ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

387

ON THE FIRST FACTOR OF THE CLASS NUMBER OF THE CYCLOTOMIC FIELD AND DIRICHLET'S *L*-FUNCTIONS

BY

TIMO LEPISTÖ

HELSINKI 1966
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1966.387

Communicated 12 November 1965 by P. J. Myrberg and K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1966

Preface

I wish to express my deep gratitude to Professor K. INKERI, Ph. D., for suggesting the present problem and for his invaluable advice and encouragement at all stages of my work. I am indebted to Professor S. HYYRÖ, Ph. D., who has made many useful suggestions during the revision of this paper. My gratitude is also due to Professor A. SALOMAA, Ph. D. and Mr. T. METSÄNKYLÄ, Ph. M. for many illuminating discussions. In addition I should like to thank the Personnel of the Mathematical Institute of the University of Turku for the interest they have taken in my work. For the revision of the English manuscript, I am grateful to Lector A. T. LANDON, M. A.

I also wish to record my indebtedness to the Finnish Academy of Sciences for accepting this publication for inclusion in the Annals of the Academy.

Turku, November, 1965

TIMO LEPISTÖ

Contents

Introduction

1. Consider a cyclotomic field $k(\zeta)$, where ζ is a primitive mth root of unity. We suppose that the natural number m is > 1 and in addition we exclude those even values of m, which are not divisible by 4. This restriction is not essential because both the primitive mth and $(m/2)$th roots of unity generate the same field if m has some excluded value. It is known that the class number $h(m)$ can be represented in the form

$$h(m) = h_1(m)h_2(m) ,$$

where $h_1(m)$ and $h_2(m)$ are the so-called first and second factors of the class number.

In the present paper we mainly consider the factor $h_1(m)$ especially its behaviour, when m tends to infinity.

2. If p denotes an odd prime, KUMMER [11] conjectured that

$$h_1(p) \sim G(p) = 2^{(3-p)/2}\ \pi^{(1-p)/2}\ p^{(p+3)/4} . \tag{1}$$

The sign used here is the sign of asymptotic equality, when $p \to \infty$. He also calculated $h_1(p)$ for $p \leqq 97$ and found $h_1(p) = 1$ for $p \leqq 19$, $h_1(97) = 411\ 322\ 823\ 001$. It should be noted that $G(97)$ calculated by means of (1) is $455 \cdot 10^9$ to 3 significant figures. No proof of (1) has yet been published.

ANKENY and CHOWLA [1], [2] showed that

$$\lim_{p\to\infty} \frac{\log(h_1(p)/G(p))}{\log p} = 0 . \tag{2}$$

They also announced as a consequence of this, that there exists a p_0 such that $h_1(p)$ is strictly increasing for $p > p_0$, in other words, if $p_2 > p_1 > p_0$ then

$$h_1(p_2) > h_1(p_1) .$$

TATUZAWA [17] proved that

$$2p(p^{\frac{1}{2}}/2\pi)^{(p-1)/2}\, c(\varepsilon)p^{-\varepsilon} < h_1(p) < 2p(p^{\frac{1}{2}}/2\pi)^{(p-1)/2}\, (\log p)^c , \tag{3}$$

where the upper bound is sharper than the upper bound given by (2). Here c and $c(\varepsilon)$ denote respectively an absolute positive constant and a positive constant depending on parameter $\varepsilon\,(>0)$ alone.

Among the asymptotic estimations of $h_1(m)$ we further have the result

$$\log h_1(p) \sim (p \log p)/4 \tag{4}$$

introduced by SIEGEL [15]. We can, however, find that this formally very simple estimation is not so sharp as (2) and (3).

The above asymptotic estimations (2) and (3) give for $h_1(p)$ a good approximation, whenever p exceeds a sufficiently large limit, the greatness of which being, however, unknown. Therefore we need for $h_1(p)$ also the estimations which are useful for every value of p. The upper bound

$$h_1(p) < 2^{(1-p)/4}\, p^{(p+3)/4} \tag{5}$$

and its improvement

$$h_1(p) \leqq \begin{cases} (k-1)! & (p = 4k+1)\,, \\ (k-1)!\, k^{\frac{1}{2}} & (p = 4k+3 \geqq 7) \end{cases} \tag{6}$$

introduced by CARLITZ [3] are of this kind. Although (5) and (6) give a better upper bound than (4), we can, however, verify that, for great values of p, they do not give as good results as the asymptotic estimations (2) and (3).

3. In the first chapter of this work we consider the asymptotic estimation of $h_1(m)$. By using TATUZAWA's method in the general case we have

$$c(\varepsilon)m^{-\varepsilon} < h_1(m)/G(m) < \exp(c(\log\log m + \omega(m)))\,, \tag{7}$$

where $\omega(m)$ denotes the number of different prime factors of m, c and $c(\varepsilon)$ are defined in the same way as in (3), and

$$G(m) = \varrho\, \varrho'(2\pi)^{-\varphi(m)/2}\, |d^{1/4}|\, m\,, \tag{8}$$

where φ denotes EULER's function and d is the discriminant of $k(\zeta)$. The number $\varrho' = 1$ or 2 if m is even or odd respectively and ϱ, defined by (1.3), differs from 1 only if $\omega(m) = 1$. The result (7) implies the estimation

$$\lim_{p^u \to \infty} \frac{\log(h_1(p^u)/G(p^u))}{\log p^u} = 0\,,$$

which we obtained in [13] by an extension of the method of ANKENY and CHOWLA.

If in (8) we replace m by an odd prime p, we get the expression

$G(p)$, which appeared in KUMMER's conjecture (1). The most that has been shown in the direction of KUMMER's conjecture is the result (3) of TATUZAWA. Since we have shown that in the general case it is possible to get the estimation, which has respectively the same accuracy in essence, it seems in consequence of the present knowledge meaningful to extend KUMMER's conjecture as follows:

$$h_1(m) \sim G(m) \ (m \to \infty) .$$

4. At the end of the first chapter we show, by means of (7), that there exists an m_0 such that, for $m > m_0$,

$$h_1(m) < h_1(pm) \text{ if } \begin{cases} 2 \mid m \text{ and } p \text{ is a prime,} \\ 2 \nmid m \text{ and } p \text{ is an odd prime or 4.} \end{cases}$$

In addition, if we write $m = p^u k$, where p is a prime $(p \nmid k)$ and u is a natural number, we prove that $h_1(m)$ is strictly increasing for $m > m_0'$, when m increases in such a way that u and k remain constants. If $k = 1$, this yields our result (cf. [13]), which includes the corresponding result of ANKENY and CHOWLA.

5. In the second chapter we consider DIRICHLET's L-functions

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

closely associated with the conception of the class number. Here $\chi(n)$ denotes a character (mod k), where k is a natural number.

By using a similar method as in the proof of (2) ANKENY and CHOWLA [1], [2] showed that on the assumption of the extended RIEMANN hypothesis there exists for every positive ε and for every s satisfying the condition

$$\tfrac{1}{2} < \Theta_1 < s < \Theta_2 < 1$$

a non-principal character $\chi(n)$ (mod p) such that

$$|L(s , \chi)| < 1 + \varepsilon ,$$

when the prime $p > p_0(\varepsilon)$.

We prove that the method of ANKENY and CHOWLA can also in this case be extended. Here we must assume that

$$(9) \qquad s \geqq \eta = (\tau + \delta)/(\tau + 1) , \ k > k_0(\varepsilon , \delta) \ (0 < \delta < \tfrac{1}{2}) ,$$

where $\tau = \omega(k)$ or $\omega(k) + 1$ if k is odd or even respectively. We show that for every s and k satisfying the conditions (9) there exists a non-principal $\chi(n) \pmod k$ such that

$$|L(s, \chi)| < 1 + \varepsilon \ (\varepsilon > 0) .$$

If k is an odd prime, this leads to the result of ANKENY and CHOWLA.

6. In the third chapter we consider the case $m = p^u$, where p is a prime and u is a natural number. It has been shown (cf. e.g. [19], pp. 796—802) that $h_1 = h_1(2^u)$ can be written in the form

$$h_1 = K h_1' , \tag{10}$$

where h_1' is the first factor of the class number of the cyclotomic field $k(\exp(2\pi i/2^{u-1}))$ and K (see (8.4)) is an integer.

WESTLUND [20] showed that also in the case $p \geqq 3$, $u \geqq 2$, $h_1(p^u)$ can be represented in the form (10). In this case K, defined by (8.6), is also an integer and h_1' is respectively the first factor of the class number of the cyclotomic field $k(\exp(2\pi i/p^{u-1}))$.

INKERI [9] expressed $h_1(p)$ $(p \geqq 3)$ as a determinant (see (8.2)), from which we can among other things conclude that $h_1(p)$ is an integer.

CARLITZ and OLSON [4] started from the so-called MAILLET's determinant D_p and obtained the result

$$h_1(p) = \pm p^{(3-p)/2} D_p \ (p \geqq 3) .$$

In the third chapter, we show first that the connection with INKERI's and MAILLET's determinants can be verified directly without reference to the factor $h_1(p)$. Our main purpose, however, is to treat the factor K, and we derive for it some new expressions as determinants, which among other things enable us to represent $h_1(p^u)$ as a product of determinants. By applying the above results we finally estimate an upper bound for the factor K, which further yields an upper bound for the factor $h_1(p^u)$. It should be noted that these results were given in [13].

Chapter I

AN ASYMPTOTIC ESTIMATION OF THE FIRST FACTOR OF THE CLASS NUMBER OF THE CYCLOTOMIC FIELD

§ 1. Theorems

7. In this chapter we consider the behaviour of the first factor $h_1(m)$ of the class number of the cyclotomic field $k(e^{2\pi i/m})$, when m tends to infinity. It should be noted that $m \geqq 3$ throughout this paper. This fact follows from the restrictions for m introduced in section 1. In this paper p always denotes a prime and u a natural number. Our primary object is to prove

Theorem 1. *Let c and $c(\varepsilon)$ denote, respectively, an absolute positive constant and a positive constant depending on parameter $\varepsilon(>0)$ alone. Then*

$$c(\varepsilon)m^{-\varepsilon} < h_1(m)/G < \exp(c(\log\log m + \omega(m)))\,,$$

where

$$G = G(m) = \varrho\,\varrho'(2\pi)^{-q(m)/2} \mid d^{1/4} \mid m\,. \tag{1.1}$$

Here d denotes the discriminant of the field $k(e^{2\pi i/m})$ and

$$\varrho' = \varrho'(m) = \begin{cases} 1 \text{ if } 2 \mid m\,, \\ 2 \text{ if } 2+m\,, \end{cases} \tag{1.2}$$

$$\varrho = \varrho(m) = \begin{cases} 2^{\frac{1}{2}} \text{ if } m = 2^u\,, \\ p^{1/4} \text{ if } m = p^u\ (p > 2), \\ 1 \text{ elsewhere.} \end{cases} \tag{1.3}$$

As a consequence of this we have

Theorem 2. *Let $m = p^u k$, where $p+k$. If q is a prime such that $q > p$ and $q+k$ then*

$$h_1(q^u k) > h_1(p^u k)\,,$$

when $p^u k$ *is great enough. In addition there exists an* m_0 *such that, for* $m > m_0$,

$$h_1(m) < \begin{cases} h_1(pm) & \text{if } 2 \mid m \text{ and } p \geqq 2 , \\ h_1(pm) & \text{if } 2 + m \text{ and } p \geqq 3 , \\ h_1(4m) & \text{if } 2 + m . \end{cases}$$

When $m = p$ is an odd prime, it follows from (1.2) and (1.3) that $\varrho' = 2$ and $\varrho = p^{1/4}$. Since $|d| = p^{p-2}$ (cf. e.g. [6], p. 506), we get, by (1.1),

$$G = 2p(p^{\frac{1}{2}}/2\pi)^{(p-1)/2} .$$

We have

$$\exp(c(\log\log p + 1)) < (\log p)^{c'} ,$$

where c' is a positive constant. Because $\omega(p) = 1$, we can thus conclude that theorem 1 implies the result (3) introduced by TATUZAWA [17].

8. In order to prove the above theorems we first, in paragraph 2, consider the so-called characters and present some preliminary results, which are needed particularly in paragraphs 3 and 4. In paragraph 3 we investigate the factor $h_1(m)$ in order to find for it the expression, which would give a proper starting point for estimation. In paragraph 4 we focus our attention on the asymptotic estimation of $h_1(m)$, and finally, in paragraph 5, we prove theorem 2.

§ 2. Characters

9. Let k be a natural number. A function χ (of an integral variable) is a character (mod k) if it has the following three properties:

(i) $\chi(n) = 0$ if and only if $(n , k) > 1$,

(ii) $\chi(n) = \chi(l)$ if $n \equiv l \pmod{k}$,

(iii) $\chi(nl) = \chi(n)\,\chi(l)$ for every pair of integers n , l .

It follows from these basic properties (cf. e.g. [7], pp. 216—224 and [14], pp. 99—103) that the number of characters (mod k) is $\varphi(k)$ and one of them is the so-called principal character χ_0 , for which $\chi_0(n) = 1$, whenever $(n , k) = 1$. Further we have

$$\sum_{n=1}^{k} \chi(n) = \begin{cases} \varphi(k) & \text{if } \chi = \chi_0 , \\ 0 & \text{if } \chi \neq \chi_0 , \end{cases} \tag{2.1}$$

$$\sum_{\chi \in R(k)} \chi(n) = \begin{cases} \varphi(k) & \text{if } n \equiv 1 \pmod{k}, \\ 0 & \text{elsewhere,} \end{cases} \tag{2.2}$$

where $R(k)$ denotes the set of the characters (**mod** k).

