Q_m^+ is cyclic with generator $\bar{14}$. By this process, we see that it remains to consider h_m^+ for $m = 24, 40, 48, 60$, and 84. We first show that each of these class number has no odd prime divisor. For $m = 24$, Q_8^+ and Q_{12}^+ are both properly contained in Q_{24}^+. But $Q_8^+ = Q(\cos(\frac{\pi}{4})) = Q(\sqrt{2})$ and $Q_{12}^+ = Q(\cos(\frac{\pi}{6})) = Q(\sqrt{3})$ and so $\sqrt{2} \cdot \sqrt{3} = \sqrt{6} \in Q_{24}^+$. Hence, $Q(\sqrt{6}) \subsetneq Q_{24}^+$. Hence, we have the following diagram where Q_{24}^+ is of



degree 4 over Q with Galois group of type (2, 2). Now we have from above that Q_8^+ and Q_{12}^+ have class number one. Similarly, $Q(\sqrt{6})$ has class number one and so no odd prime divisor divides h_{24}^+ by Lemma 2.9.

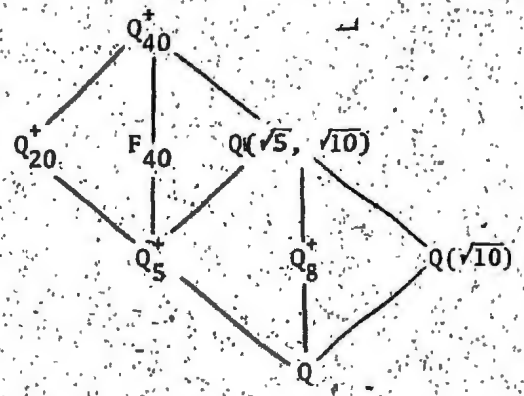
For $m = 48$, Q_{48}^+/Q_8^+ is of degree 4, $Q_8^+ \subsetneq Q_{16}^+ \subsetneq Q_{48}^+$, $Q_8^+ \subsetneq Q_{24}^+ \subsetneq Q_{48}^+$. Hence, as we have already obtained two proper intermediate fields,

the Galois group of Q_{48}^+/Q_8^+ must be of type (2, 2). We call the third proper intermediate field F_{48}, and we have the following diagram where

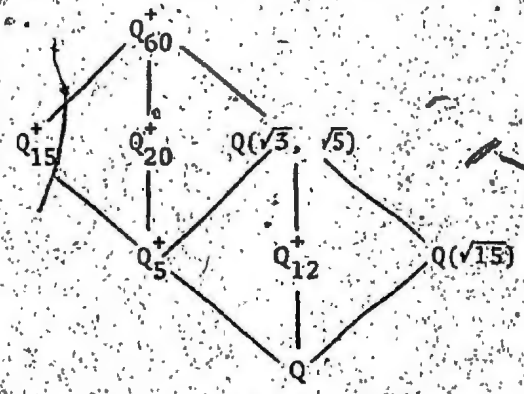


F_{48} is real with conductor 48. We now see that F_{48} is cyclic over Q. The Galois group H of Q_{48}^+/Q_8^+ are those elements of the Galois group of Q_{48}^+/Q which fix Q_8^+. Using the fact that $Q_8^+ = Q(\zeta_8 + \zeta_8^{-1}) = Q(\zeta_{48}^6 + \zeta_{48}^{-6})$, we see that $H = \{\tilde{1}, \tilde{7}, \tilde{17}, \tilde{23}\}$. For example, $\sigma_{17}(\zeta_{48}^6 + \zeta_{48}^{-6}) = \zeta_{48}^{102} + \zeta_{48}^{-102} = \zeta_{48}^6 + \zeta_{48}^{-6}$. Similarly, the Galois Group H' of Q_{48}^+/Q_{16}^+ are those elements of H which fix Q_{16}^+ and so $H' = \{\tilde{1}, \tilde{17}\}$. Further, $H'' = \{\tilde{1}, \tilde{23}\}$ where H'' is the Galois group of Q_{48}^+/Q_{24}^+. Therefore, the Galois group of Q_{48}^+/F_{48} is $\{\tilde{1}, \tilde{7}\}$. But then the Galois group of $F_{48}/Q = \{\tilde{1}, \tilde{5}, \tilde{7}, \tilde{11}, \tilde{13}, \tilde{17}, \tilde{19}, \tilde{23}\}/\{\tilde{1}, \tilde{7}\} = \{\bar{1}, \bar{5}, \bar{11}, \bar{17}\}$, and $\bar{5}$ generates this group. Hence the Galois group of F_{48}/Q is cyclic. Then by Bauer [3], F_{48} has class number one. We have already from above that Q_8^+, Q_{16}^+ and Q_{24}^+ have class number one, so no odd prime divides h_{48}^+.

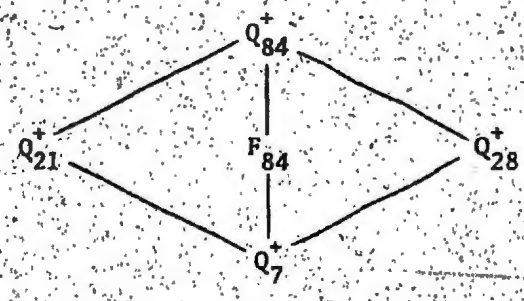
For $m = 40$, $Q_5^+ = Q(\sqrt{5})$, $Q_8^+ = Q(\sqrt{2})$ and Q_{20}^+ are properly contained in Q_{40}^+ and so $Q(\sqrt{5}, \sqrt{10})$ is also properly contained in Q_{40}^+. Now Q_{40}^+/Q_5^+ is of degree 4 and the Galois group of this extension is of type (2, 2) as we have two proper subfields. We call the third proper



subfield F_{40}, and then we have the following diagram where F_{40} is real with conductor 40. F_{40} is cyclic (same argument as for F_{48}) and so, by Bauer, it has class number one. We have from above that $h^+_{20} = 1$. Further, no odd prime divides the class number of $Q(\sqrt{5}, \sqrt{10})$ by Lemma 2.9 and, hence, no odd prime divides h^+_{40} (again by Lemma 2.9).

