THE CLASS NUMBER OF THE CYCLOTOMIC FIELD

N. C. ANKENY AND S. CHOWLA

1. Introduction. Let g denote an odd prime, and $h = h(g)$ the class number of the cyclotomic field $R(\zeta)$, where ζ is a primitive gth root of unity. It is known that we can write

$$h = h_1 h_2$$

where h_1 and h_2 (both integers) are the so-called first and second factors of the class-number; in fact h_2 is the class-number of the real field of degree 2 under $R(\zeta)$, namely the field $R(\zeta + \zeta^{-1})$.

Kummer conjectured (J. de Math., **16**, 1851, 473) that

$$(1.1) \qquad h_1 \sim \frac{g^{(g+3)/4}}{2^{(g-3)/2}\,\pi^{(g-1)/2}} = G.$$

(The sign used here is the sign of asymptotic equality.) He also calculated h_1 for $g \leqslant 97$ and found $h_1 = 1$ for $g \leqslant 19$, $h_1 = 411{,}322{,}823{,}001$ for $g = 97$. No proof of (1.1) has yet been published.

In this paper we show that

$$(1.2) \qquad \log (h_1/G)/\log g \to 0 \qquad (g \to \infty)$$

and this is the most that we can prove in the direction of Kummer's conjecture (1.1); an interesting consequence of (1.2) is that:

There exists a g_0 such that $h_1(g)$ is monotonic increasing for $g > g_0$; in fact if $g_2 > g_1 > g_0$, we have

$$h_1(g_2) > h_1(g_1).$$

We further show that if Kummer's conjecture is true we must have

$$(1.3) \qquad \sum C_p \,.\, p^{-1} = O(g^{-1})$$

as $g \to \infty$, where:

$$\begin{aligned} C_p &= 1 \text{ if } p \equiv 1 \pmod g, \\ C_p &= -1 \text{ if } p \equiv -1 \pmod g, \\ C_p &= 0 \text{ in all other cases.} \end{aligned}$$

Here p stands for a typical prime.

We are unable to prove (1.3), which if true, must lie very deep. We remark that the convergence of the series on the left side of (1.3) has been known for a long time [**3**]. As far as the authors are aware, the result $h = h(g) \to \infty$ as $g \to \infty$, is explicitly proved here for the first time, excepting a recent paper of R. Brauer [**2**], who also gets a sharper form of this result.

Received July 28, 1949; revised March 13, 1951.

In §5, we assume the extended Riemann hypothesis and prove the following result, which is naturally suggested by the methods of this paper.

Let θ_1 and θ_2 denote any fixed constants such that $\frac{1}{2} < \theta_1 < s < \theta_2 < 1$. If the extended Riemann hypothesis is true, there exists, for every given $\epsilon > 0$, a non-principal character $\chi(n)$ (mod g) such that

$$|L(s)| = \left|\sum_{1}^{\infty} \chi(n) n^{-s}\right| < 1 + \epsilon \tag{1.4}$$

for all $g > g_0(\epsilon)$, g prime.

This result with the larger constant $(\zeta(2s))^{\frac{1}{2}} + \epsilon$ on the right hand side of the inequality is implicit in some recent work of Atle Selberg [**4**], but it (in this weaker form) is proved by him without any hypothesis. (Here $\zeta(s)$ denotes Reimann's Zeta Function; hence $\zeta(2s) > 1$ for $s > \frac{1}{2}$).

2. For n not a multiple of g we define

$$\chi_t(n) = \exp\{2\pi i n' t/(g-1)\}$$

where n' is defined as follows: let r denote a primitive root of g, then

$$r^{n'} \equiv n \pmod{g};$$

t runs through the odd numbers $1, 3, 5, \ldots, g-2$. If n is a multiple of g we define

$$\chi_t(n) = 0.$$

It is easy to see that $\chi_t(n)$ is a non-principal character (mod g) and that

$$\sum_t \chi_t(n) = \begin{cases} \frac{1}{2}(g-1) & [n \equiv 1(g)], \\ -\frac{1}{2}(g-1) & [n \equiv -1(g)], \\ 0 & [n \not\equiv \pm 1(g)]. \end{cases}$$

