JOURNAL OF NUMBER THEORY 2, 414–422 (1970)

The Number of Steps in the Euclidean Algorithm

JOHN D. DIXON*

Department of Mathematics, Carleton University, Ottawa, Ontario, Canada

Communicated by P. T. Bateman

Received August 29, 1969; revised March 2, 1970

For all pairs of positive integers u, v with $u \leqslant v$ we define $L(u, v)$ to be the number of steps required in applying the Euclidean algorithm to the pair u, v. Then given any $\epsilon > 0$ there exists $c_0 > 0$ such that

$$| L(u, v) - (12\pi^{-2} \log 2) \log v | < (\log v)^{\frac{1}{2}+\epsilon}$$

for all except at most $x^2 \exp\{-c_0(\log x)^{\epsilon/2}\}$ of the pairs u, v with $1 \leqslant u \leqslant v \leqslant x$.

1. INTRODUCTION

Given any two integers u and v with $1 \leqslant u \leqslant v$, the usual Euclidean algorithm for computing the greatest common divisor will give a series of equations

$$r_0 = v, r_1 = u \text{ and } r_{m-1} = q_m r_m + r_{m+1} \qquad (m = 1, 2,...), \quad (1.1)$$

where the q_i are positive integers and the r_i are integers such that $r_0 \geqslant r_1 > \cdots > r_{n+1} = 0$. The greatest common divisor is r_n and we shall denote the number n of steps in applying the algorithm by $L(u, v)$.

Trivially $L(u, v) \geqslant 1$ and $L(u, v) = 1$ exactly when $u \mid v$. It is also easy to see that we get the largest possible value for $L(u, v)$ with respect to the sizes of u and v when $r_n = 1$ and each q_i in (1.1) is 1. Then the equations (1.1) define u and v, respectively, as the n-th and $(n + 1)$st Fibonacci numbers. As is well known, in this case,

$$v = \frac{\alpha^{n+1} + (-1)^n \alpha^{-n-1}}{\alpha + \alpha^{-1}}$$

where $\alpha > 1$ satisfies $\alpha^2 = \alpha + 1$. Since $\alpha + \alpha^{-1} = 5^{1/2}$, v is the closest

* Research supported in part by the National Research Council of Canada under Grant No. A-7171.

integer to $5^{-1/2}\alpha^{n+1}$. Thus we conclude that if we are given x, then for all pairs u, v with $1 \leqslant u \leqslant v \leqslant x$ we have

$$L(u, v) \leqslant (\log x + 1)/\log \alpha = (2.07...)(\log x + 1). \tag{1.2}$$

Moreover, this bound is asymptotic to the least upper bound for all $L(u, v)$ with $1 \leqslant u \leqslant v \leqslant x$.

The object of this paper is to prove the following theorem.

THEOREM. *For all positive ϵ there exists $c_0 > 0$ such that*

$$| L(u, v) - (12\pi^{-2} \log 2) \log v | < (\log v)^{1/2+\epsilon}$$

for all except at most $x^2 \exp\{-c_0(\log x)^{\epsilon/2}\}$ of the pairs of integers u, v with $1 \leqslant u \leqslant v \leqslant x$.

Note. $12\pi^{-2} \log 2 = 0.84276....$ We shall denote the reciprocal of this constant by λ.

Remarks. Heilbronn recently showed in [1] that for each integer v

$$\varphi(v)^{-1} \sum L(u, v) = (12\pi^{-2} \log 2) \log v + O(\log \log v)^4$$

where the sum is over all positive integers $u \leqslant v$ which are relatively prime to v and $\varphi(v)$ is the Euler function. Heilbronn's methods are quite different from ours and he states his result in terms of continued fractions. There are very close links between our problem and certain problems in the theory of continued fractions (see Section 2); in this connection the constant λ is already familiar from work of Lévy [2, Section 79]. Indeed the proof of our theorem involves an application of results due to Philipp in the metric theory of continued fractions (although Philipp presents his results in a more general context). The work of this paper arose from a question put to me by D. Knuth in 1963. At that time Knuth obtained a great deal of computational evidence for a theorem like the one proved in this paper, and has since published an analysis of his results in [5, pp. 316–338].

I should like to acknowledge the helpful criticisms made by W. Philipp of an earlier version of this paper. At his suggestion I have used a number of his results to simplify this paper and to strengthen the main theorem.

