Tôhoku Math Journ.
23(1971), 573-580.

CLASS NUMBERS OF IMAGINARY ABELIAN NUMBER FIELDS, III

KÔJI UCHIDA

(Rec. Aug. 1, 1971)

Let l be a prime number, and let K_l be the field of the l-th roots of unity. Let h_1 be the first factor of the class number of K_l. It has been conjectured that $h_1 > 1$ for all $l \geqq 23$. We shall prove this conjecture in this paper. It has been known by M.Newman [2] that $h_1 > 1$ for all primes such that $23 \leqq l < 200$. We have proved in the previous paper [3] that $h_1 > 1$ for all $l > 2400$. We have obtained an improvement of this estimate, i. e., we have shown that $h_1 > 1$ for all $l > 500$ (See section 2). It is known $h_1 > 1$ for $l \equiv 3 (\text{mod } 4)$ and $l > 200$, and also $h_1 > 1$ for irregular primes. There remain 13 regular primes such that $200 < l < 500$ and $l \equiv 1 (\text{mod } 4)$. They are 229, 241, 269, 277, 281, 313, 317, 337, 349, 373, 397, 449 and 457. It will be shown in section 3 that $h_1 > 1$ for 7 primes among them such that $l \equiv 5 (\text{mod } 8)$. Final step for concluding the conjecture was done by M.Newman by making use of a computer. Our original manuscript was revised to include his results. We wish to express our hearty thanks to Dr. M.Newman for these and other computations. In fact his method is to compute h_1 modulo some prime number. The results are as follows:

l	h_1 mod 101	l	h_1 mod 101
241	42	337	89
281	5	449	27
313	51	457	11

Therefore $h_1 > 1$ for these primes.

1. We prove two lemmas which are key points in this paper.

LEMMA 9. *Let l be a prime number. Let K and L be imaginary subfields of the field of the l^f-th roots of unity for some integer f. Let $h_{1,K}$ and $h_{1,L}$ be first factors of class numbers of K and L, respectively. If K is a subfield of L, $h_{1,K}$ divides $h_{1,L}$.*

PROOF. Let K_0 and L_0 be maximal real subfields of K and L, respectively.

Let E, F, E_0 and F_0 be absolute class fields of K, L, K_0 and L_0, respectively. We put $E_1=E_0K$ and $F_1=F_0L$. Then

$$h_{1,K}=[E:E_1] \text{ and } h_{1,L}=[F:F_1]$$

hold. It is known that F_0/K_0 is a Galois extension. We show that E_0L_0/K_0 is the maximal abelian extension contained in F_0/K_0. Let F_2/K_0 denote the maximal abelian extension contained in F_0. The inertia subfield of l in F_2/K_0 is then unramified abelian extension over K_0 because there exists only one divisor of l in K_0 and that is the only prime ramified at F_0/K_0. Then the inertia field is equal to E_0. Then $F_2=E_0L_0$ is clear. We put $H=EL$ and $H_1=E_1L=E_0L$. The same argument shows that H is the maximal abelian extension of K contained in F. As the Galois group of F_1/K is isomorphic to that of F_0/K_0, H_1 is the maximal abelian extension of K contained in F_1. Then it holds $H_1=F_1\cap H$. Then $[H:H_1]=[HF_1:F_1]$ is a divisor of $[F:F_1]$. It holds $[E:E_1]=[H:H_1]$ because l is completely ramified at L/K. This proves the lemma.

REMARK. This lemma will also be proved from Hasse's class number formula [1]. Weak form of this lemma was given as Lemma 2 of [3]. M.Newman thought about divisibility and has calculated for biquadratic subfields of K_l for $l\equiv 5 \pmod 8$ and $l<400$. His method of computation is somewhat different from ours in section 3.

Now we assume $l\equiv 1 \pmod 4$ and we put $l=4m+1$. This restriction may not be necessary in Lemma 10, but simplifies notations. Let $L(s, \chi)$ be an L-function with character χ defined mod l. We put

$$L_2(s)=\prod_{\chi} L(s, \chi),$$

where χ runs over non-trivial characters such that $\chi(-1)=1$. We also define $L_1(s)$ as a product of $L(s, \chi)$ for characters χ such that $\chi(-1)=-1$. $L_1(s)$ will appear in the next section.