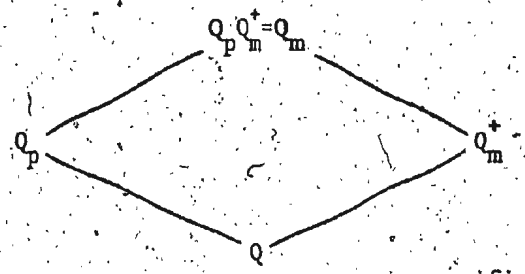


Similar considerations to the above cases show that no odd prime divides h^+_{60} or h^+_{84}.



We now show that $2 \nmid h_m^+$ for $m = 24, 40, 48, 60$ and 84. For each of these m let m_o be the largest odd divisor of m. Then Q_m/Q_{m_o} and $Q_m^+/Q_{m_o}^+$ are Galois extensions whose degrees are powers of 2. In each case, we also know that $h_{m_o} = h_{m_o}^+ = 1$. For $m = 24$, 40, or 48, the least positive integer f such that $2^f \equiv 1 \pmod{m_o}$ is $\phi(m_o)$ so the ideal generated by 2 in Q_{m_o} is prime. Then this is the only prime ramified in Q_m/Q_{m_o} (see Ribenboim [20], p. 269). For example, when $m = 24$, only 2 and 3 are ramified in Q_{24}/Q. Now, 2 as an ideal in Q_3 is prime and so this prime is ramified in Q_{24}/Q_3. However, 3, as an ideal in Q_{24}, equals $(p_1p_2)^2$ for some prime ideals p_1 and p_2 and, as an ideal in Q_3, equals p^2 for some prime ideal p. Hence, 3 does not ramify in Q_{24}/Q_3. Hence, by Lemma 2.8, $2 \nmid h_m = h_m^+$ for $m = 24$, 40 or 48 and so $h_m = h_m^+ = 1$ for these m.

For $m = 60$ and 84, we consider $Q_m^+/Q_{m_o}^+$. For $p \mid m_o$ the ramification index of p for Q_m/Q is equal to that of p for Q_{m_o}/Q. Further, the ramification index of p for $Q_{m_o}^+/Q$ is equal to that of p for Q_{m_o}/Q (see Ribenboim [20], p. 211 and p. 219). Hence, the prime divisors of the ideal generated by p in $Q_{m_o}^+$ do not ramify for $Q_m^+/Q_{m_o}^+$ and so only prime divisors of the ideal generated by 2 in $Q_{m_o}^+$ may be ramified for $Q_m^+/Q_{m_o}^+$. Now, 2 doesn't ramify in Q_{m_o}/Q (and, hence, in $Q_{m_o}^+/Q$), but 2 does ramify in Q_m/Q. Thus, in the following diagram, 2 ramifies in Q_m^+/Q since 2 does not ramify in Q_p/Q (see Ribenboim [20], p. 217) and so 2 ramifies in $Q_m^+/Q_{m_o}^+$. But for $m_o = 15$, 21,



the least positive integer f such that $2^f \equiv 1 \pm (\text{mod } m_o)$ is $\frac{\phi(m_o)}{2}$, and so the ideal generated by 2 in $Q^+_{m_o}$ is prime. (We use here the fact that $efg = \frac{\phi(m_o)}{2}$ where e is the ramification index, f the inertial degree and g the decomposition number.) Since this is the only ramified prime for $Q^+_m/Q^+_{m_o}$, Lemma 2.8 applies as before to give $h_{60} = h_{84} = h^+_{60} = h^+_{84} = 1$. //

In the situation that we have dealt with, we found that $h^+_m = 1$ whenever $h^*_m = 1$. However, it should be noted that if $K = Q(\sqrt{-1}, \sqrt{10})$, then $h^*_K = 1$, but $h^+_K = 2$ (see Hasse [10], p. 123). Thus the fact that the relative class number is one cannot then force the real factor to be one, nor does it determine the parity of the real factor.

CHAPTER III

CYCLOTOMIC FIELDS OF CLASS NUMBER TWO

In this chapter, we shall determine exactly which cyclotomic fields have class number two. We shall follow Masley's paper, "Solution of the Class Number Two Problem for Cyclotomic Fields" [15]. We shall also prove a result due to L. Carlitz [5] concerning factorization in number fields of class number two.

3.1 Cyclotomic Fields of Class Number Two

For any odd prime ℓ, we denote by $d(\ell, 2)$ the order of 2 (mod ℓ). Furthermore, for any odd integer $n > 1$, we define

$$d(n, 2) = \min. d(\ell, 2),$$

where the minimum is taken for all prime factors ℓ of n. We note that $d(n, 2) \geq 2$. Then we have the following theorem (the proof is due to Metsankyla [17]):

Theorem 3.1 - We let p be an odd prime and $p - 1 = 2^c n$, where n is odd. If h_p^* is even, then $n > 1$ and h_p^* is divisible by $2^{d(n,2)}$.

Proof - We recall formula (1.35) for h_p^*:

$$h_p^* = \pm p^{1-s} \prod_{u|n} N_u(\alpha_u); \quad \alpha_u = \sum_{k=0}^{s-1} (r_{k+1} - r_k)\zeta^{uk}$$

where $s = \frac{p-1}{2}$, $\zeta = e^{2\pi i/(p-1)}$, r a primitive root (mod p), r_k the least positive residue of r^k (mod p), and N_u the norm in the

$2^c n/u$-th cyclotomic field $Q(e^{2\pi iu/(p-1)})$.

Now if h_p^* is even, then

$$N_u(\alpha_u) \equiv 0 \pmod 2 \qquad (3.1)$$

for some fixed divisor u of n. Suppose first that $u = n$. Then, in the 2^c-th cyclotomic field, 2 is a power of the prime ideal $Z = (1 - \zeta^u)$ (for $c > 2$, see Ribenboim [20], p. 173; for $c = 1$, this is trivial) and

$$\alpha_u \equiv \sum_{k=0}^{s-1} (r_{k+1} - r_k) \equiv p - 2 \equiv 1 \pmod Z.$$

Hence, $N_u(\alpha_u) \equiv 1 \pmod 2$ which contradicts (3.1). Consequently, $u < n$ and, therefore, $n > 1$ as claimed in the theorem. Now, in the $2^c n/u$-th cyclotomic field, 2 splits into prime ideal factors p of degree f equal to the order of 2 (mod n/u). But, by (3.1), at least one of these ideals p divides α_u and so $N_u(\alpha_u)$ is divisible by $N_u(p) = 2^f$. Clearly, $f \geq d(n, 2)$, and thus the proof is complete. //

We note that as $d(n, 2) \geq 2$, then this theorem implies that if $2 | h_p^*$ then $4 | h_p^*$. We now prove the main theorem.

