Hence

$$|L(u)| = O\left(\exp\left(-\sum{}' 1/p\right)\right),$$

where, for each fixed $u \neq 0$, $\sum'$ denotes the sum over those primes which satisfy (10). By Lemmas 6 and 7 we get

$$\sum_{\substack{p\equiv 3 (\mathrm{mod}\, 4)\\ p\leqslant x}} 2/p = \log\log x + O(1).$$

Hence

$$|L(u)| = O\left(\{\exp(-c|u|^{2/3})\}\right),$$

where

$$c = \frac{1}{2}\left(\frac{4}{\pi}\right)^{2/3}\left(\frac{1}{3^{2/3}} - \frac{1}{5^{2/3}}\right) > 0.$$

So $L(u)$ is integrable and hence $L(u)$ is the characteristic function of an absolutely continuous distribution function.

Acknowledgements. The author wishes to record his deep gratitude to Prof. J. K. Ghosh for the many useful discussions he had with him during the preparation of this paper. Thanks are also due to Prof. E. M. Paul for some useful conversations regarding this subject.

References

[1] G. J. Babu, *On the distribution of additive arithmetical functions of integral polynomials*, Sankhyā, Series A, 34 (1972), pp. 323–334.
[2] P. Erdös, *On the smoothness of the asymptotic distribution of additive arithmetical functions*, Amer. J. Math. 61 (1939), pp. 722–725.
[3] P. Erdös and A. Schinzel, *Distribution of the values of some arithmetical functions*, Acta Arith. 6 (1961), pp. 473–485.
[4] W. Feller, *An Introduction to Probability Theory and Its Applications*, vol. II, New York–London 1961.
[5] J. Kubilius, *Probabilistic methods in the theory of numbers*, Translations of Math. Monographs, vol. 11, Providence 1964.
[6] E. Lukacs, *Characteristic Functions*, 2nd ed., London 1970.
[7] T. Nagell, *Introduction to Number Theory*, New York 1951.
[8] E. Novoselov, *A new method in probabilistic number theory*, Amer. Math. Soc. Trans. 52 (1966), pp. 217–275.
[9] M. Tanaka, *On the number of prime factors of integers*, Japan J. Math. 25 (1955), pp. 1–20.
[10] H. G. Tucker, *On continuous singular infinitely divisible distribution functions*, Ann. Math. Statis. 35 (1964), pp. 330–335.

INDIAN STATISTICAL INSTITUTE

Received on 15. 1. 1972 (250)

ACTA ARITHMETICA
XXIII (1973)

A simplification of the formula for $L(1,\chi)$ where χ is a totally imaginary Dirichlet character of a real quadratic field

by

DONALD E. RIDEOUT* (St. John's, Nfld.)

1. Introduction. Let $k = Q(\sqrt{\Delta})$ be a real quadratic field, and let χ be a totally imaginary Dirichlet character of k. The Dirichlet L-series $L(s,\chi)$ evaluated at $s = 1$ can be written in the following form:

$$L(1,\chi) = -\pi^2 W(\chi)^{-1} N(D_k \mathfrak{b}_\chi)^{-1/2}\left(\sum_{A} \overline{\chi(A)}\, G(A)\right)$$

where $\mathfrak{b}_\chi$ is the conductor of χ, the summation is over integral ideal representatives of the ray class group $\mathrm{Id}(\mathfrak{b}_\chi)/R(\mathfrak{b}_\chi)$, the bar denotes complex conjugation, $W(\chi)$ is a constant of absolute value 1 (see [1], page 300), $G(A)$ is a rational number with denominator at most $12\mathfrak{b}$ where $\mathfrak{b}$ is the smallest rational integer divisible by $\mathfrak{b}_\chi$, and D_k is the different of k. The rational number $G(A)$ does not depend on the class of A modulo $R(\mathfrak{b}_\chi)$. For details see [4], p. 171.

Of interest here is the rational number $G(A)$ for any given integral ideal A. We begin by defining $G(A)$ explicitly.