LEMMA 10. *Let f be the least positive integer such that $2^f\equiv \pm 1 \pmod l$ and let $fg=(l-1)/2$. Then for any real $s\geqq 1$ and for $l>270$, it holds*

$$|L_2(s)|\leqq 2^{-2m}s(1-2^{-f})^{-g}(\log l+0.7)^{2m-1}.$$

PROOF. As both sides are continuous at $s=1$, we can assume $s>1$. Then

$$L(s,\chi)=\left(1-\frac{\chi(2)}{2^s}\right)^{-1}\cdot\prod_{p:odd}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$
$$=\left(1-\frac{\chi(2)}{2^s}\right)^{-1}\sum_{n=1}^{\infty}\frac{\chi(2n-1)}{(2n-1)^s}$$

It holds $\sum_{n=1}^{4m}\chi(n)=0$ for any non-trivial χ. As $\chi(n)=\chi(l-n)$, it holds $\sum_{n=1}^{2m}\chi(n)=0$. If we put $S(2n-1)=\sum_{r=1}^{n}\chi(2r-1)$,

$$S(4m-1)=\sum_{n=1}^{2m}\chi(2n-1)=\sum_{n=1}^{4m}\chi(n)-\sum_{n=1}^{2m}\chi(2n)$$
$$=\sum_{n=1}^{4m}\chi(n)-\chi(2)\sum_{n=1}^{2m}\chi(n)=0,$$

also $S(l+4m)=0$. Then it holds $|S(2n-1)|\leqq m$ for any n, and

$$\left|\sum_{n=2m+1}^{\infty}\frac{\chi(2n-1)}{(2n-1)^s}\right|=\left|\sum_{n=2m+1}^{\infty}S(2n-1)\left\{\frac{1}{(2n-1)^s}-\frac{1}{(2n+1)^s}\right\}\right|$$
$$\leqq\sum_{n=2m+1}^{\infty}m\left\{\frac{1}{(2n-1)^s}-\frac{1}{(2n+1)^s}\right\}=\frac{m}{(4m+1)^s}<\frac{1}{4}.$$

It also holds

$$\left|\sum_{n=1}^{2m}\frac{\chi(2n-1)}{(2n-1)^s}\right|=\left|\sum_{n=1}^{2m}\left\{\frac{\chi(2n-1)}{(2n-1)^s}-\frac{\chi(2n-1)}{(2m)^s}\right\}\right|$$
$$\leqq\sum_{n=1}^{m}\left\{\frac{1}{(2n-1)^s}-\frac{1}{(2m+2n-1)^s}\right\}$$
$$\leqq 1+\frac{1}{3}+\sum_{n=3}^{m}\frac{2m}{(2n-1)(2m+2n-1)}$$
$$\leqq 1+\frac{1}{3}+\int_2^m\frac{2m\,dx}{(2x-1)(2m+2x-1)}$$
$$=1+\frac{1}{3}+\frac{1}{2}\log\left(m-\frac{1}{2}\right)-\frac{1}{2}\log\frac{3}{2}$$
$$-\frac{1}{2}\log\left(2m-\frac{1}{2}\right)+\frac{1}{2}\log\left(m+\frac{3}{2}\right)$$

$$
\begin{aligned}
&< 1+\frac{1}{3}-\frac{1}{2}\log 3+\frac{1}{2}\log\left(m+\frac{3}{2}\right)\\
&= 1+\frac{1}{3}-\frac{1}{2}\log 3-\log 2+\frac{1}{2}\log(l+5)\\
&< 0.1+\frac{1}{2}\log\ l \ \text{ if } l>270\,.
\end{aligned}
$$

Then

$$
|L(s,\chi)|<\frac{1}{2}\left|1-\frac{\chi(2)}{2^s}\right|^{-1}(\log\ l+0.7)
$$

holds for $l>270$. We have the desired inequality by multiplying for χ, as

$$
\begin{aligned}
\prod_{\substack{\chi\neq 1\\ \chi(-1)=1}}(1-\chi(2)2^{-s})^{-1} &= (1-2^{-s})\prod_{\chi(-1=1}(1-\chi(2)2^{-s})^{-1}\\
&= (1-2^{-s})(1-2^{-sf})^{-g}\\
&\leqq 2^{-1}s(1-2^{-f})^{-g}\,.
\end{aligned}
$$

2. We now prove the following theorem. In the following, Lemmas 1 to 8 mean those of [3].

THEOREM. *Let l be a prime number, and let K_l be the field of the l-th roots of unity. Let h_1 denote the first factor of the class number of K_l. Then h_1 is greater than* 1 *for all* $l\geqq 23$.