Theorem 3.2 - There are precisely two cyclotomic fields Q_m with class number $h_m = 2$. They are given by $m = 39, 56$.

(We are assuming, as usual, that $m \not\equiv 2 \pmod 4$, as $Q_{78} = Q_{39}$ has class number two.)

Proof - We have that $h_m^+ | h_m$ and $h_m = h_m^* h_m^+$ with h_m^* a natural number. For $h_m = 2$, we must have $h_m^* = 2$ and $h_m^+ = 1$ because we have shown in Chapter two that $h_m = 1$ whenever $h_m^* = 1$.

We first determine when $h_m^* = 2$. Lemma 2.5 says that $h_m^* | h_n^*$ if $m|n$ and Lemma 2.6 says that $4 | h_m^*$ if four distinct primes divide m. Consequently, for $h_m^* = 2$, the integer m must be of the form $m = p_1^{a_1} p_2^{a_2} p_3^{a_3}$ with p_i prime such that $h_{p_i}^* < 2$. Now, we have seen above that $h_p^* \neq 2$ for any prime p because $2 | h_p^*$ implies $4 | h_p^*$. Hence, by Corollary 2.2 and by Lemma 2.7, $p_1, p_2, p_3 \leq 19$ and $p_i^{a_i} < 32$.

Now for m of this type with $\phi(m) < 256$, we can use the tables of Schrutka [23] or Appendix A (if $m \leq 200$) to find h_m^*. For $m = 17^2$ or $m = 19^2$, we have seen in the proof of Lemma 2.7 that $h_m^* > 2$. For other m of this type with $\phi(m) > 256$, we use formula (1.37) and Theorem 1.1 to show that $h_m^* > 2$. For example, we consider h_m^* for $m = 17 \cdot 19$:

Since $h_{17}^* = 1$, then

$$h_{17\cdot 19}^* = \frac{h_{17\cdot 19}^*}{h_{17}^*} = 38 \prod_{\substack{19 | f(\psi) \\ \psi(-1)=-1}} N_\psi(H_\psi) \quad \text{(see the proof of Lemma 2.5)}$$

$$= 38 \prod_{\substack{f(\psi)=19 \\ \psi(-1)=-1}} N_\psi(H_\psi) \times \prod_{\substack{f(\psi)=17\cdot 19 \\ \psi(-1)=-1}} N_\psi(H_\psi).$$

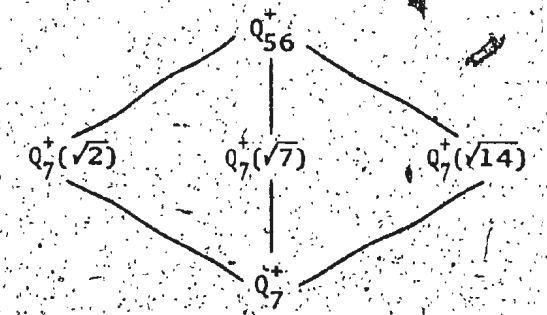
Now since the character group of $(Z/19Z)^*$ is cyclic, it is easy to determine all odd orbits and then to see by Theorem 1.1; part C, that the denominator (in lowest terms) of $\prod_{\substack{f(\psi)=19 \\ \psi(-1)=-1}} N_\psi(H_\psi)$ is at most 38.

Now if χ_1 is a generator of the character group of $(Z/19Z)^*$ and χ_2 a generator of the character group of $(Z/17Z)^*$, then $\chi = \chi_1^9 \chi_2^4$ has conductor $f(\chi) = 17 \cdot 19$ and has order $n_\chi = 4$. Further, $\chi' = \chi_1^9 \chi_2^2$ has conductor $f(\chi') = 17 \cdot 19$ and has order $n_{\chi'} = 8$. Hence, by Theorem 1.1; parts A and C, $\prod_{\substack{f(\psi)=17\cdot 19 \\ \psi(-1)=-1}} N_\psi(H_\psi) \in 4Z$ and so $h^*_{17\cdot 19} > 2$.

Using the above process, we see that $h^*_m = 2$ precisely for $m = 39$ and 56. We now show for these m that $h^+_m = 1$.

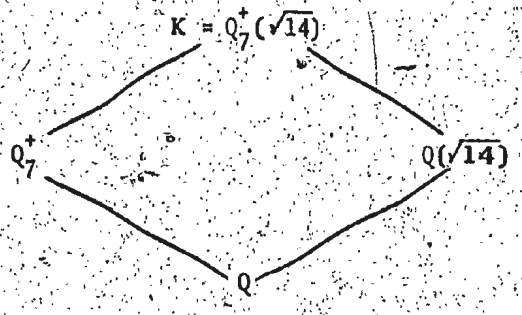
As in the proof of Theorem 2.1, it is easily seen that Q^+_{39} is cyclic with generator $\overline{2}$; further, Q^+_{39} is real with Minkowski-Rogers bound $< 50{,}000$ and conductor 39. Hence, $h^+_{39} = 1$ by the computations of Bauer [3] (see Appendix C).

We now show $h^+_{56} = 1$. We have immediately that Q^+_{56}/Q^+_7 is a Galois extension of order 4. The only quadratic field contained in Q_7 is $Q(\sqrt{-7})$ (Weiss [26], p. 260) and since $i = \sqrt{-1}$ is a 56th root of unity, then $\sqrt{7} \in Q^+_{56}$. Further, $Q^+_8 = Q(\sqrt{2}) \subset Q^+_{56}$. Hence, we have the following diagram:



Therefore, Q_{56}^+/Q_7^+ is a Galois extension with group of type (2, 2). Again all three intermediate fields are easily seen to be cyclic with Minkowski-Rogers bound < 50,000 and conductor 56. Hence, they all have class number one (Bauer [3]). But then by Lemma 2.9, h_{56}^+ is a power of 2.