For rational numbers u, v with $u, v \in [0,1)$ and $(u,v) \neq (0,0)$ we introduce the following modified theta function:

$$\theta\left(z \,\middle|\, \begin{matrix} u \\ v \end{matrix}\right) = q^{\frac{1}{2}\left(\frac{1}{6} - v + v^2\right)} \prod_{m=0}^{\infty}(1 - q^m t) \prod_{m=1}^{\infty}(1 - q^m t^{-1})$$

where $q = e^{2\pi i z}$ and $t = e^{2\pi i (vz - u)}$.

If u' and v' are any rational numbers, we denote by $\overline{\begin{pmatrix} u' \\ v' \end{pmatrix}}$ the *normalized* pair $\begin{pmatrix} u \\ v \end{pmatrix}$ with $0 \leqslant u, v < 1$ and $u' \equiv u$, $v' \equiv v \pmod 1$.

Let $\mathrm{SL}(2, Z)$ denote the special linear group of two by two matrices with entries in Z and determinant $+1$. For any matrix M in $\mathrm{SL}(2, Z)$

* Research supported in part by a National Research Council of Canada Grant No. A-8080.

and rational numbers u, v with $u, v \in [0, 1)$ and $(u, v) \neq (0, 0)$ we introduce rational numbers $\mathfrak{S}\left(M\middle|\begin{matrix}u\\v\end{matrix}\right)$ by the following formula [1]:

$$(1)\qquad \mathfrak{S}\left(M\middle|\begin{matrix}u\\v\end{matrix}\right) = \frac{1}{2\pi i}\left(\log\theta\left(Mz\middle|\begin{matrix}u\\v\end{matrix}\right) - \log\theta\left(z\middle|\overline{M^{-1}\begin{pmatrix}u\\v\end{pmatrix}}\right)\right)$$

where z is a complex number in the upper half plane, $M = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$, and $Mz = \dfrac{az+b}{cz+d}$.

Let a_1, a_2 be a basis for the fractional ideal $AD_k^{-1}\mathfrak{b}_k^{-1}$ considered as a Z-module and such that $a_1'a_2 - a_1a_2' > 0$ where the prime denotes conjugation. Let ε denote the last unit of k greater than 1 and congruent to 1 (modulo $\mathfrak{b}_\chi$), i.e. the finite part of $\mathfrak{b}_\chi$ divides the principal ideal generated by $\varepsilon - 1$ where ε and its conjugate are positive. Then there exists $a, b, c, d \in Z$ such that

$$\varepsilon a_1 = a a_1 + b a_2,$$
$$\varepsilon a_2 = c a_1 + d a_2$$

and $ad - bc = 1$. Let $M = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $U = a_1 + a_1'$, and $V = a_2 + a_2'$. Then $U, V \in Q$ since $a_1 + a_1'$ and $a_2 + a_2'$ are just the trace of a_1 and a_2, respectively, the trace mapping being from k to Q. Let $\begin{pmatrix}u\\v\end{pmatrix} = \overline{\begin{pmatrix}U\\V\end{pmatrix}}$. Then $G(A)$ is defined by the following formula:

$$G(A) = \mathfrak{S}\left(M\middle|\begin{matrix}u\\v\end{matrix}\right).$$

For an explicit determination of $G(A)$ in terms of elementary arithmetical functions see [4], p. 183. However, from a computational point of view this formula is not suitable because there are $|c|$ summations to be carried out and $|c|$ can be extremely large. This will be clearly shown in an example in the next section.

Using the fact that the left side of (1) does not depend on the z chosen in the upper half plane, it is straightforward to show that for $M, N \in \mathrm{SL}(2, Z)$

$$\mathfrak{S}\left(MN\middle|\begin{matrix}u\\v\end{matrix}\right) = \mathfrak{S}\left(M\middle|\begin{matrix}u\\v\end{matrix}\right) + \mathfrak{S}\left(N\middle|\overline{M^{-1}\begin{pmatrix}u\\v\end{pmatrix}}\right).$$

(This fact was pointed out to me by A. Brumer.)

