INT. J. MATH. EDUC. SCI. TECHNOL., 1976, VOL. 7, NO. 3, 307–313

The algorithms of Euclid and Jacobi†

by R. W. JOHNSON
Lewistown College Center, Lewistown, Montana, U.S.A.

and M. S. WATERMAN
Los Alamos Scientific Laboratory, Los Alamos,
New Mexico, U.S.A.

(*Received* 28 *November* 1975)

The connection between Euclid's algorithm and continued fractions is given in a fashion that allows easy generalization to higher dimensions. We explore this generalization which yields Jacobi's algorithm and two-dimensional continued fractions. In addition, the computer science problem of efficient computation of Euclid's or Jacobi's algorithm is solved by generalizing a technique of D. H. Lehmer. Also, some open problems are mentioned for Jacobi's algorithm.

1. Introduction

The Doctor of Arts (D.A.) programme at Idaho State University was created in 1971 and is designed to be a terminal degree programme in mathematics with an emphasis of undergraduate teaching. The programme includes a thesis. This paper is an account of some of the contents of one such thesis. The first author (R.W.J.) was the thesis student and the second author (M.S.W.) was the thesis adviser.

Since an honest attempt to direct D.A. theses requires a rethinking of the classical Ph.D. thesis idea, it is perhaps of interest to list some of the criteria that the second author has developed with the help of his students. The thesis should be on a topic strongly connected with undergraduate mathematics and should not be a 'weak' Ph.D. thesis. The topic, of course, should not be inaccessible to a student with a broad course background (such as D.A. students). The thesis should accomplish something of value to some group of mathematicians, mathematics teachers or scientists. Publishable work, while publication has never been a primary goal, has almost always followed. It is hoped that the thesis student will find that doing mathematics is enjoyable, relevant and possible. This view of the D.A. thesis is not necessarily standard as there is not yet a universally accepted view.

An area rich in D.A. thesis topics is computer science, especially as set forth by Donald Knuth [1, 2]. One of the major interests of modern computer science is the study of algorithms where an algorithm is defined as a set of rules to accomplish a given task. Of course, the search for efficient algorithms is the main task. Frequently, if a problem can be posed as an algorithm problem, then new problems and insights follow.

† This work was performed under the auspices of the United States Energy Research and Development Administration.

Such a study has been made of Euclid's algorithm by Knuth [1, pp. 293–338]. Jacobi's algorithm has been studied in a similar manner by the authors. We have found what is perhaps a new way of showing the connection between Euclid's algorithm and continued fractions. This leads in a natural way to a two-dimensional generalization known as Jacobi's algorithm [3]. In our opinion a natural motivation for Jacobi's algorithm has not been given before and this motivation, along with related material, will be presented below.

2. Euclid's algorithm and continued fractions

The usual statement of Euclid's algorithm [4] is to begin with $m_2 > m_1 > 0$ and derive the following set of equations

$$\left.\begin{aligned} m_2 &= a_1 m_1 + r_1 \\ m_1 &= a_2 r_1 + r_2 \\ &\cdots \\ r_{n-3} &= a_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= a_n r_{n-1} \end{aligned}\right\} \tag{2.1}$$

and show $r_{n-1} = \gcd(m_1, m_2)$ (r_{n-1} is the greatest common divisor of m_1 and m_2). For our purposes this algorithm will be written in the form:

$$\left.\begin{aligned} Q(m_1, m_2) &= (m_2 \bmod m_1, m_1) \\ &= (m_2 - [m_2/m_1]m_1, m_1) \end{aligned}\right\} \tag{2.2}$$

where [ ] is the usual greatest integer function. Repeated operation by Q will now be referred to as Euclid's algorithm. Of course

$$\gcd(m_1, m_2) = \gcd Q(m_1, m_2)$$

and the algorithm ends when the first coordinate is zero. The second coordinate is then $\gcd(m_1, m_2)$.

Knuth states [1] that Euclid's algorithm is the world's oldest non-trivial algorithm. It is perhaps even more surprising that Euclid's algorithm is one of the most efficient practical methods of computing greatest common divisors used on computers today. There are even several unsolved problems of interest that involve Euclid's algorithm [1, p. 333].

