THE CLASS NUMBER OF THE CYCLOTOMIC FIELD

BY N. C. ANKENY AND S. CHOWLA

PRINCETON UNIVERSITY AND INSTITUTE FOR ADVANCED STUDY

Communicated by Marston Morse, July 21, 1949

1. Let g denote any odd prime and $h = h(g)$ the class number of the cyclotomic field $R(\zeta)$, where ζ is the primitive gth root of unity, R the rational numbers. It is known that we can write: $h = h_1h_2$, 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. Math.*, **16**, 473 (1851)) that

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

He also calculated h_1 for $g \leqq 97$ and found $h_1 = 1$ for $g \leqq 19$, $h_1 = 411322823001$ for $g = 97$. No proof of (1) has yet been published.

In this paper we prove the following result:

$$\log\left(\frac{h_1}{G}\right)/\log g \to 0 \qquad (g \to \infty). \tag{2}$$

An interesting consequence of (2) is that there exists a g_0 such that $h_1(g)$ is (strictly) monotonic increasing for $g > g_0$; in fact if $g_2 > g_1 > g_0$, we have

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

Let p stand for a typical prime. Define

$$c_p = +1, -1, 0 \qquad [p \equiv 1(g), p \equiv -1(g), p \not\equiv \pm 1(g)]$$

It is well known that the series

$$\Sigma c_p \cdot p^{-1}$$

is convergent. We can show that *if Kummer's conjecture is true, we must have:*

$$\Sigma c_p \cdot p^{-1} = O(g^{-1}) \qquad [g \to \infty]. \tag{3}$$

It is hard to say whether (3) is even probably true. We cannot prove (3) even on the assumption of the "extended Riemann hypothesis" (or e. R. h.).

The method used to prove the above results can also be applied to prove the following results:

Let θ_1 and θ_2 denote any fixed constants such that

$$1/2 < \theta_1 < s < \theta_2 < 1.$$

If the e. R. h. is true, there exists for every given $\epsilon > 0$, a non-principal character $X(n) (\text{mod } g)$ such that

$$|L(s)| = |\sum_1^\infty X(n)\cdot n^{-s}| < 1 + \epsilon \tag{4}$$

for all primes $g > g_0(\epsilon, \theta_1, \theta_2)$.

This result with the larger constant $\sqrt{\zeta(2s)} + \epsilon$ on the right hand side of the inequality (4) (here, $\zeta(s)$ denotes Riemann's Zeta function; hence $\zeta(2s) > 1$ for $s > 1/2$) is implicit in some recent work of Atle Selberg, but it (with the larger constant) is proved by him without any hypothesis (*Skrifter Norske Videnskaps-Akad. Oslo*, Nr. 3 (1946)).

2. We give only a sketch of the methods used to prove the above results. Complete proofs will be published elsewhere.

Notation: We write

$$a \equiv b(c) \text{ for } a \equiv b \pmod c$$

Let X_t denote the $1/2(g - 1)$ characters (mod g), such that $X_t(-1) = -1$. $\pi(x; k, l)$ denotes the number of primes $\equiv l(k)$ and not exceeding x; $\phi(k)$ is the number of positive integers not exceeding k and prime to k.

$X_t(n)$ is a non-principal character (mod g), hence

$$L_t(s) = \sum_1^\infty X_t(n)\cdot n^{-s} \qquad [R(s) > 0]$$

It now easily follows that for $s > 1$ we have

$$\pi_t L_t(s) = \exp\left\{g'\sum_p \sum_{m\geq 1} \frac{c_{p,m}}{mp^{ms}}\right\} \tag{5}$$

where $g' = 1/2(g - 1)$ and

$$c_{p,m} = +1, -1, 0[p^m \equiv 1(g), p^m \equiv -1(g), p^m \not\equiv \pm 1(g)].$$

From (5) and

$$\frac{h_1}{G} = \pi_t L_t(1) \tag{6}$$

we deduce that

$$\frac{h_1}{G} = \exp\left\{g'\sum \frac{c_p}{p} + g'\sum_p \sum_{m>2} \frac{c_{p,m}}{mp^m}\right\} \tag{7}$$

Write

$$C = \sum c_p\cdot p^{-1} = C_1 + C_2 + C_3 \tag{8}$$

where for any given $\epsilon > 0$:
C_1 is the contribution to C of the terms with $2g - 1 \leqq p < g^{1+\epsilon}$
C_2 is the contribution to C of the terms with

$$g^{1+\epsilon} < p < \exp(g^{2\theta});$$

C_3, the rest.
It is trivial that (B is an absolute positive constant)

$$|C_1| \leqq B\frac{\epsilon}{g}\log g. \tag{9}$$

Now write

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

Then the sum C_2 is essentially

$$\sum \frac{C(n)}{n(n+1)} \tag{10}$$

where the summation is for all integers n lying between

$$g^{1+\epsilon} \text{ and } \exp(g^{2\gamma}).$$

To deal with the sum (10) we use the following result:

$$\pi(x;\ k,\ l) = O\left\{\frac{x}{\phi(k)\log x}\right\} \qquad [x \geqq k^{1+\epsilon}]. \tag{11}$$

This result follows from the work of Viggo Brun, but was first implicitly stated by Titchmarsh (*Rendiconti Circolo Mat. Palermo*, **54**, 414–429 (1930)). The constant implied in the O symbol is independent of x and k but may depend on ϵ.

From (11) one easily deduces that

$$|C_2| \leqq \frac{A\theta K(\epsilon)\log g}{g} \tag{12}$$

where A is an absolute positive constant.

Finally to estimate C_3 we use the following theorem (*Walfisz, Math. Ztschr.*, **40**, 598–599 (1936)): If $(k, l) = 1$, then

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

where the constant implied in the O symbol is independent of x and k, but may depend on m (arbitrarily large) and θ (arbitrarily small). By the application of this result we can easily obtain:

$$C_3 = O[g^{(1 - m)2\theta} + g^{-1 - 2\theta}] \tag{13}$$

We first fix ϵ (small), then θ sufficiently small, and finally m sufficiently large, to obtain from (8), (9), (12) and (13):

$$\left(\frac{g}{\log g}\right) \Sigma c_p \cdot p^{-1} \rightarrow 0 \ (g \rightarrow \infty) \tag{14}$$

We next indicate the proof of

$$C_4 = \sum_{p} \sum_{m \geq 2} \frac{c_{p,m}}{mp^m} = O(g^{-1}) \tag{15}$$

(14) shows that (2) follows from (15). In fact,

$$|C_4| \leqq \sum_{p} \sum_{m \geq 2} \frac{1}{mp^m} \qquad [p^m \equiv \pm 1(g)]$$

The part of this sum with $p > g$ is shown to be $0(g^{-1})$ by a very short argument.

Since $X^m \equiv 1(g)$ has at most m incongruent solutions, we derive that

$$C_4 = O\left\{ \sum_{m=2}^{\infty} \frac{1}{m} \left[\sum_{a = A(m)}^{B(m)} \left(\frac{1}{ag + 1} + \frac{1}{ag - 1}\right)\right]\right.$$

where

$$A(m) = {}^1/_2(m^2 - m) + 1, \qquad B(m) = {}^1/_2(m^2 + m)$$

And this indicates the proof of (15).

To prove (4) we start from the result

$$C(X) = O(\sqrt{x} \log x)$$

which is true on the assumption of the e. R. h. The rest of the arguments are similar to those used above.

Also, on the assumption of the e. R. h. we can improve (2) to

$$\log\left(\frac{h_1}{G}\right) = O\{(\log g)^{1/2} \log \log g\}$$