[1] It is convenient to use the notation $\mathfrak{S}\left(M\middle|\begin{matrix}u\\v\end{matrix}\right)$ rather than the usual notation $\mathfrak{S}(M, u, v)$.

By a simple induction argument it follows that for $M_1, M_2, \ldots, M_m \in \mathrm{SL}(2, Z)$

$$(2)\qquad \mathfrak{S}\left(\prod_{k=1}^{m} M_k\middle|\begin{matrix}u\\v\end{matrix}\right) = \sum_{k=1}^{m}\mathfrak{S}\left(M_k\middle|\overline{\left(\prod_{i=0}^{k-1} M_i\right)^{-1}\begin{pmatrix}u\\v\end{pmatrix}}\right)$$

where M_0 is the identity matrix.

By mimicking the method for determining $G(A)$ in terms of elementary arithmetical functions in [4], we can calculate $\mathfrak{S}\left(T\middle|\begin{matrix}u\\v\end{matrix}\right)$ and $\mathfrak{S}\left(S\middle|\begin{matrix}u\\v\end{matrix}\right)$ explicitly where $T = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $S = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ are generators of the group $\mathrm{SL}(2, Z)$

$$(3)\qquad \begin{aligned}\mathfrak{S}\left(T\middle|\begin{matrix}u\\v\end{matrix}\right) &= \tfrac{1}{2}\left(\tfrac{1}{6} - v + v^2\right),\\ \mathfrak{S}\left(S\middle|\begin{matrix}u\\v\end{matrix}\right) &= \begin{cases}\left(\tfrac{1}{2} - u\right)\left(\tfrac{1}{2} - v\right) & \text{if } u \neq 0,\\ -\tfrac{1}{2}\left(\tfrac{1}{2} - v\right) & \text{if } u = 0.\end{cases}\end{aligned}$$

(The author is again indebted to A. Brumer for pointing out this fact. For the generator S^3 there is no need for two cases as for S, $\mathfrak{S}\left(S^3\middle|\begin{matrix}u\\v\end{matrix}\right) = \left(\frac{1}{2} - u\right)\left(\frac{1}{2} - v\right)$ for all $u, v \in [0, 1)$ with $(u, v) \neq (0, 0)$.)

In this paper we prove the following results.

LEMMA 1. *Let $a, b, c, d \in Z$ where $ad - bc = 1$, $a, c > 0$, $a \neq 1$, $|b| \neq 0$ or 1, $d \neq 0$. Then $a/|b|$ can be written as a continued fraction $\langle a_1, a_2, \ldots, a_{n-1}\rangle$ such that*

(i) *if $a > c$, $c/|d| = \langle a_1, a_2, \ldots, a_{n-2}\rangle$,*
(ii) *if $a < c$, $c/|d| = \langle a_1, a_2, \ldots, a_{n-1}, a_n\rangle$*

where $a_n = (cQ - |d|P)/(a|d| - |b|c)$ and P, Q are relatively prime positive integers defined by the formula $P/Q = \langle a_1, a_2, \ldots, a_{n-2}\rangle$.

LEMMA 2. *Let $M = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{SL}(2, Z)$ with $a, c > 0$, $b, d \neq 0$, then M can be factored as follows:*

$$(4)\qquad M = N_{q_1}N_{q_2}\ldots N_{q_n}S$$

or

$$(5)\qquad M = N_{q_1}N_{q_2}\ldots N_{q_n}S^3$$

where $N_r = S^3T^{-r} = \begin{pmatrix}0 & 1\\ -1 & r\end{pmatrix}$ and $q_1 = 0$ if $a > c$, $q_{i+1} = (-1)^i a_{n-i}$ or $q_{i+1} = (-1)^{i+1}a_{n-i}$, $0 \leqslant i \leqslant n-1$, unless $a = 1$ or $|b| = 1$ in which cases we have

$$M = \begin{cases}N_cN_{-b}N_0S^3 & \text{if } a = 1,\\ N_dN_aS & \text{if } b = 1,\\ N_{-d}N_{-a}S^3 & \text{if } b = -1.\end{cases}$$