The connection between continued fractions and Euclid's algorithm is well known [4], but it will be useful here to derive it in a different manner. Let $0 \leqslant m_1 < m_2$ be associated with a point in [0, 1] by

$$(m_1, m_2) \sim m_1/m_2 \tag{2.3}$$

then

$$Q(m_1, m_2) = (m_2 - [m_2/m_1]m_1, m_1) \sim m_2/m_1 - [m_2/m_1] = T(m_1/m_2)$$

where

$$T(x) = 1/x - [1/x]$$

Now, if

$$x = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} = [a_1, a_2, \ldots]$$

is the simple continued fraction expansion of x, then

$$T([a_1,a_2,\ldots])=[a_2,a_3,\ldots]$$

Therefore T ' slides ' the partial quotients of x along. T is known as the shift on the digits of the continued fraction.

It is important to notice that $a_1=[m_2/m_1]$ and that the first step of Euclid's algorithm,

$$Q(m_1,m_2)=(m_2-[m_2/m_1]m_1,m_1)$$

utilizes exactly the same integer $[m_2/m_1]$ in (2.2) as is used for the first partial quotient in the continued fraction expansion of x. This observation is true for succeeding partial quotients as well.

3. Lehmer's method

In a paper that has become quite well known in computer science, Lehmer [5] in 1938 published a technique that is very useful for efficient computation of gcd (m_1,m_2) when m_1 and m_2 are large (multi-precision) integers. Lehmer's motivation was to find correct partial quotients of an irrational that was known correctly to a certain number of decimal digits.

While Knuth [1] does not write out a proof of Lehmer's method, our techniques from the previous section allow an easy proof. Let m_1 and m_2 be the multi-precision integers mentioned above and let m_1',m_2',m_1'',m_2'' be single precision integers satisfying

$$m_1'/m_2' < m_1/m_2 < m_1''/m_2'' \tag{3.1}$$

It follows that

$$m_2''/m_1'' < m_2/m_1 < m_2'/m_1'$$

and, if

$$[m_2'/m_1']=[m_2''/m_1'']=a$$

then

$$[m_2/m_1]=a$$

Consequently,

$$T(m_1''/m_2'')=m_2''/m_1''-a<T(m_1/m_2)<T(m_1'/m_2')$$

and the procedure beginning with (3.1) can be repeated doing only single precision arithmetic until the a's (partial quotients) disagree. Then one multiprecision catch up step is performed and the procedure can be repeated.

To illustrate, consider $m_2=2953641$ and $m_1=2718281$. The above conditions are satisfied with

$$m_1'=2718 \qquad m_1''=2719$$
$$m_2'=2954 \qquad m_2''=2953$$

The word size of our computer is assumed to be four.

m_1'	m_2'	a'	m_1''	m_2''	a''
2718	2954	1	2719	2953	1
236	2718	11	234	2719	11
122	236	1	145	234	1
114	122	1	89	145	1
8	114	14	56	89	1

On the last line $a' \neq a''$ so that it is only certain that $a_1=1$, $a_2=11$, $a_3=1$, $a_4=1$, and $1 \leqslant a_5 \leqslant 14$. The calculation proceeds by

m_1	m_2	a
m_1	m_2	1
m_2-m_1	m_1	11
$12m_1-11m_2$	m_2-m_1	1
$12m_2-13m_1$	$12m_1-11m_2$	1
$-23m_2+25m_1$	$12m_2-13m_1$	?

so that only the last line of multiprecision calculation need be done to continue the computation:

$$\gcd(2718281,2953641)=\gcd(106039,23282).$$

4. Jacobi's algorithm

In a posthumous paper in 1868 Jacobi published a generalization of continued fractions to two-dimensions [3]. An effort was made to characterize cubic irrationals as Lagrange had characterized quadratic irrationals with the one-dimensional continued fraction. This effort failed to characterize all cubic irrationals and the problem of whether this is possible with any Jacobi algorithm has never been settled. It has been a fruitful area and Bernstein has written a book on the subject [6].

An introduction to Jacobi's algorithm is provided by considering three integers $0<m_1 \leqslant m_2 < m_3$ and

$$Q(m_1,m_2,m_3)=(m_2-[m_2/m_1]m_1,m_3-[m_3/m_1]m_1,m_1)$$

Again

$$\gcd(m_1,m_2,m_3)=\gcd Q(m_1,m_2,m_3)$$

and Q is seen to be a natural generalization of Euclid's algorithm. An examination of another paper of Jacobi's [7] shows that he was aware of the connection between his algorithm and greatest common divisors.