Further write

$$L_t(s) = \sum_{1}^{\infty} \chi_t(n) n^{-s} \qquad [R(s) > 0].$$

It now easily follows that for $s > 1$,

$$\prod_t L_t(s) = \exp\{g' \sum_p \sum_{m \geq 1} C_{p,m}\, m^{-1} p^{-ms}\},$$

where $g' = \frac{1}{2}(g-1)$, and

$$\begin{aligned} C_{p,m} &= 1 & [p^m &\equiv 1(g)], \\ C_{p,m} &= -1 & [p^m &\equiv -1(g)], \\ C_{p,m} &= 0 & [p^m &\not\equiv \pm 1(g)]. \end{aligned}$$

Since, as is well known,

$$\frac{h_1}{G} = \prod_t L_t(1)$$

and $\sum C_p\, p^{-1}$ is convergent, it follows that

$$\frac{h_1}{G} = \exp\{g' \sum C_p \,.\, p^{-1} + g' \sum_p \sum_{m \geq 2} C_{p,m} m^{-1} p^{-m}\}. \tag{2.1}$$

In the rest of this section we show that

$$\frac{g}{\log g}\sum C_p p^{-1} \to 0 \qquad (g \to \infty). \tag{2.2}$$

Let us write

$$C(x) = \sum_{p \leqslant x} C_p.$$

Denote by $\pi(x; k, l)$ the number of primes $\equiv l \pmod{k}$ not exceeding x; $\phi(k)$ is the number of positive integers not exceeding k and prime to k: we shall need the following lemmas.

LEMMA 1. *For any positive* ϵ

$$\pi(x; k, l) = O\left\{\frac{x}{\phi(k)\log x}\right\} \qquad [x > k^{1+\epsilon}].$$

Here the constant implied in the O depends on ϵ alone. Although this result follows from the method of Viggo Brun, it was first stated explicitly by Titchmarsh [**5**].

LEMMA 2. *If* $(k, l) = 1$ *then for arbitrary positive* θ,

$$\pi(x; k, l) - \frac{1}{\phi(k)}\int_2^x \frac{du}{\log u} = O(xe^{-A(\log x)^{\frac{1}{2}}}) + O\left(\frac{x^{1-ck^{-\theta}}}{\phi(k)\log x}\right).$$

Here the constant implied in the O is an absolute one, A is an absolute positive constant, c is a positive constant depending on θ alone. This result is due to Walfisz [**6**].

Applying Lemma 1 with $k = g$, $l = 1$ and $l = g - 1$, we obtain

$$C(x) = O\left(\frac{x}{g\log x}\right) \qquad [x > g^{1+\epsilon}], \tag{2.3}$$

where the constant implied in the O symbol may depend on ϵ.

We have for $x \geqslant 2g - 1$, since $C(2g - 2) = 0$,

$$\sum_{p \leqslant x} C_p p^{-1} = \sum_{2g-1 \leqslant p \leqslant x} C_p p^{-1} = \sum_{2g-1}^{x} \frac{C(n) - C(n-1)}{n}$$

$$= \frac{C(x)}{x} + \sum_{2g-1}^{x-1} \frac{C(n)}{n(n+1)}. \tag{2.4}$$

We split the sum

$$S = \sum_{2g-1}^{x-1} \frac{C(n)}{n(n+1)}$$

into three parts, thus:

$$S = S_1 + S_2 + S_3.$$

In

S_1,	n goes from $2g - 1$	to $g^{1+\epsilon}$,
S_2,	n goes from $1 + g^{1+\epsilon}$	to $\exp(g^{2\theta})$,
S_3,	n goes from $1 + \exp(g^{2\theta})$	to $x - 1$;

θ is a small positive number whose exact specification will be given later.

https://doi.org/10.4153/CJM-1951-049-7 Published online by Cambridge University Press

Clearly,

$$|S_1| \leqslant \sum_{\substack{m \\ mg-1 \leqslant g^{1+\epsilon}}} (mg-1)^{-1} + \sum_{\substack{m \\ mg+1 \leqslant g^{1+\epsilon}}} (mg+1)^{-1} \tag{2.5}$$
$$= O\{g^{-1} \sum_{m \leqslant 2g^{\epsilon}} m^{-1}\} = O\left\{\frac{\epsilon \log g}{g}\right\},$$

where the constant in the last O symbol is independent of both ϵ and g.