10. We say that the character $\chi_1 \pmod{k_1}$ is equivalent to $\chi_2 \pmod{k_2}$ and write

$$\chi_1 \approx \chi_2$$

if and only if

$$\chi_1(n) = \chi_2(n)$$

for every n, which satisfies the conditions

$$(n, k_1) = (n, k_2) = 1.$$

Obviously this ($\approx$) is an equivalence relation on the set of the characters. If $\chi_1 \approx \chi_2$ then we say that the character χ_1 is definable modulo k_2, and we call k_2 a defining modulus for χ_1. If k_2 is a defining modulus for χ_1 then the corresponding character χ_2 is completely determined by χ_1.

We now present some results, which follow from the above definitions (cf. [6], pp. 67—70 and [7], pp. 216—224).

Lemma 1. *Let k' be a divisor of k. In order that a character $\chi \pmod{k}$ be definable modulo k', it is necessary and sufficient that $\chi(n) = 1$ for*

$$(n, k) = 1, \quad n \equiv 1 \pmod{k'}.$$

Lemma 2. *If k' is any multiple of k then a character $\chi \pmod{k}$ is definable modulo k'. If k_1 and k_2 are defining moduli for χ, then so is (k_1, k_2).*

Lemma 3. *If χ is a character then all defining moduli for χ are multiples of the least modulus. This is denoted by $f(\chi)$ and is called the conductor of χ.*

A character $\chi \pmod{k}$ is said to be a primitive character (mod k) (denoted usually by χ^*) if $k = f(\chi)$, the conductor of χ. Otherwise χ is called an imprimitive character (mod k).

Lemma 4. *If χ is a character $\pmod{k}$ and $f(\chi)$ its conductor then there exists a unique character $\chi^* \pmod{f(\chi)}$ equivalent to χ. Moreover, χ^* is primitive.*

Lemma 5. *Let χ be a character $\pmod{k}$ and suppose that*

$$k = k_1 k_2 \ldots k_l$$

is a decomposition of k into pairwise coprime positive integers. Then there exists a unique decomposition of χ into characters $\chi_j \pmod{k_j}$

$$\chi = \chi_1 \chi_2 \cdots \chi_l$$

such that

$$f(\chi) = f(\chi_1) f(\chi_2) \cdots f(\chi_l) ,$$

where $f(\chi_j)$ *is the conductor of* χ_j .

In the following we consider especially the characters $\chi \pmod m$, where m is fixed. There exists, by lemma 4, for each character $\chi \pmod m$ a unique character $\chi^* \pmod f$ equivalent to χ , where $f = f(\chi)$ is the conductor of χ. We denote by S the set of all these characters $\chi^* \pmod{f(\chi)}$. Obviously S is also the set of all the primitive characters, each of which is equivalent to a character (mod m) (cf. lemma 4). Throughout this paper we use the notation χ instead of χ^* where there exists no danger of misconception.

We say that the character χ is even or odd if $\chi(-1) = +1$ or -1 respectively. Further we denote by $a(k)$ and $b(k)$, respectively, the number of the even and the odd characters $\chi \pmod k$, which belong to the set S . In addition we have

$$n(k) = a(k) + b(k) ,$$

where $n(k)$ is the number of all the characters in S , which are primitive characters (mod k). It follows from lemma 3 that $k \mid m$.

11. With the help of the above lemmas we now prove the following

Lemma 6. *Let* k *be a divisor of* m . *If* k *is divisible by the square of an odd prime or by* 8 *then*

$$a(k) = b(k) = \tfrac{1}{2}\, n(k) . \tag{2.3}$$

If k *is divisible neither by the square of an odd prime nor by* 8, *then*

$$a(k) = b(k) = n(k) = 0 \quad \text{if } 2 \mid k \text{ and } 4 \nmid k , \tag{2.4}$$

but

$$b(k) = \tfrac{1}{2}\,(n(k) - (-1)^{\omega(k)}) \quad \text{if } 2 \nmid k \text{ or } 4 \mid k . \tag{2.5}$$

Proof. If $\omega(k) = 0$ then (2.5) is true, since now $k = 1$, $n(k) = 1$ and $b(k) = 0$. Consider next the case $\omega(k) = 1$. Now k is of the form p^u .

If $p^u = 2$ then $n(k) = 0$, since there exists no primitive character (mod 2).

Suppose $p^u > 2$. If we denote by χ_p a character (mod p^u) then it follows from (2.2) that

$$\sum\nolimits' \chi_p(-1) + \sum\nolimits'' \chi_p(-1) = 0 , \tag{2.6}$$

where, in Σ' and Σ'', the summation occurs over all the primitive and all the imprimitive characters (mod p^u) respectively. The characters in the

sum Σ'' are characters (mod p^{u-1}) ($u \geqq 2$). Since, on the other hand, every character (mod p^{u-1}) is also a character (mod p^u) (see lemma 2), we can decide that every character (mod p^{u-1}) occurs in the sum Σ''.

Suppose first that $u \geqq 2$ and $p^u \geqq 8$. It then follows from (2.2) that $\Sigma'' = 0$. According to the definitions of the even and the odd characters we now conclude, by the equation (2.6), that

$$a(p^u) = b(p^u) = \tfrac{1}{2}\, n(p^u) .$$

Let $p^u = 4$. Consequently $\Sigma' = -1$, since, by (2.2), $\Sigma'' = 1$. Hence we get

$$b(4) = \tfrac{1}{2}\,(n(4) + 1) .$$

Let p be an odd prime and $u = 1$. In this case the sum Σ'' contains, by lemma 1, only the principal character. Hence $\Sigma'' = 1$, and we can write

$$b(p) = \tfrac{1}{2}\,(n(p) + 1) .$$

We have thus shown that our theorem is true, when $\omega(k) = 1$. Suppose now that $\omega(k) > 1$. Let χ (mod k) be a character in S. It follows from lemma 5 that χ can be written in the form

$$\chi = \chi_p\, \chi_1 , \quad k = p^u k_1 \quad (p \nmid k_1) , \tag{2.7}$$

where χ_p and χ_1 are characters (mod p^u) and (mod k_1) respectively. Further we get

$$k = f(\chi) = f(\chi_p)\, f(\chi_1) . \tag{2.8}$$

Since $f(\chi_p) \leqq p^u$ and $f(\chi_1) \leqq k_1$, it follows from (2.7) and (2.8) that

$$f(\chi_p) = p^u , \; f(\chi_1) = k_1 .$$

We can thus conclude that S contains also the characters χ_p and χ_1. Suppose, on the other hand, that χ_p (mod p^u) and χ_1 (mod k_1) are characters in S. Then it is clear that $\chi = \chi_p\, \chi_1$ is a character (mod k) and we can, by lemma 5, decide that

$$f(\chi) = p^u k_1 ,$$

which yields that $f(\chi) = k$. Consequently we find that χ belongs to S.

Suppose now that k is divisible by the square of an odd prime or by the number 8. It is then possible to assume that in (2.7) $u \geqq 2$ and $p^u \geqq 8$. Hence we get

$$\begin{aligned} b(k) &= a(p^u)\, b(k_1) + b(p^u)\, a(k_1) \\ &= \tfrac{1}{2}\, n(p^u)\, (a(k_1) + b(k_1)) = \tfrac{1}{2}\, n(k) . \end{aligned}$$

We thus observe that the first part of our lemma is true.

If k is divisible neither by the square of an odd prime nor by 8, let us suppose first that $2 \mid k$ but $4 \nmid k$. In this case we can in (2.7) choose $p = 2$ and $u = 1$, and we get

$$n(k) = n(2)\, n(k_1) = 0 .$$

The cases $2 \nmid k$ or $4 \mid k$, so far not considered, we prove by induction on $\omega(k)$. Suppose that k ($\omega(k) > 1$) is such a divisor of m, and assume that the lemma is true for all the divisors k' in question, which satisfy the condition

$$\omega(k') < \omega(k) .$$

In (2.7) we may assume that p is an odd prime and $u = 1$. Since

$$\omega(k_1) = \omega(k) - 1 ,$$

it now follows from (2.5) that

$$b(k) = b(k_1)\, a(p) + a(k_1)\, b(p)$$

$$= \tfrac{1}{2}(n(k_1) - (-1)^{\omega(k)-1})\, \tfrac{1}{2}(n(p) - 1) + \tfrac{1}{2}(n(k_1) + (-1)^{\omega(k)-1})\, \tfrac{1}{2}(n(p) + 1)$$

$$= \tfrac{1}{2}\,(n(k) - (-1)^{\omega(k)}) .$$

We now decide that also in this case our lemma is true, and thus the proof is concluded.

12. For the odd characters we finally prove the following

Lemma 7. *Let k be a natural number and denote by $Q(k)$ the set of the odd characters $\chi \pmod k$. If n is an integer then*

$$\sum_{\chi \in Q(k)} \chi(n) = \begin{cases} \tfrac{1}{2}\varphi(k) & \text{if } n \equiv 1 \pmod k \text{ and } k > 2 , \\ -\tfrac{1}{2}\varphi(k) & \text{if } n \equiv -1 \pmod k \text{ and } k > 2 , \\ 0 & \text{elsewhere} . \end{cases} \tag{2.9}$$

Further

$$\sum_{\chi \in P} \chi(n) = \sum_{\chi \in Q(m_n)} \chi(n) , \tag{2.10}$$

where m_n is the greatest divisor of m prime to n, and P denotes the set of the odd characters in S.

Proof. Suppose first that $k = 1$ or 2. Since there exists only one character both (mod 1) and (mod 2), namely the principal character, which is even, it follows that the sum in (2.9) is empty. Consequently the value of the sum is zero, and in this case our lemma is true.

If $k > 2$ we get, by (2.2),

$$\sum_{\chi \in R(k)} \chi(-1) = 0 .$$

We now find that the number of the even characters is equal to the number of the odd characters. Since, on the other hand, the number of all the characters (mod k) is $\varphi(k)$, we can conclude that

$$\sum_{\chi \in Q(k)} \chi(n) = \begin{cases} \frac{1}{2}\varphi(k) & \text{if } n \equiv 1 \pmod{k}, \\ -\frac{1}{2}\varphi(k) & \text{if } n \equiv -1 \pmod{k}. \end{cases}$$

Suppose now that

$$n \not\equiv \pm 1 \pmod{k}.$$

In this case we can write

$$\sum_{\chi \in R(k)} \chi(n) = \sum_{\chi \in T(k)} \chi(n) + \sum_{\chi \in Q(k)} \chi(n) = 0,$$

$$\sum_{\chi \in R(k)} \chi(-n) = \sum_{\chi \in T(k)} \chi(n) - \sum_{\chi \in Q(k)} \chi(n) = 0,$$

where $T(k)$ denotes the set of the even characters in $R(k)$. If we subtract both sides of the above equations from each other, we get

$$\sum_{\chi \in Q(k)} \chi(n) = 0,$$

which proves (2.9).

Consider now the equation (2.10). We find that $\chi(n)$ $(\chi \in S)$ is different from zero if and only if $f(\chi) | m_n$. We denote by S_n the set of all these characters in S. According to lemma 2 there exists for every character in S_n a character (mod m_n) equivalent to it. Since $m_n | m$, there exists, on the other hand, for every character (mod m_n) a unique character (mod m) equivalent to it, and it follows from this and lemma 3 that there exists for every character χ_n (mod m_n) a unique character χ in S_n such that

$$\chi \approx \chi_n.$$

We can thus conclude that there exists one-to-one map of S_n onto the set of the characters (mod m_n). From the definition of m_n we get

$$(n, m_n) = (n, f(\chi)) = 1 \quad (\chi \in S_n),$$

and hence

$$\chi(n) = \chi_n(n). \tag{2.11}$$

The sum $\Sigma_{\chi \in P} \chi(n)$ may now, by (2.11), be written in the form

$$\sum_{\chi \in P} \chi(n) = \sum_{\chi \in P \cap S_n} \chi(n) = \sum_{\chi \in Q(m_n)} \chi(n). \tag{2.12}$$

(It should be noted that (2.12) holds also in the case $m_n = 1$. In this case the sets $P \cap S_n$ and $Q(m_n)$ are empty, and all the sums in (2.12) have the value zero.)

§ 3. Expression for $h_1(m)/G(m)$

13. Our intention here is to treat the factor $h_1(m)$ in such a way that in later work we are able to estimate it with the help of series. We need the following lemmas:

Lemma 8. *The factor* $h_1(m)$ *can be expressed in the form*

$$h_1(m) = 2^{\alpha}\,(2m)^{1-q(m)/2} \prod_{\chi \in P} \sum_{n=1}^{m} \chi(n)n\ ,$$

where $\alpha = -1$ *or* 0 *if* m *is even or odd respectively* (cf. [8], p. 376).

Lemma 9. *If* d *denotes the discriminant of the field* $k(e^{2\pi i/m})$ *then*

$$|d| = \prod_{\chi \in S} f(\chi)$$

(cf. [7], p. 403).

We consider the DIRICHLET L-series

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

where $s = \sigma + it$. For these series we have

Lemma 10. *Let* χ *be an arbitrary odd character. If* $f = f(\chi)$ *is the conductor of* χ *then*

$$|L(1\ ,\ \chi)| = \pi f^{-3/2} \left| \sum_{n=1}^{f} \bar{\chi}(n)n \right|,$$

where $\bar{\chi}$ *denotes the inverse of the character* χ (cf. [7], pp. 400—401).

Lemma 11. *If* χ^* *is an odd character primitive* (mod f) *then*

$$\left| \sum_{n=1}^{m} \bar{\chi}^*(n)n \right| = m f^{\frac{1}{2}}\, \pi^{-1}\, |L(1\ ,\ \chi^*)|\ .$$

Proof. If we denote $m = kf$ then

$$\sum_{n=1}^{m} \bar{\chi}^*(n)n = \sum_{j=0}^{k-1} \sum_{n=1}^{f} \bar{\chi}^*(n)n + \sum_{j=0}^{k-1} \sum_{n=1}^{f} \bar{\chi}^*(n)jf = k \sum_{n=1}^{f} \bar{\chi}^*(n)n\ . \tag{3.1}$$

Here we have made use of (2.1). By lemma 10 we get

$$\left| \sum_{n=1}^{f} \bar{\chi}^*(n)n \right| = f^{3/2}\, \pi^{-1}\, |L(1\ ,\ \chi^*)|\ .$$

This together with (3.1) yields our lemma.

