Hence

$$|L(u)| = O\left(\exp\left( - \sum_{p \text{ prime}} \frac{1}{p} \right) \right),$$

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

$$\sum_{p \in S \setminus \{2\}} 2/p = \log \log \omega + O(1).$$

Hence

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

where

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

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


Indian Statistical Institute

Received on 15. 1. 1972
and rational numbers \( u, v \) with \( u, v \in \mathbb{Q} \) and \( (u, v) \neq (0, 0) \) we introduce rational numbers \( \mathcal{S}(M|v) \) by the following formula (1):

\[
\mathcal{S}(M|v) = \frac{1}{2\pi i} \left( \log \theta \left( M \right| \frac{u}{v} \right) - \log \theta \left( z | M^{-1} \right( \frac{u}{v} \right) ) \)
\]

where \( z \) is a complex number in the upper half plane, \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \), and

\[
Mz = \frac{az + b}{cz + d}.
\]

Let \( a_1, a_2 \) be a basis for the fractional ideal \( \mathcal{A}D_0^{-1}b_0^{-1} \) considered as a \( \mathbb{Z} \)-module such that \( a_1a_2 - a_1a_2^* > 0 \) where the prime denotes conjugation. Let \( \varepsilon \) denote the last unit of \( k \) greater than 1 and congruent to 1 (modulo \( b_0 \)), i.e. the finite part of \( b_0 \) divides the principal ideal generated by \( \varepsilon - 1 \) where \( \varepsilon \) and its conjugate are positive. Then there exists \( a, b, c, d \in \mathbb{Z} \) such that

\[
\begin{align*}
ca_1 &= ba_2 + b(a_1a_2 - a_1a_2^*)c,
ca_2 &= ba_1 + (a_1a_2 - a_1a_2^*)d,
\end{align*}
\]

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 \( U, V \in \mathcal{O} \) since \( a_1 + a^*_1 \) and \( a_2 + a^*_2 \) are just the trace of \( a_1 \) and \( a_1^* \), respectively, the trace mapping being from \( k \) to \( Q \). Let \( \frac{u}{v} = \frac{U}{V} \). Then \( G(A) \) is defined by the following formula:

\[
G(A) = \mathcal{S}(M|u|v).
\]

For an explicit determination of \( G(A) \) in terms of elementary arithmetical functions see [4], p. 153. However, from a computational point of view this formula is not suitable because there are \([\varepsilon]\) summations to be carried out and \([\varepsilon]\) 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 straight forward to show that for \( M, N \in \text{SL}(2, \mathbb{Z}) \)

\[
\mathcal{S}(MN|u|v) = \mathcal{S}(M|u|v) \mathcal{S}(N|v|v).
\]

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

---

(1) It is convenient to use the notation \( \mathcal{S}(M|u|v) \) rather than the usual notation \( \mathcal{S}(M, u, v) \).
Theorem. For \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \), \( a, c > 0 \), \( b, d \neq 0 \),

\[
\mathbb{E}(M \mid u) = \sum_{i=1}^{n} \left[ \frac{-q_i}{2} \left( \frac{1}{2} - u_i + u_i^2 \right) + \left( \frac{1}{2} - u_i \right) \left( \frac{1}{2} - u_{i+1} \right) \right] + \\
+ \left( \frac{1}{2} - u_{n+1} \right) \left( \frac{1}{2} - u_{n} \right) + \delta(u_{n+1})
\]

where \( u_0 = u, \ u_1 = u \), and for \( 2 \leq i \leq n+1, \ u_i = q_i u_{i-1} - u_{i-1} \) (mod 1) where \( 0 \leq u_i < 1 \), 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 \( \delta(u_{n+1}) = \frac{1}{2} \left( 1 - u_n \right) \).

Corollary. In the particular case when \( M \) arises from an ideal \( A \) as discussed above, then

\[
G(A) = \mathbb{E}(M \mid u) = \frac{n-1}{4} - \frac{1}{2} \sum_{i=1}^{n} q_i + \\
+ \frac{1}{2} \sum_{i=1}^{n} \left( q_i u_i - u_{i-1} - u_{i+1} \right) \left( 1 - u_i \right) + \lambda(M)
\]

where \( \lambda(M) = \frac{1}{2} \left( 1 - u \right) \) if \( M \) is factored as in (4) and \( \lambda(M) = -\frac{1}{2} u \) 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 \( Q(\sqrt{1}) \) of \( k \) then the conductor of \( \chi \) is the principal ideal generated by \( \sqrt{p} \) in the ring of integers of \( k \), times the two infinite primes. The difference \( D_k \) is the ideal generated by \( \sqrt{p} \). Hence for any ideal \( A \), \( AD_k^{-1}(1) = \frac{1}{p} A \). It is also straightforward to check that the least unit \( \epsilon \) of \( k \) greater than 1 and congruent to 1 modulo \( b \) is just the fourth power of the fundamental unit \( \epsilon > 1 \).