Notation. In dealing with continued fractions our notation will follow closely that of Khinchin's book [6]. In particular, $[a_1, a_2, ...]$ denotes the continued fraction

$$\cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

where $a_1, a_2, \ldots$ are positive integers (this is different from [1]). The letter c (with appropriate indices) will always denote a positive constant. The letter θ always denotes a real quantity of absolute value $\leqslant 1$; it may take different values at different places. Finally $\langle 0, 1 \rangle$ denotes the open interval from 0 to 1, and μS denotes the (Lebesgue) measure of a subset S of $\langle 0, 1 \rangle$.

2. The Relation with Continued Fractions

We first review some elementary results on continued fractions (see [6; Chap. 1]). Let $0 < \alpha \leqslant 1$. Then α may be expanded as a continued fraction $[a_1, a_2, \ldots]$ with positive integers $a_1, a_2, \ldots$; this expansion is unique if we make a suitable convention in the rational case. The m-th *convergent* of this continued fraction is P_m/Q_m where

$$\begin{aligned} &P_0 = 0, \quad P_1 = 1 \quad \text{and} \quad P_m = a_m P_{m-1} + P_{m-2} \quad (m = 2, 3, \ldots) \\ &Q_0 = 1, \quad Q_1 = a_1 \quad \text{and} \quad Q_m = a_m Q_{m-1} + Q_{m-2} \quad (m = 2, 3, \ldots) \end{aligned} \tag{2.1}$$

and $P_m/Q_m \to \alpha$ as $m \to \infty$. The continued fraction is finite (that is, $a_n \neq 0$ but $a_m = 0$ for all $m > n$) if and only if α is rational, and in this case $P_n/Q_n = \alpha$. There is an obvious relation between the equations (2.1) and (1.1); indeed with the notation of (1.1) we have $u/v = [q_1, \ldots, q_n]$. In particular, when the greatest common divisor of u and v is 1, then $r_n = 1$ and u and v are precisely the numbers P_n and Q_n computed from (2.1) with $a_m = q_m (m = 1, \ldots, n)$.

If $\alpha = [a_1, a_2, \ldots]$, then we define the m-th *complete quotient* $z_m(\alpha)$ to be equal to $[a_{m+1}, a_{m+2}, \ldots]$ if $a_{m+1} \neq 0$ and otherwise $z_m(\alpha) = 0$. Note that $0 \leqslant z_m(\alpha) \leqslant 1$ and that

$$z_0(\alpha) = \alpha \text{ and } z_{m-1}(\alpha) = 1/(a_m + z_m(\alpha)) \text{ if } m \geqslant 1 \text{ and } a_m \neq 0. \tag{2.2}$$

We now have three elementary theorems on continued fractions. The first follows readily from (2.2).

LEMMA 1. *Let u and v be relatively prime integers with $1 \leqslant u \leqslant v$. Then*

$$v = \prod_{m=0}^{n-1} z_m(u/v)^{-1}.$$

The proof of the next result may be found in [6, Section 12].

LEMMA 2. *Let $a_1, \ldots, a_n$ be n positive integers. Let J be the set of all $\xi \in \langle 0, 1\rangle$ such that the first n terms in the continued fraction expansion of ξ are $a_1, \ldots, a_n$. If P_m and Q_m are defined by* (2.1), *then J is an interval with end points P_n/Q_n and $(P_n + P_{n-1})/(Q_n + Q_{n-1})$ and of length*

$$\mu J = \{Q_n(Q_n + Q_{n-1})\}^{-1}.$$

Note that because $Q_n \geqslant Q_{n-1}$, $\frac{1}{2}Q_n^{-2} \leqslant \mu J \leqslant Q_n^{-2}$.

LEMMA 3. *Let J be defined as in Lemma 2, and let $\xi, \xi' \in J$. Then for each $m < n$ we have*

$$| z_m(\xi) - z_m(\xi')| < 2^{-(n-m-1)} \tag{2.3}$$

and

$$| \log z_m(\xi) - \log z_m(\xi')| < 2^{-\frac{1}{2}(n-m-1)}. \tag{2.4}$$

Proof. From the definition of z_m it is enough to consider the case $m = 0$; then $z_0(\xi) = \xi$ and $z_0(\xi') = \xi'$.

To prove (2.3) we note that, in the notation of Lemma 2, $| \xi - \xi' | < \{Q_n(Q_n + Q_{n-1})\}^{-1}$. Since an easy induction (see [6, Section 4]) shows that $Q_n \geqslant 2^{\frac{1}{2}(n-1)}$, $| \xi - \xi' | < 2^{-(n-1)}$ as required.