14. Lemma 6 presented in the preceding paragraph enables us to prove

Lemma 12. *If* ϱ *is defined by* (1.3) *then*

$$\prod_{\chi \in P} f^{\frac{1}{2}} = \varrho \, | d^{1/4} | \, .$$

Proof. We write

$$\prod_{\chi \in P} f = \prod_{k \mid m} k^{b(k)} = \prod\nolimits_1 k^{b(k)} \prod\nolimits_2 k^{b(k)},$$

where, in Π_1, k runs through the divisors of m divisible by the square of an odd prime or which are $\equiv 0 \pmod 8$ or $\equiv 2 \pmod 4$, and, in Π_2, k runs through all the rest of divisors of m. It follows now from lemma 6 that

$$\prod\nolimits_1 k^{b(k)} = \prod\nolimits_1 k^{n(k)/2} \, , \quad \prod\nolimits_2 k^{b(k)} = \varrho^2 \prod\nolimits_2 k^{n(k)/2} \, ,$$

where

$$\varrho^4 = \prod\nolimits_2 k^{-(-1)^{\omega(k)}} \, . \tag{3.2}$$

By lemma 9 we have

$$\prod_{\chi \in P} f = \varrho^2 \prod_{k \mid m} k^{n(k)/2} = | d^{\frac{1}{2}} | \, \varrho^2 \, .$$

Suppose first $\omega(m) = 1$. In this case $m = p^u$, where p is an odd prime $(u \geqq 1)$, or $m = 2^u$ $(u \geqq 2)$, and we conclude from (3.2) that $\varrho^4 = p$ or $\varrho^4 = 4$ respectively.

We may now assume that $\omega(m) > 1$. Let p be a prime such that $p \mid m$. If we distinguish from ϱ^2 the power of p, we get for odd p the exponent

$$\tfrac{1}{2}(1 - \tbinom{\omega(m)-1}{1} + \tbinom{\omega(m)-1}{2} - \ldots \pm 1) = \tfrac{1}{2}(1 - 1)^{\omega(m)-1} = 0 \, . \tag{3.3}$$

If, on the other hand, $p = 2$, we get for it the exponent in (3.3) multiplied by 2. We thus have

$$\varrho^2 = 1 \; (\omega(m) > 1) \, .$$

This completes the proof.

15. It now follows from the above lemmas that

$$h_1(m)/G = | \prod_{\chi \in P} L(1 \, , \chi) | \, , \tag{3.4}$$

where G is defined by (1.1). From lemmas 11 and 12 we namely get

$$|\prod_{\chi\in P}\sum_{n=1}^{m}\chi(n)n| = (m/\pi)^{\varphi(m)/2}\prod_{\chi\in P}(f^{\frac{1}{2}}\,|\,L(1\,,\,\chi)\,|)$$
$$= (m/\pi)^{\varphi(m)/2}\,\varrho\,|\,d^{1/4}\prod_{\chi\in P}L(1\,,\,\chi)\,|\,.$$

Hence, by lemma 8,

$$h_1(m) = 2^{\alpha+1}(2\pi)^{-\varphi(m)/2}\,m\,\varrho\,|\,d^{1/4}\prod_{\chi\in P}L(1\,,\,\chi)\,|\,,$$

which leads to (3.4).

§ 4. Estimation for $h_1(m)$

16. In order to find an asymptotic estimation for the factor $h_1(m)$ we consider the expression

$$|\prod_{\chi\in P}L(1\,,\,\chi)\,|\,.$$

Throughout this and the next paragraph we use c and $c(\varepsilon)$ to denote respectively an absolute positive constant and a positive constant depending only on parameter $\varepsilon\ (>0)$ not necessarily the same in their various occurrences. In addition, in this paragraph, the constant implied in O is always an absolute one. We need the following lemmas:

Lemma 13. *Let* $\chi(\neq\chi_0)$ *be a character* (mod m), *which has the conductor* f. *Then*

$$L(1\,,\,\chi^*) = L(1\,,\,\chi)\prod_{p\,|\,m}(1-\chi^*(p)/p)^{-1}\,, \tag{4.1}$$

where χ^* *is the corresponding primitive character* (mod f) *and* p *runs through the prime factors of* m (cf. [14], p. 127).

Lemma 14. *If* $x\geqq 3$ *then*

$$\sum_{p\leqq x}p^{-1} = O(\log\log x)$$

(cf. [14], p. 20).

Lemma 15. *Let* $(m\,,\,l)=1$ *and* $0\leqq l<m$. *If* $\pi(x\,,\,m\,,\,l)$ *is the number of primes* $\equiv l$ (mod m) *not exceeding* x *then*

$$\pi(x\,,\,m\,,\,l) = O(\varphi(m)^{-1}\,x/\log(x/m))\ (x>m)$$

(cf. [14], p. 44).

In the further procedure we require the conception of the so-called exceptional character χ'. Let $s=\sigma+it$. If

$$\sigma\geqq 1-c/\log(m(\,|\,t\,|+2))\geqq 3/4\,,$$

then

$$L(s\ ,\ \chi) \neq 0$$

for every $\chi \pmod m$ with one possible exception. If such an exceptional character exists, it is a real one and we denote it by χ' (cf. [14], p. 130). We can now formulate the following lemmas:

Lemma 16. *Let* $m \leqq \exp(\log^{\frac{1}{2}} x)$ *and* $\chi \neq \chi_0\ ,\ \chi'$. *Then*

$$\sum_{n \leqq x} \chi(n)\, \Lambda(n) = O(x \exp(-\ c\ \log^{\frac{1}{2}} x)\ )\ ,$$

where

$$\Lambda(n) = \begin{cases} \log\ p & \text{if}\ \ n = p^j\ \ (j \geqq 1)\ , \\ 0 & \text{otherwise} \end{cases}$$

(cf. [14], pp. 133—136).

Lemma 17. *Let*

$$U(x) = \sum_{\chi \in Q'} \sum_{n \leqq x} \chi(n)\, \Lambda(n)\ ,$$

where Q' *denotes the set* $Q(m)$ *excluded* χ' . *If*

$$x \geqq \exp(\log^3 m)$$

then $U(x) = O(x/\log x)$.

Proof. Since

$$\log m \leqq \log^{1/3} x\ ,$$

it follows, by lemma 16, that

$$U(x) = O(\varphi(m)\ x \exp(-\ c \log^{\frac{1}{2}} x)) = O(x \exp(\log m - c \log^{\frac{1}{2}} x)) = O(x/\log x)\ .$$

Lemma 18. *The exceptional character* χ' *satisfies the inequality*

$$|L(1\ ,\ \chi')| > c(\varepsilon) m^{-\varepsilon}$$

(cf. [5], p. 275, and [16], p. 163).

The proof of this lemma is also included in PRACHAR's considerations (cf. [14], p. 145—146).

17. The number of prime factors of m denoted by $\omega(m)$ plays an important role in our estimations. For it we present the following three lemmas:

Lemma 19. $\omega(m) = O(\log m/\log\log m)$
(cf. [17], p. 108).

Lemma 20. *If* n *is a natural number and* a *is an integer such that* $(a, m) = 1$ *then the number of solutions of*

$$x^n \equiv a \pmod{m} \tag{4.2}$$

is at most $n^{\omega(m)+1}$.

This follows immediately if we denote

$$m = p_1^{u_1} p_2^{u_2} \dots p_l^{u_l} ,$$

where the numbers p_j are distinct primes and the integers $u_j \geqq 1$. Suppose namely that n_j denotes the number of solutions of the congruence

$$x^n \equiv a \pmod{p_j^{n_j}} ,$$

where j assumes the values $1, 2, \dots, l$. Since

$$n_j \leqq \begin{cases} n & \text{if } p_j \neq 2 , \\ n^2 & \text{if } p_j = 2 , \end{cases}$$

we get that the number of solutions of (4.2) equal to

$$\prod_{j=1}^{n} n_j$$

is at most $n^{\omega(m)+1}$.

The following lemma has an important meaning for the estimation of $h_1(m)$. Therefore we give for it a detailed proof, which in some degree differs from the proof of TATUZAWA [17].

Lemma 21. *If*

$$p^n \equiv \pm 1 \pmod{m} \tag{4.3}$$

then

$$\sum_{n \geqq 2} \sum_{p} (np^n)^{-1} = O(\omega(m)/m) . \tag{4.4}$$

Proof. We divide the series in the left-hand side of (4.4) into two parts S_1 and S_2 , where, in S_1 and in S_2, p runs through all the values, which satisfy (4.3), and which are smaller and greater than m respectively. In order to estimate S_1 we write

$$S_1 = \sum_{n=2}^{\infty}{}' n^{-1} \sum_{\substack{p<m \\ p^n \equiv \pm 1 \pmod{m}}} p^{-n} . \tag{4.5}$$

Let us denote

$$M(n) = 2(n-1)^{2\omega(m)+1} + 1 , \; N(n) = 2n^{2\omega(m)+1} ,$$

whence it follows that

$$N(n) - M(n) > 2n^{2\omega(m)},$$

since $n \geqq 2$. It follows from lemma 20 that we can write (for a fixed n)

$$p^n = v_j m \pm 1 \quad (j = M(n),\ M(n)+1,\ \ldots,\ M(n)+\beta_n - 1), \tag{4.6}$$

where v_j denotes a natural number and β_n is the number of incongruent solutions p of the congruences (4.3). Further we define

$$v_j = A^j \quad (M(n) + \beta_n \leqq j \leqq N(n)), \tag{4.7}$$

where A is the product of all the primes not exceeding m. We thus have

$$\sum_{\substack{p<m \\ p^n \equiv \pm 1 \pmod m}} p^{-n} \leqq \sum_{j=M(n)}^{N(n)} (v_j m - 1)^{-1} < 2m^{-1} \sum_{j=M(n)}^{N(n)} v_j^{-1}. \tag{4.8}$$

Denote

$$V_n = \sum_{j=M(n)}^{N(n)} v_j^{-1}, \quad V(x) = \sum_{2 \leqq n \leqq x} V_n.$$

By using ABEL's method of partial summation we now get

$$\sum_{2 \leqq n \leqq x} V_n/n = V(x)/[x] + \sum_{2 \leqq n \leqq x-1} n^{-1}(n+1)^{-1} V(n), \tag{4.9}$$

where $[x]$ denotes the largest integer $\leqq x$. Since $M(n+1) = N(n) + 1$, we get

$$V(n) = \sum_{j=3}^{N(n)} v_j^{-1}.$$

Here the integers v_j are positive and the same number occurs at most two times. We replace distinct numbers v_j in order of ascending magnitude by the numbers 1, 2, 3, ... Hence

$$V(n) \leqq 2 \sum_{j=1}^{N(n)} j^{-1} = O(\log N(n)) = O(\omega(m) \log n),$$

It now follows from (4.9) that

$$\sum_{2 \leqq n \leqq x} V_n/n = O(\omega(m) x^{-1} \log x) + O(\omega(m) \sum_{2 \leqq n \leqq x-1} n^{-1}(n+1)^{-1} \log n).$$

If x tends to infinity, this yields

$$\sum_{n=2}^{\infty} V_n/n = O(\omega(m)).$$

This together with (4.5) and (4.8) leads to the result

$$S_1 = O(\omega(m)/m).$$

We estimate the series S_2 as follows:

$$S_2 = O(\sum_{p>m} \sum_{n\geqq 2} p^{-n}) = O(\sum_{p>m} p^{-1}(p-1)^{-1}) = O(m^{-1}) .$$

This, combined with the above estimation of S_1, proves our lemma.

18. According to (4.1) we can decide that

$$\prod_{\chi \in P} L(1, \chi) = \prod_{\chi \in Q(m)} L(1, \chi) \prod_{\chi \in P} \prod_{p \mid m} (1 - \chi(p)/p)^{-1} . \tag{4.10}$$

The product in the right-hand side of (4.10) can be treated in two parts. We estimate the product

$$\prod_{\chi \in Q(m)} L(1, \chi)$$

by using TATUZAWA's method [17].

