84.40 Reflections on Euclid's Algorithm
Author(s): A. F. Beardon
Source: *The Mathematical Gazette*, Vol. 84, No. 500 (Jul., 2000), pp. 294-296
Published by: The Mathematical Association
Stable URL: http://www.jstor.org/stable/3621668
Accessed: 24/03/2010 19:51

$$c_{2n+1} = 2c_{2n} + c_{2n-1}$$

$$c_{2n} = 2c_{2n-1} + c_{2n-2}.$$

From the last two equations, $2c_{2n+1} = 4c_{2n} + (c_{2n} - c_{2n-2})$. Substituting this into the first equation, we get $c_{2n+2} = 4c_{2n} + (c_{2n} - c_{2n-2}) + c_{2n}$ and so $v_{n+1} - 6v_n + v_{n-1} = 0$ is a recurrence relation for the square roots of all the square/triangular numbers.

Reference

1. T. Cross, Square-triangular numbers, *Math. Gaz.* **75** (October 1991), pp. 320-323.
2. H. Davenport, *The higher arithmetic: an introduction to the theory of numbers*, Hutchinson, London (1952).

DONALD KEEDWELL

Department of Mathematics and Statistics, University of Surrey, Guildford GU2 7XH

84.40 Reflections on Euclid's algorithm

Euclid's algorithm enables one to find the greatest common divisor of two numbers and solutions of linear Diophantine equations. The purpose of this short note is to draw attention to the fact that the algorithm operates on *pairs of integers*, and to emphasise this by rewriting it explicitly in these terms. An example will suffice to give the main ideas.

Consider the problem of solving the equation $58x + 11y = 1$. This is accomplished in the usual way from the equations

$$58 = 5 \times 11 + 3$$

$$11 = 3 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

(although the last equation is usually omitted). The algorithm can be displayed geometrically by representing each pair of integers (a, b) by a rectangle. In the example we are considering, the pair (58, 11) is represented by a 58-by-11 rectangle, which is then partitioned into five 11-by-11 squares and a residual 11-by-3 rectangle. This residual rectangle is now partitioned into three 3-by-3 squares, leaving a new residual rectangle of size 3-by-2. The process continues until there is no residual rectangle. Clearly, this graphical representation exactly mirrors the steps in the algorithm, and so perhaps makes the process more accessible to a younger audience. Articles written along these lines for upper secondary school students, together with an interactive computer program, can be found at http: //nrich.maths.org.

Working with the same example, we can also write

$$\begin{pmatrix}58\\11\end{pmatrix} = \begin{pmatrix}5 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}11\\3\end{pmatrix}$$
$$\begin{pmatrix}11\\3\end{pmatrix} = \begin{pmatrix}3 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}3\\2\end{pmatrix}$$
$$\begin{pmatrix}3\\2\end{pmatrix} = \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix} \qquad (1)$$
$$\begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}2 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix},$$

from which we obtain

$$\begin{aligned}\begin{pmatrix}1\\0\end{pmatrix} &= \begin{pmatrix}2 & 1\\1 & 0\end{pmatrix}^{-1}\begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}^{-1}\begin{pmatrix}3 & 1\\1 & 0\end{pmatrix}^{-1}\begin{pmatrix}5 & 1\\1 & 0\end{pmatrix}^{-1}\begin{pmatrix}58\\11\end{pmatrix}\\ &= \begin{pmatrix}0 & 1\\1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -5\end{pmatrix}\begin{pmatrix}58\\11\end{pmatrix}\\ &= \begin{pmatrix}4 & -21\\ * & *\end{pmatrix}\begin{pmatrix}58\\11\end{pmatrix},\end{aligned}$$

where * denotes a term that need not be computed. By equating the top rows in this last equation, we obtain the solution $x = 4$ and $y = -21$ of $58x + 11y = 1$. Observe that, as all matrices here have a determinant of 1 or -1, we can also write this as

$$\begin{pmatrix}58\\11\end{pmatrix} = \begin{pmatrix}4 & -21\\p & q\end{pmatrix}^{-1}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}q & 21\\-p & 4\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}, \text{ where } 21p + 4q = 1.$$

Thus the solution can be found simply by multiplying the matrices in (1) (instead of the usual repeated substitution and simplification).

This approach to Euclid's algorithm is simpler than (but equivalent to) the description of the algorithm in terms of continued fractions. An explanation of what follows can be found in almost any text that discusses continued fractions. Briefly, the expression

$$\begin{pmatrix}u\\v\end{pmatrix} = \begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$$

is the homogeneous form of the Möbius map

$$u/v = \frac{a(x/y) + b}{c(x/y) + d},$$

with the usual conventions regarding ∞. In the special case when $b = c = 1$ and $d = 0$ this reduces to

$$u/v = a + \frac{1}{x/y},$$

and the composition of such maps (which corresponds to the product of the matrices) leads directly to continued fractions. In our example we have

$$\frac{58}{11} = 5 + \frac{1}{11/3} = 5 + \cfrac{1}{3 + \cfrac{1}{3/2}} = 5 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2}}}$$

In fact, the columns of the successive matrix products are the convergents of the continued fraction expansion for 58/11, as can be seen from the calculations

$$\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 16 & 5 \\ 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 21 & 16 \\ 4 & 3 \end{pmatrix},$$

and

$$5 + \frac{1}{3} = \frac{16}{3}, \quad 5 + \cfrac{1}{3 + \cfrac{1}{1}} = \frac{21}{4}.$$

A. F. BEARDON

DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB

84.41 An interesting conjecture

The column vector $\mathbf{v} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ is called a Diophantine triplet if each of $ab + 1$, $bc + 1$, $ca + 1$ is a perfect square. Take the matrix $A = \begin{pmatrix} 0 & \frac{1}{2} & 0 \\ 0 & 0 & 2 \\ -1 & \frac{3}{2} & 3 \end{pmatrix}$ and the vector $\mathbf{v}_0 = \begin{pmatrix} 0 \\ 2 \\ 4 \end{pmatrix}$. Define the $\mathbf{v}_i (i = 1, 2, 3, \dots)$ by $\mathbf{v}_i = A\mathbf{v}_{i-1}$. Then we conjecture that $\mathbf{v}_i$ is a Diophantine triplet for all non-negative integers i. This has been verified for many values of i. Perhaps an interested reader could supply a proof (or counter-example) of this conjecture.

M. N. DESHPANDE

Institute of Science, Nagpur 440001, India

Editor's Note

Consider the set of vectors of the form $\mathbf{v} = \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 2t - \alpha \\ 2t \\ 2t + \alpha \end{pmatrix}$ where t and α are integers such that $1 + 3t^2 = \alpha^2$. Then

$$\begin{pmatrix} ab + 1 \\ bc + 1 \\ ac + 1 \end{pmatrix} = \begin{pmatrix} 4t^2 - 2\alpha t + 1 \\ 4t^2 + 2\alpha t + 1 \\ 4t^2 - \alpha^2 + 1 \end{pmatrix} = \begin{pmatrix} t^2 - 2\alpha t + \alpha^2 \\ t^2 + 2\alpha t + \alpha^2 \\ t^2 \end{pmatrix} = \begin{pmatrix} (t - \alpha)^2 \\ (t + \alpha)^2 \\ t^2 \end{pmatrix},$$