To prove (2.4) we note that Lemma 2 shows that ξ/ξ' lies between

$$\frac{P_n(Q_n + Q_{n-1})}{Q_n(P_n + P_{n-1})} \quad \text{and} \quad \frac{Q_n(P_n + P_{n-1})}{P_n(Q_n + Q_{n-1})}. \tag{2.5}$$

Since we always have $| P_nQ_{n-1} - Q_nP_{n-1} | = 1$ (see [6; Section 2]), the ratios in (2.5) differ from 1 by $\{Q_n(P_n + P_{n-1})\}^{-1}$ and $\{P_n(Q_n + Q_{n-1})\}^{-1}$, respectively. Hence as in the first part of the proof

$$| 1 - \xi/\xi' | < Q_n^{-1} \leqslant 2^{-\frac{1}{2}(n-1)}.$$

Since we may suppose $\xi \geqslant \xi'$, we have

$$0 \leqslant \log \xi - \log \xi' \leqslant \log\{1 + 2^{-\frac{1}{2}(n-1)}\} < 2^{-\frac{1}{2}(n-1)}.$$

This completes the proof.

3. The Principal Lemma

The following inequality lies at the heart of the proof of our Theorem.

Lemma 4. *For all positive integers n and k we have*

$$\frac{1}{2}\sum_{a_1,\dots,a_n}\frac{(\log Q_n - n\lambda + 4\theta)^{2k}}{{Q_n}^2} < \int_0^1 \left\{\sum_{m=0}^{n-1}\log z_m(\xi) + n\lambda\right\}^{2k} d\xi \quad (3.1)$$

where the sum on the left is over all n-tuples of positive integers $a_1,\dots, a_n$, *and* Q_n *is defined in terms of the* a_i *by* (2.1).

Remark. We are using θ as a generic symbol to represent quantities of absolute value $\leqslant 1$ and the value of θ will differ from term to term in the sum. We shall apply (3.1) in the case where λ has the value defined in the Theorem; however the inequality (3.1) is valid for arbitrary values of λ.

Proof. Let J be defined as in Lemma 2. Then when P_n and Q_n are defined by (2.1) we have $\xi' = P_n/Q_n \in J$. Thus for any $\xi \in J$, Lemmas 1 and 3 show that

$$\left|\sum_{m=0}^{n-1}\log z_m(\xi) + \log Q_n\right| \leqslant \sum_{m=0}^{n-1} 2^{-\frac{1}{2}(n-m-1)} < 4.$$

Hence

$$\begin{aligned}\int_J \left\{\sum_{m=0}^{n-1}\log z_m(\xi) + n\lambda\right\}^{2k} d\xi &= \int_J \{\log Q_n - n\lambda + 4\theta\}^{2k}\, d\xi \\ &= \{\log Q_n - n\lambda + 4\theta\}^{2k}\,\mu J > \tfrac{1}{2}Q_n^{-2}\{\log Q_n - n\lambda + 4\theta\}^{2k}\end{aligned}$$

by Lemma 2.

Since the interval $\langle 0, 1\rangle$ is a disjoint union of all intervals J as $a_1,\dots, a_n$ run through the set of all n-tuples of positive integers, we obtain (3.1) by summing the last inequality over all such n-tuples. This proves Lemma 4.

Our next step is to estimate the right side of (3.1), and we proceed as follows. For each integrable g we define

$$E(g) = \int_0^1 g(\xi)\frac{d\xi}{(1+\xi)\log 2}.$$

Let J_m denote the set of all $\xi \in \langle 0, 1\rangle$ such that $[1/\xi] = m$ $(m = 1, 2,...)$. Then for each integrable g

$$E(g \circ z_1) = \sum_{m=1}^{\infty} \int_{J_m} g(z_1(\xi)) \frac{d\xi}{(1+\xi)\log 2}$$

$$= \sum_{m=1}^{\infty} \int_0^1 g(\eta) \frac{d\eta}{(m+\eta)(m+\eta+1)\log 2}$$

$$= \int_0^1 g(\eta) \sum_{m=1}^{\infty} \left\{\frac{1}{m+\eta} - \frac{1}{m+\eta+1}\right\} \frac{d\eta}{\log 2}$$

$$= \int_0^1 g(\eta) \frac{d\eta}{(1+\eta)\log 2} = E(g).$$

Then by induction we get the (known) result

$$E(g \circ z_h) = E(g) \qquad \text{for } h = 0, 1,.... \tag{3.2}$$

The constant λ now enters the picture. Direct calculation shows

$$E(\log \xi) = -\lambda, \tag{3.3}$$

and so, if we put $f(\xi) = \log \xi + \lambda$ and $y_h = f \circ z_h (h = 0, 1,...)$, then

$$E(y_h) = 0 \qquad \text{for } h = 0, 1,.... \tag{3.4}$$

The calculations of [4, p. 84] now show that the following result holds:

