Teaching Notes

The extended Euclidean Algorithm made easy

The Euclidean algorithm [1] calculates the greatest common divisor (GCD) of two integers a and b. A theorem by Bézout and Bachet asserts that this GCD can be written as a linear combination of a and b:

$$\mathrm{GCD}\,(a,\,b)\;=\;x\,\times\,a\,+\,y\,\times\,b$$

with x and y integers. The extended Euclidean Algorithm calculates GCD (a, b) and also x and y. One of the implementations of this algorithm is due to Donald Knuth [1, 2]. It works just fine if you use a computer, but if you want to do the calculations by hand this is not the method to use.

In this Note we look at an alternative that is easier to use on a blackboard (with chalk). We start with an example: GCD(1239,735). At the left you see the Euclidean algorithm in action. The GCD is 21 and is in the box just above the one with the zero. At the right the value of y is determined. The structure of the Euclidean algorithm at the left (without the last equation) is copied, but with the boxes empty. The values in the grey boxes are then calculated starting from the 0 and the 1s in the top right corner. The arrows tell you how. The value of y is the last one calculated. If the number of equations is odd, a minus sign has to be added.

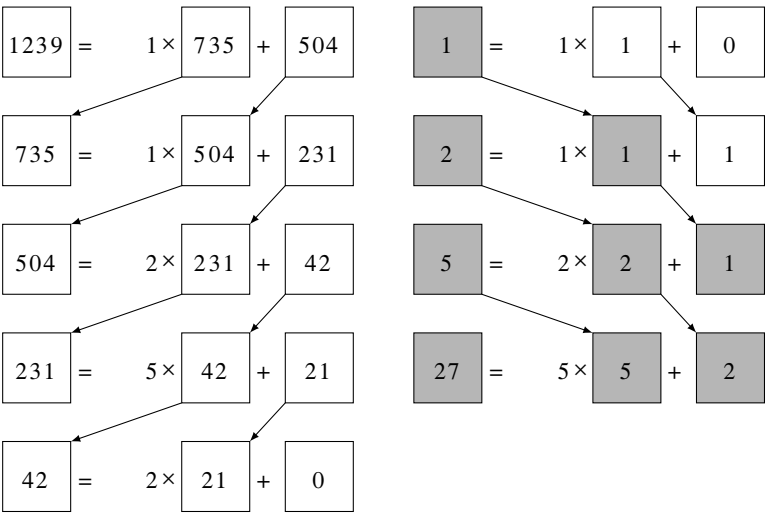


FIGURE 1

Hence here we have: $y\;=\;27$. From

$$x\,\times\,1239\,+\,27\,\times\,735\;=\;21$$

it is now easy to calculate x:

$$x\;=\;\frac{21\;-\;27\,\times\,735}{1239}\;=\;-16.$$

https://doi.org/10.1017/mag.2016.25 Published online by Cambridge University Press

Why does this work? Let us write out the equations for the general case:

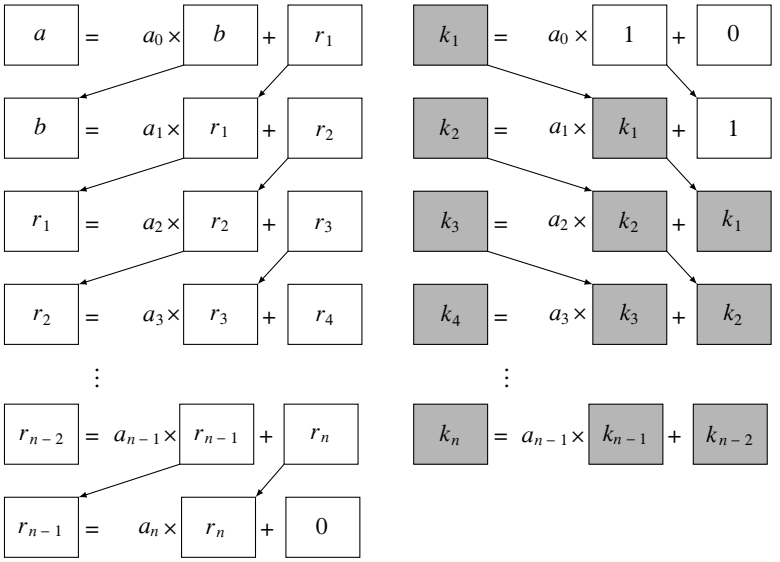


FIGURE 2

In this case we have that GCD $(a, b) = r_n$. Note that since r_1 is a linear combination of a and b, the same is true for r_2 (just replace r_1 in the second equation by its value obtained from the first equation), and for r_3 and so on.