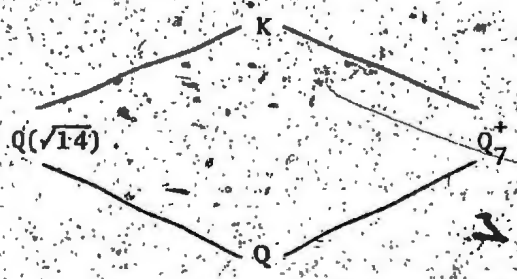
We now show h_{56}^+ is no positive power of 2. Let $K = Q_7^+(\sqrt{14})$ and $L = Q_{56}^+ = K(\sqrt{2})$. Only primes above 2 and 7 are ramified in Q_{56} with ramification indices 4 and 6, respectively (Ribenboim [20], p. 269). Hence, only primes above 2 and 7 are ramified in L. But in the following diagram;



7 ramifies in $Q(\sqrt{14})$ with ramification index 2 (Ribenboim [20], p. 169). 7 ramifies in $Q_7^+|Q$ with ramification index 3 since 7 completely ramifies in Q_7/Q with ramification index 6. Therefore, 2 and 3 divide the ramification index of 7 in K/Q. But K/Q is of degree 6 and, hence, 7 is fully ramified in K/Q. But the ramification index of 7 in Q_{56}/Q is 6 and, therefore, the

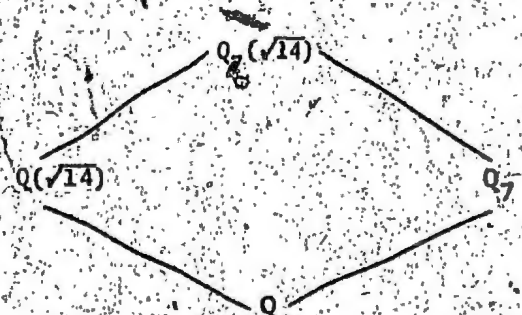
prime above 7 in K doesn't ramify in L/K. So the only primes which might ramify in L/K are those above 2.

We have that 2 doesn't ramify in Q_7^+. Moreover, since 3 is the inertial degree of 2 in Q_7/Q, then 3 is the inertial degree of 2 in Q_7^+/Q. Hence, since for the extension Q_7^+/Q, $efg = \frac{\phi(7)}{2} = 3$, $e = 1$ and $g = 1$, and so 2 remains prime in Q_7^+. (We note that here e means the ramification index, f the inertial degree and g the decomposition number.) But in the following diagram:

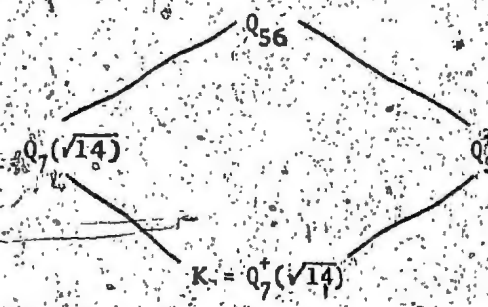


2 does not ramify in Q_7^+/Q, 2 ramifies in $Q(\sqrt{14})/Q$ with index 2 (Ribenboim [20], p. 171) and so 2 divides the ramification index of 2 in K/Q. Therefore, the prime divisor above 2 in Q_7^+ ramifies in K/Q_7^+ with ramification index 2 and so, we have only one prime divisor above 2 in K.

Now the prime above 2 in K ramifies in Q_{56}/K since the ramification index of 2 for Q_{56}/Q is 4. We want that this prime ramify in Q_{56}^+/K. We have by the following diagram that 2 ramifies in $Q_7(\sqrt{14})/Q$ with ramification index 2, and, by the above, that 2 ramifies in $Q_7^+(\sqrt{14})/Q$ with ramification index 2. Hence, the prime above 2 in K doesn't



ramify in $Q_7(\sqrt{14})/K$. But then in the following diagram:



the prime above 2 in K must ramify in $Q_{56}/Q^+_7(\sqrt{14})$ as it ramifies in Q_{56}/K but not in $Q_7(\sqrt{14})/K$ (see Ribenboim [20], p. 217).

So only one prime divisor ramifies in L/K. Therefore, by Lemma 2.8, if the class number of L, h^+_{56}, were even, then K would have an even class number. But we have seen above that the class number of K is one so h^+_{56} is no positive power of 2 and hence $h^+_{56} = 1$. //

3.2 Factorization in Algebraic Number Fields of Class Number Two.

We have seen that algebraic number fields have unique factorization if and only if they have class number one. We finish this report with the following result of L. Carlitz [5], in which we see what can be said about factorization in algebraic number fields of class number two.

Theorem 3.3 - The algebraic number field K has class number ≤ 2 if and only if for every nonzero integer $\alpha \in K$ the number of primes Π_j in every factorization

$$\alpha = \Pi_1 \cdots \Pi_k \tag{3.2}$$

depends only on α.

Proof - Suppose first that $h = 2$ and consider the factorization into prime ideals

$$(\alpha) = p_1 \cdots p_s \mathfrak{r}_1 \cdots \mathfrak{r}_t \qquad (3.3)$$

where the p_j are principal ideals while the $\mathfrak{r}_j$ are not. Then

$$p_j = (\Pi_j)$$

where the Π_j are prime. Since $h = 2$, it follows that

$$\mathfrak{r}_i \mathfrak{r}_j = (\rho_{ij}) \quad (i, j = 1, \ldots, t),$$

and it is very easily seen that ρ_{ij} is prime $\forall i,j$. Moreover, t must be even, $= 2u$, say, for otherwise $(\alpha) = \gamma$ where γ is non-principal. Thus every factorization into primes implied by (3.3), for example

$$\alpha = \varepsilon \Pi_1 \cdots \Pi_s \rho_{12} \cdots \rho_{t-1,t},$$

where ε is a unit, will contain exactly $s + u$ primes.

We now show that when $h > 2$, there occur factorizations (3.2) with different values of k. The proof makes use of the fact that every class of ideals contains at least one prime ideal. (See Hecke [11], p. 316).

We consider two cases. We first assume that there exists a class A of period $m > 2$. Let p be a prime ideal in A and p' a prime ideal in A^{-1}. Then we have

$$p^m = (\Pi), \quad p'^m = (\Pi'), \quad pp' = (\Pi_1) \tag{3.4}$$

and again, it is easily verified that Π, Π', Π_1 are primes. Clearly, (3.4) implies

$$\Pi_1^m = \varepsilon \Pi \Pi' \tag{3.5}$$

where ε is a unit.