There is an absolute constant $c_1 > 0$ such that for all integers $1 \leqslant j < r$; $0 \leqslant i_1 < \cdots < i_r$; and $k_1,..., k_r \geqslant 0$ we have

$$|E(y_{i_1}^{k_1} \cdots y_{i_r}^{k_r}) - E(y_{i_1}^{k_1} \cdots y_{i_j}^{k_j})\, E(y_{i_{j+1}}^{k_{j+1}} \cdots y_{i_r}^{k_r})|$$

$$\leqslant \exp\{-c_1(i_{j+1} - i_j)^{1/2}\} \sup_i E\,|\,y_i\,|^{\Sigma k_h}. \tag{3.5}$$

(In Philipp's notation we are considering the transformation T of type C defined by $T\xi = z_1(\xi)$. It follows from our (2.4) that his condition (15) is satisfied with $C_0 = 1$ and $\delta = \frac{1}{2}$; his inequality (20) then gives our (3.5) where $S = 1$ because T is of type C.)

Finally [3, Hilfssatz 1.3] gives the estimate we require.

LEMMA 5. (Philipp). *There exists $c_2 > 0$ such that, if k and n are positive integers with $4(k+1) \leqslant c_1\sqrt{n}/\log n$, then*

$$\int_0^1 \left\{ \sum_{h=0}^{n-1} \log z_h(\xi) + n\lambda \right\}^{2k} \frac{d\xi}{(1+\xi)\log 2} \leqslant (c_2 n k^4)^k. \tag{3.6}$$

(In Philipp's notation we have $L(2k) = 1$ and $c(s) = \exp\{-c_1\sqrt{s}\}$ from our (3.5), and we are taking $x_h = y_h$. His conditions (1.1) and (1.2) are guaranteed by our (3.4) and (3.5), respectively.)

4. THE PROOF OF THE THEOREM

Let n be a positive integer and x be real and > 0. We define $L_n(x)$ as the number of pairs u, v of integers with $1 \leqslant u \leqslant v \leqslant x$ such that $L(u, v) = n$. We also define $L_n^*(x)$ as the corresponding number of pairs with the additional condition that u and v are relatively prime. Note that

$$L_n(x) = \sum_{d \leqslant x} L_n^*(x/d) \tag{4.1}$$

because, if u and v have greatest common divisor d, then

$$L(u, v) = L(u/d, v/d).$$

Our final lemma estimates $L_n(x)$.

LEMMA 6. *For each positive $\epsilon < 1$ there exists $c_3 > 0$ such that for all sufficiently large x*

$$L_n(x) < x^2 \exp\{-c_3(\log x)^{\epsilon/2}\} \tag{4.2}$$

whenever n satisfies

$$|\lambda n - \log x| \geqslant (\log x)^{1/2+\epsilon}. \tag{4.3}$$

Remark. If we classify the pairs u, v counted in $L_n(x)$ according to the value of $k = [v/u]$, it is clear that $L_n(x) \leqslant \sum L_{n-1}(x/k)$ summed over $k \leqslant x$. Thus induction on n shows that $L_n(x) \leqslant x(\log x + 1)^n$. In particular, if $n < \log x/2 \log\log x$, then (4.2) always holds for sufficiently large x. Thus in the proof that follows we shall assume that $n \geqslant \log x/2 \log\log x$.

Proof. First consider $L_n^*(x)$. As we saw in §2, $L_n^*(x)$ is precisely the number of n-tuples $a_1, \ldots, a_n$ of positive integers such that Q_n defined in (2.1) is $\leqslant x$. Now $(\log \xi - n\lambda + 4\theta)^{2k}\, \xi^{-2}$ decreases as ξ increases except when $0 \leqslant \log \xi - n\lambda + 4\theta \leqslant k$. Hence, if $|\log x - n\lambda| > k + 4$, then

$$L_n^*(x) < \frac{x^2}{(|\log x - n\lambda| - 4)^{2k}} \sum_{a_1, \ldots, a_n} \frac{(\log Q_n - n\lambda + 4\theta)^{2k}}{{Q_n}^2}.$$

So, by Lemmas 4 and 5,

$$L_n^*(x) < \frac{x^2}{(|\log x - n\lambda| - 4)^{2k}} (c_2 n k^4)^k$$

whenever $k \leqslant c_1\sqrt{n}/8 \log n$.