We first write ([17], p. 109; cf. [12], p. 449)

$$\prod_{\chi \in Q'} L(1, \chi) = \exp(\sum_{\chi \in Q'} \sum_{n\geqq 2} \chi(n) \Lambda(n) (n \log n)^{-1}) . \tag{4.11}$$

From the exponent of the equation (4.11) we distinguish a finite sum being extended over all integers n such that

$$2 \leqq n \leqq W = [\exp(\log^3 m)] .$$

We denote $V = 3m$ and divide this sum into five parts as follows:

$$\Sigma_1 = \sum_{p<V} p^{-1} (\sum_\chi \chi(p)) , \quad \Sigma_2 = \sum_{V<p\leqq W} p^{-1} (\sum_\chi \chi(p)) ,$$

$$\Sigma_3 = -\sum_{p\leqq W} p^{-1} \chi'(p) , \quad \Sigma_4 = \sum_{p^n \leqq W} \sum_{n\geqq 2} (np^n)^{-1} (\sum_\chi \chi(p^n)) ,$$

$$\Sigma_5 = -\sum_{p^n \leqq W} \sum_{n\geqq 2} (np^n)^{-1} \chi'(p^n) ,$$

where in Σ_χ χ runs through all the characters of $Q(m)$. In addition we denote

$$\Sigma_6 = \sum_{n>W} \sum_{\chi \in Q'} \chi(n) \Lambda(n) (n \log n)^{-1} .$$

Now our object is to estimate Σ_j by using the above lemmas. It follows. by lemma 7, that

$$|\Sigma_1| \leqq \tfrac{1}{2}\varphi(m) \sum_{\substack{p<V \\ p \equiv \pm 1 (\mathrm{mod}\ m)}} p^{-1}$$

$$\leqq \varphi(m) \sum_{mj-1<V} (mj-1)^{-1} = O(\varphi(m)\, m^{-1} \sum_{j\leqq 4} j^{-1}) = O(1).$$

From lemma 15 we get, by using ABEL's partial summation,

$$|\sum_2| \leqq \tfrac{1}{2}\varphi(m) \sum_{\substack{V<p\leqq W \\ p\equiv \pm 1 (\mathrm{mod}\ m)}} p^{-1}$$

$$= \tfrac{1}{2}\varphi(m) \sum_{V<n\leqq W-1} (\pi(n\ ,\ m\ ,\ +1) + \pi(n\ ,\ m\ ,\ -1))\ (n^{-1} - (n+1)^{-1}) + O(1)$$

$$= O\left(\int_V^W (\xi \log(\xi/m))^{-1}\, d\xi\right) + O(1) = O(\log\log m)\ .$$

By lemma 14, we get

$$\sum_3 = O(\log\log m)\ ,$$

and from lemma 21 it follows that

$$|\sum_4| \leqq \tfrac{1}{2}\varphi(m) \sum_{\substack{p^n\leqq W \\ p^n\equiv \pm 1\ (\mathrm{mod}\ m)}} \sum_{n\geqq 2} (np^n)^{-1} = O(\omega(m))\ .$$

It is easy to verify that

$$\sum_5 = O(1)\ .$$

From lemma 17 we finally get, by ABEL's partial summation,

$$\sum_6 = \sum_{n>W} U(n)\ (n^{-1}/\log n - (n+1)^{-1}/\log(n+1))$$

$$+ (U(W+1) - U(W))/((W+1)\log(W+1)) - U(W+1)/((W+1)\log(W+1))$$

$$= O\left(\int_W^\infty \xi^{-1}\log^{-2}\xi\, d\xi\right) + O(1) = O(1)\ .$$

Combining the above estimations we may, by (4.11), write

$$\exp(-c(\log\log m + \omega(m))) < |\prod_{\chi\in Q'} L(1\ ,\ \chi)| < \exp(c(\log\log m + \omega(m)))\ .$$

It is known that

$$L(1\ ,\ \chi) = O(\log m)\ .$$

This and lemma 18 yields

$$c(\varepsilon)\ m^{-\varepsilon} < |L(1\ ,\ \chi')| < e^{c\log\log m}\ .$$

In addition we have, by lemma 19,

$$\exp(-c(\log\log m + \omega(m))) > m^{-c/\log\log m} > c(\varepsilon)\ m^{-\varepsilon}\ . \tag{4.12}$$

Collecting these results we obtain

$$c(\varepsilon)\ m^{-\varepsilon} < |\prod_{\chi\in Q(m)} L(1\ ,\ \chi)| < \exp(c(\log\log m + \omega(m)))\ . \tag{4.13}$$

19. In order to estimate the product (cf. (4.10))

$$\Pi = \prod_{\chi \in P} \prod_{p \mid m} (1 - \chi(p)/p)^{-1}$$

we write

$$\Pi = \exp\Big(\sum_{\chi \in P} \sum_{p \mid m} \sum_{n=1}^{\infty} \chi(p^n) n^{-1} p^{-n} \Big) . \tag{4.14}$$

It follows from lemma 7 that

$$\Big| \sum_{\chi \in P} \chi(p^n) \Big| = \begin{cases} \frac{1}{2}\varphi(m_p) & \text{if } p^n \equiv \pm 1 \pmod{m_p} \text{ and } m_p > 1 , \\ 0 & \text{otherwise,} \end{cases}$$

where m_p denotes the greatest divisor of m prime to p. Let ζ denote the least positive exponent such that

$$p^{\zeta} \equiv \pm 1 \pmod{m_p} .$$

Now if

$$p^{\nu} \equiv \pm 1 \pmod{m_p} \tag{4.15}$$

then $\zeta \mid \nu$ and, on the other hand, if $\zeta \mid \nu$ then (4.15) holds. Since we can write

$$\sum_{j=1}^{\infty} (p^{-\zeta})^j = (p^{\zeta} - 1)^{-1} \leqq 3(p^{\zeta} \pm 1)^{-1} \leqq 3\, m_p^{-1} ,$$

we have

$$\sum_{\chi \in P} \sum_{p \mid m} \sum_{n=1}^{\infty} \chi(p^n) n^{-1} p^{-n} = O\Big(\sum_{p \mid m} \varphi(m_p)/m_p \Big) = O(\omega(m)) .$$

Hence

$$e^{-c\omega(m)} < |\, \Pi \,| < e^{c\omega(m)} .$$

This, together with (4.13) and lemma 19 (cf. (4.12)), yields

$$c(\varepsilon) m^{-\varepsilon} < \Big| \prod_{\chi \in P} L(1 , \chi) \Big| < \exp(c(\log\log m + \omega(m))) . \tag{4.16}$$

From (3.4) and (4.16), it now follows that theorem 1 is true. As we see, the upper bound in (4.16) depends essentially on $\omega(m)$, because there exists an infinity of the numbers m such that

$$\omega(m) > c \log m / \log\log m .$$

In order to get a sharper upper bound we find, on the other hand, that we must mainly focus our attention on the series appearing in lemma 21 and in (4.14).

§ 5. Proof of theorem 2

20. From theorem 1 and lemma 19, it follows that

$$c(\varepsilon)m^{-\varepsilon} < h_1(m)/G < c(\varepsilon)m^{\varepsilon} .$$

This can be also represented in the form

$$\log(h_1(m)/G)/\log m = \varepsilon(m) , \tag{5.1}$$

where $\varepsilon(m) \to 0$, when m tends to infinity.

Let us denote

$$m = p_1^{u_1} p_2^{u_2} \dots p_l^{u_l} ,$$

where $p_1 , p_2 , \dots , p_l$ are distinct primes. We define

$$E(m) = \sum_{j=1}^{l} (u_j - (p_j - 1)^{-1}) \log p_j . \tag{5.2}$$

Since $4 \mid m$, whenever m is even, we get

$$(p_j - 1)^{-1} \leqq \tfrac{1}{2} u_j .$$

This yields the inequality

$$E(m) \geqq \tfrac{1}{2} \log m . \tag{5.3}$$

From the prime divisors of m we choose p_j arbitrarily and denote $p = p_j$ and $u = u_j$. We can thus write the discriminant d in the form (cf. [6], p. 508)

$$\log|d| = \varphi(m)E(m) = \varphi\, \varphi_p((u - (p - 1)^{-1}) \log p + E(k)) , \tag{5.4}$$

where $k = m/p^u$, $\varphi = \varphi(k)$ and $\varphi_p = \varphi(p^u)$. Let $q > p$ be a prime such that $q + k$. We denote by d_1 the discriminant of the cyclotomic field $k(\exp(2\pi i/m_1))$ $(m_1 = q^u k)$. We now get, by (5.2) and (5.4),

$$\begin{aligned} \log|d_1/d| &= \varphi(\varphi_q(u - (q - 1)^{-1}) \log q - \varphi_p(u - (p - 1)^{-1}) \log p) \\ &\quad + \varphi(\varphi_q - \varphi_p) E(k) > \varphi(\varphi_q - \varphi_p)E(m) . \end{aligned} \tag{5.5}$$

It now follows from the equation (1.1) and the inequality (5.5) that

$$\begin{aligned} \log(G_1/G) > \log(\varrho_1/\varrho) + \log(\varrho_1'/\varrho') - \tfrac{1}{2}\varphi(\varphi_q - \varphi_p)\log 2\pi \\ + \varphi(\varphi_q - \varphi_p)E(m)/4 + u \log(q/p) , \end{aligned}$$

where $G_1 = G(m_1)$, $\varrho_1 = \varrho(m_1)$ and $\varrho_1' = \varrho'(m_1)$. We get, by (5.3),

$$(1/4 - c)E(m) > \tfrac{1}{2} \log 2\pi \qquad (0 < c < 1/4) , \tag{5.6.}$$

when m is great enough. It is easy to verify that

$$\log(\varrho_1/\varrho) + \log(\varrho_1'/\varrho') \geqq 0 .$$

Hence

$$\log(G_1/G) > c\,\varphi\, p^{u-1}\, E(m) + u \log(q/p) . \tag{5.7}$$

By (5.1) and (5.7), we obtain

$$\log(h_1(m_1)/h_1(m)) > c\,\varphi\, p^{u-1}\, E(m) + u \log(q/p) + \varepsilon(m_1) \log m_1 - \varepsilon(m) \log m .$$

Let m now be so great that $|\varepsilon(m_1)|$ and $|\varepsilon(m)|$ are less than $c/4$. Furthermore, we have, by (5.3),

$$\log(h_1(m_1)/h_1(m)) > \tfrac{1}{2}\, c\, (\varphi\, p^{u-1} - 1) \log m \geqq 0 .$$

This implies the result

$$h_1(q^u k)/h_1(p^u k) > 1 ,$$

when $q > p$, $(pq, k) = 1$, and $m = p^u k$ is great enough.

21. We denote by d_2 the discriminant of the cyclotomic field $k(e^{2\pi i/pm})$, where $p\ (\geqq 2)$ is a prime factor of m. Then

$$\log|d_2/d| = (\varphi_p'(u + 1 - (p-1)^{-1}) - \varphi_p(u - (p-1)^{-1}))\,\varphi \log p + \varphi(\varphi_p' - \varphi_p) E(k) ,$$

where $\varphi_p' = \varphi(p^{u+1})$. This leads to the inequality

$$\log|d_2/d| > \varphi(\varphi_p' - \varphi_p) E(m) . \tag{5.8}$$

It now follows from (1.1) and (5.8) that

$$\log(G_2/G) > \log(\varrho_2/\varrho) + \log(\varrho_2'/\varrho') - \tfrac{1}{2}\,\varphi(\varphi_p' - \varphi_p) \log 2\pi + \varphi(\varphi_p' - \varphi_p) E(m)/4 + \log p ,$$

where $G_2 = G(pm)$, $\varrho_2 = \varrho(pm)$ and $\varrho_2' = \varrho'(pm)$. When m is great enough then (5.6) holds and

$$\log(G_2/G) > c\varphi(\varphi_p' - \varphi_p) E(m) + \log p . \tag{5.9}$$

We can decide, by (5.1) and (5.9), that

$$\log(h_1(pm)/h_1(m)) > c\,\varphi\, p^{u-1}\, E(m) + \log p + \varepsilon(pm) \log pm - \varepsilon(m) \log m .$$

We choose m so great that $|\varepsilon(pm)|$ and $|\varepsilon(m)|$ are less than $c/4$. If in addition we apply (5.3), we thus get

$$\log(h_1(pm)/h_1(m)) > \tfrac{1}{2}\, c(\varphi p^{u-1} - 1) \log m \geqq 0 .$$

Hence

$$h_1(pm)/h_1(m) > 1 .$$

22. We suppose that q is an odd prime such that $q \nmid m$. Let us denote by d_3 the discriminant of the cyclotomic field $k(e^{2\pi i/qm})$. We may now write, by (5.4),

$$\log|d_3/d| = (q-1)\varphi(m)((q-2)(q-1)^{-1}\log q + E(m)) - \varphi(m)E(m)$$
$$> (q-2)\varphi(m)E(m) .$$

Furthermore, we get

$$\log(G_3/G) > \log(\varrho_3/\varrho) + \log(\varrho_3'/\varrho') - \tfrac{1}{2}(q-2)\varphi(m)\log 2\pi$$
$$+ (q-2)\varphi(m)E(m)/4 + \log q ,$$

where $G_3 = G(qm)$, $\varrho_3 = \varrho(qm)$ and $\varrho_3' = \varrho'(qm)$. It is easy to verify that

$$\log(\varrho_3'/\varrho') = 0 , \quad \log(\varrho_3/\varrho) \geqq -\log m^{1/4} .$$

If m is great enough then

$$\log(G_3/G) > c(q-2)\varphi(m)E(m) + \log(q/m^{1/4}) .$$

Further we have

$$\log(h_1(qm)/h_1(m)) > c(q-2)\varphi(m)E(m) + \log(q/m^{1/4}) + \varepsilon(qm)\log(qm)$$
$$- \varepsilon(m)\log m .$$

If m is great then $|\varepsilon(qm)|$ and $|\varepsilon(m)| < c/4$, and

$$\log(h_1(qm)/h_1(m)) > \tfrac{1}{2}c((q-2)\varphi(m) - 1 - (2c)^{-1})\log m .$$

Since $\varphi(m) \to \infty$, when m tends to infinity, then

$$(q-2)\varphi(m) > 1 + (2c)^{-1}$$

for great values of m. Hence

$$h_1(qm)/h_1(m) > 1 .$$

In the same way we can show that if m is odd then

$$h_1(4m) > h_1(m) , \tag{5.10}$$

when m is great enough. Namely, if we denote by d_4 the discriminant of the cyclotomic field $k(e^{2\pi i/4m})$, we have

$$\log|d_4/d| \geqq \varphi(m)E(m) + 4\log 2 .$$

This yields, by (5.6),

$$\log(G_4/G) > c\varphi(m)E(m) + \log(4/m^{1/4}) ,$$

where $G_4 = G(4m)$ and m is great enough. For great values of m we thus get, by (5.1) and (5.3),

$$\log(h_1(4m)/h_1(m)) > \tfrac{1}{2}\, c(\varphi(m) - 1 - (2c)^{-1}) \log m .$$

This implies (5.10).

Our theorem is thus established.