In the second case, we assume that there exists no class of period $m > 2$, so we may choose two classes A_1 and A_2 of period 2 such that they are not inverses of each other. Then $A_3 = A_1 A_2$ is non-principal (of order 2). Choose prime ideals $p_j \in A_j$ $(j = 1, 2, 3)$. Then we have

$$p_j^2 = (\Pi_j) \quad (j = 1, 2, 3) \quad p_1 p_2 p_3 = (\Pi) \tag{3.6}$$

where again, we have that Π_1, Π_2, Π_3 and Π are all primes. From (3.6), we get

$$\Pi^2 = \varepsilon \Pi_1 \Pi_2 \Pi_3 \tag{3.7}$$

where ε is a unit.

Using (3.5) and (3.7), it is evident that when $h > 2$, the number of primes k in (3.2) is not independent of the factorization.

Since the case $h = 1$ requires no further discussion, this completes the proof of the theorem. //

APPENDICES

APPENDIX A

TABLE 1: RELATIVE CLASS NUMBERS OF $Q(\exp 2\pi i/m)$ FOR $m \leq 200$

m	$\phi(m)$	h_m^*
3(6)	2	1
4	2	1
5(10)	4	1
7(14)	6	1
8	4	1
9(18)	6	1
11(22)	10	1
12	4	1
13(26)	12	1
15(30)	8	1
16	8	1
17(34)	16	1
19(38)	18	1
20	8	1
21(42)	12	1
23(46)	22	3
24	8	1
25(50)	20	1
27(54)	18	1
28	12	1
29(58)	28	2.2.2
31(62)	30	3.3
32	16	1
33(66)	20	1
35(70)	24	1
36	12	1
37(74)	36	37
39(78)	24	2
40	16	1
41(82)	40	11.11
43(86)	42	211
44	20	1
45(90)	24	1
47(94)	46	5.139
48	16	1
49(98)	42	43
51(102)	32	5
52	24	3
53(106)	52	4889
55(110)	40	2.5
56	24	2
57(114)	36	3.3
59(118)	58	3.59.233
60	16	1
61(122)	60	41.1861
63(126)	36	7

TABLE 1(continued)

m	$\phi(m)$	h_m^*
64	32	17
65(130)	48	2.2.2.2.2.2
67(134)	66	67.12739
68	32	2.2.2
69(138)	44	3.23
71(142)	70	7.7.79241
72	24	3
73(146)	72	89.134353
75(150)	40	11
76	36	19
77(154)	60	2.2.2.2.2.2.2.2.5
79(158)	78	5.53.377911
80	32	5
81(162)	54	2593
83(166)	82	3.279405653
84	24	1
85(170)	64	5.17273
87(174)	56	2.2.2.2.2.2.2.2.2.3
88	40	5.11
89(178)	88	113.11801449
91(182)	72	2.2.2.2.7.13.37
92	44	3.67
93(186)	60	3.3.5.151
95(190)	72	2.2.13.19.109
96	32	3.3
97(194)	96	577.3457.206209
99(198)	60	3.31.31
100	40	5.11
101	100	5.5.5.5.5.101.601.18701
103	102	5.103.1021.17247691
104	48	3.3.3.13
105	48	13
107	106	3.743.9859.2886593
108	36	19
109	108	17.1009.9431866153
111	72	2.2.3.3.19.19.37
112	48	2.2.3.3.13
113	112	2.2.2.17.11853470598257
115	88	3.331.45013
116	56	2.2.2.2.2.2.2.2.3.7
117	72	2.3.3.3.3.3.3.7.13
119	96	3.3.3.3.5.5.5.13.97.97
120	32	2.2
121	110	67.353.20021.25741
123	80	2.2.2.2.2.2.2.2.2.2.2.11.11.17
124	60	2.2.3.3.31.41
125	100	2801.20602801
127	126	5.13.43.547.883.3079.626599

TABLE 1(continued)

m	ϕ (m)	h_m^*
192	64	3.3.17.401
193	192	6529.15361.29761.91969.10369729.192026280449
195	96	2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.13.13
196	84	43.71.27091
197	196	2.2.2.5.1877.7841.939830268487086656225611549
199	198	3.3.3.3.19.727.25645093.2072935.8177.31681904.12839
200	80	5.11.11.41.601

TABLE 1(continued)

m	$\phi(m)$	h_m^*
128	64	17.21121
129	84	7.29.211.883
131	130	3.3.3.5.5.53.131.1301.4673706701
132	40	11
133	108	2.2.3.3.3.3.3.3.3.3.3.3.13.19.37.73
135	72	37.2053
136	64	2.2.2.2.2.2.3.3.97
137	136	17.17.47737.468905406211 21
139	138	3.3.47.47.277.277.967.1188961909
140	48	3.13
141	92	5.47.139.139.277
143	120	5.5.7.61.61.661.83701
144	48	3.13.13
145	112	2.2.2.2.2.2.2.2.2.2.2.2.2.281.421.757
147	84	7.29.43.673
148	72	3.3.7.19.37.109
149	148	3.3.149.5129663383200408054 61
151	150	7.11.11.281.25951.1207501.312885301
152	72	3.3.3.3.3.19.19.19
153	96	2.2.2.2.2.2.2.2.5.11.11.15601
155	120	2.2.2.2.2.2.2.2.2.3.3.3.3.5.5.631.129121
156	48	2.2.3.13
157	156	5.13.13.157.157.1093.1873.418861.3148601
159	104	5.53.53.3251.4889
160	64	3.3.5.17.41
161	132	3.3.11.67.67.67.22111.25873
163	162	2.2.181.23167.365473.4418458171 62679
164	80	2.2.2.5.11.11.71.241
165	80	2.2.5.11.421
167	166	11.499.5123189985484229035947419
168	48	2.2.3.7
169	156	313.1873.4733.196953296289361
171	108	2.2.3.3.3.3.3.3.7.19.73.109.163
172	84	2.2.43.211.21841
173	172	5.20297.231169.725717293 02851870621
175	120	2.2.2.2.2.2.2.2.61.271.601.1861
176	80	5.5.5.11.41.521
177	116	3.59.233.523.3789257
179	178	5.1069.1445866739233494828676 4635121
180	48	3.5.5
181	180	5.5.5.37.41.61.1321.2521.5488435782589277701
183	120	2.2.2.2.2.2.5.5.31.31.31.41.211.1861
184	88	2.3.23.67.67.2399
185	144	5.5.7.7.13.37.37.53.53.9433.23833
187	160	17.17.41.241.4801.299681.9447601
188	92	5.47.139.742717
189	108	7.37.109.127.163.181
191	190	11.13.51263.612771091.3673395066973371 3761

