Euclid's Algorithm for Large Numbers

D. H. Lehmer

American Mathematical Monthly, Volume 45, Issue 4 (Apr., 1938), 227-233.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28193804%2945%3A4%3C227%3AEAFLN%3E2.0.CO%3B2-Y

EUCLID'S ALGORITHM FOR LARGE NUMBERS

D. H. LEHMER, Lehigh University

Euclid's algorithm which is so fundamental to the theory of regular continued fractions and elementary theory of numbers, is also of immense practical value in such well known problems as discovering the partial quotients in the regular continued fraction expansion of a given real number, and the solution of linear diophantine equations, to mention only two applications. In these problems, which occur frequently in experimental research, it is often necessary to carry the algorithm to a great many stages, as for example when one needs the greatest common divisor of two numbers each having, let us say, 30 digits, or when one wishes an extremely accurate rational approximation to a given irrational. In such cases, in which one would naturally use a computing machine, the algorithm involves numerous trivial operations with extremely large numbers. The purpose of this note is to show how more than 90% of these operations with large numbers may be eliminated. If one wishes historical evidence of the difficulties or rather the tedium of Euclid's algorithm in such cases, one may take the problem of expanding π in a regular continued fraction. In 1685 Wallis* computed the first 34 partial quotients of π. This calculation, made nearly a century before π was proved irrational, was verified as far as the 26th partial quotient by Lambert in 1770. But since then no one has extended the calculation of Lambert, and the fact that the 34th partial quotient given by Wallis should be 99 instead of unity has remained unnoticed until today.

1. Notation and general formulas. Let x_0 and x_1 be a pair of positive real numbers. Then Euclid's algorithm generates from x_0 and x_1 a set $\{x_\nu\}$ of real numbers and a set $\{q_\nu\}$ of integers by means of the equations

$$\begin{aligned}
x_0 &= q_0x_1 + x_2, \\
x_1 &= q_1x_2 + x_3, \\
x_2 &= q_2x_3 + x_4, \\
&\cdots\cdots\cdots \\
x_\nu &= q_\nu x_{\nu+1} + x_{\nu+2}, \\
&\cdots\cdots\cdots,
\end{aligned} \tag{1}$$

in which q_ν is the greatest integer not exceeding $x_\nu/x_{\nu+1}=\xi_\nu$. Eliminating $x_2, x_3, x_4, \cdots$ from (1) we obtain the regular continued fraction for ξ_0,

$$\xi_0 = \frac{x_0}{x_1} = q_0 + \frac{1}{q_1 +}\ \frac{1}{q_2 + \cdots} = [q_0, q_1, q_2, \cdots].$$

Similarly

* John Wallis, A Treatise of Algebra, London, 1685, pp. 46–55.

$$\xi_\nu = \frac{x_\nu}{x_{\nu+1}} = [q_\nu, q_{\nu+1}, q_{\nu+2} \cdots]. \tag{2}$$

The nth convergent of ξ_0, namely

$$[q_0, q_1, q_2, \cdots, q_n],$$

is usually denoted by A_n/B_n, but to avoid the use of too many sub-subscripts in what follows we shall also write $A(n)$ and $B(n)$ for the numerator and denominator of the nth convergent of ξ_0. More generally, the nth convergent of ξ_ν,

$$[q_\nu, q_{\nu+1}, \cdots, q_{\nu+n}], \tag{3}$$

will be denoted by $A(n, \nu)/B(n, \nu)$ so that

$$A_n = A(n) = A(n, 0) \qquad \text{and} \qquad B_n = B(n) = B(n, 0).$$

The A's and B's satisfy the following recursion formulas

$$\begin{aligned} A(m, \nu) &= A(m-1, \nu)q_{m+\nu} + A(m-2, \nu), \\ B(m, \nu) &= B(m-1, \nu)q_{m+\nu} + B(m-2, \nu), \end{aligned} \tag{4}$$

with the initial conditions

$$\begin{aligned} A(-1, \nu) &= 1, \qquad A(0, \nu) = q_\nu, \\ B(-1, \nu) &= 0, \qquad B(0, \nu) = 1. \end{aligned} \tag{5}$$