Again from (2.3) we have

$$0 \leqslant C(x) \leqslant \frac{K(\epsilon)x}{g \log x} \qquad [x \geqslant g^{1+\epsilon}], \tag{2.6}$$

where $K(\epsilon)$ is a constant depending on ϵ alone. Hence

$$|S_2| \leqslant \frac{K(\epsilon)}{g} \sum (n \log n)^{-1} \qquad [g^{1+\epsilon} \leqslant n \leqslant \exp(g^{2\theta})]$$
$$\leqslant \frac{A\theta K(\epsilon) \log g}{g}, \tag{2.7}$$

where A is an absolute positive constant. Here we used the well-known

$$\sum_2^x (n \log n)^{-1} = O\left(\int_2^x \frac{du}{u \log u}\right) = O(\log \log x).$$

It remains to estimate S_3, for which purpose we use lemma 2.

From lemma 2,

$$C(x) = O(xe^{-A(\log x)^{\frac{1}{2}}}) + O\left(\frac{x^{1-cg^{-\theta}}}{g \log x}\right).$$

It follows that

$$S_3 = \sum \frac{C(n)}{n(n+1)} \qquad [1 + \exp(g^{2\theta}) \leqslant n \leqslant x - 1]$$
$$= O\{\sum n^{-1} e^{-A(\log n)^{\frac{1}{2}}}\} + O\{\sum g^{-1} n^{-1} (\log n)^{-2}\} \quad [\exp(g^{2\theta}) \leqslant n \leqslant x]$$

since, for $x > \exp(g^{2\theta})$,

$$x^{cg^{-\theta}} > \log x \qquad [g > g_0(\theta)].$$

Hence, interchanging the O terms,

$$S_3 = O\{\sum_{n > \exp(g^{2\theta})} g^{-1} n^{-1} (\log n)^{-2}\} + O\{\sum_{n \geqq \exp(g^{2\theta})} n^{-1} (\log n)^{-3/\theta}\},$$

since we have

$$(\log n)^{3/\theta} < e^{A(\log n)^{\frac{1}{2}}} \qquad [n \geqslant \exp(g^{2\theta}), g > g_0(\theta)].$$

Thus for $g > g_0(\theta)$, $\theta \leqslant \frac{1}{10}$,

$$S_3 = O(g^{-1-2\theta}) + O(\theta^{-1} g^{-2\theta(3/\theta - 1)}) = O(g^{-1-2\theta}\theta^{-1}). \tag{2.8}$$

From (2.5), (2.7), (2.8), we obtain

https://doi.org/10.4153/CJM-1951-049-7 Published online by Cambridge University Press

(2.9) $$|S| \leqslant O(\epsilon g^{-1} \log g) + O(\theta K(\epsilon) g^{-1} \log g) + O(g^{-1-2\theta}\,\theta^{-1}),$$

where the constants implied in the O symbols are independent of ϵ and θ and g. For any given ϵ we can choose θ so that $\theta K(\epsilon) < \epsilon$. Hence (2.4) and (2.9) give

(2.10) $$\frac{g}{\log g} \sum_{p \leqslant x} C_p p^{-1} \to 0 \qquad (g \to \infty),$$

which is (2.2).

3. In this section we prove

(3.1) $$S = \sum_{p} \sum_{m \geqq 2} C_{p,m} m^{-1} p^{-m} = O(g^{-1}).$$

Clearly,

(3.2) $$\begin{aligned} |S| &\leqslant \sum_{p} \sum_{m \geqq 2} m^{-1} p^{-m} \qquad [p^m \equiv \pm 1(g)], \\ &= S_1 + S_2, \end{aligned}$$

where S_1 is the contribution of the sum from the terms with $p < g$, S_2 the contribution of the terms with $p > g$ (clearly $p = g$ contributes nothing).

First consider

(3.3) $$\begin{aligned} |S_2| \leqslant \sum_{m \geqq 2} \sum_{p > g} p^{-m} &= O\left\{ \sum_{p > g} p^{-2} \right\} \\ &= O\left\{ \sum_{x > g} \pi(x) \, . \, x^{-3} \right\} \\ &= O\,(g^{-1} (\log g)^{-1}). \end{aligned}$$

Since $\pi(x)$, the number of primes $\leqslant x$, is of the order of $x/\log x$.