Chapter II

DIRICHLET'S L-FUNCTIONS

§ 6. Theorem 3 and preliminary lemmas

23. In this chapter we consider the functions

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

where $\chi(n)$ is a character (mod k). Our intention is to prove the following

Theorem 3. *Let* $k(\geqq 3)$ *be a natural number,* ε *an arbitrary positive number,* δ *a positive number* $< \frac{1}{2}$ *and*

$$\tau = \tau(k) = \begin{cases} \omega(k) & \text{if } 2 \nmid k\ , \\ \omega(k) + 1 & \text{if } 2 \mid k\ . \end{cases}$$

If the extended Riemann hypothesis is true, there exists for every given pair s *and* k *, where*

$$s \geqq \eta = (\tau + \delta)/(\tau + 1)\ ,\ k > k_0(\varepsilon\ ,\ \delta)\ , \tag{6.1}$$

a non-principal character $\chi(n)$ (mod k) *such that*

$$|L(s\ ,\ \chi)| < 1 + \varepsilon\ .$$

If $k = p^u$, where p is an odd prime, we get for s the condition

$$s \geqq (1 + \delta)/2\ ,$$

and we can thus decide that the above theorem implies the result of ANKENY and CHOWLA (cf. e.g. [2], p. 487).

24. In order to prove theorem 3 we apply some lemmas expressed in the preceding chapter. In addition we need the following lemmas:

Lemma 22. *If the extended Riemann hypothesis is true and* $(k\ ,\ l) = 1$ *then*

$$\pi(x\ ,\ k\ ,\ l) = \varphi(k)^{-1} \int_{\frac{1}{2}}^{x} d\xi/\log\xi + O(x^{\frac{1}{2}} \log x)\ ,$$

where the constant implied in the O symbol is independent on k (cf. e.g. [14], p. 236).

It should be noted that the restriction $x \geqq k$ made for instance in PRACHAR's book is plainly unnecessary, for

$$\pi(x\,,\,k\,,\,l) = O(1)\,,\quad \varphi(k)^{-1}\int_2^x d\xi/\log\xi = O(x^{\frac{1}{2}}\log x)\,,$$

when $x < k$.

Lemma 23. *If s denotes a complex number then*

$$L(s\,,\ \chi) = \exp(\sum_{p\,,\,n}\chi(p^n)n^{-1}p^{-ns})\quad(\sigma > 1)\,,$$

where σ is the real part of s, p runs through the primes and n through all the natural numbers (cf. e.g. [12], p. 459).

§ 7. Proof of theorem 3

25. Let us define

$$b_{np} = \begin{cases} 1 \text{ if } p^n \equiv 1 \pmod k\,, \\ -1 \text{ if } p^n \equiv -1 \pmod k\,, \\ 0 \text{ elsewhere} \end{cases}$$

($k \geqq 3$ according to the hypothesis). Combining this definition with lemma 7 we get

$$\sum_{\chi\,\in\,Q(k)}\chi(p^n) = \tfrac{1}{2}\varphi(k)b_{np}\,.$$

If we first assume that s is a complex number, we thus have, by lemma 23,

$$(7.1)\qquad \prod_{\chi\,\in\,Q(k)} L(s\,,\ \chi) = \exp(\tfrac{1}{2}\varphi(k)\,(\sum_p b_p\,p^{-s} + \sum_p\sum_{n=2}^{\infty} b_{np}\,n^{-1}\,p^{-ns}))\quad(\sigma > 1)\,,$$

where $b_p = b_{1p}$.

Denote

$$B(x) = \sum_{p\,\leqq\,x} b_p\,.$$

From lemma 22 we now obtain

$$(7.2)\qquad B(x) = \pi(x\,,\ k\,,\ 1) - \pi(x\,,\ k\,,\ -1) = O(x^{\frac{1}{2}}\log x)\,.$$

Suppose $\sigma > \frac{1}{2}$. By using ABEL's partial summation we obtain

$$\sum_{y < p \leqq x} b_p\, p^{-\sigma} = \sum_{y < n \leqq x-1} B(n)\,(n^{-\sigma} - (n+1)^{-\sigma}) + B(x)[x]^{-\sigma} - B(y)\,([y]+1)^{-\sigma}\,. \tag{7.3}$$

Since

$$n^{-\sigma} - (n+1)^{-\sigma} = \sigma \int_n^{n+1} \xi^{-\sigma-1} d\xi \leqq \sigma n^{-\sigma-1}\,, \tag{7.4}$$

it follows from (7.2), (7.3), and (7.4) that

$$\sum_{y < p \leqq x} b_p\, p^{-\sigma} = O(\sigma \sum_{y < n \leqq x-1} n^{-\sigma-\frac{1}{2}} \log n + x^{-\sigma+\frac{1}{2}} \log x + y^{-\sigma+\frac{1}{2}} \log y)\,. \tag{7.5}$$

Since $\sigma > \frac{1}{2}$, the series

$$\sum_{n=2}^{\infty} n^{-\sigma-\frac{1}{2}} \log n$$

converges, and from (7.5) we get

$$\sum_{y < p \leqq x} b_p\, p^{-\sigma} = O(\varepsilon')\ (y > y_0(\varepsilon'))\,,$$

where ε' is an arbitrary positive number. We can thus conclude that the DIRICHLET series

$$\sum_p b_p\, p^{-s}$$

converges. Therefore it presents an analytic function of s, whenever $\sigma > \frac{1}{2}$ (cf. [12], p. 157). Further the series

$$\sum_p \sum_{n=2}^{\infty} b_{np}\, n^{-1}\, p^{-ns} \tag{7.6}$$

is clearly an analytic function of s for $\sigma > \frac{1}{2}$, in fact without any hypothesis. Hence by the theory of analytic continuation it follows that (7.1) proved for $\sigma > 1$, is also true for $\sigma > \frac{1}{2}$ on the assumption of the extended RIEMANN hypothesis.

26. Our intention is to estimate the series in the right-hand side of (7.1) as a function of k. Let us restrict s to be real, and in addition we assume that s satisfies the inequality in (6.1). If we in (7.3) take $y = k - 2$ and if x tends to infinity, we get (cf. (7.5.))

$$\sum_p b_p\, p^{-s} = O(s \sum_{n=k-1}^{\infty} n^{-s-\frac{1}{2}} \log n)$$

$$= O(s \int_{k-2}^{\infty} \xi^{-s-\frac{1}{2}} \log \xi \, d\xi) = O(\,(k-2)^{-\delta/2} \log k)\,, \tag{7.7}$$

where the constant implied in O depends only on δ. Here we have made use of the inequalities

$$2s - 1 \geqq \delta\,, \quad 2s/(2s-1) \leqq (1+\delta)/\delta\,. \tag{7.8}$$

We next estimate the series (7.6) by applying the same method as before in the proof of lemma 21. We denote the series by S_3 and write

$$|S_3| \leqq S_4 + S_5\,,$$

where

$$S_4 = \sum_{\substack{p<k \\ p^n \equiv \pm 1 (\mathrm{mod}\ k)}} \sum_{n=2}^{\infty} n^{-1} p^{-ns}\,, \quad S_5 = \sum_{\substack{p>k \\ p^n \equiv \pm 1 (\mathrm{mod}\ k)}} \sum_{n=2}^{\infty} n^{-1} p^{-ns}\,.$$

In order to estimate S_4 we write

$$S_4 = \sum_{\substack{n=2 \\ p^n \equiv \pm 1 (\mathrm{mod}\ k)}}^{\infty} n^{-1} \sum_{p<k} p^{-ns}\,. \tag{7.9}$$

Denote

$$M(n) = 2(n-1)^{r-1} + 1\,, \quad N(n) = 2n^{r-1}\,, \tag{7.10}$$

whence it follows that

$$N(n) - M(n) > 2n^r\,,$$

since $n \geqq 2$. From lemma 20 it now follows that we can express the numbers p^n in the form (4.6), where $M(n)$ and $N(n)$ are defined by (7.10). If we make use of the definition (4.7), we obtain

$$\sum_{p<k} p^{-ns} \leqq \sum_{j=M(n)}^{N(n)} (v_j k - 1)^{-s} < (k-1)^{-s} \sum_{j=M(n)}^{N(n)} v_j^{-s}\,.$$

We denote

$$V_n = \sum_{j=M(n)}^{N(n)} v_j^{-s}\,, \quad V(x) = \sum_{2 \leqq n \leqq x} V_n\,.$$

By using ABEL's partial summation we now get

$$\sum_{2 \leqq n \leqq x} V_n/n = \sum_{2 \leqq n \leqq x-1} V(n) n^{-1}(n+1)^{-1} + V(x)/[x]\,.$$

Since $M(n+1) = N(n) + 1$, we have

$$V(n) = \sum_{j=3}^{N(n)} v_j^{-s} \leqq 2 \sum_{j=1}^{N(n)} j^{-\eta} .$$

Hence

$$V(n) = O\left(\int_0^{N(n)} \xi^{-\eta}\, d\xi \right) = O((\tau + 1) n^{1-\delta}) ,$$

where the constant implied in O is an absolute one. Furthermore, we get

$$\sum_{2 \leqq n \leqq x} V_n/n = O((\tau+1)\,(\sum_{2 \leqq n \leqq x-1} n^{-1-\delta} + x^{-\delta})) = O(\tau + 1) ,$$

where the constant implied in O depends on δ alone. From lemma 19 and from the equation (7.9) it follows that

$$S_4 = O(\tau(k-1)^{-\eta}) = O((k-1)^{-\frac{1}{2}} \log k) , \tag{7.11}$$

where the symbol O implies a constant, which depends on δ alone.

Finally we estimate the series S_5 as follows:

$$S_5 = O(\sum_{p>k} p^{-2s}) = O(\sum_{n>k} (\pi(n) - \pi(n-1)) n^{-2s}) ,$$

where $\pi(n)$ denotes, as usual, the number of primes not exceeding n. Since $\pi(n) = O(n/\log n)$, we have

$$S_5 = O(s \sum_{n>k} n^{-2s}/\log n) + O(k^{1-2s}/\log k) = O(k^{-\delta}/\log k) , \tag{7.12}$$

where the constant in O depends only on δ. Here we have made use of the inequalities (7.8). Combining the results (7.1), (7.7), (7.11), and (7.12) we get

$$\prod_{\chi \in Q(k)} L(s\,,\ \chi) = \exp(\varphi(k)\ \psi\ (k)\ ) ,$$

where $\psi(k) \to 0$, when k tends to infinity. This proves our theorem.

Chapter III

THE FIRST FACTOR OF THE CLASS NUMBER OF THE CYCLOTOMIC FIELD $k(\exp(2\pi i/p^u))$

§ 8. Theorems and preliminaries

27. In this chapter we restrict ourselves to the case $m = p^u$.

Let r denote a primitive root (mod m), r_j the smallest positive remainder of r^j (mod m), $g = \frac{1}{2}\varphi(m)$, and

$$q_j = (rr_j - r_{j+1})/m . \tag{8.1}$$

When p is an odd prime, INKERI [9] has shown that $h_1(p)$ can be expressed as a determinant as follows:

$$h_1(p) = D = \begin{vmatrix} q_g & q_{g-1} & \cdots & q_1 & q_0 \\ q_{g+1} & q_g & \cdots & q_2 & q_1 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ q_{2g-2} & q_{2g-3} & \cdots & q_{g-1} & q_{g-2} \\ r_g & r_{g-1} & \cdots & r_1 & r_0 \\ 1 & 1 & \cdots & 1 & 1 \end{vmatrix} . \tag{8.2}$$

If p is further an odd prime and $(k, p) = 1$, we define k' by the congruence $kk' \equiv 1 \pmod{p}$. Denote by D_p the so-called MAILLET's determinant

$$\det(\lambda(jk')) \quad (j, k = 1, 2, \ldots, \tfrac{1}{2}(p-1)) , \tag{8.3}$$

where $\lambda(j)$ is the smallest positive remainder of j (mod p). In section 6 we mentioned that the determinant (8.3) is equal to $h_1(p)$ multiplied by a power of p. Therefore there exists a connection with the determinants (8.2) and (8.3). In this chapter we show that this connection can be found without applying the theory of class number.

28. Denote $\mu = p^{u-1}$, $w = \frac{1}{2}\varphi(\mu)$, and $v = (p-1)w$. In section 6 we mentioned the factor K. In the case $p = 2$, $u \geqq 3$ it can be represented in the form (cf. e.g. [19], pp. 796—802)

$$K = 2^{-w+1} \prod_{j} F(\vartheta^j) . \tag{8.4}$$

Here $\vartheta = \exp(2\pi i/\varphi(\mu))$, j takes the values $1, 3, \ldots, 2w-1$, and

$$F(x) = \sum_{j=0}^{w-1} c_j x^j , \tag{8.5}$$

where $c_j = +1$ or -1 if the absolutely smallest remainder of $5^j \pmod{2^u}$ is positive or negative respectively.

In the case $p \geqq 3$, $u \geqq 2$ the factor K can be written in the form (cf. [20], p. 204)

$$K = 2^{-v} p^{-vu+1} \prod_{j} H(\Theta^j) . \tag{8.6}$$

Here j assumes all odd values less than $\varphi(p^u)$, except the multiples of p, $\Theta = \exp(2\pi i/\varphi(p^u))$ and

$$H(x) = \sum_{n} n\, x^k ,$$

where $k = \operatorname{ind}_r n \pmod{p^u}$ and n runs through the numbers $1, 2, \ldots, p^u - 1$, except the multiples of p.

Our intention is to prove the following theorems:

Theorem 4. *If $p = 2$ and $u \geqq 3$, the factor K can be represented in the form*

$$K = \pm D(2^u) = \pm \begin{vmatrix} c_0 & c_1 & c_2 \ldots c_{w-1} \\ e_0 & e_1 & e_2 \ldots e_{w-1} \\ e_1 & e_2 & e_3 \ldots e_w \\ . & . & . \ldots . \\ e_{w-2} & e_{w-1} & e_w \ldots e_{2w-3} \end{vmatrix} , \tag{8.7}$$

where $e_j = \frac{1}{2}(c_j + c_{j+1})$.