If we eliminate $x_{\nu+2}, x_{\nu+3}, \cdots, x_{\nu+n-1}$ between the $(\nu+1)$st, $(\nu+2)$nd, $\cdots$ $(\nu+n-1)$st equations of the system (1) we obtain

$$x_{\nu+n} = (-1)^n\{B(n-2, \nu)x_\nu - A(n-2, \nu)x_{\nu+1}\}, \tag{6}$$

a formula which is readily proved by induction using (1), (4), and (5), and which lies at the root of our modification of the Euclid algorithm. The following formulas will also be of use and are easily established by induction from (4) and (5).

$$\begin{aligned} A_{\nu+n} &= A_\nu A(n-1, \nu+1) + A_{\nu-1}B(n-1, \nu+1), \\ B_{\nu+n} &= B_\nu A(n-1, \nu+1) + B_{\nu-1}B(n-1, \nu+1). \end{aligned} \tag{7}$$

Given the two numbers x_0 and x_1 having a very large number of significant figures, the application of Euclid's algorithm begins with the computation of the partial quotients q_ν $(\nu=0, 1, 2, \cdots)$. We note first that since q_0 is merely the greatest integer in x_0/x_1, crude approximations to x_0 and x_1 will in general be sufficient to determine q_0. More generally, if (x_0, x_1) are replaced by approximate values (y_0, y_1), then the first few partial quotients of x_0/x_1 and y_0/y_1 will be the same. If y_0 and y_1 have only a few significant figures, the first few partial quotients are easily obtained. Of course, if the Eulcid's algorithm for y_0/y_1 is carried too far, the q's will begin to disagree with those for x_0/x_1. There are two ways to find out how far the q's may be trusted. Perhaps the safest way is to choose a second pair (z_0, z_1) such that x_0/x_1 lies between y_0/y_1 and z_0/z_1. Then the partial quotients of y_0/y_1 and x_0/x_1 will agree at least as far as those of y_0/y_1 and z_0/z_1 agree. Since the whole calculation is based on the first few q's, the fact that they are obtained in two ways is a welcome check on the work, rather than a waste of effort. The other method of telling how far we may trust the q's will be discussed presently.

Having obtained the first few partial quotients, up to say q_{k_1}, we next compute the numbers

$$A(k_1, 0), \quad B(k_1, 0), \quad A(k_1 - 1, 0), \quad B(k_1 - 1, 0) \tag{8}$$

by the recurrence formulas (4) with $\nu = 0$. The relation

$$A(k_1, 0)B(k_1 - 1, 0) - A(k_1 - 1, 0)B(k_1, 0) = (-1)^{k_1 - 1}$$

affords an almost infallible check on the work.

Thus far the calculation has involved only small numbers. In fact we have not used x_0 and x_1, but merely approximations to them. By setting $\nu = 0$, and $n = k_1 + 1$ and $k_1 + 2$ in (6) we get

$$x_{k_1+1} = (-1)^{k_1+1}\{B(k_1 - 1, 0)x_0 - A(k_1 - 1, 0)x_1\}, \tag{9}$$

$$x_{k_1+2} = (-1)^{k_1+2}\{B(k_1, 0)x_0 - A(k_1, 0)x_1\}. \tag{10}$$

Here we encounter for the first time operations with really large numbers. To be quite certain that we are on the right track we may apply the following well known* theorem.

THEOREM A. *Let A_k/B_k, A_{k-1}/B_{k-1}, be two consecutive convergents to a number η. Then these fractions are consecutive convergents of ξ if and only if*

$$\left| \xi - \frac{A_k}{B_k} \right| < \frac{1}{B_k(B_k + B_{k-1})}.$$

Setting $\xi_0 = x_0/x_1$ and $k = k_1$ we obtain from (10) the condition

$$x_{k_1+2} < \frac{x_1}{B(k_1, 0) + B(k_1 - 1, 0)} \tag{11}$$

which is necessary for the correctness of the q's so far. We now replace x_{k_1+1} and x_{k_1+2} by approximations y_{k_1+1} and y_{k_1+2} and compute as before the first few partial quotients of y_{k_1+1}/y_{k_1+2}. By (2) these partial quotients will be

