ZAREMBA'S CONJECTURE AND SUMS OF THE DIVISOR FUNCTION

T. W. CUSICK

Dedicated to the memory of D. H. Lehmer

Abstract. Zaremba conjectured that given any integer $m > 1$, there exists an integer $a < m$ with $a$ relatively prime to $m$ such that the simple continued fraction $[0, c_1, \ldots, c_r]$ for $a/m$ has $c_i \leq B$ for $i = 1, 2, \ldots, r$, where $B$ is a small absolute constant (say $B = 5$). Zaremba was only able to prove an estimate of the form $c_i \leq C \log m$ for an absolute constant $C$. His first proof only applied to the case where $m$ is a prime; later he gave a very much more complicated proof for the case of composite $m$. Building upon some earlier work which implies Zaremba's estimate in the case of prime $m$, the present paper gives a much simpler proof of the corresponding estimate for composite $m$.

1. Introduction

Apparently, Zaremba [5, pp. 69 and 76] was the first to state the following:

Conjecture. Given any integer $m > 1$, there is a constant $B$ such that for some integer $a < m$ with $a$ relatively prime to $m$ the simple continued fraction $[0, c_1, \ldots, c_r]$ for $a/m$ has $c_i \leq B$ for $i = 1, 2, \ldots, r$.

This conjecture is still unproved, though numerical evidence suggests that $B = 5$ would suffice. The best result known replaces the inequality in the conjecture by $c_i \leq C \log m$ for some constant $C$; this was first proved by Zaremba [5, Theorem 4.6 with $s = 2$, p. 74] for prime values of $m$. Later, Zaremba [6] gave a very much more complicated proof for composite values of $m$.

As a byproduct of a more general investigation, I proved in an earlier paper [1, p. 154] that the inequality in the conjecture can be replaced by $c_i \leq 4(m/\varphi(m))^2 \log m$, where $\varphi(m)$ is Euler's function. Of course, this implies $c_i \leq C \log m$ if $m$ is prime, but only gives $c_i \leq C \log m(\log \log m)^2$ in general. In the present paper, I show how the argument of [1] can be refined to eliminate the $\log \log$ factors. The result is

Theorem 1. Given any integer $m > 1$, there is an integer $a < m$ with a relatively prime to $m$ such that the simple continued fraction $[0, c_1, \ldots, c_r]$ for $a/m$ has $c_i \leq 3 \log m$ for $i = 1, 2, \ldots, r$.
The proof is much simpler than the proof of the corresponding result in Zaremba [6]. I am grateful to Harald Niederreiter for suggesting that it would be worthwhile to publish this simpler proof.

2. Proof of Theorem 1

Let $\|x\|$ denote the distance from $x$ to the nearest integer. We shall actually prove the following sharpening of the case $n = 2$ of the theorem in [1].

**Theorem 2.** Given any integer $m \geq 8$, there exist integers $a_1, a_2$ relatively prime to $m$ such that

$$\prod_{i=1}^{2} \|ka_{i}/m\| > (3m \log m)^{-1} \text{ for each } k, \ 1 \leq k < m.$$  

As in [1], it is easy to deduce Theorem 1 from Theorem 2: We may assume $a_1 = 1$ and $a_2 = a$ in Theorem 2, since we may replace $a_i$ by $ba_i$ ($i = 1, 2$), where $ba_1 \equiv 1 \mod m$. Thus, Theorem 2 implies that for any $m \geq 8$ there exists an integer $a < m$ with $a$ relatively prime to $m$ such that

$$\prod_{i=1}^{2} \|ka_{i}/m\| > (3m \log m)^{-1} \text{ for each } k, \ 1 \leq k < m.$$  

If $[0, c_1, \ldots, c_r]$ is the simple continued fraction for $a/m$ with convergents $q_i/q_i$ ($0 \leq i \leq r$), then we have $q_i \|q_i a/m\| < 1/c_{i+1}$ for $i = 0, 1, \ldots, r - 1$. Therefore, (1) implies Theorem 1. (For $m < 8$ it is easy to verify Theorem 1 by calculation.)

We begin the proof of Theorem 2 with some definitions taken from [1, p. 155]. Given any integer $m > 1$ and positive integers $a_1, a_2$, we let $L$ denote a positive real number which we shall specify later. We say that the pair $a_1, a_2$ is exceptional (with respect to $m$ and $L$) if

$$\prod_{i=1}^{2} \|ka_{i}/m\| > L^{-1} \text{ for each } k, \ 1 \leq k < m.$$  

Obviously, the pair $a_1, a_2$ can be exceptional only if each $a_i$ is relatively prime to $m$. If for some $k$, $1 \leq k < m$, the inequality in (2) is false, then we say that $k$ excludes the pair $a_1, a_2$. We shall estimate the integer $J = J(k) = J(k, m, L) = \text{number of pairs } a_1, a_2 \text{ with each } a_i \text{ relatively prime to } m \text{ which are excluded by } k \text{ and which satisfy } 1 \leq a_1, a_2 \leq m/2.$

The requirement that $a_1$ and $a_2$ be different is convenient later on.