THEOREM. *For* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, Z)$, $a, c > 0$, $b, d \neq 0$

$$\mathfrak{S}\left(M \left| \begin{matrix} u \\ v \end{matrix}\right.\right) = \sum_{i=1}^{n} \left\{ \frac{-q_i}{2} \left(\tfrac{1}{6} - u_i + u_i^2\right) + \left(\tfrac{1}{2} - u_i\right)\left(\tfrac{1}{2} - u_{i-1}\right) \right\} + \\ + \left(\tfrac{1}{2} - u_{n+1}\right)\left(\tfrac{1}{2} - u_n\right) + \delta(u_{n+1})$$

where $u_0 = v$, $u_1 = u$, *and for* $2 \leqslant i \leqslant n+1$, $u_i \equiv q_{i-1} u_{i-1} - u_{i-2} \pmod 1$ *where* $0 \leqslant u_i < 1$, *the* q_i*'s are defined in Lemma* 2, *and* $\delta(u_{n+1}) = 0$ *unless* $u_{n+1} = 0$ *and* M *is factored as in* (4), *then* $\delta(u_{n+1}) = -\left(\tfrac{1}{2} - u_n\right)$.

COROLLARY. *In the particular case where* M *arises from an ideal* A *as discussed above, then*

$$G(A) = \mathfrak{S}\left(M \left| \begin{matrix} u \\ v \end{matrix}\right.\right) = \frac{n-1}{4} - \frac{1}{12} \sum_{i=1}^{n} q_i + \\ + \frac{1}{2} \sum_{i=1}^{n} \{q_i u_i - u_{i-1} - u_{i+1}\}(1 - u_i) + \lambda(M)$$

where $\lambda(M) = \tfrac{1}{2}(1-u)$ *if* M *is factored as in* (4) *and* $\lambda(M) = \tfrac{1}{2}v$ *if* M *is factored as in* (5).

2. An example. Our claim is that the formula given in the corollary is much better suited for computations than the existing formula. In the case that $k = Q(\sqrt{p})$ where p is a prime congruent to 1 modulo 4, and for the extension $Q(\sqrt[p]{1})$ of k then the conductor of χ is the principal ideal generated by $\sqrt{p}$, in the ring of integers of k, times the two infinite primes. The different D_k is the ideal generated by $\sqrt{p}$. Hence for any ideal A, $AD_k^{-1}\mathfrak{b}_\chi^{-1} = \dfrac{1}{p} A$. It is also straightforward to check that the least unit ε of k greater than 1 and congruent to 1 modulo $\mathfrak{b}_\chi$ is just the fourth power of the fundamental unit > 1.

For $p = 1297$, $\varepsilon = 13073905 + 7467840\theta$ where $\theta = \dfrac{1+\sqrt{p}}{2}$. For the ideal $A = \{2a + b\theta \mid a, b \in Z\}$ (which, incidentally, is a generator of the class group of $Q(\sqrt{1297})$ of order 11) $\alpha_1 = 2/1297$, $\alpha_2 = \theta/1297$, $M = \begin{pmatrix} 13073905 & 1493568 \\ 120979008 & 13820689 \end{pmatrix}$, $u_1 = u = 4/1297$ and $u_0 = v = 1/1297$. The fraction $120979008/13820689$ written as a continued fraction is $\langle 8, 1, 3, 17, 1, 3, 17, 1, 3, 17, 1, 3, 9\rangle$. To compute $G(A)$ we compute the following table where $A_i = pu_i$, $B_i = q_i A_i - A_{i-1}$, $C_i = B_i - A_{i+1}$, $D_i = p - A_i$ and $E_i = (C_i D_i)/p$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
q_i		9	-3	1	-17	3	-1	17	-3	1	-17	3	-1	8	
A_i	1	4	35	1188	1153	1260	33	4	35	1188	1153	1260	33	4	1296
B_i		35	-109	1153	-20789	2627	-1293	35	-109	1153	-20789	2627	-1293	-1	
C_i		0	$-p$	0	$-17p$	$2p$	$-p$	0	$-p$	0	$-17p$	$2p$	$-p$	$-p$	
D_i		1293	1262	109	144	37	1264	1293	1262	109	144	37	1264	1293	
E_i		0	-1262	0	-2448	74	-1264	0	-1262	0	-2448	74	-1264	-1293	

