

How to Implement Euclid's Algorithm

I am going to write these notes on how to implement Euclid's algorithm on a spreadsheet. I think it's easier than Prof. Kleitman's implementation, but I don't want to change his notes because he'll be teaching from them next year, and he might not agree with me. In the simple version of Euclid's algorithm, where we just want to find the greatest common divisor (gcd), we agree on how to implement it. You start by making a column containing the two numbers A and B that you want to find the greatest common divisor of. You then obtain the i^{th} iterate by dividing the $(i-2)^{\text{nd}}$ iterate by the $(i-1)^{\text{st}}$ iterate. Eventually, the numbers in the first column will hit zero. The number just before that will be the gcd of A and B. We now want to find two integers α and β so that

$$\alpha A + \beta B = \text{gcd}(A,B).$$

You can find α and β by going to the last column and working backwards. But I think it's easier to construct a spreadsheet that finds them by working down from the top. Here is an example:

	D	E	F	G
7	iterate	ratio	$\alpha A +$	βB
8	8721		1	0
9	5593		0	1
10	3128	1	1	-1
11	2465	1	-1	2
12	663	1	2	-3
13	476	3	-7	11
14	187	1	9	-14
15	102	2	-25	39
16	85	1	34	-53
17	17	1	-59	92
18	0	5	329	-513

We started off by putting A and B in cells D8 and D9. We then put $\text{int}(D8/D9)$ in cell E10, and $D8-E10*D9$ in cell D10. Copying D10 and E10 down to lower rows will give you the gcd in column D, in the row before the value hits 0. If you don't need to find the inverse of A mod B, this is good enough. In fact, we could easily have done it using just one column by using the single instruction $\text{mod}(D8,D9)$. I didn't do this because I actually want to use the 'ratio' column elsewhere in the spreadsheet to help compute columns F and G, and once you have it, there's no point in not using it to compute column D.

What we are doing in the two columns F and G is keeping track of the integers so that, say, $A*F13 + B*G13 = D13$. How do we do that? We start in rows 8 and 9 with the values 1, 0 and 0, 1. These are the right values to start out with, because $A*1 + B*0 = D8 = A$, and $A*0 + B*1 = D9 = B$. In subsequent rows, we get columns F and G by subtracting the same multiple of the $(k-1)^{\text{st}}$ row from the $(k-2)^{\text{nd}}$ row that we used for column D. (This is the multiple from column E.) Thus, we always maintain the equation

$$A*F_r + B*G_r = D_r,$$

where r stands for the row number. In the row when column D hits 0, we get B/gcd and A/gcd in columns B and G. That is, for our example, $329*A - 513*B = 0$, so $329 = B/17$ and $513 = A/17$. The row before this row gives numbers α and β so that $\alpha*A + \beta*B = \text{gcd}$. For our example, $-59*A + 92*B = 17$. If the gcd is 1, this

row before the last row (where column D hits 0) will give the values $A^{-1} \bmod B$, and $B^{-1} \bmod A$, although you do will think to make sure you get their signs right. We will use these to implement the RSA algorithm.

If you keep on going after the 18th row in our example, what happens in the 19th row is that you divide by zero, which means your spreadsheet fills with ugly symbols. There generally isn't any way of predicting how many iterations Euclid's algorithm is going to take in advance, so if you don't want to divide by zero, what you will need to do is use an IF statement to avoid it. Alternatively, you could leave the divide by zeros and use an IF statement to pick out the first zero in column D, which tells you that the row above contains the gcd and the α and β that you are looking for. There are lots of fairly easy ways of doing this. I wasn't able to come up with any particularly nice one, so I'll let you figure out how to do it on your own. If you use the `mod(D8,D9)` statement in cell D10, and copy it down, you have the same problem with dividing by 0, and again you have to figure out some way of picking out the right row.