We first estimate $J(k, m, L)$ in the case where the greatest common divisor $(k, m)$ is 1. Such a $k$ excludes the pair $a_1, a_2$ if and only if 1 excludes the pair $ka_1, ka_2$; therefore.

$$J(k) = J(1) \text{ whenever } (k, m) = 1.$$  

We shall prove

$$J(1) < \frac{\varphi(m)^2}{2L} (\log(m^2/L) + \log \log m).$$  

In order to do this, we need to define the following sums $D(x, r, m)$ of the divisor function $d(n)$ (= the number of positive integer divisors of the positive
integer \( n \) over arithmetic progressions with difference \( m \):

\[
D(x, r, m) = \sum_{n \leq x, n = r \mod m} d(n).
\]

A pair \( a_1, a_2 \) with \( a_i \leq m/2 \) \((i = 1, 2)\) is excluded by \( k = 1 \) if

\[
(5) \quad a_1 a_2 \leq m^2/L.
\]

The number of ways of writing any positive integer \( n \leq m^2/L \) as \( a_1 a_2 \) is just \( d(n) \), and the factors are both relatively prime to \( m \) if and only if \( n \) is relatively prime to \( m \). Hence, the number of pairs \( a_1, a_2 \) satisfying (5) and the additional conditions \((a_i, m) = 1 \quad (i = 1, 2)\) and \( 1 \leq a_1 < a_2 \leq m/2 \) does not exceed

\[
\frac{1}{2} \sum_{n \leq m^2/L, (n, m) = 1} d(n) = \frac{1}{2} \sum_{r = 1}^{m} D(m^2/L, r, m)
\]

(the factor of \( \frac{1}{2} \) comes from the fact that \( d(n) \) counts each factorization \( n = a_1 a_2 \) with distinct \( a_1 \) and \( a_2 \) twice; this is where our assumption that \( a_1 \) and \( a_2 \) are distinct is convenient). Thus, we have proved

\[
(6) \quad J(1, m, L) \leq \frac{1}{2} \sum_{(r, m) = 1}^{m} D(m^2/L, r, m).
\]

In order to estimate the sum in (6), we need some results of D. H. Lehmer [4] concerning the sums \( H(x, r, m) \) defined by

\[
H(x, r, m) = \sum_{n \leq x, n = r \mod m} 1/n.
\]

Lehmer [4, p. 126] proved the existence of the generalized Euler constants \( \gamma(r, m) \) defined for any integers \( r \) and \( m > 0 \) by

\[
(7) \quad \gamma(r, m) = \lim_{x \to \infty} (H(x, r, m) - m^{-1} \log x).
\]

Clearly, Euler's constant \( \gamma \) is \( \gamma(0, 1) \), and \( \gamma(r, m) \) is a periodic function of \( r \) with period \( m \).

**Lemma 1.** For any integers \( r, m \) with \( m > 0 \) and \( 0 \leq r < m \), we have

\[
0 < H(x, r, m) - m^{-1} \log x - \gamma(r, m) < 1/x
\]

for all \( x \geq m \).

**Proof.** This follows easily from the proof of the existence of the limit in (7), as given by Lehmer [4, p. 126]. \( \square \)

In order to state our next two lemmas, it is convenient to define the arithmetical functions \( v(n) \) and \( w(n) \) by

\[
v(n) = -\sum_{d | n} \mu(d) d^{-1} \log d
\]

\[
w(n) = \sum_{d | n} \mu(d) d^{-1} \log d
\]

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(here, \( \mu(d) \) is the Möbius function and the sum is taken over all positive integer divisors \( d \) of \( n \)) and
\[
w(n) = n\nu(n)/\varphi(n) = \sum_{p|n} (\log p)/(p - 1)
\]
(here, the sum is taken over all prime divisors \( p \) of \( n \)).

**Lemma 2.** For every positive integer \( m \),
\[
\sum_{\substack{r=1 \\
(r,m)=1}}^{m} \gamma(r, m) = \varphi(m)m^{-1}(\gamma + w(m)).
\]

**Proof.** This is equation (16) of Lehmer [4, p. 132]. \( \square \)

**Lemma 3.** For every integer \( m \geq 8 \),
\[
\gamma + w(m) < (m/\varphi(m))\log \log m.
\]

**Proof.** Theorem 5 of Davenport [2, p. 294] states
\[
\lim_{m \to \infty} \frac{\nu(m)}{\log \log m} = \frac{1}{4},
\]
which implies the lemma for all large \( m \). Some simple calculations (using \( \gamma = .577\ldots \)) gives the inequality as stated. \( \square \)

Our final lemma gives an upper bound on the sum \( D(x, r, m) \) when \( r \) is relatively prime to \( m \).