From the formula given in the corollary we have

$$G(A) = \frac{n-1}{4} + \frac{1}{2p} \sum_{i=1}^{n} E_i + \frac{1}{2p}(p - A_1)$$

where $n = 13$. From the table it is clear that $G(A) = -1009/1297$. This calculation involved a summation of 13 terms. In the formula listed in [4], p. 183, the calculation involved a summation of 120979008 terms! The formula above clearly simplifies the existing formula for $G(A)$ and is easily adaptable to computers.

3. Proofs of Lemmas 1 and 2. We use some elementary results about continued fractions that are listed, for example, in [3], Chapter 7. It is convenient to extend the definition of a finite continued fraction, denoted by $\langle a_1, a_2, \ldots, a_n\rangle$ where the a_i's are positive integers, so that a_n may be negative. In the case where a_n could possibly be negative but $a_{n-1} + \dfrac{1}{a_n} \neq 0$ define $\langle a_1, a_2, \ldots, a_n\rangle$ to be the continued fraction $\left\langle a_1, a_2, \ldots \ldots, a_{n-2}, a_{n-1} + \dfrac{1}{a_n}\right\rangle$. This definition agrees with the usual definition when $a_n > 0$.

Lemma 1 can be divided into two parts.

Part 1. *Let* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, Z)$ *and* $a, c > 0$, $a \neq 1$, $|b| \neq 0$ *or* 1, $d \neq 0$. *Let* $\langle a_1, a_2, \ldots, a_{n-1}\rangle$ *where* $a_{n-1} > 1$ *be the continued fraction expansion of* $a/|b|$, *and let* $a_n = (cQ - |d|P)/(a|d| - |b|c)$ *where* P, Q *are relatively prime positive integers such that* $P/Q = \langle a_1, a_2, \ldots, a_{n-2}\rangle$. *Then*

(i) *if* $a_n = 0$, $c/|d| = \langle a_1, a_2, \ldots, a_{n-2}\rangle$,

(ii) *if* $a_n \neq 0$, $c/|d| = \langle a_1, a_2, \ldots, a_{n-1}, a_n\rangle$.

Part 2. *If* a, c, a_n *are defined as in Part* 1, *then* $a_n = 0$ *or* -1 *if and only if* $a > c$.

In the case where $a_n = -1$, it is convenient to write

$$a/|b| = \langle a_1, a_2, \ldots, a_{n-1}-1, 1\rangle = \langle a_1, a_2, \ldots, a_{n-1}\rangle.$$

These are the only two ways of writing a finite continued fraction. Hence in this case we can write $a/|b|$ in such a way as a continued fraction by relabeling the a_i's so that $a_{n-1} = 1$ and from Part 1 $c/|d| = \langle a_1, \ldots, a_{n-2}\rangle$. Hence the statement of Lemma 1 is a summary of parts 1 and 2 above, hence we now prove Parts 1 and 2 in that order.

We need the fact about continued fractions that for x any non-zero complex number (and hence, in particular, for x a negative real),

$$\langle a_1, a_2, \ldots, a_k, x\rangle = \frac{xP'+P''}{xQ'+Q''} \tag{6}$$

where $k \geqslant 2, P', P'', Q', Q''$ are positive integers and $(P', Q') = 1 = (P'', Q'')$, $P''/Q'' = \langle a_1, \ldots, a_{k-1}\rangle$ and $P'/Q' = \langle a_1, \ldots, a_k\rangle$. Note that $a|d|-|b|c = \pm 1$ since a and $c > 0$ imply that both b and d are negative or both are positive. Hence the a_n defined in Part 1 is an integer. If $a_n = 0$ then clearly $c/|d| = P/Q$. For $a_n \neq 0$

$$\langle a_1, \ldots, a_{n-1}, a_n\rangle = \frac{a_n a+P}{a_n|b|+Q}$$

by (6), and clearly

$$\frac{a_n a+P}{a_n|b|+Q} = \frac{c}{|d|}.$$

To prove Part 2 we first remark that, since a, $|b| \neq 1$, $|b| > |d|$ if and only if $a > c$, and $|d| > |b|$ if and only if $c > a$. Also the denominator of the *convergents* (see [3], Chapter 7) of a continued fraction form an increasing sequence of positive integers.