APPENDIX B

COMPUTATIONS FOR $h^*_{17^2}$ AND $h^*_{19^2}$

Let ψ be an odd primitive character with $f(\psi) = p^2$ for p an odd prime. The numbers $x + yp$, $1 \le x \le p-1$, $0 \le y \le p-1$ form a complete set of representatives of $(\mathbb{Z}/p^2\mathbb{Z})^*$ and so by (1.36), we have

$$-2p^2 H_\psi = \sum_{x=1}^{p-1} \sum_{y=0}^{p-1} \psi(x + yp) \cdot (x + yp).$$

But $(x + yp) \equiv x(1 + yx^{-1}p) \equiv x(1 + p)^{yx^{-1}} \pmod{p^2}$ where x^{-1} is an integer such that $xx^{-1} \equiv 1 \pmod{p}$. Now $1 + p$ has order p in $(\mathbb{Z}/p^2\mathbb{Z})^*$ (This was seen in the proof of Theorem 1.1, part C), and so $\psi(1 + p)$ is a p-th root of unity. If $\psi(1 + p) = 1$, then $\psi(1 + kp) = 1$ for $k \in \mathbb{N}$, since $1 + kp \equiv (1 + p)^k \pmod{p^2}$. But then by the above, $\psi(x + yp) = \psi[x(1 + yx^{-1}p)] = \psi(x) \cdot \psi(1 + yx^{-1}p) = \psi(x)$ and so $f(\psi) = p$, a contradiction. So $\psi(1 + p) = \zeta$, ζ a primitive p-th root of unity, and $\psi(1 + kp) = \zeta^k$. Then

$$-2p^2 H_\psi = \sum_{x=1}^{p-1} \psi(x) \sum_{y=0}^{p-1} (x + yp)\zeta^{yx^{-1}}$$

$$= \sum_{x=1}^{p-1} \psi(x) \left[x \sum_{y=0}^{p-1} \zeta^{yx^{-1}} + p \sum_{y=0}^{p-1} y(\zeta^{x^{-1}})^y\right]$$

$$= \sum_{x=1}^{p-1} \psi(x) \frac{p^2}{\zeta^{x^{-1}} - 1}$$

since for any primitive p-th root of unity $[\zeta + 2\zeta^2 + \ldots + (p-1)\zeta^{p-1}][\zeta - 1] = p$. Consequently,

$$H_\psi = \frac{1}{2}\sum_{x=1}^{p-1} \frac{\psi(x)}{1 - \zeta^{x^{-1}}} \qquad (A.1)$$

Now $\psi(p - x) = \psi(-x(1 - x^{-1}p)) = -\psi(x)\zeta^{-x^{-1}}$ so

$$\frac{\psi(p-x)}{1-\zeta^{-x^{-1}}} = \frac{-\psi(x)\zeta^{-x^{-1}}}{1-\zeta^{-x^{-1}}} = \frac{\psi(x)}{1-\zeta^{x^{-1}}}.$$

Then (A.1) becomes

$$H_\psi = \sum_{x=1}^{\frac{p-1}{2}} \frac{\psi(x)}{1-\zeta^{x^{-1}}} = \frac{1}{1-\zeta}\sum_{x=1}^{\frac{p-1}{2}} \psi(x)\frac{1-\zeta}{1-\zeta^{x^{-1}}}$$

and so

$$H_\psi = \frac{1}{1-\zeta}\sum_{x=1}^{\frac{p-1}{2}} \psi(x)[1 + \zeta^{x^{-1}} + \ldots + \zeta^{(x-1)x^{-1}}] \qquad (A.2)$$

(see Ribenboim [20], p. 82).

We now calculate $N_\psi((1-\zeta)H_\psi)$ for ψ, ζ as above with $f(\psi) = 17^2$. We first compute a generator ψ of the character group of Q_{17^2}. All congruences are now mod 17^2. Then

$$4^{16} \equiv 2^8 \equiv 1 + 15\cdot 17 \qquad 5^{16} \equiv 1 + 12\cdot 17 \qquad 7^{16} \equiv 1 + 3\cdot 17$$

$$3^{16} \equiv 1 + 10\cdot 17 \qquad 6^{16} \equiv 1 + 6\cdot 17 \qquad 8^8 \equiv 1 + 11\cdot 17$$

We may compute a character χ of Q_{17^2} of order 17 as follows. $\chi(1 + 17) = \zeta$, a primitive 17-th root of unity. We have $\chi(3) = \zeta^k$ and $\chi(3^{16}) = (\chi(1 + 10.17) = \zeta^{10} = \chi^{16}(3) = \zeta^{16k}$ so $k = 7$. In this manner, we compute $\chi(2) = \zeta^4$, $\chi(4) = \zeta^8$, $\chi(5) = \zeta^5$, $\chi(7) = \zeta^{14}$, and $\chi(8) = \zeta^{12}$. Now let ξ be a generator of the character group of Q_{17}. Then $\alpha = \xi(3)$ is a primitive 16-th root of unity since 3 is a primitive root mod 17. Then, for example, $\xi(2) = \xi(3^{14}) = \alpha^{14} = \alpha^8\alpha^6 = -\alpha^6$. We let $\psi = \xi\chi$. Then ψ has conductor 17^2 and order 16.17 and

x	$\psi(x)$
2	$-\alpha^6\zeta^4$
3	$\alpha\,\zeta^7$
4	$-\alpha^4\zeta^8$
5	$\alpha^5\zeta^5$
6	$-\alpha^7\zeta^{11}$
7	$-\alpha^3\zeta^{14}$
8	$-\alpha^2\zeta^{12}$

