Journal of Mathematics and System Science 8 (2018) 175-176
doi: 10.17265/2159-5291/2018.06.003

A Note on the Euclidean Algorithm

Shiva Soleimany Dizicheh[1] and Kiavash Bagheri[2]

1. Department of Software Engineering, University of Isfahan, Isfahan 841568311, Iran

2. Department of Industrial Engineering, Islamic Azad University West Tehran Branch, Tehran 44220857, Iran

Abstract: The problem of determining the number of steps needed to find the greatest common divisor of two positive integers by Euclidean algorithm has been investigated in elementary number theory for decades. Different upper bounds have been found for this problem. Here, we provide a sharp upper bound for a function which has a direct relation to the numbers whom the greatest common divisor we are trying to calculate. We mainly use some features of Fibonacci numbers as our tools.

Key words: Euclidean algorithm, Fibonacci numbers.

1. Introduction

Definition 1.1: The function $\lambda: \mathbb{N} \times \mathbb{N} \to \mathbb{N} \cup \{0\}$ is defined by:

$$\lambda(a, b) = \begin{cases} 0, \text{a} < b \\ \text{the number of steps needed} \\ \text{to find the greatest common a} \geq \text{b} \\ \text{divisor of a and b,} \end{cases}$$

For example $\lambda(42, 15) = 3$ since we have

$$42 = 2 \times 15 + 12$$
$$15 = 1 \times 12 + 3$$
$$12 = 4 \times 3 + 0$$

Now let a and b be positive integers such that $\lambda(a, b) = m \geq 1$ and $\frac{a}{b} \leq <a_1, a_2, \ldots, a_n>$ where $< >$ denotes continued fraction symbol. It can easily be verified that $m = n$. It has been proven that if a, b and N are positive integers with $1 \leq b < a < \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^N$ then $\lambda(a, b) \leq N$. Furthermore, $\lambda(a, b) \leq 1 + 2\log_2 a$ for any integers $a > b \geq 1$. For more details see Ref. [1].

Definition 1.2: Let $f: \mathbb{N} \to \mathbb{N}$ be defined via the rule $f(n) = \max\{\lambda(n, m) | \ m \in \mathbb{N}\}$, for any $n \in \mathbb{N}$. According the above statement, $f(n) \leq N$ if $n < \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^N$. This theorem determines an upper bound for f which depends on the value of n. This result inspires us to find a lower bound for f. In what follows, we assert a property of the λ function using Fibonacci numbers. For example see the following theorem.

Theorem 1.3: If $\lambda(a, b) = n \geq 1$ then $a \geq u_{n+2}$ and $b \geq u_{n+1}$, where u_{n+2} and u_{n+1} denote $(n+1)$th and $(n+2)$th Fibonacci numbers, respectively [2].

Theorem 1.4: For any positive integer n, $\lambda(u_{n+1}, u_n) = n - 1$. For more results concerning the above-mentioned theorem see Ref. [2].

It seems we can approach the problem of finding lower bound for function f by using the some properties of Fibonacci numbers. In the next section, we will study the relations between two consecutive Fibonacci numbers to find a lower bound for f.

Theorem 1.5: For any integer $n > 6$, $f(n) \geq 3$.

First it is necessary to mention that for any positive integer such as a and b, if $\frac{a}{2} > b$ then $\lambda(a, b) = \lambda(a - b, b)$. Moreover, this is easy to see that in Euclidean algorithm $\lambda(a, b) = \lambda(a, a - b)$, where a and b are positive integers and $\frac{a}{2} < b \leq a$.

Proof of Theorem 1.5: By using these two relations of the function λ, we can compute the value of $\lambda(2n,$

Corresponding author: Shiva Soleimany Dizicheh, bachelor of science, research fields: data mining, theoretical computer science, machine learning, computer vision.

n+1):

$$\begin{aligned}\lambda(2n, n+1) &= \lambda(2n, n-1) + 1 \\ &= \lambda(n+1, n-1) + 1 \\ &= \lambda(n+1, 2) + 2 \\ &\geq 3.\end{aligned}$$

So, $f(2n) \geq 3$ for $n \geq 2$. Repeating a similar computation for $\lambda(2n+1, n+1)$:

$$\begin{aligned}\lambda(2n+1, n+1) &= \lambda(2n+1, n) + 1 \\ &= \lambda(n+1, n) + 1 \\ &= \lambda(n+1, 1) + 2 \\ &\geq 3\end{aligned}$$

So, $f(2n+1) \geq 3$ for $n \geq 1$ as claimed.