**Lemma 4.** For any integers \( r, m \) with \( r \) relatively prime to \( m \) and \( m \geq 8 \), we have
\[
D(x, r, m) < \varphi(m)m^{-2}x \log x + 2xm^{-1} \log \log m.
\]

**Proof.** We adapt the standard proof of Dirichlet's theorem on summing \( d(n) \) for \( n \leq x \). The sum \( D(x, r, m) \) is the number of lattice points \((u, v)\) with \( uv \equiv r \mod m \) lying below the curve \( uv = x \) in the first quadrant of the \( u, v \) plane. By using the symmetry in the line \( u = v \), if we define \( T = [x^{1/2}] \), then we have
\[
D(x, r, m) < 2 \sum_{i=1}^{T} F_i(x),
\]
where \( F_i(x) \) denotes the number of integers \( v \) such that \( iv \equiv r \mod m \) and \( iv \leq x \); we have strict inequality here since we are double counting the lattice points in the square of side \( T \) formed by portions of the \( u \)- and \( v \)-axes. (For a more elaborate version of this argument, which leads to a \( O \)-estimate analogous to the one for the usual Dirichlet divisor problem, see Satz 2 of Kopetzky [3]. The simple inequality of Lemma 4 suffices for our purposes, since the more detailed argument does not affect the main term.) If \( r \) is relatively prime to \( m \), then \( iv \equiv r \mod m \) is solvable if and only if \( i \) is also relatively prime to \( m \), and in that case there is exactly one solution \( v \mod m \). It follows that \( F_i(x) = 0 \) unless \( i \) is relatively prime to \( m \) and that
\[
F_i(x) \leq x(i m)^{-1} \quad \text{for } (i, m) = 1.
\]
Now (9) implies
\[ \sum_{i=1}^{T} F_i(x) \leq \left( \frac{x}{m} \right) \sum_{r=1}^{m} H(T, r, m). \]

Finally, Lemmas 1, 2, and 3 give the inequality in Lemma 4. □

It follows from (3), (6) and Lemma 4 that
\[ J(k, m, L) < \frac{1}{2} \phi(m)^2 L^{-1} \log(m^2 L^{-1}) + m \phi(m) L^{-1} \log \log m \]
holds for all \( k \) with \( k \) relatively prime to \( m \). By the argument in [1, pp. 156–157], the inequality in (10) is still true if \( k \) is not relatively prime to \( m \) (indeed, in that case we can even insert a factor of \( 8/9 \) on the right-hand side of (10)).

We can now complete the proof of Theorem 2 (and so of Theorem 1) as in [1, p. 157]: Clearly, (2) holds if and only if the inequality in (2) is true for each \( k \leq m/2 \). The total number of pairs \( a_1, a_2 \) with each \( a_i \) relatively prime to \( m \) and \( 1 \leq a_1 < a_2 \leq m/2 \) is
\[ \left( \frac{\phi(m)}{2} \right) > \phi(m)^2/8. \]

By (10) and the definition of \( J(k, m, L) \), an exceptional pair \( a_1, a_2 \) certainly exists if
\[ \phi(m)^2/8 > \frac{1}{2} m \left( \frac{1}{2} \phi(m)^2 L^{-1} \log(m^2 L^{-1}) + m \phi(m) L^{-1} \log \log m \right). \]

Computation (using the well-known fact that \( \limsup m(\phi(m) \log \log m)^{-1} = e^\gamma = 1.781 \ldots \)) shows that (11) is true for \( m \geq 8 \) if \( L \geq 3m \log m \). This completes the proof of Theorem 2.

3. Generalizations

It was pointed out in [1, pp. 154–155] that something like Theorem 2 can be proved in the case of \( n \) integers. The main result of [1] was

**Theorem 3.** Given any integers \( d > 4n \) and \( n > 1 \), there exist integers \( a_1, \ldots, a_n \) relatively prime to \( m \) such that
\[ \prod_{i=1}^{n} \|k a_i/m\| > 4^{-n} (\phi(m)/m)^n (m \log^{n-1} m)^{-1} \quad \text{for each } k, \ 1 \leq k < m. \]

In view of the connection of Theorems 1 and 2 above, this can be regarded as an \( n \)-dimensional generalization of a weakened form of Zaremba’s conjecture. In [1, p. 155], I proposed the following general conjecture; Zaremba’s conjecture is the case \( n = 2 \).

**Conjecture.** For each \( n \geq 2 \), the lower bound in (12) can be replaced by \( c(n)(m \log^{n-2} m)^{-1} \).

The proof of Theorem 2 above removed the factors \( \phi(m)/m \) in the case \( n = 2 \) of (12). One might hope to achieve the same result for arbitrary \( n \) by generalizing the proof of Theorem 2; this would require working with the
generalized divisor functions $d_n(t) = \text{the number of ways of writing the positive integer } t \text{ as a product of } n \text{ positive integer factors.}$

To conclude, I repeat another speculation from [1, p. 155]: It is possible that the lower bound in (12) could be replaced by $c(n)m^{-1}$ for $n = 3$, or even for all $n \geq 2$. A small amount of computer testing of this for $n = 3$ was reported in [1, p. 155]. Further computer experiments might be worthwhile.

**Bibliography**


**Department of Mathematics, State University of New York at Buffalo, South Campus, Buffalo, New York 14214**

E-mail address: v360eakb@ubvms.cc.buffalo.edu