PROOF. M.Newman [2] has shown the theorem is true for $23\leqq l<200$. Lemma 9 combined with Stark's result for imaginary quadratic fields shows $h_1>1$ for all primes $l\equiv 3 \pmod 4$ and $l>200$. Now we prove $h_1>1$ for all $l>500$ such that that $l\equiv 1 \pmod 4$. This part of proof has no change from the proof of Proposition in [3], except the application of Lemma 10. We do not repeat detailed calculations there. Like a proof of the proposition of [3], we first estimate $L_1(1)$. Let $a=4(1+\sqrt{2})(l-2)$ and let $s_0=1+(a\log l)^{-1}$. Then

$$
\begin{aligned}
-\log L_1(1) &= -\Re\log L_1(s_0)+\int_1^{s_0}\Re\frac{L_1'}{L_1}(s)ds\\
&\leqq \Re\log L_2(s_0)+\log\ \zeta(s_0)+3.\ 101
\end{aligned}
$$

by Lemma 5(1) and by the estimate for the integral [3, p. 347]. Then Lemmas 8 and 10 show

$$\begin{aligned}-\log L_1(1) \leqq & -2m \log 2 + \frac{2}{a \log l} - g \log(1-2^{-f}) \\ & + 2m \log(\log l + 0.7) + \log 4(1+\sqrt{2}) \\ & + \log(l-2) + 3.101 \\ \leqq & -2m \log 2 + 2m \log(\log l + 0.7) \\ & + \log(l-2) - g \log(1-2^{-f}) + 5.371.\end{aligned}$$

As $f \geqq 9$ for $l > 400$,

$$\begin{aligned}-\log L_1(1) \leqq & -2m \log 2 + 2m \log(\log l + 0.7) \\ & + \log(l-2) - \frac{2m}{9} \log(1-2^{-9}) + 5.371 \\ \leqq & \, 2m\{-\log 2 + \log(\log l + 0.7) + \log 1.001\} \\ & + \log(l-2) + \log 216.\end{aligned}$$

Then it holds

$$L_1(1)^{-1} \leqq 216(l-2)\left\{\frac{1.001}{2}(\log l + 0.7)\right\}^{2m}.$$

As

$$\begin{aligned}h_1 &= 2\, l(\sqrt{l}/2\pi)^{2m} L_1(1) \\ &> \frac{2\, l}{216(l-2)}\left(\frac{\sqrt{l}}{1.001\pi(\log l + 0.7)}\right)^{2m} \\ &> \frac{1}{108}\left(\frac{\sqrt{l}}{1.001\pi(\log l + 0.7)}\right)^{2m},\end{aligned}$$

$h_1 > 1$ if

$$\sqrt{l} > 108^{1/2m} 1.001\pi(\log l + 0.7).$$

If we put $l = 500$,

$$108^{1/250} \times 1.001 \times 3.142(\log 500 + 0.7)$$
$$< 1.02 \times 1.001 \times 3.142 \times 6.92 < 22.3 < \sqrt{500}.$$

So above inequality holds for any $l > 500$. Now there remain primes such that $200 < l < 500$ and $l \equiv 1 (\mathrm{mod}\ 4)$. There is nothing to prove for irregular primes where h_1 is divisible by l. The rest are 13 primes in the introduction. M.Newman's calculation shows $h_1 > 1$ for six of them which are congruent to 1 mod 8. Proofs for primes such that $l \equiv 5 (\mathrm{mod}\ 8)$ are included in the next section.

REMARK. Let K_{l^2} be the field of the l^2-th roots of unity. If $l \geqq 23$, h_1 of K_{l^2} is greater than 1, because h_1 of K_l is so by our theorem. It is known that h_1 is equal to 1 for $l = 2$, 3 and 5, and $h_1 > 1$ for $l = 7$[1]. In the case $l = 11$, we can show that the subfield of K_{l^2} of degree 22 has $h_1 = 67 \times 353$. So h_1 of K_{l^2} is greater than 1 in this case. We do not know if $h_1 = 1$ or not for $l = 13, 17$ and 19.