The terms of the sequence k_i that are calculated at the right (starting with $k_{-1} = 0$ and $k_0 = 1$), keep score of the multiple of b contained in r_i. We have in general:

Theorem: The remainder r_i $(i = 1, \ldots, n)$ in the Euclidean algorithm applied to a and b satisfies

$$r_i = x_i \times a + (-1)^i k_i \times b$$

for some integer x_i and with k_i $(i = 1, \ldots, n)$ the solution of the recurrence relation

$$k_i = a_{i-1}k_{i-1} + k_{i-2}, \qquad k_{-1} = 0, k_0 = 1.$$

Proof: (Adapted from [1].)

This is easily proved using induction. It is clearly true for $i = -1$ (assuming that $r_{-1} = a$) and $i = 0$ (with $r_0 = b$). Now assume it is true for r_{i-2} and r_{i-1}. Then from

$$r_{i-2} = x_{i-2} \times a + (-1)^{i-2} k_{i-2} \times b \text{ and } r_{i-1} = x_{i-1} \times a + (-1)^{i-1} k_{i-1} \times b$$

we find that

$$r_i = r_{i-2} - a_{i-1} \times r_{i-1} = \left(x_{i-2} - a_{i-1}x_{i-1}\right) \times a + (-1)^i \left(k_{i-2} + a_{i-1}k_{i-1}\right) \times b.$$

https://doi.org/10.1017/mag.2016.25 Published online by Cambridge University Press

Since $k_{i-2} + a_{i-1}k_{i-1} = k_i$, this finishes the proof (with $x_i = -a_{i-1}x_{i-1} + x_{i-2}$).

Hence if we want to find values x and y for which

$$\mathrm{GCD}\,(a, b) = x \times a + y \times b$$

it follows from

$$r_n = \mathrm{GCD}\,(a, b) = x_n \times a + (-1)^n k_n \times b$$

that $y = (-1)^n k_n$ and $x = x_n = \frac{1}{a}\left(\mathrm{GCD}\,(a, b) - (-1)^n k_n \times b\right)$ provide a solution.

You might want to try this example: $\mathrm{GCD}\,(766,\ 240) = 2$. Don't forget the minus sign!

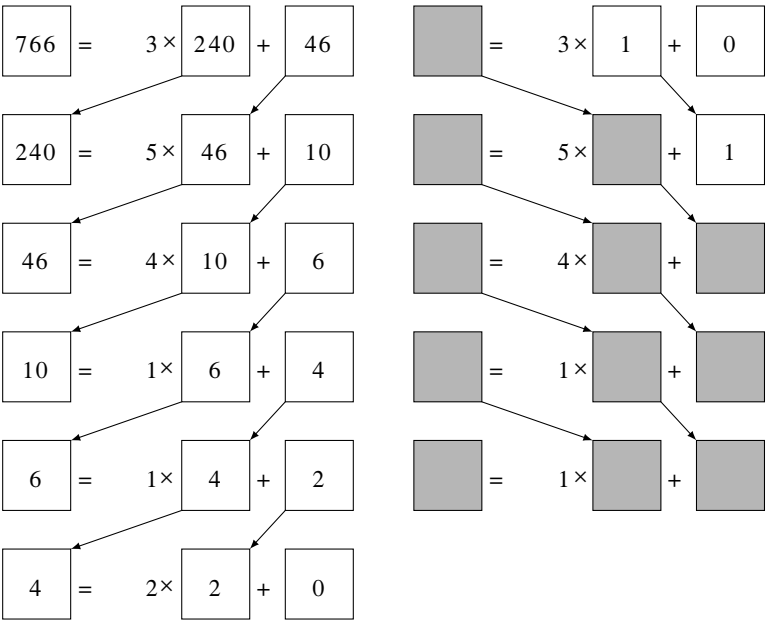


FIGURE 3

References

1. K. H. Rosen, *Elementary number theory and its applications* (4th edn.), Addison-Wesley Longman, Reading MA (2000).
2. D. Knuth, *The art of computer programming*, *Volume* 2: *seminumerical algorithms* (3rd edn), Addison-Wesley Longman, Boston MA (1998).

doi:10.1017/mag.2016.25

PAUL LEVRIE[1] and RUDI PENNE[2]

[1,2]*Faculty of Applied Engineering, University of Antwerp, B-2660 Hoboken, Belgium*

[1]*Department of Computer Science, KU Leuven, B-3001 Heverlee, Belgium*

e-mail: *paul.levrie@cs.kuleuven.be*

https://doi.org/10.1017/mag.2016.25 Published online by Cambridge University Press