With these values, we use (A.2) to obtain the following value for the algebraic integer $(1 - \zeta)H_\psi$:

$$\begin{aligned}(1-\zeta)H_\psi = 1 &+ \alpha(\zeta^2 + \zeta^7 + \zeta^{13})\\ &-\alpha^2(1 + \zeta^2 + \zeta^4 + \zeta^6 + \zeta^8 + \zeta^{10} + \zeta^{12} + \zeta^{15})\\ &-\alpha^3(1 + \zeta^2 + \zeta^5 + \zeta^7 + \zeta^{10} + \zeta^{12} + \zeta^{14})\\ &-\alpha^4(1 + \zeta^4 + \zeta^8 + \zeta^{13})\\ &+\alpha^5(\zeta^2 + \zeta^5 + \zeta^9 + \zeta^{12} + \zeta^{16}) - \alpha^6(\zeta^4 + \zeta^{13})\\ &-\alpha^7(1 + \zeta^3 + \zeta^6 + \zeta^9 + \zeta^{11} + \zeta^{14}).\end{aligned}$$

If we use $1, \zeta^2, \zeta^3, \ldots, \zeta^{16}, \alpha, \alpha\zeta^2, \ldots, \alpha\zeta^{16}, \alpha^2, \alpha^2\zeta^2, \ldots, \alpha^7\zeta^{16}$ as an ordered basis of $Q_{16\cdot 17}$, then we can set up the matrix whose determinant equals $N_\psi((1-\zeta)H_\psi)$ (see Samuel [22], p. 36). Although this is an $(8\cdot 64) \times (8\cdot 64)$ matrix, we need only compute seven 16×16 matrices because $\alpha^i\zeta^j(1-\zeta)H_\psi$ and $\alpha^k\zeta^j(1-\zeta)H_\psi$ have almost $(\alpha^8 = -1)$ the same coefficients merely cyclically shifted. Masley [14] uses a computer program which computes determinants of matrices mod primes to show that this matrix has determinant congruent to 5 (mod 7).

For $h_{19^2}^*$ we let χ be a generator of the character group of Q_{19^2}. We wish to find values for χ^9, a generator for the character group of K, the subfield of degree 38 over Q.

We let all congruences be (mod 19^2). Then if $a \equiv 1 + 19k \equiv (1+19)^k$, $\chi(a) = \zeta^k$ where $\chi(1+19) = \zeta$ is a primitive 19-th root of 1. Now $2^{18} \equiv 1 + 3\cdot 19$ so $\chi(2^{18}) = \zeta^3$ and $\chi^{18}(2) = \chi^9(4) = \zeta^3$. $8^{18} \equiv 1 + 9\cdot 19 \equiv -3^9$ so $\chi^9(3) = \chi(3^9) = \chi(-8^{18}) = -\chi((2^{18})^3) = -\zeta^9$. Then $\chi^9(9) = \zeta^{18}$. Now $5^9 \equiv 1 + 6\cdot 19$ so $\chi^9(5) = \zeta^6$. We have $-1 = \chi^9(360) = \chi^9(8)\chi^9(5)\chi^9(9) = \chi^9(8)\zeta^6\zeta^{18}$ so $\chi^9(8) = -\zeta^{14}$ and since $\chi^9(2)\chi^9(4) = -\zeta^{14}$, we get $\chi^9(2) = -\zeta^{11}$. $\chi^9(6) = \chi^9(2)\chi^9(3) = (-\zeta^{11})(-\zeta^9) = \zeta$ and $\chi^9(7) = \chi^9(3^6) = (-\zeta^9)^6 = \zeta^{16}$. In our actual computations for $N_{\chi^9}(H_{\chi^9})$, we used the representative $\psi = \chi^{9\cdot 17}$ which is a conjugate of χ^9 via $\zeta \to \zeta^{-2}$. Using (A.2), we computed that

$$H_\psi = 1 - \zeta - 2\zeta^3 + \zeta^5 - 2\zeta^8 - 2\zeta^{10} - \zeta^{14} - 2\zeta^{16} - \zeta^{18}.$$

We made essential use of the fact that $1 + \zeta + \ldots + \zeta^{18} = 0$ to compute the transpose of the matrix for H_ψ in a regular representation of Q_{19} with respect to the basis $1, \zeta^2, \zeta^3, \ldots, \zeta^{18}$. The matrix we used is given at the end of this discussion. The determinant of this matrix is equal to $N_{\psi}(H_\psi) = N_{Q_{38}}(H_\psi) = N_{Q_{19}}(H_\psi)$. Masley [14] computed this determinant to be congruent to 6 (mod 11). We computed the actual value of the determinant to be 301,952,899.

We now compute $N_{\psi^{19}}(H_{\psi^{19}})$ where $\psi^{19} = (\chi^9)^{19}$. Now, it is easily seen that ψ^{19} has conductor 19. Also, $N_{\psi^{19}} = N_{Q_2} = N_Q$ so $N_{\psi^{19}}(H_{\psi^{19}}) = H_{\psi^{19}}$. We have by (1.36) that

$$H_{\psi^{19}} = \frac{-1}{2\cdot 19}\sum_{a=1}^{18} \psi^{19}(a)a.$$

Now if a is a square mod 19, then $\psi^{19}(a) = 1$. Now 2 is not a square (mod 19). If we assume that $\psi^{19}(2) = +1$, then we easily see that $\psi^{19}(a) = +1$ for all a (mod 19). Hence, $\psi^{19}(2) = -1$ which, in turn, implies that $\psi(a) = -1$ for all non-squares a (mod 19). Therefore,

$$H_{\psi^{19}} = \frac{-1}{2\cdot 19}\sum_{a=1}^{18} a\left(\frac{a}{19}\right)$$

$$= \frac{-1}{2\cdot 19}(-95 + 76) = \frac{1}{2}.$$

The following matrix has determinant equal to h_K^* where $K \subset \mathbb{Q}(\zeta_{19^2})$ and $|K:\mathbb{Q}| = 38$.