Theorem 5. *If $p \geqq 3$ and $u \geqq 2$, K is equal to the determinant*

$$\pm \begin{vmatrix} e_{00} & e_{01} & \ldots e_{0,w-1} & e_{1,0} & \ldots e_{1,w-1} & \ldots e_{p-2,w-1} \\ g_{00} & g_{01} & \ldots g_{0,w-1} & g_{1,0} & \ldots g_{1,w-1} & \ldots g_{p-2,w-1} \\ g_{01} & g_{02} & \ldots g_{0,w} & g_{1,1} & \ldots g_{1,w} & \ldots g_{p-2,w} \\ . & . & \ldots . & . & \ldots . & \ldots . \\ g_{0,v-2} & g_{0,v-1} & \ldots g_{0,v+w-3} & g_{1,v-2} & \ldots g_{1,v+w-3} & \ldots g_{p-2,v+w-3} \end{vmatrix} ,$$

where the integers e_{jk} *and* g_{jk} *are defined by the equations*

$$e_{jk} = \begin{cases} (r_{jw+k} - r_{v+k})/\mu & \text{if } 2 \mid j\,, \\ (r_{(p+j)w+k} - r_{v+k})/\mu & \text{if } 2 \nmid j\,, \end{cases} \tag{8.8}$$

$$g_{jk} = \begin{cases} q_{jw+k} - q_{v+k} & \text{if } 2 \mid j\,, \\ q_{(p+j)w+k} - q_{v+k} & \text{if } 2 \nmid j\,. \end{cases} \tag{8.9}$$

If $D(m)$ denotes the determinant in theorem 5 then it follows from the above results that $h_1(p^u)$ can be written as a product of the determinants in the form

$$h_1(p^u) = \pm DD(p^2)D(p^3)\cdots D(p^u)\,,$$

where $D = D(p^2) = 1$, when $p = 2$.

From the theorems 4 and 5 we can conclude that the factors K and $h_1(p^u)$ are integers. These results have been shown earlier by means of different methods.

As a consequence of theorems 4 and 5 we can prove

Theorem 6. *The integer* K *satisfies an inequality*

$$K \leqq \begin{cases} 2^{(u-3)w/2} & \text{if } p = 2\,, \\ 2^{w(2p-1)/(p-1)-(v+3)/2}\, p^{(vu+w)/2+1} & \text{if } p > 2\,. \end{cases} \tag{8.10}$$

If we apply theorem 6 for the case $p = 2$, we obtain, by means of (10), for $h_1(2^u)$ an upper bound

$$h_1(2^u) \leqq 2^{(u-4)w+1}\,. \tag{8.11}$$

Also in the case $p > 2$ it is possible to get, by means of (10) and (8.10) an upper bound for $h_1(p^u)$, which, however, we do not give explicitly.

It is easy to verify that if p^u is great, the asymptotic approximation (7) gives for $h_1(p^u)$ an upper bound better than the above estimations.

§ 9. The connection with Inkeri's and Maillet's determinants

29. In this paragraph we denote by p an odd prime. Further denote

$$D_p(x) = \det(x + \lambda(jk')) \qquad (j\,,\, k = 1\,,\, 2\,,\, \ldots\,,\, \tfrac{1}{2}(p-1))\,.$$

From the definition (8.3) of MAILLET's determinant it follows that

$$D_p(0) = D_p\,. \tag{9.1}$$

We observe that the last column of D_p has the elements $p-2$, $p-4$, $\ldots$, 1. If we add the doubled first column to the last column both in D_p and in $D_p(x)$, we get, by (9.1),

$$D_p(x) = (3x + p)D_p/p . \tag{9.2}$$

If $x = -\frac{1}{2}p$, it follows from (9.2) that

$$D_p' = -\tfrac{1}{2}D_p , \tag{9.3}$$

where

$$D_p' = D_p(-\tfrac{1}{2}p) = \det(\{jk'\}) \qquad (j, k = 1, 2, \ldots, \tfrac{1}{2}(p-1))$$

and

$$\{k\} = \lambda(k) - \tfrac{1}{2}p . \tag{9.4}$$

Denote by r^{-j} an integer, which satisfies the congruence

$$x\, r^j \equiv 1 \pmod{p} .$$

Further denote

$$D_p'' = \det(\{r^{j-k}\}) \qquad (j, k = 0, 1, \ldots, \tfrac{1}{2}(p-3)) .$$

The absolute values of the elements in the first column of D_p'' are

$$|\{r^0\}|, |\{r^1\}|, |\{r^2\}|, \ldots, |\{r^{(p-3)/2}\}| . \tag{9.5}$$

We get by (9.4)

$$|\{r^j\}| = |r_j - \tfrac{1}{2}p| < \tfrac{1}{2}p . \tag{9.6}$$

We further have

$$|r_j - \tfrac{1}{2}p| \neq |r_k - \tfrac{1}{2}p|$$

if $j \neq k$ and $0 \leqq j, k \leqq \frac{1}{2}(p-3)$. Thus it follows that all the numbers in (9.5) are distinct. By means of (9.6) we can now deduce that the numbers in (9.5) are the numbers

$$1/2, 3/2, 5/2, \ldots, (p-2)/2 \tag{9.7}$$

disregarding the order. The numbers $|\{j\}|$ $(j = 1, 2, \ldots, \frac{1}{2}(p-1))$ are also the numbers (9.7) disregarding the order. Consequently we can decide that the numbers

$$\{r^0\}, \{r^1\}, \{r^2\}, \ldots, \{r^{(p-3)/2}\}$$

coincide with the numbers $\{j\}$ $(j = 1, 2, \ldots, \frac{1}{2}(p-1))$ disregarding the order and the sign. In the same way we can show that the numbers

$$\{r^0\}, \{r^{-1}\}, \{r^{-2}\}, \ldots, \{r^{-(p-3)/2}\}$$

coincide with the numbers $\{j'\}$ $(j = 1, 2, \ldots, \frac{1}{2}(p-1))$ disregarding the order and the sign. In addition we find that

$$\{r^{j-k}\} = \begin{cases} \{ln'\} & \text{if } \{r^j\} = \pm\{l\} \text{ and } \{r^{-k}\} = \pm\{n'\}, \\ -\{ln'\} & \text{if } \{r^j\} = \pm\{l\} \text{ and } \{r^{-k}\} = \mp\{n'\}. \end{cases}$$

By interchanging rows (columns) suitably and by changing the signs of some rows (columns) we get

$$D'_p = \pm D''_p. \tag{9.8}$$

Here we have made use of the above results.

30. It follows from (9.4) that D''_p may be written in the form

$$\begin{vmatrix} r_0 - \frac{1}{2}p & r_{-1} - \frac{1}{2}p & \ldots r_{-g+1} - \frac{1}{2}p \\ r_1 - \frac{1}{2}p & r_0 - \frac{1}{2}p & \ldots r_{-g+2} - \frac{1}{2}p \\ \cdot & \cdot & \ldots \cdot \\ r_{g-1} - \frac{1}{2}p & r_{g-2} - \frac{1}{2}p & \ldots r_0 - \frac{1}{2}p \end{vmatrix},$$

where $g = \frac{1}{2}(p-1)$ and $r_{-j} = \lambda(r^{-j})$. We double every column and interchange the jth and the $(g-j+2)$nd columns, when j runs through the numbers $2, \ldots, \frac{1}{2}g$ if $2 \mid g$ or through the numbers $2, \ldots, \frac{1}{2}(g+1)$ if $2 \nmid g$. Then, by means of the equation

$$2r_{-j} - p = -(2r_{g-j} - p),$$

we get

$$\pm 2^g D''_p = \begin{vmatrix} 2r_0 - p & 2r_1 - p \ldots 2r_{g-1} - p \\ 2r_1 - p & 2r_2 - p \ldots 2r_g - p \\ \cdot & \cdot \quad \ldots \quad \cdot \\ 2r_{g-1} - p & 2r_g - p \ldots 2r_{2g-2} - p \end{vmatrix}. \tag{9.9}$$

The determinant in the right-hand side of (9.9) appears in [9]. If we treat this determinant, we get (cf. [9], p. 9) the result

$$2D''_p = \pm p^{g-1} D, \tag{9.10}$$

where D denotes INKERI's determinant defined by (8.2). From (9.3), (9.8), and (9.10) we finally conclude that

$$D_p = \pm p^{(p-3)/2} D.$$

§ 10. Proof of theorem 4

31. In order to write the product in (8.4) as a determinant we replace x in (8.5) by ϑ and multiply both sides of the equation thus obtained by ϑ^{-1}. Since

$$-\vartheta^{-1} = \vartheta^{w-1}, \tag{10.1}$$

we get

$$0 = c_1 + c_2\vartheta + c_3\vartheta^2 + \ldots - (c_0 - F(\vartheta))\vartheta^{w-1}. \tag{10.2}$$

We further multiply both sides of (10.2) by ϑ^{-1} and repeating this procedure $w - 1$ times we have, by means of (10.1),

$$\left|\begin{array}{llll} 0 = c_0 - F(\vartheta) & + c_1\vartheta + \ldots & + c_{w-1}\vartheta^{w-1}, \\ 0 = c_1 & + c_2\vartheta + \ldots - (c_0 - F(\vartheta))\vartheta^{w-1}, \\ \cdot \quad \cdot & \cdot \quad \ldots \quad \cdot \\ 0 = c_{w-1} - (c_0 - F(\vartheta))\vartheta - \ldots & - c_{w-2}\vartheta^{w-1}. \end{array}\right. \tag{10.3}$$

By (10.3), we can deduce that

$$\left|\begin{array}{llll} c_0 - F(\vartheta) & c_1 & \ldots & c_{w-1} \\ c_1 & c_2 & & -c_0 + F(\vartheta) \\ \cdot & \cdot & \ldots & \cdot \\ c_{w-1} & -c_0 + F(\vartheta) & \ldots & -c_{w-2} \end{array}\right| = 0. \tag{10.4}$$

The expression (10.4) is an equation in $F(\vartheta)$ of degree w. This equation has solutions $F(\vartheta^j)$ when j assumes the values $1, 3, \ldots, 2w - 1$. The product of the solutions is equal to the constant coefficient of the equation disregarding the sign. We get this constant coefficient from (10.4) by replacing $F(\vartheta)$ by zero. We thus get

$$\prod_j F(\vartheta^j) = \pm \left|\begin{array}{llll} c_0 & c_1 & c_2 \ldots & c_{w-1} \\ c_1 & c_2 & c_3 \ldots & -c_0 \\ \cdot & \cdot & \cdot \quad \ldots & \cdot \\ c_{w-1} & -c_0 & -c_1 \ldots & -c_{w-2} \end{array}\right|, \tag{10.5}$$

where j runs through the values $1, 3, 5, \ldots, 2w - 1$.

32. It is known that

$$5^w \equiv 1 + 2^{u-1} \pmod{2^u}$$

($u \geqq 3$ according to the hypothesis). Suppose

$$b \equiv 5^j \pmod{2^u} \quad (|b| < 2^{u-1}) .$$

Since b is an odd integer, we may write

$$5^{w+j} \equiv (1 + 2^{u-1})b \equiv 2^{u-1} + b \pmod{2^u} .$$

From this we conclude that

$$c_{w+j} = \begin{cases} -1 \text{ if } c_j = +1 \text{ or } b > 0 , \\ +1 \text{ if } c_j = -1 \text{ or } b < 0 . \end{cases}$$

This relation yields

$$c_j = -c_{w+j} . \tag{10.6}$$

The determinant in (10.5) may be written, by means of (10.6), in the form

$$D'(2^u) = \begin{vmatrix} c_0 & c_1 & \dots & c_{w-1} \\ c_1 & c_2 & \dots & c_w \\ . & . & \dots & . \\ c_{w-1} & c_w & \dots & c_{2w-2} \end{vmatrix} .$$

We add the jth row to the $(j+1)$st row, when j takes the values $w-1$, $w-2, \dots, 1$. We thus get

$$D'(2^u) = 2^{w-1} D(2^u) ,$$

where $D(2^u)$ denotes the determinant defined in section 28. This together with (8.4) proves theorem 4.

§ 11. Proof of theorem 5

33. Consider the expression (8.6). By a slight alteration of $H(x)$ we get

$$H(x) = \sum_{n=0}^{\varphi(m)-1} r_n x^n . \tag{11.1}$$

Consider the product

$$T = \prod_j H(\Theta^j) , \tag{11.2}$$

where j assumes all odd values less than $\varphi(m)$ except the multiples of p. We find that the numbers Θ^j satisfy an equation

$$x^g + 1 = 0 , \tag{11.3}$$

where $g = \frac{1}{2}\varphi(p^u)$. Further we have, by (11.3),

$$\Theta^{g+j} = -\Theta^j . \tag{11.4}$$

By (11.1) and (11.4), we can now write $H(\Theta)$ in the form

$$H(\Theta) = \sum_{n=0}^{g-1} a_n \Theta^n ,$$

where

$$a_n = r_n - r_{g+n} . \tag{11.5}$$

We define a function $H(\Theta , x)$ as follows:

$$H(\Theta , x) = a_0 + (a_1 + x)\Theta + a_2 \Theta^2 + \ldots + a_{g-1} \Theta^{g-1} , \tag{11.6}$$

whence

$$H(\Theta , 0) = H(\Theta) . \tag{11.7}$$

34. Since (cf. [18], p. 417)

$$\prod_j (r - \Theta^j) = (r^g + 1)/(r^w + 1) ,$$

the numbers Θ^j satisfy an equation

$$x^{(p-1)w} = - 1 + x^w - x^{2w} + \ldots + x^{(p-2)w} . \tag{11.8}$$

In order to formulate the expression $H(\Theta , x)$ for our purposes we need the equation

$$\Theta^{v+j} = - \Theta^j + \Theta^{w+j} - \Theta^{2w+j} + \ldots + \Theta^{(p-2)w+j} , \tag{11.9}$$

which follows from (11.8).