$$q_{k_1+1}, q_{k_1+2}, \cdots, q_{k_1+1+k_2}. \tag{12}$$

Using these q's we next compute the numbers

$$A(k_2, k_1 + 1), \quad B(k_2, k_1 + 1), \quad A(k_2 - 1, k_1 + 1), \quad B(k_2 - 1, k_1 + 1) \tag{13}$$

by (4) and check them by means of the relation

$$A(k_2, k_1 + 1)B(k_2 - 1, k_1 + 1) - A(k_2 - 1, k_1 + 1)B(k_2, k_1 + 1) = (-1)^{k_2 - 1}.$$

Using (6) with $\nu = k_1 + 1$ and $n = k_2 + 1$ and $k_2 + 2$ we get the equations

* See for instance Lucas, Théorie des Nombres, p. 449.

$$(14)\qquad x_{k_1+k_2+2} = (-1)^{k_2+1}\{B(k_2-1,\, k_1+1)x_{k_1+1} - A(k_2-1,\, k_1+1)k_{k_1+2}\},$$

$$(15)\qquad x_{k_1+k_2+3} = (-1)^{k_2}\{B(k_2,\, k_1+1)x_{k_1+1} - A(k_2,\, k_1+1)x_{k_1+2}\},$$

which involve for the second time operations with large numbers. A test of the correctness of the set (12) of new q's is this time

$$(16)\qquad x_{k_1+k_2+3} < \frac{x_{k_1+2}}{B(k_2,\, k_1+1) + B(k_2-1,\, k_1+1)}.$$

The process may now be continued using approximate values of $x_{k_1+k_2+2}$ and $x_{k_1+k_2+3}$ and obtaining a new set of q's, a new pair of A's and B's, and a new pair of x's. In this way the partial quotients may be extended as far as desirable.

In some problems the convergents A_n/B_n are of no interest. In these cases the above process is adequate. For example if we have a given number ξ_0 expressed let us say in decimals, and we wish to examine its partial quotients to see if they terminate, become periodic, or obey some law or other, we have only to choose $x_0=\xi_0$, and $x_1=1$ and apply the above process. As a second example we may wish to find the greatest common divisor $\delta=(x_0,\, x_1)$ of two large integers x_0 and x_1. From (9) and (10) we see that any divisor common to x_0 and x_1 will divide x_{k_1+1} and x_{k_1+2} and conversely. Hence from (14) and (15) and all further similar equations we have

$$\delta = (x_0,\, x_1) = (x_{k_1+1},\, x_{k_1+2}) = (x_{k_1+k_2+2},\, x_{k_1+k_2+3}) = \cdots.$$

Since these x's decrease rapidly (by (11), (16), etc.) we soon come to a pair whose G.C.D. is easily found.

Of those problems in which the convergents are of importance a large majority require merely one convergent. This is the case for example when one wishes to get a rational approximation to a real number, or in the solution of linear diophantine equations, in which case the penultimate convergent of a rational number is needed. Sometimes one needs a sequence of convergents (or even intermediate convergents) beginning with A_n/B_n, the earlier convergents being of no use. This happens for example when one is looking for a rational approximation to a given real number which not only is sufficiently accurate but whose numerator or denominator has some further property.

In all these cases one may use formulas (7) to advantage as follows. We have already found the numbers (8), (13), etc. Substituting them in (7) with $\nu=k_1$ and first $n=k_2$ and then $n=k_2+1$, we get at once

$$(17)\qquad \begin{aligned} A_{k_1+k_2} &= A_{k_1}A(k_2-1,\, k_1+1) + A_{k_1-1}B(k_2-1,\, k_1+1),\\ B_{k_1+k_2} &= B_{k_1}A(k_2-1,\, k_1+1) + B_{k_1-1}B(k_2-1,\, k_1+1),\\ A_{k_1+k_2+1} &= A_{k_1}A(k_2,\, k_1+1) + A_{k_1-1}B(k_2,\, k_1+1),\\ B_{k_1+k_2+1} &= B_{k_1}A(k_2,\, k_1+1) + B_{k_1-1}B(k_2,\, k_1+1).\end{aligned}$$

Thus we proceed from the numerators and denominators of one pair of consecutive convergents (8) to those of another isolated pair (17). Repeating the process as many times as is necessary one obtains a consecutive pair of convergents A_n/B_n, A_{n-1}/B_{n-1} for whatever value of n one may wish. The relation

$$A_nB_{n-1} - A_{n-1}B_n = (-1)^{n-1}$$

serves as a final check. One may also examine consecutive convergents (or intermediate convergents) in the neighborhood of A_n/B_n using (4) with $\nu = 0$.