If $a_n = 0$, then by Part 1 $|d|$ and $|b|$ are denominators of successive convergents, hence $|b| > |d|$ (we cannot have $|b| = |d|$) which implies that $a > c$. If $a_n = -1$ then $c/|d| = \langle a_1, a_2, \ldots, a_{n-1}-1\rangle$ by Part 1. But $a_{n-1} > 1$ so that $a/|b| = \langle a_1, \ldots, a_{n-1}-1, 1\rangle$ so that again $|b| > |d|$ since $a/|b|$, $c/|d|$ form consecutive convergents. Hence $a > c$.

Conversely assume that $a_n \neq 0, -1$, then we shall prove that $c > a$. If $a_n > 0$, then $|d| > |b|$ because by Part 1, $a/|b|$, $c/|d|$ are consecutive convergents. Hence $c > a$. If $a_n < 0$, $a_n \neq -1$, then

$$c/|d| = \left\langle a_1, \ldots, a_{n-1}+\frac{1}{a_n}\right\rangle = \langle a_1, \ldots, a_{n-1}-1, x\rangle$$

where $x = a_n/(1+a_n)$, a positive rational number, $1 < a_n/(1+a_n) \leqslant 2$, so that the usual continued fraction for $c/|d|$ will have more terms than that for $a/|b| = \langle a_1, \ldots, a_{n-1}-1, 1\rangle$. Hence $|d| > |b|$ which implies that $c > a$. This completes the proof of Part 2 and hence of Lemma 1.

In proving Lemma 2 we first dispose of the cases when $a = 1$ or $|b| = 1$. In those cases the factorization of M is explicitly given and can be easily checked to be correct. Hence we assume that $a \neq 1$ and $|b| \neq 1$ so that we can use the result stated in Lemma 1. We can assume that $a/|b|$ is written in one of the two possible ways as a continued fraction so that the conclusions of Lemma 1 hold. By the Euclidean algorithm, there exist nonnegative remainder terms $r_1, r_2, \ldots, r_{n-1}$ such that $a = a_1|b|+r_1$, $|b| = a_2 r_1+r_2$, $r_1 = a_3 r_2+r_3, \ldots, r_{n-3} = a_{n-1}r_{n-2}+r_{n-1}$ where $r_{n-1} = 0$ and $r_{n-2} = 1$.

If $a > c$ then by Lemma 1 $c/|d| = \langle a_1, a_2, \ldots, a_{n-2}\rangle$ hence by the Euclidean algorithm there exist nonnegative remainder terms $r'_1, r'_2, \ldots, r'_{n-2}$ such that $c = a_1|d|+r'_1$, $|d| = a_2 r'_1+r'_2$, $r'_1 = a_3 r'_2+r'_3, \ldots, r'_{n-4} = a_{n-2}r'_{n-3}+r'_{n-2}$ where $r'_{n-2} = 0$ and $r'_{n-3} = 1$. If $a < c$ then $c/|d| = \langle a_1, a_2, \ldots, a_{n-1}, a_n\rangle$. For the case $a_n > 0$ there exist nonnegative remainder terms $r'_1, \ldots, r'_n$ such that $c = a_1|d|+r'_1$, $|d| = a_2 r'_1+r'_2$, $r'_1 = a_3 r'_2+r'_3, \ldots, r'_{n-2} = a_n r'_{n-1}+r'_n$ where $r'_n = 0$ and $r'_{n-1} = 1$. If $a_n < 0$ (note $a_n \neq -1$), then the remainder terms $r'_1, \ldots, r'_{n-2}$ can be chosen positive and $r'_n = 0$, $r'_{n-1} = -1$. It is advantageous to make a table of the various cases that can occur where "def" means that the corresponding r_i or r'_i is defined by that value.