2	1	-1	1	2	1	1	-1	1	-1	1	-1	1	0	1	-1	1	0
1	2	0	-1	-1	1	2	1	1	-1	1	-1	1	1	1	0	1	-1
-2	-1	1	-1	0	-2	0	1	0	0	-2	0	-2	0	0	0	-1	0
2	2	1	3	1	2	0	2	3	2	2	0	2	0	2	2	2	1
-1	-2	0	-1	1	-1	0	-2	0	1	0	0	-2	0	-2	0	0	0
1	1	-1	1	0	2	0	1	-1	1	2	1	1	-1	1	-1	1	1
0	-1	0	-2	0	-1	1	-1	0	-2	0	1	0	0	-2	0	-2	0
0	0	-1	0	-2	0	-1	1	-1	0	-2	0	1	0	0	-2	0	-2
-2	0	0	-1	0	-2	0	-1	1	-1	0	-2	0	1	0	0	-2	0
2	2	2	2	1	2	0	2	1	3	1	2	0	2	3	2	2	0
-2	-2	0	0	0	-1	0	-2	0	-1	1	-1	0	-2	0	1	0	0
2	2	0	2	2	2	1	2	0	2	1	3	1	2	0	2	3	2
0	-2	0	-2	0	0	0	-1	0	-2	0	-1	1	-1	0	-2	0	1
1	0	-2	0	-2	0	0	0	-1	0	-2	0	-1	1	-1	0	-2	0
1	1	1	-1	1	-1	1	1	1	0	1	-1	1	0	2	0	1	-1
-2	1	0	0	-2	0	-2	0	0	0	-1	0	-2	0	-1	1	-1	0
2	2	3	2	2	0	2	0	2	2	2	1	2	0	2	1	3	1
-1	-2	0	1	0	0	-2	0	-2	0	0	0	-1	0	-2	0	-1	1

APPENDIX C

BAUER'S COMPUTATIONS

Bauer [3] has computed the class numbers of real cyclic fields with conductor $f < 100$ and Minkowski-Rogers bound $M < 50{,}000$. (The Minkowski bound for a field K of degree n over Q with discriminant d is given by

$$B = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|},$$

where $2r_2$ is the number of complex conjugate fields appertaining to K. Bauer has used an improved version of this bound due to C. A. Rogers (see Hasse [9], p. 590-592). In the cases where we apply Bauer's results, one has by computation that the Minkowski-Rogers bound is $< 50{,}000$.

Bauer's computations depend on Leopoldt's p-adic class number formula [14]. The results of his computations are as follows:

In the following table, the field of conductor f and degree n is denoted by f, n; if it is not thus uniquely determined, there will be an additional corresponding statement in parentheses.

1. In the range $f < 100$, $n < 50{,}000$, we have

Class #1: All those fields not mentioned under the following cases.

Class #2: 40, 2; 60, 2; 65, 12 (both fields); 65, 6 (with quadratic subfield of conductor 65); 65, 4 (both fields); 65, 2; 80, 4 (all three fields); 85, 8; 85, 4; 85, 2;

Class #3: 63, 6 (both fields with a cubic subfield of conductor 63); 63, 3 (both fields); 91, 6 (both fields with a cubic subfield of conductor 91); 91, 3 (both fields).

BIBLIOGRAPHY

[1] N. C. Ankeny, S. Chowla and H. Hasse, On the Class Number of the Maximal Real Subfield of a Cyclotomic Field, J. reine angew. Math. Vol. 217 (1965), 217-220.

[2] T. M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[3] H. Bauer, Numerische Bestimmung von Klassenzahlen reeler zyklischer Zahlkörper, J. of Number Theory, Vol. 1 (1969), 161-162.

[4] Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, New York, 1966.

[5] L. Carlitz, A Characterization of Algebraic Number Fields with Class Number Two, Proc. AMS., Vol. 11 (1960), 391-392.

[6] R. V. Churchill, Complex Variables and Applications, McGraw-Hill, 2nd edition, Toronto, 1960.

[7] H. Davenport, Multiplicative Number Theory, Markham Pub. Co., Chicago, 1967.

[8] T. Estermann, Introduction to Modern Prime Number Theory, Cambridge University Press, Cambridge, 1961.

[9] H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1963.

[10] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.

[11] E. Hecke, Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. IIa (1917), 299-318.

[12] K. Iwasawa, A Note on Class Numbers of Algebraic Number Fields, Abh. Math. Sem. Univ. Hamburg, Vol. 20 (1956), 257-258.

[13] E. Kummer, Über die Klassenzahl der aus nten Einheitswurzeln gebildeten complexen Zahlen, Monatsh. Preuss. Akad. Wiss. Berlin, 1861, 1051-1053.

[13'] E. Kummer. Über diejenigen Primzahlen λ, für welche die Klassenzahl der aus λ ten Einheitswurzeln gebildeten complexen Zahlen durch λ theilbar ist, Monatsh. Preuss. Akad. Wiss., Berlin, 1874, 239-248.

[14'] H. W. Leopoldt, Über Fermatquotienten von Kreiseinheiten und Klassenzahlformelm mod p, Rend. Circ. Math. Palermo (2), Vol. 9 (1960), 1-12.

[14] J. Masley, On the Class Number of Cyclotomic Fields, Diss. Princeton, 1972.

[15] J. Masley, Solution of the Class Number Two Problem for Cyclotomic Fields, Inventiones Math., 28 (1975), 243-244.

[16] J. Masley and H. L. Montgomery, Cyclotomic Fields with Unique Factorization, J. reine angew Math., Vol. 286/287 (1976), 248-256.

[17'] T. Metsankyla, On Prime Factors of the Relative Class Numbers of Cyclotomic Fields, Ann. Univ. Turku, Ser A I 149 (1971).

[17] H. L. Montgomery and R. C. Vaughan, The Large Sieve, Mathematika, Vol. 20 (1973), 119-134.

[18] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Polish Scientific Publishers, Warsaw, 1974.

[19] M. Newman, A Table of the First Factor for Prime Cyclotomic Fields, Math. Comp., Vol. 24 (1970), 215-219.

[20] P. Ribenboim, Algebraic Numbers, Wiley-Interscience, Toronto, 1972.

[21] J. J. Rotman, The Theory of Groups: An Introduction, Allyn and Bacon, Boston, 1965.

[22] P. Samuel, Algebraic Theory of Numbers, Houghton Mifflin Company, Boston, 1970.

[23] G. Schrutka V. Rechtenstamm, Tabelle der (relativ-) Klassenzahlen von Kreiskörpern, Abh. Deutsche Akad. Wiss., Berlin, 1964, Math. Nat. Kl Nr. 2.

[24] J. P. Serre, A Course in Arithmetic, Springer-Verlag, New York, 1973.

[25] K. Uchida, Class Numbers of Imaginary Abelian Number Fields, III, Tōhoku Math. J., Vol. 23 (1971), 573-580.

[26] E. Weiss, Algebraic Number Theory, McGraw-Hill, New York, 1963.

[27] A. Yokoyama, On Class Numbers of Finite Algebraic Number Fields, Tōhoku Math. J., Vol. 17 (1965), 349-357.