2. An application. To illustrate the foregoing method we consider the regular continued fraction for π. Taking a value of π correct to 100 decimal places* we shall first find the partial quotients

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, \cdots], \tag{18}$$

from which

$$\begin{aligned} A_{17} &= 2549491779, & B_{17} &= 811528438, \\ A_{18} &= 6167950454, & B_{18} &= 1963319607. \end{aligned} \tag{19}$$

Using now our 100 figure accuracy we find† (by (6) with $\nu = 0$, $n = 19, 20$)

$$\begin{aligned} x_{19} &= A_{17} - B_{17}\pi = 4.474 \cdot 10^{-10}, \\ x_{20} &= -A_{18} + B_{18}\pi = 1.497 \cdot 10^{-10}. \end{aligned} \tag{20}$$

As a check (11) gives

$$x_{20} < 1/(B_{18} + B_{17}) = 3.603 \cdot 10^{-10}$$

which is in accord with (20).

Next we find that

$$\begin{aligned} \xi_{19} = x_{19}/x_{20} &= [q_{19}, q_{20}, \cdots , q_{32}, \cdots] \\ &= [2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4, 2, 6, 6, \cdots]. \end{aligned} \tag{21}$$

Hence

$$\begin{aligned} A(12, 19) &= 61245426, & B(12, 19) &= 20495141, \\ A(13, 19) &= 376962143, & B(13, 19) &= 126146437. \end{aligned} \tag{22}$$

Next we compute

$$\begin{aligned} x_{33} &= B(12, 19)x_{19} - A(12, 19)x_{20} = 1.185 \cdot 10^{-18}, \\ x_{34} &= A(13, 19)x_{20} - B(13, 19)x_{19} = 1.188 \cdot 10^{-20}. \end{aligned}$$

As a check (16) gives

$$x_{34} < x_{20}/(B(13, 19) + B(12, 19)) = 1.021 \cdot 10^{-18}.$$

* π=3.14159 26535 89793 23846 26433 83279 50288 41971 69399 37510 58209 74944 59230 78164 06286 20899 86280 34825 34211 70680.

† The actual values of the x's have been suppressed to save space.

Next we find

$$\begin{aligned}\xi_{33} &= x_{33}/x_{34} = [q_{33}, q_{34}, \cdots, q_{50}, \cdots] \\ &= [99, 1, 2, 2, 6, 3, 5, 1, 1, 6, 8, 1, 7, 1, 2, 3, 7, 1, \cdots],\end{aligned} \tag{23}$$

from which

$$\begin{aligned}A(16, 33) &= 6185428223, \qquad B(16, 33) = 62033398, \\ A(17, 33) &= 7032882291, \qquad B(17, 33) = 70532479,\end{aligned} \tag{24}$$

and

$$x_{51} = B(16, 33)x_{33} - A(16, 33)x_{34} = 1.249\cdot 10^{-28},$$

$$x_{52} = A(17, 33)x_{34} - B(16, 33)x_{33} = 4.958\cdot 10^{-29}.$$

As a check

$$x_{52} < x_{34}/(B(17, 33) + B(16, 33)) = 8.965\cdot 10^{-29}.$$

Next we find

$$\begin{aligned}\xi_{51} &= x_{51}/x_{52} = [q_{51}, q_{52}, \cdots, q_{76}, \cdots] \\ &= [2, 1, 1, 12, 1, 1, 1, 3, 1, 1, 8, 1, 1, 2, 1, 6, 1, 1, 5, 2, 2, 3, 1, 2, 4, 4, \cdots],\end{aligned} \tag{25}$$