	$a > c$	$a < c,\ a_n > 0$	$a < c,\ a_n < 0$
$r'_{n-3} = a_{n-1}r'_{n-2} + r'_{n-1}$	$r'_{n-1} \overset{\text{def}}{=} 1,\ r'_{n-2} = 0$		
$r_{n-2} = a_n r_{n-1}+r_n$	$r_n \overset{\text{def}}{=} 1,\ r_{n-1} = 0$	$r_n \overset{\text{def}}{=} 1,\ r_{n-1} = 0$	$r_n \overset{\text{def}}{=} 1,\ r_{n-1} = 0$
$r'_{n-2} = a_n r'_{n-1}+r'_n$	$r'_n \overset{\text{def}}{=} 0,\ r'_{n-1} = 1$	$r'_n = 0,\ r'_{n-1} = 1$	$r'_n = 0,\ r'_{n-1} = -1$

From the equations above we can compute the following sequence of matrices. For the case $b, d > 0$

$$\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} 1 & 0 \\ -a_1 & 1\end{pmatrix} = \begin{pmatrix} r_1 & b \\ r'_1 & d\end{pmatrix}; \quad \begin{pmatrix} r_1 & b \\ r'_1 & d\end{pmatrix}\begin{pmatrix} -a_2 & -1 \\ 1 & 0\end{pmatrix} = \begin{pmatrix} r_2 & -r_1 \\ r'_2 & -r'_1\end{pmatrix}; \quad \ldots \tag{7}$$

At the nth step the last matrix will be one of the following matrices:

$$\begin{pmatrix} r_n & r_{n-1} \\ r'_n & r'_{n-1}\end{pmatrix}; \quad \begin{pmatrix} r_n & -r_{n-1} \\ r'_n & -r'_{n-1}\end{pmatrix}; \quad \begin{pmatrix} -r_n & -r_{n-1} \\ -r'_n & -r'_{n-1}\end{pmatrix}; \quad \begin{pmatrix} -r_n & r_{n-1} \\ -r'_n & r'_{n-1}\end{pmatrix}$$

if $n \equiv 1, 2, 3, 0 \pmod 4$ respectively. Hence from the above table we see that each of these four matrices must be either $I = \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}$ or S^2

$= \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$. Note that the matrices $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ and $\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$ cannot occur since the determinant of each matrix is forced to be $+1$. Hence it is clear from the sequence of matrices (7) that

$$\left.\begin{matrix} I \\ \text{or } S^2\end{matrix}\right\} = M(N_{a_1}S)^{-1}N_{-a_2}^{-1}N_{a_3}^{-1}\dots N_{\pm a_n}^{-1}$$

so that

$$M = N_{\pm a_n}\dots N_{a_3}N_{-a_2}N_{a_1}\cdot\left\{\begin{matrix} S \\ \text{or } S^3\end{matrix}\right.$$

which proves Lemma 2 in the case $b, d > 0$ where $q_n = a_1$, $q_{n-1} = -a_2$, $q_{n-2} = a_3$ etc.

By the same method it is easy to verify that in the case $b, d < 0$

$$M = N_{\pm a_n}\dots N_{-a_3}N_{a_2}N_{-a_1}\cdot\left\{\begin{matrix} S \\ \text{or } S_3\end{matrix}\right.$$

where $q_n = -a_1$, $q_{n-1} = a_2$, $q_{n-2} = -a_3$, etc. This completes the proof of Lemma 2.