Split S_1 into two parts:

(3.4) $$S_1 = S_3 + S_4$$

where

(3.5) $$S_3 = \sum_{p} \sum_{m \geqq 2} m^{-1} p^{-m}$$

and the variables m, p are subject to $p < g$, $p^m \equiv 1(g)$; S_4 is the same sum but with variables m, p subject to $p < g$, $p^m \equiv -1(g)$.

We first treat S_3. Since the congruence $x^m \equiv 1(g)$ has at most m solutions with $0 < x < g$, it follows that S_3 can be written as

(3.6) $$S_3 = \sum_{m=2}^{\infty} \frac{1}{m} \left\{ \sum_{a = A(m)}^{B(m)} \frac{\theta_a}{u_a g + 1} \right\}$$

where

$$A(m) = \tfrac{1}{2}(m^2 - m) + 1,$$
$$B(m) = \tfrac{1}{2}(m^2 + m),$$

each θ is 1 or 0, and the u's are different positive integers. We clearly have

(3.7) $$S_3 < g^{-1} \sum_{m=2}^{\infty} m^{-1} \left\{ \sum_{a = A(m)}^{B(m)} \frac{\theta_a}{u_a} \right\} = g^{-1} \sum_{m=2}^{\infty} d_m m^{-1}.$$

Write

$$D_2 = d_2,\ D_3 = d_2 + d_3,\ D_4 = d_2 + d_3 + d_4, \ldots,$$

Then

$$(3.8)\quad \sum_2^x \frac{d_m}{m} = \frac{D_2}{2} + \frac{D_3 - D_2}{3} + \ldots + \frac{D_x - D_{x-1}}{x} = \frac{D_x}{x} + \sum_2^{x-1} \frac{D_n}{n(n+1)}.$$

Clearly

$$(3.9)\quad 0 < D_n \leqslant \sum_{a=1}^{\frac{1}{2}(n^2+n)-1} a^{-1}.$$

From (3.6) to (3.9) we obtain

$$(3.10)\quad 0 < S_3 < g^{-1} \sum_{m=2}^{\infty} \frac{1}{m(m+1)} \left\{ \sum_{a=1}^{\frac{1}{2}(m^2+m)-1} \frac{1}{m} \right\} = O(g^{-1}).$$

Again

$$S_4 = \sum_{m=2}^{\infty} \frac{1}{m} \sum_{a=A(m)}^{B(m)} \frac{\phi_a}{v_a g - 1},$$

where each ϕ is 0 or 1, and the v's are different positive integers.
Since

$$\sum_{A(m)}^{B(m)} \frac{\phi_a}{v_a g - 1} = \sum_{A(m)}^{B(m)} \frac{\phi_a}{v_a g + 1} + O\left(g^{-2} \sum \frac{\phi_a}{v_a^2}\right)$$
$$= \sum_{A(m)}^{B(m)} \frac{\phi_a}{v_a g + 1} + O(g^{-2})$$

it follows, as in the case of S_3 that

$$(3.11)\quad S_4 = O(g^{-1}).$$

From (3.2), (3.3), (3.4), (3.10), (3.11) we derive (3.1).

4. From (2.2) and (3.1),

$$(4.1)\quad \sum_p \sum_m \frac{C_{p,m}}{mp^m} = o\left(\frac{\log g}{g}\right).$$

From (2.1) and (4.1)

$$(4.2)\quad \log\left(\frac{h_1}{G}\right) = o\,(\log g),$$

which is our main result stated in the introduction. Further we have proved that if Kummer's conjecture is true we must have

$$(4.3)\quad \sum C_p p^{-1} = O(g^{-1}).$$

5. In this section we assume the truth of the "extended Riemann hypothesis." For $R(s) > 1$, it is easy to see that

$$(5.1)\quad \prod_t L_t(s) = \exp\left\{g' \sum C_p \cdot p^{-s} + g' \sum_p \sum_{m \geq 2} C_{p,m} m^{-1} p^{-ms}\right\}$$

where $g' = \frac{1}{2}(g-1)$. In the sequel we shall need the following result due to Titchmarsh, [5], which we state as a lemma.