For \( p = 1297 \), \( \epsilon = 13073905 + 7467849 \) where \( \theta = \frac{1 + \sqrt{1297}}{2} \). For the ideal \( A = \langle 2a + b \mid a, b \in \mathbb{Z} \rangle \) (which, incidentally, is a generator of the class group of \( Q(\sqrt{1297}) \) of order 11), \( a_1 = 2/1297, \ a_2 = 6/1297, \ M = 13073905 \ 1893568, \ u_2 = u = 4/1297 \) and \( u_0 = v = 1/1297 \).

The fraction \( \frac{120979008}{13820689} \) written as a continued fraction is \( \langle 8, 1, 3, 17, 1, 3, 17, 1, 3, 17, 1, 3 \rangle \). To compute \( G(A) \) we compute the following table where \( A_i = p u_i, \ B_i = q_i A_i - A_{i-1}, \ C_i = B_i - A_{i+1}, \ D_i = p - A_i \) and \( E_i = (C_i D_i) / p \).

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A_i )</td>
<td>4</td>
<td>35</td>
<td>1188</td>
<td>1153</td>
<td>1290</td>
<td>25</td>
<td>4</td>
<td>35</td>
<td>1188</td>
<td>1153</td>
<td>1290</td>
<td>32</td>
<td>6</td>
<td>1996</td>
<td></td>
</tr>
<tr>
<td>( B_i )</td>
<td>120979008</td>
<td>13820689</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td>20790</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 \( G(A) = -1069/1297 \). 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 \( a_{n-k} + \frac{1}{a_n} \neq 0 \) define \( \langle a_1, a_2, \ldots, a_n \rangle \) to be the continued fraction \( \langle a_1, a_2, \ldots, a_{n-1}, a_n \rangle + \frac{1}{a_n} \). This definition agrees with the usual definition when \( a_n > 0 \).

Lemma 1 can be divided into two parts.

Part 1. Let \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \) and \( a, c > 0, \ a + 1, |b| \neq 0 \) 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 \( a_1/b \), and let \( a_n = (c Q - d P) / (a P - d Q) \) where \( P, Q \) are relatively prime positive integers such that \( PQ = \langle a_1, a_2, \ldots, a_{n-1} \rangle \).

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

(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
\[
\mathcal{a} = \langle a_2, a_3, \ldots, a_{n-1} - 1, 1 \rangle = \langle a_1, a_2, \ldots, a_{n-1} \rangle.
\]
These are the only two ways of writing a 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 \(\pi\) any non-zero complex number (and hence, in particular, for \(a\) a negative real),
\[
\langle a_1, a_2, \ldots, a_p, a \rangle = \frac{a P + P'}{a Q + Q'}
\]
where \(k \geq 2\), \(P, P', Q, Q'\) are positive integers and \((P', Q') = \{P, Q\}\), \(P'/Q' = \langle a_1, \ldots, a_{n-1} \rangle\) and \(P'/Q' = \langle a_1, \ldots, a_p \rangle\). 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 \(a_n \neq 0\)
\[
\langle a_1, \ldots, a_{n-1}, a_n \rangle = \frac{a_n \alpha + P}{a_n \beta + Q}
\]
by (6), and clearly
\[
\frac{a_n \alpha + P}{a_n \beta + Q} = \frac{c}{|d|}.
\]
To prove Part 2 we first remark that, since \(a, b, c, d\) are denominators of successive convergents, hence \(|b| > |d|\) (we cannot have \(|b| = |d|\) which implies that \(a > c\). If \(a = -1\) then \(c/d = \langle a_1, a_2, \ldots, a_{n-1}, 1 \rangle\) by Part 1. But \(a_{n-1} > 1\) so that \(a|d| = \langle a_1, \ldots, a_{n-1}, 1 \rangle\) so that again \(|b| > |d|\) since \(|b|/|d|\) form consecutive convergents. Hence \(a > c\).

Conversely assume that \(a_n \neq 0\) and \(a_n \neq -1\), 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
\[
c/|d| = \langle a_1, \ldots, a_{n-1}, 1 \rangle = \frac{1}{a_n} = \langle a_1, \ldots, a_{n-1} - 1, 1 \rangle.
\]
where \(\alpha = a_n/(1+a_n)\), a positive rational number, \(1 < a_n/(1+a_n) < 1\), so that the usual continued fraction for \(c/|d|\) will have more terms than that for \(a/|b| = \langle a_1, \ldots, a_{n-1}, 1 \rangle\). Hence \(|b| > |d|\) 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 results 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 \(a = a_1 |b| + r_1, \ldots, r_{n-1} = a_{n-1} |b| + r_{n-1}\).