Using (11.9) in (11.6) we get

$$\begin{aligned} 0 = c_{00} - H(\Theta , x) + (c_{01} + x)\Theta + \ldots + c_{0,w-1} \Theta^{w-1} \\ + c_{1,0} \Theta^w + c_{1,1} \Theta^{w+1} + \ldots + c_{1,w-1} \Theta^{2w-1} + \\ \cdot \qquad \cdot \qquad \ldots \qquad \cdot \\ + c_{p-2,0} \Theta^{(p-2)w} + c_{p-2,1} \Theta^{(p-2)w+1} + \ldots + c_{p-2,w-1} \Theta^{v-1} , \end{aligned} \tag{11.10}$$

where

$$c_{jk} = a_{jw+k} + (- 1)^{j-1} a_{v+k} . \tag{11.11}$$

It is easy to verify that

$$r_j + r_{g+j} = m = p^u ,$$

from which it follows, by (11.5), that

$$a_{g+j} = - a_j . \tag{11.12}$$

We can now conclude that

$$(11.13)\qquad \begin{cases} c_{jk} + (-1)^{j-1} c_{0k} = c_{j-1,\,w+k}\,, \\ c_{0k} = -c_{p-2,\,w+k}\,. \end{cases}$$

Here we have made use of (11.11) and (11.12).

35. It follows from (11.4) and (11.9) that

$$(11.14)\quad (c_{00} - H(\Theta, x))\Theta^{-1} = -(c_{00} - H(\Theta, x))(-\Theta^{w-1} + \Theta^{2w-1} - \Theta^{3w-1} + \ldots + \Theta^{v-1})\,.$$

Multiplying both sides of (11.10) by Θ^{-1} we get, by means of (11.13) and (11.14),

$$\begin{aligned} 0 = {} & c_{01} + x + c_{02}\Theta + c_{03}\Theta^2 + \ldots + (c_{0w} - H(\Theta, x))\Theta^{w-1} \\ & + c_{1,1}\Theta^w + c_{1,2}\Theta^{w+1} + c_{1,3}\Theta^{w+2} + \ldots + (c_{1,w} + H(\Theta, x))\Theta^{2w-1} + \\ & \cdots \\ & + c_{p-2,1}\Theta^{(p-2)w} + c_{p-2,2}\Theta^{(p-2)w+1} + \ldots + (c_{p-2,w} + H(\Theta, x))\Theta^{v-1}\,. \end{aligned}$$

We further multiply both sides of this by Θ^{-1}. By (11.13), we thus get

$$\begin{aligned} 0 = {} & c_{02} + c_{03}\Theta + \ldots + (c_{0,w+1} + x)\Theta^{w-1} \\ & + c_{1,2}\Theta^w + c_{1,3}\Theta^{w+1} + \ldots + (c_{1,w+1} - x)\Theta^{2w-1} + \\ & \cdots \\ & + c_{p-2,2}\Theta^{(p-2)w} + c_{p-2,3}\Theta^{(p-2)w+1} + \ldots + (c_{p-2,w+1} - x)\Theta^{v-1}\,. \end{aligned}$$

Repeating this procedure $v - 1$ times we finally have

$$\begin{aligned} 0 = {} & c_{0,v-1} + c_{0v}\Theta + \ldots + c_{0,v+w-2}\Theta^{w-1} \\ & + c_{1,v-1}\Theta^w + c_{1,v}\Theta^{w+1} + \ldots + c_{1,v+w-2}\Theta^{2w-1} + \\ & \cdots \\ & + c_{p-2,v-1}\Theta^{(p-2)w} + c_{p-2,v}\Theta^{(p-2)w+1} + \ldots + c_{p-2,v+w-2}\Theta^{v-1}\,. \end{aligned}$$

If we consider the system of all the equations thus obtained, we see that the coefficient determinant

$$\begin{vmatrix} c_{00} - H & c_{01} + x & \ldots & c_{0,w-1} & c_{1,0} & \ldots & c_{1,w-1} & \ldots & c_{p-2,w-1} \\ c_{01} + x & c_{02} & \ldots & c_{0w} - H & c_{1,1} & \ldots & c_{1,w} + H & \ldots & c_{p-2,w} + H \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{0,v-1} & c_{0v} & \ldots & c_{0,v+w-2} & c_{1,v-1} & \ldots & c_{1,v+w-2} & \ldots & c_{p-2,v+w-2} \end{vmatrix}$$

vanishes. Here we have shortly denoted $H = H(\Theta , x)$. We denote this determinant by $D'(m , x)$. Consider first the positions of H in $D'(m , x)$. Then we can write the following schema:

	$1 \dots w-1$	w	$w+1$	$w+2 \dots 2w-1$	$2w$	$2w+1 \dots (p-2)w+1 \dots v-1$	v
1	$-H$						
2		$-H$			$+H$		$+H$
3	$-H$			$+H$			$+H$
$w+1$	$-H$		$+H$		$-H$	$+H$	
$w+2$							$+H$
$w+3$							$+H$
$2w+1$						$+H$	
$(p-2)w+1$					$+H$		
$(p-2)w+2$				$+H$			
v			$+H$				

The numbers in the schema show the order of the columns and the rows. We can now observe that by adding and subtracting the rows appropriately we get $D'(m , x)$ in a form, which proves that

$$D'(m , x) = 0 \tag{11.15}$$

is an equation in $H(\Theta , x)$ of degree v , when x has some fixed value. We find that the expression (11.6) of $H(\Theta , x)$ is a solution of (11.15). We now replace in (11.6) Θ by Θ^j , where j assumes all odd values (> 1) less than $\varphi(m)$ except the multiples of p . In the same way as before we treat this expression and it is evident that we get also in this case the same equation (11.15). It is now clear that there exists an infinity of the values of x such that all the expressions $H(\Theta^j , x)$ are distinct for each x . Since the number of the possible values of j is v , each solution of (11.15) is included in the expressions $H(\Theta^j , x)$ The product of the solutions is equal to the constant coefficient of (11.15) disregarding the sign. We get this coefficient from (11.15) replacing $H(\Theta , x)$ by zero. Hence

$$\prod_j H(\Theta^j , x) = \pm D(m , x) , \tag{11.16}$$

where j runs through all odd values less than $\varphi(m)$ except the multiples of p and $D(m , x)$ denotes the determinant

$$\begin{vmatrix} c_{00} & c_{01}+x & \dots & c_{0,w-1} & c_{1,0} & \dots & c_{1,w-1} & \dots & c_{p-2,w-1} \\ c_{01}+x & c_{02} & \dots & c_{0w} & c_{1,1} & \dots & c_{1,w} & \dots & c_{p-2,w} \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \cdot & \dots & \cdot \\ c_{0,v-1} & c_{0v} & \dots & c_{0,v+w-2} & c_{1,v-1} & \dots & c_{1,v+w-2} & \dots & c_{p-2,v+w-2} \end{vmatrix} .$$

36. The expression (11.16) is an equation in x of degree $\leqq v$. Therefore it must be an identity, since it has an infinity of solutions. Consequently the value $x = 0$ satisfies the equation, and it follows from (11.2), (11.7) and (11.16) that

$$T = \pm D(m, 0) . \tag{11.17}$$

Consider the determinant $D(m, 0)$. We first observe that

$$\begin{aligned} c_{jk} &= a_{jw+k} + (-1)^{j-1} a_{v+k} = -m + 2r_{jw+k} + (-1)^{j-1}(2r_{v+k} - m) \\ &= m - 2r_{(p+j)w+k} + (-1)^{j-1}(2r_{v+k} - m) . \end{aligned}$$

Hence

$$c_{jk} = \begin{cases} 2(r_{jw+k} - r_{v+k}) & \text{if } 2 \mid j , \\ -2(r_{(p+j)w+k} - r_{v+k}) & \text{if } 2 \nmid j . \end{cases} \tag{11.18}$$

Since each column is divisible by 2, $D(m, 0)$ can be written, by means of (11.18), in the form

$$\pm 2^v \begin{vmatrix} r_0 - r_v & \dots & r_{w-1} - r_{pw-1} & r_{(p+1)w} - r_v & \dots & r_{(2p-1)w-1} - r_{pw-1} \\ r_1 - r_{v+1} & \dots & r_w - r_{pw} & r_{(p+1)w+1} - r_{v+1} & \dots & r_{(2p-1)w} - r_{pw} \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ r_{v-1} - r_{2v-1} & \dots & r_{pw-2} - r_{(2p-1)w-2} & r_{2pw-1} - r_{2v-1} & \dots & r_{(3p-2)w-2} - r_{(2p-1)w-2} \end{vmatrix} .$$

From the jth $(j = v, v-1, \dots, 2)$ row we subtract the preceding row multiplied by r. A general element of the determinant may be treated as follows:

$$r_{j+1} - r_{k+1} - r(r_j - r_k) = -m(q_j - q_k) ,$$

where we have made use of (8.1). From this it follows that $D(m, 0)$ can be represented in the form

$$\pm 2^v m^{v-1} \begin{vmatrix} r_0 - r_v & \dots & r_{w-1} - r_{pw-1} & \dots & r_{(2p-1)w-1} - r_{pw-1} \\ q_0 - q_v & \dots & q_{w-1} - q_{pw-1} & \dots & q_{(2p-1)w-1} - q_{pw-1} \\ q_1 - q_{v+1} & \dots & q_w - q_{pw} & \dots & q_{(2p-1)w} - q_{pw} \\ \cdot & \dots & \cdot & \dots & \cdot \\ q_{v-2} - q_{2v-2} & \dots & q_{pw-3} - q_{(2p-1)w-3} & \dots & q_{(3p-2)w-3} - q_{(2p-1)w-3} \end{vmatrix} .$$

37. In (8.8) we defined the numbers e_{jk}. In order to show that these numbers are integers, we first write

$$r_{jw+k} - r_{v+k} \equiv - r^{jw+k} (r^{(p-1-j)w} - 1) \pmod{m} \tag{11.19}$$

and

$$r_{(p+j)w+k} - r_{v+k} \equiv r^{v+k} (r^{(j+1)w} - 1) \pmod{m} . \tag{11.20}$$

It follows from (8.8) that j in (11.19) is even and in (11.20) odd. Consequently both expressions $p - 1 - j$ and $j + 1$ in the exponents of (11.19) and (11.20) respectively are divisible by 2. In addition it is known that

$$r^{2w} \equiv r^{q(\mu)} \equiv 1 \pmod{\mu} ,$$

from which it immediately follows, by (8.8), (11.19), and (11.20), that the numbers e_{jk} are integers. On the other hand it is easy to verify, by (8.1) and (8.9), that also the numbers g_{jk} are integers. Hence

$$D(m , 0) = \pm 2^v m^{v-1} \mu D(m) , \tag{11.21}$$

where $D(m)$ is the determinant in theorem 5. This result together with (8.6), (11.2), and (11.17) proves our theorem.

§ 12. Some new expressions for K and proof of theorem 6

38. Consider the determinant $D(m , 0)$ defined in section 35. We replace the numbers c_{jk} by the expressions (11.11) and write the determinant of order v as a determinant of order g. We thus get

$$D(m , 0) = \begin{vmatrix} a_0 & a_1 \ldots a_{w-1} & a_w & \ldots a_v & a_{v+1} \ldots a_{g-1} \\ a_1 & a_2 \ldots a_w & a_{w+1} & \ldots a_{v+1} & a_{v+2} \ldots a_g \\ . & . \ldots . & . & \ldots . & . \ldots . \\ a_{v-1} & a_v \ldots a_{v+w-2} & a_{v+w-1} & \ldots a_{2v-1} & a_{2v} \ldots a_{g+v-2} \\ 1 & 0 \ldots 0 & -1 & \ldots 1 & 0 \ldots 0 \\ 0 & 1 \ldots 0 & 0 & \ldots 0 & 1 \ldots 0 \\ . & . \ldots . & . & \ldots . & . \ldots . \\ 0 & 0 \ldots 1 & 0 & \ldots 0 & 0 \ldots 1 \end{vmatrix} ,$$

Since $r_j + r_{g+j} = m$, it follows by (11.5) that

$$a_j = 2r_j - m .$$

Applying this in the above determinant we have

$$D(m\ ,\ 0) = 2^v \begin{vmatrix} r_0 - \frac{1}{2}m & r_1 - \frac{1}{2}m & \dots & r_{g-1} - \frac{1}{2}m \\ r_1 - \frac{1}{2}m & r_2 - \frac{1}{2}m & \dots & r_g - \frac{1}{2}m \\ \cdot & \cdot & \dots & \cdot \\ r_{v-1} - \frac{1}{2}m & r_v - \frac{1}{2}m & \dots & r_{g+v-2} - \frac{1}{2}m \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 1 \end{vmatrix} . \tag{12.1}$$