If each such triple of integers is associated with a point in $(0, 1)^2$ by

$$(m_1,m_2,m_3)\sim(m_1/m_3,m_2/m_3)$$

then

$$Q(m_1,m_2,m_3)\sim(m_2/m_1-[m_2/m_1],m_3/m_1-[m_3/m_1])=T(m_1/m_3,m_2/m_3)$$

where

$$T(x_1,x_2)=(x_2/x_1-[x_2/x_1],1/x_1-[1/x_1])$$

The transformation T is the shift on the digits of the two-dimensional continued fraction defined by Jacobi but that subject will be omitted here.

The transformation Q is probably not the best method for finding the greatest common divisor of three integers. We conjecture that the algorithm defined by

$$\gcd(\gcd(m_1,m_2),m_3)$$

is faster, but no comparison, theoretical or experimental, has appeared.

5. Generalized Lehmer's method

It is not entirely trivial to generalize Lehmer's method to two-dimensions. This was, in fact, begun in [8] for another problem and will be completed here. Define

$$\Psi(x,y)=(y/x,1/x) \tag{5.1}$$

then

$$T(x,y)=\Psi(x,y)-a(x,y) \tag{5.2}$$

where

$$a(x,y)=([y/x],[1/x])$$

The crucial observation is that Ψ maps triangles (with their interior) in $(0,1)^2$ into triangles (with their interior) in $(0,\infty)^2$. To prove this we first let

$$\alpha_0+\alpha_1 x+\alpha_2 y=0$$

be a line with $x\neq 0$. Then

$$\alpha_0(1/x)+\alpha_1+\alpha_2(y/x)=0$$

is a line in the image of Ψ. Since Ψ is continuous, the interior of a triangle is mapped to the interior or exterior of the triangle in the image. The interior of the triangle in $(0,\infty)^2$ has finite area but the exterior has infinite area. Let A be the triangle in $(0,1)^2$. Then, by a change of variable theorem [9, p. 271], if $J(x,y)$ is the Jacobian of Ψ^{-1},

$$\text{area of } \Psi(A)=\int_A |J(x,y)|\,dx\,dy=\int_A y^{-3}dx\,dy<\infty$$

The last inequality follows from the boundedness of y^{-3} on a closed subset of $(0,1)^2$. This completes the proof of the above assertion.

The utility of our observation about Ψ comes from a consideration of (5.2). If (x,y) belongs to the triangle formed by three points and if the $a(\ ,\ )$ values are identical for these points, then $T(x,y)$ belongs to the triangle formed by the three $T(\ ,\ )$ values. Thus Lehmer's method has been generalized if (x,y) belongs to an easily found triangle.

The triangles we consider are right triangles. Assume $0<\epsilon_i,w<x$ and $z<y$. Then (x,y) belongs to the triangle formed by (w,z), $(w+\epsilon_1,z)$ and $(w,z+\epsilon_2)$ if and only if

$$(x-w)/\epsilon_1+(y-z)/\epsilon_2<1 \tag{5.3}$$

This follows since (x,y) belongs to the triangle if and only if

$$(x,y)=\alpha_0(w,z)+\alpha_1(w+\epsilon_1,z)+\alpha_2(w,z+\epsilon_2)$$

where

$$\alpha_i\geq 0 \quad \text{and} \quad \alpha_0+\alpha_1+\alpha_2=1$$

But this means

$$(x,y)=(w+\alpha_1\epsilon_1,z+\alpha_2\epsilon_2)$$

or

$$\alpha_1=(x-w)/\epsilon_1, \qquad \alpha_2=(y-z)/\epsilon_2.$$

Clearly

$$\alpha_1>0,\alpha_2>0$$

Now

$$\alpha_0=1-\alpha_1-\alpha_2=1-(x-w)/\epsilon_1-(y-z)/\epsilon_2\geq 0$$

if and only if (5.3) holds.

The final step in the generalization of Lehmer's method is, given a vector of three integers corresponding to (x,y), to find a vector of three integers corresponding to (w,z) and to find appropriate ϵ_1 and ϵ_2. This is handled in the following manner. Take the vector of leading places of (m_1,m_2,m_3), and add 1 to the leading digits of m_3. Then add 5 to first component for the second vector and add 5 to the second component for the third vector. A proof for this procedure is contained in [10] and is omitted here.

To clarify these concepts, consider the vector (129345,37713,197645). Again the computer word size is assumed to be four. The triangle is formed by

$$\begin{array}{lll} m_1' = 1293 & m_1'' = 1298 & m_1''' = 1293 \\ m_2' = 377 & m_2'' = 377 & m_2''' = 382 \\ m_3' = 1977 & m_3'' = 1977 & m_3''' = 1977 \end{array}$$

As calculation for all three triples is lengthy to present, only that for m' appears.

m_1'	m_2'	m_3'	a_1'	a_2'
1293	377	1977	0	1
377	684	1293	1	3
307	162	377	0	1
162	70	307	?	?