LEMMA 3. *If the extended Riemann hypothesis is true, and* $(k, l) = 1$, *we have*

$$\pi(x; k, l) = \frac{1}{\phi(k)} \int_2^x \frac{du}{\log u} + O(x^{\frac{1}{2}} \log x) \tag{5.2}$$

where the constant implied in the O is independent of both x and k.

Titchmarsh makes the restriction $x \geqslant k$ but this is plainly unnecessary for $\pi(x; k, l) = O(1)$ if $x < k$.

From (5.2) it follows that

$$C(x) = \sum_{p \leqslant x} C_p = O\,(x^{\frac{1}{2}} \log x) \qquad [x \geqslant 2], \tag{5.3}$$

where the constant implied in the O is independent of g.

Hence the series

$$\sum C_p\, p^{-s}$$

is convergent and represents an analytic function of s whenever $R(s) > \frac{1}{2}$. Further, the series

$$\sum_p \sum_{m \geqq 2} C_{p,m}\, m^{-1}\, p^{-ms}$$

is clearly an analytic function of s for $R(s) > \frac{1}{2}$, in fact without any hypothesis. Hence, by the theory of analytic continuation it follows that (5.1), proved for $R(s) > 1$, is also true for $R(s) > \frac{1}{2}$ on the assumption of the extended Riemann hypothesis.

We next estimate the series on the right hand side of (5.1) *qua* function of g. We restrict s to be real and to lie between θ_1 and θ_2 where $\frac{1}{2} < \theta_1 < \theta_2 < 1$. We have

$$\sum C_p \,.\, p^{-s} = \sum_{2g\,-\,1 < p < g^2} C_p \,.\, p^{-s} + \sum_{p > g^2} C_p \,.\, p^{-s} = G_1 + G_2.$$

Clearly

$$G_1 = O\{g^{-s}(1^{-s} + 2^{-s} + \ldots + g^{-s})\} = O(g^{1-2s}). \tag{5.5}$$

To estimate G_2 we use (5.3) and obtain

$$\sum_{p > g^2} C_p p^{-s} = O\left\{\sum_{x > g^2} \frac{C(x)}{x^{s+1}}\right\} = O\left(\frac{\log g}{g^{2s-1}}\right). \tag{5.6}$$

From (5.4), (5.5), (5.6) we obtain

$$\sum C_p\, p^{-s} = O\,(g^{1-2s} \log g). \tag{5.7}$$

To estimate

$$\sum_p \sum_{m \geqq 2} C_{p,m}\, m^{-1}\, p^{-ms}$$

qua function of g, we use the method of §3. Write

$$G_3 = \sum_p \sum_{m \geqq 2} m^{-1} p^{-ms} \qquad [p^m \equiv \pm 1 (g)].$$

Put

(5.8) $$G_3 = G_4 + G_5,$$

where G_4 is the part which arises from the terms of G_3 with $p < g$, G_5 the remaining part (terms with $p > g$, for $p = g$ contributes nothing). We have

$$\sum_{p>g}\sum_{m\geqq 2} p^{-ms} = O\left\{\sum_{p>g} p^{-2s}\right\} = O\left\{\sum_{n=g}^{\infty}\frac{\pi(n)}{n^{1+2s}}\right\}$$
$$= O\left\{g^{1-2s}/\log g\right\}.$$

Hence

(5.9) $$G_5 = O\left\{g^{1-2s}/\log g\right\}.$$

To estimate G_4 we again use the method of §3. We write

(5.10) $$G_4 = G_6 + G_7,$$

$$G_6 = \sum_{m=2}^{\infty}\frac{1}{m}\left\{\sum_{a=A(m)}^{B(m)}\frac{\theta_a}{(u_a g+1)^s}\right\},$$

$$G_7 = \sum_{m=2}^{\infty}\frac{1}{m}\left\{\sum_{a=A(m)}^{B(m)}\frac{\phi_a}{(v_a g-1)^s}\right\},$$

where $A(m) = \frac{1}{2}(m^2 - m) + 1$, $B(m) = \frac{1}{2}(m^2 + m)$; the u's are different positive integers, each θ is 1 or 0; the v's are different positive integers, each ϕ is 1 or 0.
Since