Consider first the elements in the first row. Denote

$$\{n\} = \lambda(n) - \tfrac{1}{2}m\ , \tag{12.2}$$

where $\lambda(n)$ denotes the smallest positive remainder of n (mod m) (see section 29, the case $m = p$). Hence

$$|\{r_j\}| = |r_j - \tfrac{1}{2}m| \leqq \tfrac{1}{2}m - 1\ . \tag{12.3}$$

Since r_j is not a multiple of p, $|\{r_j\}|$ cannot be expressed in the form $p(k - \frac{1}{2})$, where k is a natural number. Since

$$|r_j - \tfrac{1}{2}m| \neq |r_k - \tfrac{1}{2}m|\ ,$$

when $j \neq k$ and $0 \leqq j\ ,\ k < g$, we can deduce that the numbers $|\{r_j\}|$ take exactly g distinct values, when j runs through the numbers 0, 1, $2, \dots,\ g - 1$. By (12.3), it follows that the numbers $|\{r_j\}|$ can take only the values

$$1/2\ ,\ 3/2\ ,\ \dots\ ,\ (m - 2)/2\ , \tag{12.4}$$

except the numbers of the form $p(k - \frac{1}{2})$. The number of the numbers (12.4) is clearly $\frac{1}{2}(m - 1)$ whereas the number of the numbers $p(k - \frac{1}{2})$ occurring in (12.4) is $\frac{1}{2}(\mu - 1)$. Their difference is g, and it follows that if we strike out the numbers $p(k - \frac{1}{2})$, the remaining numbers in (12.4) coincide with the numbers

$$|\{r_0\}|\ ,\ |\{r_1\}|\ ,\ \dots\ ,\ |\{r_{g-1}\}|$$

disregarding the order. We can thus conclude that the first row of the determinant (12.1) may be written as follows:

$$1 - \tfrac{1}{2}m \quad 2 - \tfrac{1}{2}m \dots p - 1 - \tfrac{1}{2}m \quad p + 1 - \tfrac{1}{2}m \dots \tfrac{1}{2}(m - 1) - \tfrac{1}{2}m$$

if the order and the sign are not taken into consideration. Furthermore, we get

$$\{r_{j+k}\} = \begin{cases} \{r_j n\} & \text{if } \{r_k\} = \quad n - \tfrac{1}{2}m = \{n\}, \\ -\{r_j n\} & \text{if } \{r_k\} = -n + \tfrac{1}{2}m = -\{n\}, \end{cases}$$

where $1 \leqq n \leqq \gamma$ $(\gamma = \frac{1}{2}(m-1))$. By means of this and the above results $D(m\,,\,0)$ can be written in the form

$$\pm 2^v \begin{vmatrix} \{1\} & \{2\} & \dots & \{p-1\} & \{p+1\} & \dots & \{\gamma\} \\ \{r_1\} & \{2r_1\} & \dots & \{(p-1)r_1\} & \{(p+1)r_1\} & \dots & \{\gamma r_1\} \\ \{r_2\} & \{2r_2\} & \dots & \{(p-1)r_2\} & \{(p+1)r_2\} & \dots & \{\gamma r_2\} \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ \{r_{v-1}\} & \{2r_{v-1}\} & \dots & \{(p-1)r_{v-1}\} & \{(p+1)r_{v-1}\} & \dots & \{\gamma r_{v-1}\} \\ v_{1,1} & v_{1,2} & \dots & v_{1,p-1} & v_{1,p+1} & \dots & v_{1,\gamma} \\ v_{2,1} & v_{2,2} & \dots & v_{2,p-1} & v_{2,p+1} & \dots & v_{2,\gamma} \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ v_{w,1} & v_{w,2} & \dots & v_{w,p-1} & v_{w,p+1} & \dots & v_{w,\gamma} \end{vmatrix},$$

where $\gamma = \frac{1}{2}(m-1)$ and v_{jn} is either $+1$, -1 or 0. We subtract from the jth row $(j = 2\,,\,3\,,\,\dots\,,\,v)$ the first row multiplied by r_{j-1}. Then a general element of the jth row may be treated as follows:

$$\{nr_{j-1}\} - r_{j-1}\{n\} = m\,[j\,,\,n]\,, \tag{12.5}$$

where

$$[j\,,\,n] = \tfrac{1}{2}(r_{j-1} - 1) - (n\,r_{j-1} - \lambda(nr_{j-1}))/m\,. \tag{12.6}$$

We want to note that the numbers $[j\,,\,n]$ need not be integers, but if we double them, we get integers. By means of (12.5) and (12.6) $D(m\,,\,0)$ may be represented in the form

$$\pm 2^v m^{v-1} \begin{vmatrix} \{1\} & \{2\} & \dots & \{p-1\} & \{p+1\} & \dots & \{\gamma\} \\ [2,1] & [2,2] & \dots & [2,p-1] & [2,p+1] & \dots & [2,\gamma] \\ [3,1] & [3,2] & \dots & [3,p-1] & [3,p+1] & \dots & [3,\gamma] \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ [v,1] & [v,2] & \dots & [v,p-1] & [v,p+1] & \dots & [v,\gamma] \\ v_{1,1} & v_{1,2} & \dots & v_{1,p-1} & v_{1,p+1} & \dots & v_{1,\gamma} \\ v_{2,1} & v_{2,2} & \dots & v_{2,p-1} & v_{2,p+1} & \dots & v_{2,\gamma} \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ v_{w,1} & v_{w,2} & \dots & v_{w,p-1} & v_{w,p+1} & \dots & v_{w,\gamma} \end{vmatrix}.$$

Denote

$$(j\,;\,n) = \begin{cases} 1 \text{ if } j = 1 \text{ and } n \neq kp+1\,, \\ 2 \text{ if } j = 1 \text{ and } n = kp+1\,, \\ [j\,,n] - [j\,,n-1] \text{ if } j \geqq 2 \text{ and } n \neq kp+1 (n \geqq 2)\,, \\ [j\,,n] - [j\,,n-2] \text{ if } j \geqq 2 \text{ and } n = kp+1 \end{cases}$$

and

$$u_{jn} = \begin{cases} v_{jn} - v_{j,n-1} \text{ if } n \neq kp+1 \ (v_{j,0} = 0)\,, \\ v_{jn} - v_{j,n-2} \text{ if } n = kp+1\,, \end{cases}$$

where j, n, and k are natural numbers. By subtracting from the jth column $(j = g\,,\ g-1\,,\ \ldots\,,\ 2)$ the preceding column we can now express $D(m\,,\,0)$ in the form

$$(12.7) \quad \pm 2^v m^{v-1} \begin{vmatrix} \{1\} & (1;2) \ldots (1;p-1) & (1;p+1) \ldots (1;\gamma) \\ [2,1] & (2;2) \ldots (2;p-1) & (2;p+1) \ldots (2;\gamma) \\ [3,1] & (3;2) \ldots (3;p-1) & (3;p+1) \ldots (3;\gamma) \\ \cdot & \cdot \quad \ldots \quad \cdot & \cdot \quad \ldots \quad \cdot \\ [v,1] & (v;2) \ldots (v;p-1) & (v;p+1) \ldots (v;\gamma) \\ u_{1,1} & u_{1,2} \ \ldots \ u_{1,p-1} & u_{1,p+1} \ \ldots \ u_{1,\gamma} \\ u_{2,1} & u_{2,2} \ \ldots \ u_{2,p-1} & u_{2,p+1} \ \ldots \ u_{2,\gamma} \\ \cdot & \cdot \quad \ldots \quad \cdot & \cdot \quad \ldots \quad \cdot \\ u_{w,1} & u_{w,2} \ \ldots \ u_{w,p-1} & u_{w,p+1} \ \ldots \ u_{w,\gamma} \end{vmatrix}.$$

If $m = 3^u$, $\gamma = \frac{1}{2}(m-1)$ is of the form $kp+1$, elsewhere $\gamma \neq kp+1$. Denote by $D''(m)$ the determinant in (12.7). By (11.21), we thus get

$$(12.8) \qquad K = \pm p^{-u+1} D''(m)\,.$$

39. Consider the elements of $D''(m)$. All of them are integers except the first v elements in the first column. If, however, we multiply the first column by 2, we get a determinant, each element of which is an integer without any exception. It follows immediately from the definition of the numbers u_{jn} that

$$(12.9) \qquad |u_{jn}| \leqq 2\,.$$

We now estimate the elements $(j;n)$. If $j \geqq 2$ and $n \neq kp+1$ $(n \geqq 2)$, we obtain

$$|(j\,;n)| = |[j\,,n] - [j\,,n-1]| = m^{-1}\,|\,\lambda(nr_{j-1}) - \lambda((n-1)r_{j-1}) - r_{j-1}\,|$$
$$= m^{-1}(\,|\,\lambda\,(nr_{j-1}) - \lambda\,((n-1)r_{j-1})\,| + |\,r_{j-1}\,|) < 2 - m^{-1}\,.$$

If $j \geqq 2$ and $n = kp + 1$, we have

$$|(j\,;n)| = |[j\,,n] - [j\,,n-2]| = m^{-1}\,|\,\lambda(nr_{j-1}) - \lambda((n-2)r_{j-1}) - 2r_{j-1}\,|$$
$$< 3 - m^{-1}\,.$$

From this we conclude that

$$|(j\,;\,n)| \leqq \begin{cases} 1 \text{ if } n \neq kp+1\,, \\ 2 \text{ if } n = kp+1\,. \end{cases} \tag{12.10}$$

In order to estimate K by means of a determinant it is convenient to start from the expression $D''(m)$, since the absolute values of the elements in $D''(m)$ are $\leqq 2$ except possibly the first v elements in the first column (see (12.9) and (12.10)).

40. By applying the above results we now prove theorem 6. Consider first the case $m = 2^u$ $(u \geqq 3)$. We use the so-called HADAMARD's lemma (cf. e.g. [10], p. 259) in (8.7). Since each element of the determinant $D(2^u)$ is absolutely $\leqq 1$, the sum of the squares of the elements in every row is $\leqq w$. We thus obtain the result

$$K \leqq (2^{u-3})^{w/2}\,,$$

which proves the first part of our theorem.

Consider now the case $m = p^u$, where p is an odd prime and $u \geqq 2$. We divide the first column of $D''(m)$ by $\frac{1}{2}m$ and the $(k(p-1)+1)$st column $(k = 1\,,\,2\,,\,\ldots\,,\,\frac{1}{2}(\mu-1))$ by 2. Since the absolute values of the elements in the jth row $(j = 1\,,\,2\,,\,\ldots\,,\,v)$ are, by (12.10), $\leqq 1$, the sum of the squares is $\leqq g$. Let z_j $(j = v+1\,,\,v+2\,,\,\ldots\,,\,g)$ denote the number of the elements in the jth row, the absolute values of which are $= 2$. The number of non-zero elements in the jth row is thus $\leqq 2p - z_j$ and the number of the elements absolutely equal to one in the jth row is $\leqq 2(p - z_j)$. Let N_j denote the sum of the squares of the elements in the jth row. We then obtain the result

$$|\,N_j\,| \leqq \begin{cases} g \text{ if } j = 1\,,\,2\,,\,\ldots\,,\,v\,, \\ 2(p-z_j) + 4z_j < 4p \text{ if } j = v+1\,,\,v+2\,,\,\ldots\,,\,g\,. \end{cases} \tag{12.11}$$

If we apply HADAMARD's lemma, we get

$$|\,D''(m)\,| < m\;2^{(\mu-3)/2}\;g^{v/2}\;(4p)^{w/2}\,. \tag{12.12}$$

Here we have made use of (12.11). It follows now from (12.8) and (12.12) that

$$K < 2^{(u-3)/2+w}\ g^{v/2}\ p^{1+w/2}\ .$$

This implies the second part of our theorem.

Using (8.10) in order to estimate an upper bound for $h_1(2^n)$ we obtain

$$h_1 \leqq 2^z\ ,$$

where

$$z = \sum_{j=1}^{u-3} j\ 2^{j-1} = (u-4)2^{u-3} + 1$$

and this leads to (8.11).

References

[1] ANKENY, N. and CHOWLA, S.: *The class number of the cyclotomic field.* - Proc. Nat. Sci. U.S.A. 35 (1949), 529—532.

[2] —»— *The class number of the cyclotomic field.* - Canad. J. Math. 3 (1951), 486—494.

[3] CARLITZ, L.: *A generalization of Maillet's determinant and a bound for the first factor of the class number.* - Proc. Amer. Math. Soc. 12 (1961), 256—261.

[4] —»— and OLSON, F. R.: *Maillet's determinant.* - Proc. Amer. Math. Soc. 6 (1955), 265—269.

[5] ESTERMAN, T.: *On Dirichlet's L-functions.* - Journal London Math. Soc. 23 (1948), 275—279.

[6] HASSE, H.: *Zahlentheorie.* - 2. Aufl., Akademie-Verlag, Berlin (1963).

[7] —»— *Vorlesungen über Zahlentheorie.* - 2. Aufl., Springer-Verlag, Berlin-Göttingen-Heidelberg-New York (1964).

[8] HILBERT, D.: *Die Theorie der algebraischen Zahlkörper.* - Jber. Deutsch. Math.-Verein. 4 (1897).

[9] INKERI, K.: *Über die Klassenzahl des Kreiskörpers der l^{ten} Einheitswurzeln.* - Ann. Acad. Sci. Fenn. A I 199 (1955), 1—12.

[10] KOWALEWSKI, G.: *Determinantentheorie.* - 3. Aufl., New York (1948).

[11] KUMMER, E. E.: *Sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers.* - J. Math. Pures Appl. 16 (1851), 377—498.

[12] LANDAU, E.: *Handbuch der Lehre von der Verteilung der Primzahlen.* - Chelsea Publishing Company, New York (1953).

[13] LEPISTÖ, T.: *The first factor of the class number of the cyclotomic field* $k(e^{2\pi i/p^n})$. - Ann. Univ. Turkuensis, Ser. A I 70 (1963), 1—7.

[14] PRACHAR, K.: *Primzahlverteilung.* - Springer-Verlag, Berlin-Göttingen-Heidelberg (1957).

[15] SIEGEL, C. L.: *Zu zwei Bemerkungen Kummers.* - Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1964), 51—57.

[16] TATUZAWA, T.: *On a theorem of Siegel.* - Japanese Journal of Math. 21 (1951), 163—178.

[17] —»— *On the product of* $L(1, \chi)$. - Nagoya Math. J. 5 (1953), 105—111.

[18] VANDIVER, H. S.: *On the class number of the field* $k(e^{2\pi i/p^n})$ *and the second case of Fermat's last theorem.* - Proc. Nat. Acad. Sci. 6 (1920), 416—421.

[19] WEBER, H.: *Lehrbuch der Algebra II.* - Braunschweig (1899).

[20] WESTLUND, J.: *On the class number of the cyclotomic number field* $k(e^{2\pi i/p^n})$. - Trans. Amer. Math. Soc. 4 (1903), 201—212.

Printed March 1966