Now suppose that $|\lambda n - \log x| \geqslant \frac{1}{2}(\log x)^{1/2+\epsilon}$ and put

$$k = [\tfrac{1}{2} c_2^{-1/4} (\log x)^{\epsilon/2}].$$

Since $\epsilon < 1$, $k < c_1\sqrt{n}/8 \log n$ for all large x and so the last inequality for $L_n^*(x)$ shows that for some $c_3 > 0$

$$L_n^*(x) < x^2 \left\{ \frac{5n(\log x)^{2\epsilon}}{16(\log x)^{1+2\epsilon}} \right\}^k < \frac{1}{4} x^2 \exp\{-2c_3(\log x)^{\epsilon/2}\} \qquad (4.4)$$

for all sufficiently large x, whenever $|\lambda n - \log x| \geqslant \frac{1}{2}(\log x)^{1/2+\epsilon}$.

We now consider $L_n(x)$. Put $d_0 = [\exp\{c_3(\log x)^{\epsilon/2}\}]$. For all large x, $d_0 < \sqrt{x}$ and (4.3) implies $|\lambda n - \log(x/d)| \geqslant \frac{1}{2}\{\log(x/d)\}^{1/2+\epsilon}$ for $d < d_0$ Therefore if we divide the sum (4.1) into two parts — $d < d_0$ and $d \geqslant d_0$— and apply (4.4) we obtain

$$\begin{aligned} L_n(x) &= \left(\sum{}' + \sum{}''\right) L_n^*(x/d) \\ &< \tfrac{1}{4} x^2 \exp\{-c_3(\log x)^{\epsilon/2}\} \sum{}' d^{-2} + \tfrac{1}{2} x^2 \sum{}'' d^{-2} \\ &< x^2 \exp\{-c_3(\log x)^{\epsilon/2}\} \end{aligned}$$

for all sufficiently large x whenever (4.3) holds. This proves the Lemma.

Finally, we complete the proof of the Theorem. By (1.2) it is enough to consider the case $\epsilon < 1$. We must estimate the number of pairs u, v with $1 \leqslant u \leqslant v \leqslant x$ which fail to satisfy

$$|\lambda L(u, v) - \log x| < \lambda (\log v)^{1/2+\epsilon}. \qquad (4.5)$$

If x is large then such a pair satisfies at least one of the conditions:

(i) $v \leqslant x \exp\{-\frac{1}{2}(\log x)^{1/2}\}$;

(ii) $x \exp\{-\frac{1}{2}(\log x)^{1/2}\} < v \leqslant x$ and

$$| \lambda L(u, v) - \log x | \geqslant (\log x)^{1/2+\epsilon},$$

since $\lambda > 1$. But the number of pairs satisfying (i) is $< x^2 \exp\{-(\log x)^{1/2}\}$. On the other hand, the number of pairs satisfying (ii) is $\leqslant \sum L_n(x)$ summed over all n satisfying (4.3); by Lemma 6 and (1.2) this number is

$$< (3 \log x)\, x^2 \exp\{-c_3(\log x)^{\epsilon/2}\}$$

for all large x. Hence there exists $c_0 > 0$ such that for all x the total number of exceptions to (4.5) is at most $x^2 \exp\{-c_0(\log x)^{\epsilon/2}\}$. This proves the Theorem.

Note. Professor Philipp has indicated that a closer analysis shows that we may improve the exponent of log x in our final estimate from $\epsilon/2$ to ϵ.

References

1. H. Heilbronn, On the average length of a class of finite continued fractions, *in* "Abhandlungen aus Zahlentheorie und Analysis," VEB Deutscher Verlag, Berlin 1968.
2. P. Lévy, "Theorie de L'Addition des Variables Aléatoires," Gauthier-Villars, Paris 1937.
3. W. Philipp, Ein zentraler Grenzwertsatz mit Anwendungen auf die Zahlentheorie, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **8** (1967), 195–203.
4. W. Philipp, Das Gesetz vom iterierten Logarithmus mit Anwendungen auf die Zahlentheorie, *Math. Ann.* **180** (1969), 75–94.
5. D. Knuth, "The Art of Computer Programming," Vol. 2, Addison-Wesley, Reading, Mass. 1969.
6. A. I. Khinchin, "Continued Fractions," University of Chicago Press, Chicago, Ill., 1964; the Russian original was published in 1935.