$$\sum_{2}^{\infty}\frac{1}{m}\left\{\sum_{a=A(m)}^{B(m)} a^{-s}\right\} = O\left(\sum_{m=2}^{a}\frac{m}{m\,.\,m^{2s}}\right) = O(1),$$

it follows as in §3 that

(5.11) $$G_6,\ G_7 = O(g^{-s}).$$

From (5.5) and (5.8) – (5.11) it follows that

(5.12) $$\prod_t L_t(s) = \exp\left\{gf(g)\right\} \qquad [s > \tfrac{1}{2}],$$

where $f(g) \to 0$ as $g \to \infty$. (1.4) is an immediate consequence of (5.12).

6. In this section we give a direct simple proof of the result (also implied in the work of Paley and Selberg—see [**4**]:

(6.1) $$\sum_t |L_t(1)|^2 \sim \tfrac{1}{2}g\zeta(2).$$

This relation gives an upper bound for h_1/G. For, from (6.1)

(6.2) $$\prod_t |L_t(1)|^2 \leqslant \left\{\frac{1}{g'}\sum_t |L_t(1)|^2\right\}^{g'} < \exp(Ag).$$

In view of Pólya's celebrated inequality

https://doi.org/10.4153/CJM-1951-049-7 Published online by Cambridge University Press

(6.3) $$\sum_{n=a}^{b} \chi_t(n) = O\,(g^{\frac{1}{2}} \log g),$$

we obtain

(6.4) $$L_t(1) = \sum_{1}^{\infty} \chi_t(n) n^{-1} = \sum_{1}^{\frac{1}{2}g} \chi_t(n) n^{-1} + O\,(\log g)\, g^{-\frac{1}{2}}.$$

Again (6.4) for the conjugate character, reads

(6,5) $$\sum_{1}^{\infty} \bar{\chi}_t(n) n^{-1} = \sum_{1}^{\frac{1}{2}g} \bar{\chi}_t(n).\ n^{-1} + O\,(\log g)\,.\, g^{-\frac{1}{2}}.$$

From (6.4) and (6.5) we obtain on multiplication

(6.6) $$|L_t(1)|^2 = \sum_{m=1}^{\frac{1}{2}g} \sum_{n=1}^{\frac{1}{2}g} \frac{\chi_t(m)\bar{\chi}_t(n)}{mn} + O\,(\log^2 g)\,.\, g^{-\frac{1}{2}}.$$

Hence we obtain the desired result, namely:

(6.7) $$\sum_t |L_t(1)|^2 = \tfrac{1}{2}(g-1) \sum_{n < \frac{1}{2}g} n^{-2} + O\,(g^{\frac{1}{2}} \log^2 g)$$
$$= \tfrac{1}{2} g \zeta(2) + O\,(g^{\frac{1}{2}} \log^2 g),$$

using (when m, n are not multiples of g)

(6.8) $$\sum_t \chi_t(m)\bar{\chi}_t(n) = \begin{cases} \tfrac{1}{2}(g-1) & [m \equiv n(g)], \\ -\tfrac{1}{2}(g-1) & [m \equiv -n(g)], \\ 0 & [m \not\equiv \pm n(g)]. \end{cases}$$

References

1. N. C. Ankeny and S. Chowla, *On the class number of the cyclotomic field*, Proc. Nat. Acad. Sci. (U.S.A.), vol. 39 (1949), 529-532.

2. R. Brauer, *On the Zeta functions of algebraic number fields* (II), Amer. J. Math., vol. 72 (1950), 739-746.

3. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Berlin, 1909.

4. A. Selberg, *Contributions to the theory of Dirichlet's L-Functions*, Skrifter utgitt av Det Norske Videnskaps-Akademi i Oslo, I Mat.-Naturv. Klasse. 1946, No. 3.

5. E. C. Titchmarsh, *On the divisor problem*, Rendiconti del Circolo Matematico di Palermo, vol. 54 (1930), 414-429.

6. A. Walfisz, *Zur additiven Zahlentheorie*, Math. Zeit., vol. 40 (1936), 598-601.

Princeton University
and
Institute for Advanced Study