4. Proofs of Theorem and Corollary. Recall that $N_r = S^3T^{-r}$. Hence from formulas (2) and (3) it is straightforward to check that

$$\mathfrak{S}\left(N_r \,\middle|\, \begin{matrix}u\\ v\end{matrix}\right) = \frac{-r}{2}\left(\tfrac{1}{6} - u + u^2\right) + \left(\tfrac{1}{2} - u\right)\left(\tfrac{1}{2} - v\right).$$

From the factorization of M given in Lemma 2 and formula (2) we have

$$\mathfrak{S}\left(M \,\middle|\, \begin{matrix}u\\ v\end{matrix}\right) = \sum_{i=1}^{n}\mathfrak{S}\left(N_{a_i} \,\middle|\, \begin{matrix}u_i\\ v_i\end{matrix}\right) + \begin{cases}\text{either } \mathfrak{S}\left(S \,\middle|\, \begin{matrix}u_{n+1}\\ v_{n+1}\end{matrix}\right)\\ \text{or } \quad\ \mathfrak{S}\left(S^3 \,\middle|\, \begin{matrix}u_{n+1}\\ v_{n+1}\end{matrix}\right)\end{cases}$$

where $u_1 = u$, $v_1 = v$ and $\overline{N_{q_{i-1}}^{-1}\begin{pmatrix}u_{i-1}\\ v_{i-1}\end{pmatrix}} = \begin{pmatrix}u_i\\ v_i\end{pmatrix}$, $2 \leqslant i \leqslant n+1$. This is equivalent to saying for $2 \leqslant i \leqslant n+1$ that

$$u_i \equiv q_{i-1}u_{i-1} - u_{i-2} \pmod 1 \quad \text{and} \quad 0 \leqslant u_i < 1$$

where $u_0 = v$. Note that $v_i = u_{i-1}$, $1 \leqslant i \leqslant n+1$. The proof of the theorem will be complete with the following analysis of $\mathfrak{S}\left(S \,\middle|\, \begin{matrix}u_{n+1}\\ u_n\end{matrix}\right)$. From formula (2)

$$\mathfrak{S}\left(S \,\middle|\, \begin{matrix}u_{n+1}\\ u_n\end{matrix}\right) = \mathfrak{S}\left(S^3\cdot S^2 \,\middle|\, \begin{matrix}u_{n+1}\\ u_n\end{matrix}\right) = \mathfrak{S}\left(S^3 \,\middle|\, \begin{matrix}u_{n+1}\\ u_n\end{matrix}\right) + \mathfrak{S}\left(S^2 \,\middle|\, \overline{S\begin{pmatrix}u_{n+1}\\ u_n\end{pmatrix}}\right)$$

where $\overline{S\begin{pmatrix}u_{n+1}\\ u_n\end{pmatrix}} = \overline{\begin{pmatrix}-u_n\\ u_{n+1}\end{pmatrix}}$. Using formulas (3) it is easy to check that $\mathfrak{S}\left(S^2 \,\middle|\, \overline{S\begin{pmatrix}u_{n+1}\\ u_n\end{pmatrix}}\right) = 0$ unless $u_{n+1} = 0$ in which case it is $-(\frac{1}{2} - u_n)$. This explains the need for the term $\delta(u_{n+1})$. The proof of the theorem is now complete.

We now prove the Corollary. In the particular case where M arises from an ideal A, the properties of the least unit ε implies that $\overline{M\begin{pmatrix}u\\ v\end{pmatrix}} = \begin{pmatrix}u\\ v\end{pmatrix}$. From this fact it follows that $u_{n+1} = 1 - u_0$ and $u_n = u_1$ if M is factored as in formula (4), and $u_{n+1} = u_0$ and $u_n = 1 - u_1$ if M is factored as in formula (5). We used the fact here that $u_1 = u \neq 0$ and $u_0 = v \neq 0$, which is always the case for u, v arising from an ideal. It is now straightforward to show that $G(A)$ can be written in the form given in the Corollary.

Acknowledgement. The author would like to thank J. Labute for encouraging comments while working on the results of this paper, and also to thank A. Brumer for suggesting the problem and for his assistance.

References

[1] S. Lang, *Algebraic Number Theory*, Reading, Mass. 1970.
[2] H. W. Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. 209 (1962), pp. 54–71.
[3] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, New York 1962.
[4] C. L. Siegel, *Lectures on Advanced Analytic Number Theory*, Bombay 1961.

DEPARTMENT OF MATHEMATICS
MEMORIAL UNIVERSITY OF NEWFOUNDLAND
St. John's, Newfoundland, Canada

Received on 22. 4. 1972 (271)