3. Let l be an odd prime number. We put $l - 1 = 2^n \cdot a$, $(2, a) = 1$. Then K_l has a subfield of degree 2^n which is the smallest imaginary subfield of K_l. The first factor h_1' of the class number of this subfield is a divisor of h_1 by Lemma 9. We now consider the cases $n = 2$ and $n = 3$, i. e., the cases $l \equiv 5$ (mod 8) and $l \equiv 9$ (mod 16). In the case $l \equiv 5 (\mathrm{mod}\ 8)$, it is known [1] that

$$h_1' = \frac{1}{2\,l^2}\left(\sum_{n=1}^{l-1} \chi(n)n\right) \cdot \left(\sum_{n=1}^{l-1} \bar{\chi}(n)n\right)$$

for $l > 5$, where χ is a character mod l such that $\chi(-1) = -1$ and $\chi^4 = 1$. Let F be the multiplicative group of a field Z/lZ. Then the value $\chi(n)$ depends only on the class of n in F/F^4. As 2 is not a quadratic residue mod l, 2 is a generator of F/F^4. Thus 1, -1, 2 and -2 are representative of F/F^4, and $\chi(-1) = -1$, $\chi(2) = i$ and $\chi(-2) = -i$. This simplifies calculations in this case. It holds

$$\sum_{n=1}^{l-1} \chi(n)n = \sum\nolimits_1 n + i \sum\nolimits_2 n - \sum\nolimits_3 n - i \sum\nolimits_4 n,$$

where sums Σ_1, Σ_2, Σ_3 and Σ_4 are taken over n such that $1 \leqq n < l$ and $n \in F^4$, $n \in 2F^4$, $n \in -F^4$ and $n \in -2F^4$, respectively. As $n \in F^4$ if and only if $l - n \in -F^4$, and $n \in 2F^4$ if and only if $l - n \in -2F^4$, it holds

$$\sum_{n=1}^{l-1}\chi(n)n = 2\sum\nolimits_1 n - \frac{l(l-1)}{4} + 2i\sum\nolimits_2 n - \frac{l(l-1)}{4}i\,.$$

It is easily shown that both $\Sigma_1\ n$ and $\Sigma_2\ n$ are divisible by l. We put $S_1 = 2\ \Sigma_1\ n/l$ and $S_2 = 2\ \Sigma_2\ n/l$. We give a table of S_1, S_2 and h_1' for $l < 500$[1].

l	S_1	S_2	$(l-1)/4$	h_1'	l	S_1	S_2	$(l-1)/4$	h_1'
13	2	2	3	1	229	54	52	57	17
29	8	6	7	1	269	62	68	67	13
37	8	10	9	1	277	72	64	69	17
53	14	14	13	1	293	70	76	73	9
61	14	16	15	1	317	78	74	79	13
101	28	24	25	5	349	90	88	87	5
109	22	24	27	17	373	90	92	93	5
149	34	34	37	9	389	88	96	97	41
157	38	36	39	5	397	98	104	99	13
173	46	44	43	5	421	104	98	105	25
181	38	44	45	25	461	116	122	115	25
197	50	52	49	5					

In the case $l \equiv 9 (\mathrm{mod}\ 16)$, we can not fix a generator of F/F^8 for all l. So calculations are somewhat complicated. Let ζ denote a primitive 8-th root of unity such that $\zeta^2 = i$. Let x be a generator of F/F^8, and let $\Sigma_j\ n$ be the sum of n such that $1 \leqq n < l$ and $n \in x^j F$. If we put $S_j = 2\Sigma_j\ n/l$, it holds

$$h_1' = \frac{1}{2^3} N\left\{S_0 - \frac{l-1}{8} + \left(S_1 - \frac{l-1}{8}\right)\zeta + \left(S_2 - \frac{l-1}{8}\right)i \right.$$
$$\left. + \left(S_3 - \frac{l-1}{8}\right)\zeta i\right\},$$

where N denotes the absolute norm. We give values S_j and h_1' only for $l = 281$, 313 and 457, where $x = 3$ for $l = 281$ and $x = 5$ for $l = 313$ and 457.

[1] After we had prepared this manuscript, we received from M. Newman a table of h_1' in this case for $l \leqq 9013$. It should be remarked that $h_1' > 1$ for all l such that $100 < l \leqq 9013$.

l	S_0	S_1	S_2	S_3	$(l-1)/8$	h_1'
281	34	38	36	36	35	17
313	36	40	36	34	39	233
457	56	60	58	60	57	41

REFERENCES

[1] H. HASSE, Über die Klassenzahl abelscher Zahlkörper, Akademie Verlag, 1952
[2] M. NEWMAN, A table of the first factor for prime cyclotomic fields, Math. of Computation, 24, no. 109(1970)
[3] K. UCHIDA, Class numbers of imaginary abelian number fields II, Tôhoku Math. J., 23(1971)

MATHEMATICAL INSTITUTE
TÔHOKU UNIVERSITY
SENDAI, JAPAN.