and

$$\begin{aligned}A(24, 51) &= 2414289141, \qquad B(24, 51) = 958421828, \\ A(25, 51) &= 10210815077, \qquad B(25, 51) = 4053478055,\end{aligned} \tag{26}$$

from which

$$x_{77} = B(24, 51)x_{51} - A(24, 51)x_{52} = 1.206\cdot 10^{-38},$$

$$x_{78} = A(25, 51)x_{52} - B(25, 51)x_{51} = 7.099\cdot 10^{-40}.$$

As a check

$$x_{78} < x_{52}/(B(25, 51) + B(24, 51)) = 9.893\cdot 10^{-39}.$$

Finally

$$\begin{aligned}\xi_{77} &= x_{77}/x_{78} = [q_{77}, q_{78}, \cdots, q_{90}, \cdots] \\ &= [16, 1, 161, 45, 1, 22, 1, 2, 2, 1, 4, 1, 2, 24, \cdots],\end{aligned} \tag{27}$$

$$\begin{aligned}A(12, 77) &= 482872247, \qquad B(12, 77) = 28414566, \\ A(13\ 77) &= 11759887912, \qquad B(13, 77) = 692009353;\end{aligned} \tag{28}$$

hence

$$x_{92} = A(13, 77)x_{78} - B(13, 77)x_{77} = 7.328\cdot 10^{-49},$$

whereas

$$x_{92} < x_{78}/(B(13, 77) + B(12, 77)) = 9.854\cdot 10^{-49}.$$

Combining (18), (21), (23), (25), and (27) we have all the partial quotients of π from $q_0=3$ to $q_{90}=24$.

If we wish the 90th convergent A_{90}/B_{90} we proceed as follows. Setting $\nu=18$, $n=13$, 14 in (7) we have from (19) and (23)

$$\begin{aligned} A_{31} &= A_{18}A(12,19)+A_{17}B(12,19) = 430010946\ 591069243,\\ B_{31} &= B_{18}A(12,19)+B_{17}B(12,19) = 136876735\ 467187340,\\ A_{32} &= A_{18}A(13,19)+A_{17}B(13,19) = 2646693125\ 139304345,\\ B_{32} &= B_{18}A(13,19)+B_{17}B(13,19) = 842468587\ 426513207. \end{aligned} \tag{29}$$

As a check

$$A_{32}B_{31}-A_{31}B_{32} = -1.$$

Next setting $\nu=32$, $n=17$, 18 in (7) we obtain from (29) and (24),

$$\begin{aligned} A_{49} &= A_{32}A(16,33)+A_{31}B(16,33),\\ B_{49} &= B_{32}A(16,33)+B_{31}B(16,33),\\ A_{50} &= A_{32}A(17,33)+A_{31}B(17,33),\\ B_{50} &= B_{32}A(17,33)+B_{31}B(17,33). \end{aligned} \tag{30}$$

Next we set $\nu=50$, $n=25$, 26 in (7) and obtain from (30) and (26),

$$\begin{aligned} A_{75} &= A_{50}A(24,51)+A_{49}B(24,51),\\ B_{75} &= B_{50}A(24,51)+B_{49}B(24,51),\\ A_{76} &= A_{50}A(25,51)+A_{49}B(25,51),\\ B_{76} &= B_{50}A(25,51)+B_{49}B(25,51). \end{aligned} \tag{31}$$

Finally we set $\nu=76$, $n=14$ in (7) and obtain from (31) and (28),

$$\begin{aligned} A_{90} &= A_{76}A(13,77)+A_{75}B(13,77),\\ B_{90} &= B_{76}A(13,77)+B_{75}B(13,77). \end{aligned}$$

The actual values of A_{90} and B_{90} are

$$\begin{aligned} A_{90} &= 3062\ 43329\ 44969\ 82257\ 53216\ 23878\ 54374\ 05787\ 90366\ 50780,\\ B_{90} &= 974\ 80279\ 34167\ 85521\ 47430\ 34062\ 01616\ 85335\ 37806\ 95273. \end{aligned}$$

By Theorem A, $\pi-A_{90}/B_{90}$ should be less than $1.01\cdot 10^{-96}$. By actual computation we find this difference to be less than $8\cdot 10^{-97}$.