At the last step $a' = (0,1) = a''$ but $a''' = (0,2)$. The calculation proceeds by:

m_1	m_2	m_3	a_1	a_2
m_1	m_2	m_3	0	1
m_2	$m_3 - m_1$	m_1	1	3
$m_3 - m_2 - m_1$	$m_1 - 3m_2$	m_2	0	1
$m_1 - 3m_2$	$2m_2 + m_1 - m_3$	$m_3 - m_2 - m_1$	?	?

The last line of multiprecision calculation yields

$$\gcd(129345,37713,197645) = \gcd(16206,7126,30587).$$

6. Some open problems

First an attempt is made to indicate what work has been done in connection with the above material. In performing $Q(m_1,m_2,m_3)$, the last coordinate is always the largest but the first is not always the smallest. It seems clear that a permutation of the first two coordinates to assure the first coordinate is smallest would speed computation. A study of such algorithms has been done in [11] and [12] where the problems are handled in n (rather than two) dimensions. Other details connected with computational problems are dealt with in [12].

However, examples can be found where the permutation algorithm takes *more* steps. For example with (1396,7694,8593), the permutation algorithm takes six steps to find the greatest common divisor is 1, while the usual Jacobi algorithm takes five steps. An interesting problem would be to characterize those vectors of integers where this unexpected occurrence takes place. It would also be of interest to find how often this happens.

Along these lines Kronecker [4] has shown that the least remainder algorithm never takes more steps than any other Euclidean algorithm. As must now be clear, there are many Jacobi algorithms. Which one, if any, always takes no more steps than any other Jacobi algorithm?

Also Lame's Theorem considers the maximum number of divisions required to find the greatest common divisor using the Euclidean algorithm. The result is that the number of steps does not exceed five times the number of digits in the smallest integer. The proof uses Fibonacci numbers. Is there such a result for the Jacobi algorithm? What integers correspond to the worst case and are there Fibonacci type numbers for the Jacobi algorithm?

7. Conclusion

It is our hope that this paper has been of interest to teachers of mathematics and to students of number theory and computer science. Lehmer's method deserves more notice especially among undergraduates who are assigned the task of finding the first seven (say) *correct* partial quotients of π.

Also the introduction to the Jacobi algorithm should be of interest as it is an easy way to discover the transformation T. We have found no completely easy way to the two-dimensional continued fraction however.

Computer programmes (in FORTRAN) have been written to calculate greatest common divisors of three integers by both Jacobi's algorithm and the generalized Lehmer method. Also, the modification of Jacobi's algorithm to always divide by the smallest of the three integers and its Lehmer modification have been programmed. Descriptions of these algorithms with the listings of the four programmes can be obtained by requesting reference [10] from the second author.

Acknowledgments

The first author would like to express his appreciation to the Department of Mathematics at Idaho State University for providing financial support in the form of a Doctor of Arts Fellowship from 1973 to 1975.

References

[1] KNUTH, D. E., 1969, *The Art of Computer Programming*, Vol. 2/*Seminumerical Algorithms* (Reading, Massachusetts: Addison Wesley).
[2] KNUTH, D. E., 1974, *Am. math. Mon.*, **81**, 323.
[3] JACOBI, C. G. J., 1868, *J. reine angew. Math.*, **69**, 29.
[4] USPENSKY, J. V., and HEASLET, M. A., 1939, *Elementary Number Theory* (London, New York: McGraw-Hill).
[5] LEHMER, D. H., 1938, *Am. math. Mon.*, **45**, 227.
[6] BERNSTEIN, L., 1971, *The Jacobi–Perron Algorithm* (Springer).
[7] JACOBI, C. G. J., 1868, *J. reine angew. Math.*, **69**, 1.
[8] BEYER, W. A., and WATERMAN, M. S., 1972, *Num. Math.*, **19**, 195.
[9] APOSTOL, T. M., 1957, *Mathematical Analysis* (London, Reading, Massachusetts: Addison Wesley).
[10] JOHNSON, R. W., and WATERMAN, M. S., 1975, Los Alamos Scientific Laboratory Report LA-MS.
[11] WATERMAN, M. S., 1976, *J. math. Analysis Applic.* (to appear).
[12] WATERMAN, M. S., 1976, *Math. Comput.* (submitted).