Theorem 1.6: For any integer $n > 15$, $f(n) \geq 4$.

Proof: we can prove this theorem with the similar approach we used in the proof of Theorem 1.5 as following:

$\lambda(3n, 2n-1) \geq 4$,

$\lambda(3n+1, 2n-1) \geq 4$

$\lambda(3n+2, 2n) \geq 4$ for any $n > 5$.

Therefore $f(n) \geq 4$ for any $n > 15$.

Theorem 1.7: For any integer $n > 40$, $f(n) \geq 5$.

Proof: Consider $\lambda(5n, 3n+1)$, $\lambda(5n+1, 3n+1)$, $\lambda(5n+2, 3n+2)$, $\lambda(5n+3, 3n+3)$ and $\lambda(5n+4, 3n+4)$ for $n > 8$. One can check that these values are greater than 4. So, $f(n) \geq 5$ for any $n > 40$. It seems we can prove that $f(u_{m-1}n) \geq m$ for $n > u_{m-1}u_m$, where u_{m-1} and u_m denote $(m-1)$th and mth Fibonacci numbers. We will investigate this relation in the next section. See Table 1 to have a general outline of our main theorem.

Table 1: Recurrence relation table

	. . .	. . .	. . .	. . .
...	$u_4n - u_2$	$u_5n + u_1$	$u_6n - u_0$	$u_7n = 21n$
...	$u_3n + u_2$	$u_4n - u_1$	$u_5n + u_0$	$u_6n = 13n$
...	$u_2n - u_2$	$u_3n + u_1$	$u_4n - u_0$	$u_5n = 8n$
...	$u_1n + u_2$	$u_2n - u_1$	$u_3n + u_0$	$u_4n = 5n$
...	$u_0n - u_2$	$u_1n + u_1$	$u_2n - u_0$	$u_3n = 3n$
...	$u_2 = 2$	$u_0n - u_1$	$u_1n + u_0$	$u_2n = 2n$
...		$u_1 = 1$	$u_0n - u_0$	$u_1n = n$
...			$u_0 = 1$	$u_0n = n$
...				$u_{-1}n = 0$

2. Main Result

Theorem 2.1: For any positive integer m, $f(n) \geq m$ if $n > u_{m-1}u_m$.

Proof: By Euclidean algorithm and the features mentioned about the function λ, we can conclude that

$$\lambda(u_{m-1}n,\ u_{m-2} + (-1)^{m-1}) \geq m$$

therefore $f(u_{m-1}n) \geq m$.

On the other hand, we can prove that

$$f(u_{m-1}n + i) \geq m \text{ for } 1 \leq i \leq u_{m-1} - 1$$

by computation of the values.

Theorem 2.2: For any positive integer m, we have

$f(n) \geq m$ if $n > u_{m-1}u_m$.

Proof: By Euclidean algorithm and the features mentioned about the function λ, we can conclude that

$$\lambda(u_{m-1}n, u_{m-2} + (-1)^{m-1}) \geq m$$

So $f(u_{m-1}n) \geq m$.

On the other hand, we can check that $f(u_{m-1}n + i \geq m$. For $1 \leq i \leq um-1-1$ by computing the values of

$$\lambda(u_{m-1}n + 1, u_{m-2} + (-1)^{m-1}),$$
$$\lambda(u_{m-1}n + 2, u_{m-2} + (-1)^{m-1} + 1),\ldots.$$

and

$$\lambda(u_{m-1}n + u_{m-1} - 1, u_{m-2} + (-1) + u_{m-1} - 2)$$

3. Conclusions

Corollary 3.1: For any positive integer m, there exists a positive integer r such that $f(n) \geq m$ for any $n > r$.

Corollary 3.2: For any positive integer m, there exists a positive integer r such that for any integer $n > r$ there exists an integer s such that the length of the expression of $\frac{n}{s}$ as a continued fraction is greater than m.

Proof: It can be easily concluded from Theorem 2.2.

References

[1] Niven, I., Zuckerman, H. S., and Montgomery, H. L. 1991. *An Introduction to the Theory of Numbers* (5th Edition). New York: John Wiley & Sons, Inc.

[2] Weisstein, E. 1999. *CRC Concise Encyclopedia of Mathematics by Computation of the Values Mathematics*. Boca Raton, FL: CRC Press.