



---

The Euclidean Algorithm

Author(s): Philip Franklin

Source: *The American Mathematical Monthly*, Vol. 63, No. 9 (Nov., 1956), pp. 663-664

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/2310600>

Accessed: 24/03/2010 20:05

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

In the first example, it is seen that the main advantage of this method is that it avoids rationalization of an algebraic expression. The second example would be extremely difficult to carry out without the aid of a special device.

It should be noted that when multiplication by a power of  $r$  is required, the origin may be added to the original locus. In the above examples, the origin was already part of the locus, and so no alteration occurred. But the equation  $r \sin \theta \cos^2 \theta - 1 = 0$  gives a simple case where the origin appears in the Cartesian equation of the locus, but not in the polar equation.

### THE EUCLIDEAN ALGORITHM

PHILIP FRANKLIN, Massachusetts Institute of Technology

Several elementary texts on number theory, such as the recent one by Harriet Griffin (1954) and the older one by R. D. Carmichael (1914), include the following as an exercise.

Prove that the number of divisions required to find the greatest common divisor of two positive integers written in the scale of 10 by means of the Euclidean algorithm does not exceed five times the number of digits in the smaller integer.

Both authors recognized this as a hard problem by its position at the end of a set, and Carmichael added a star. Since its difficulty for students is confirmed by experience in the classroom, a short solution may be of interest to teachers or students of number theory.

We first observe that a typical step of Euclid's algorithm at any stage uses the division transformation  $a = qb + r$  to replace the pair  $a, b$  with  $a > b$  by  $b, r$  with  $b > r$ . If  $r < (5/8)b$ , this single step reduces the smaller number in the ratio  $r/b < 5/8$ .

Next suppose that  $r \geq (5/8)b$ . Then the following step of the algorithm uses  $b = q_1 r + r_1$  with  $q_1 = 1$  and  $r_1 = b - r < (3/8)b$ . This leads to the pair of numbers  $r, r_1$  with  $r > r_1$ . And the smaller number has been reduced in the ratio  $r_1/b \leq 3/8$  for two steps. This is an average ratio of reduction less than  $5/8$  per step, since  $3/8 < (5/8)^2$ .

For five steps, the average ratio of reduction is less than  $(5/8)^5 = 10^5/2^{20} = (1/10)(1000/1024)^2 < 1/10$ . Hence for  $5n$  steps the ratio will be less than  $10^{-n}$ . Let  $n$  be the number of digits in the smaller integer of the original pair. Then the smaller integer initially had a value less than  $10^n$ . Thus it would be reduced to less than unity if  $5n$  steps were required. But the process stops when the remainder used as the new smaller number is zero. This proves that at most  $5n$  steps will suffice.

The algorithm may be modified by using positive or negative remainders. In this case for a typical step we use  $a = qb + r$  with  $|r| \leq b/2$  to replace the pair  $a, b$  with  $a > b$  by  $b, |r|$  with  $b > |r|$ . If  $|r| < (3/7)b$ , the first step reduces the smaller number in the ratio  $|r|/b < 3/7$ .

Next suppose that  $|r| \geq (3/7)b$ . Then the following step of the algorithm uses  $b = q_1|r| + r_1$ , with  $q_1 = 2$ . Since  $|r| \leq b/2$ ,  $r_1 \geq 0$ . And  $r_1 = b - 2|r| < b - (6/7)b = b/7$ . This leads to the pair of numbers  $|r|$ ,  $r_1$ . And the smaller number has been reduced in the ratio  $r_1/b \leq 1/7$  for two steps. This is an average ratio of reduction less than  $3/7$  per step, since  $1/7 < (3/7)^2$ .

For three steps, the average ratio of reduction is less than  $(3/7)^3 = 27/343 < 1/10$ . Hence for  $3n$  steps the ratio will be less than  $10^{-n}$ . This shows that if  $n$  is the number of digits in the smaller integer of the original pair, for the modified algorithm  $3n$  steps will suffice.

The result for the Euclidean algorithm was found by G. Lamé in 1844. He used properties of the Fibonacci series in the proof. The result for the modified algorithm was found by Lionnet in 1857. Other references and details are given in Dickson's *History of the Theory of Numbers*, vol. I, pages 332 and 394.

## ELEMENTARY PROBLEMS AND SOLUTIONS

EDITED BY HOWARD EVES, University of Maine

*Send all communications concerning Elementary Problems and Solutions to Howard Eves, Mathematics Department, University of Maine, Orono, Maine. This department welcomes problems believed to be new and demanding no tools beyond those ordinarily furnished in the first two years of college mathematics. To facilitate their consideration, solutions should be submitted on separate, signed sheets, within three months after publication of problems.*

### PROBLEMS FOR SOLUTION

E 1236. *Proposed by Hazel E. Evans, University of Pittsburgh*

For  $a > b$  and  $N < ab$  find the maximum value of  $N$  for which the equation

$$ax + by = N$$

has a solution in non-negative integers.

E 1237. *Proposed by Viktors Linis, University of Ottawa*

Let  $E$  be an ellipse,  $r_1$  and  $r_2$  focal radii,  $\alpha$  the angle between the focal radii, and  $ds$  the element of arc. Evaluate the integrals

$$\int_E ds / (r_1 r_2)^{1/2} \quad \text{and} \quad \int_E (\cos \alpha / 2) ds.$$