If \(a > c\) then by Lemma 1 \(|c/d| = \langle a_1, a_2, \ldots, a_{n-1} \rangle\) hence by the Euclidean algorithm there exist nonnegative remainder terms \(r_1, r_2, \ldots, r_{n-1}\) such that \(c = a_1 |d| + r_1, \ldots, r_{n-1} = a_{n-1} |d| + r_{n-1}\) where \(r_{n-1} = 0\) and \(r_{n-2} = 1\). 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 \(r_1, r_2, \ldots, r_{n-1}\) such that \(c = a_1 |d| + r_1, \ldots, r_{n-1} = a_{n-1} |d| + r_{n-1}\) where \(r_{n-1} = 0\) and \(r_{n-2} = 1\). If \(a_n < 0\) (note \(a_n \neq -1\)), then the remainder terms \(r_1, \ldots, r_{n-1}\) 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 remainder can be chosen positive.

<table>
<thead>
<tr>
<th>(a_n)</th>
<th>(a &gt; c)</th>
<th>(a &lt; c)</th>
<th>(a_n &gt; 0)</th>
<th>(a_n &lt; 0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(a_1</td>
<td>d</td>
<td>+ r_1)</td>
<td>(a_1</td>
</tr>
<tr>
<td>0</td>
<td>(r_1 = 1, r_1 = 0)</td>
<td>(r_1 = 1, r_1 = 0)</td>
<td>(r_1 = 1, r_1 = 0)</td>
<td>(r_1 = 1, r_1 = 0)</td>
</tr>
<tr>
<td>-1</td>
<td>(r_1 = 1, r_1 = 0)</td>
<td>(r_1 = 1, r_1 = 0)</td>
<td>(r_1 = 1, r_1 = 0)</td>
<td>(r_1 = 1, r_1 = 0)</td>
</tr>
<tr>
<td>(r_{n-1} = a_{n-1}</td>
<td>d</td>
<td>+ r_{n-1})</td>
<td>(r_{n-1} = a_{n-1}</td>
<td>d</td>
</tr>
<tr>
<td>(r_{n-2} = a_{n-2}</td>
<td>d</td>
<td>+ r_{n-2})</td>
<td>(r_{n-2} = a_{n-2}</td>
<td>d</td>
</tr>
<tr>
<td>(r_n = 0)</td>
<td>(r_n = 0)</td>
<td>(r_n = 0)</td>
<td>(r_n = 0)</td>
<td></td>
</tr>
<tr>
<td>(r_{n-1} = -1)</td>
<td>(r_{n-1} = -1)</td>
<td>(r_{n-1} = -1)</td>
<td>(r_{n-1} = -1)</td>
<td></td>
</tr>
<tr>
<td>(r_n = 0)</td>
<td>(r_n = 0)</td>
<td>(r_n = 0)</td>
<td>(r_n = 0)</td>
<td></td>
</tr>
</tbody>
</table>

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

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} r_1 & b \\ r_1 & d \end{pmatrix}; \quad \begin{pmatrix} r_j \ b \\ r_j \ d \end{pmatrix} \left( \begin{pmatrix} a_n & -a_n \end{pmatrix} \right) = \begin{pmatrix} r_{j+1} & -r_j \\ r_{j+1} & -r_j \end{pmatrix}; \quad \ldots
\]

At the \(n\)th step the last matrix will be one of the following matrices:

\[
\begin{pmatrix} r_n & r_{n-1} \\ r_n & r_{n-1} \end{pmatrix}; \quad \begin{pmatrix} r_n - r_{n-1} \\ r_n - r_{n-1} \end{pmatrix}; \quad \begin{pmatrix} -r_n & -r_{n-1} \\ -r_n & -r_{n-1} \end{pmatrix}; \quad \begin{pmatrix} -r_{n-1} \\ -r_{n-1} \end{pmatrix}
\]

if \(a = 1, 2, 3, 0 \mod 4\) 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 \(S^2\).
A simplification of the formula for \( L(1, \chi) \)

where \( S \left( \frac{u_{n+1}}{u_n} \right) = \left( \frac{u_n}{u_{n+1}} \right) \). Using formulas (3) it is easy to check that

\[ \mathcal{G} \left( S \left( \frac{u_{n+1}}{u_n} \right) \right) = 0 \] if and only if \( u_{n+1} = 0 \) 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 \( v \) implies that \( M \left( \frac{u}{v} \right) = \left( \frac{u}{v} \right) \).

From this fact it follows that \( u_{n+1} = 1 - u_n \) and \( u_n = u_i \) if \( M \) is factored as in formula (4), and \( u_{n+1} = u_n \) if \( M \) is factored as in formula (5). We used the fact here that \( u_i = u \neq 0 \) and \( v \neq 0 \), 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. Brunner for suggesting the problem and for his assistance.

**References**


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

Received on 22.4.1973 (271)