

## The GCD algorithm

Given  $m,n$  find  $\gcd(m,n)$

We proved in class that the gcd can be found by repeatedly applying the division algorithm:  $a = bq + r$ . We start with  $a=m, b=n$ . The next pair is  $(b,r)$  [the quotient is not needed here]. We continue replacing  $a$  by the divisor and  $b$  by the remainder until we get a remainder 0. The last non-zero remainder is the gcd.

This algorithm can be performed on a spreadsheet:

	A	B	C
1	<b>m</b>	<b>n</b>	
2	123456	654321	
3	<b>a</b>	<b>b</b>	<b>r</b>
4	123456	654321	123456
5	654321	123456	37041
6	123456	37041	12333
7	37041	12333	42
8	12333	42	27
9	42	27	15
10	27	15	12
11	15	12	3
12	12	3	0
13	3	0	#DIV/0!
14	0	#DIV/0!	#DIV/0!

	A	B	C
1	<b>m</b>	<b>n</b>	
2	<b>123456</b>	654321	
3			
4	<b>=A2</b>	=B2	=MOD(A4,B4)
5	<b>=B4</b>	=C4	=MOD(A5,B5)
6	<b>=B5</b>	=C5	=MOD(A6,B6)
7	<b>=B6</b>	=C6	=MOD(A7,B7)
8	<b>=B7</b>	=C7	=MOD(A8,B8)
9	<b>=B8</b>	=C8	=MOD(A9,B9)
10	<b>=B9</b>	=C9	=MOD(A10,B10)
11	<b>=B10</b>	=C10	=MOD(A11,B11)
12	<b>=B11</b>	=C11	=MOD(A12,B12)
13	<b>=B12</b>	=C12	=MOD(A13,B13)
14	<b>=B13</b>	=C13	=MOD(A14,B14)

Once row 5 is entered, it is copied to all lower rows. The spreadsheet automatically updates the formulas (that is what spreadsheets do!). A new pair of numbers can be entered in A2 and B2. Note that when a zero remainder occurs, the spreadsheet gives an error message on the following line.

We can produce a more economical version of this by using only one column: the column of remainders.

12345	m
54321	n
12345	
4941	
2463	
15	
3	
0	
#DIV/0!	
#DIV/0!	

12345	m
54321	n
=MOD(A2,A3)	
=MOD(A3,A4)	
=MOD(A4,A5)	
=MOD(A5,A6)	
=MOD(A6,A7)	
=MOD(A7,A8)	
=MOD(A8,A9)	
=MOD(A9,A10)	

The formula is entered in the 3<sup>rd</sup> row and copied to the rows below.

### Extended GCD algorithm

Given  $m, n$  find  $A, B$  so that  $\text{gcd}(m, n) = Am + Bn$

Set up a spreadsheet as follows. The numbers  $m$  and  $n$  in cells A3 and B3 can be changed for different problems -- the rest of the spreadsheet does calculations based on what is in these cells.

	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
<b>1</b>					
<b>2</b>	<i>m</i>	<i>n</i>			
<b>3</b>	12345	54321			
<b>4</b>	<i>A</i>	<i>B</i>	<i>rem</i>		<i>quot</i>
<b>5</b>	1	0	=A3		
<b>6</b>	0	1	=B3		=INT(C5/C6)
<b>7</b>	=A5-E6*A6	=B5-E6*B6	=C5-E6*C6		=INT(C6/C7)

Now copy and paste row 7 as many times as you wish to rows 8, 9, .... Notice that the formulas adjust themselves.

Here is an example with  $m=12345$  and  $n=54321$

	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
<b>1</b>					
<b>2</b>	<i>m</i>	<i>n</i>			
<b>3</b>	12345	54321			
<b>4</b>	<i>A</i>	<i>B</i>	<i>rem</i>		<i>quot</i>
<b>5</b>	1	0	12345		
<b>6</b>	0	1	54321		0
<b>7</b>	1	0	12345		4
<b>8</b>	-4	1	4941		2
<b>9</b>	9	-2	2463		2
<b>10</b>	-22	5	15		164
<b>11</b>	3617	-822	3		5
<b>12</b>	-18107	4115	0		#DIV/0!
<b>13</b>	#DIV/0!	#DIV/0!	#DIV/0!		#DIV/0!

Notice that the last non-zero remainder (Column C) is 3. So  $\text{gcd}(m,n)=3$ .

**One can prove that**  
 $A_k * m + B_k * n = C_k$

In this case the numbers on line 12 show give the result  
 $3 = (3617)m + (-822)n$

In the spreadsheet we have retained all the A, B, r and q that arise in the calculation. When writing a computer program to perform this calculation we note that each row depends only on the two previous rows. We do not have to store all the A, B, r -- just the most recent two values of each. This makes the program a bit harder to understand than the spreadsheet.

We will use variables  $A_0, B_0,$  and  $r_0$  to represent the previous values,  $A_1, B_1$  and  $r_1$  to represent the current values, and q to represent the current quotient.

**Program:** Extended Greatest Common Divisor (EGCD)

**Input:** positive integers m,n

**Output:** integers A, B ,g  
 so that  $g=\text{gcd}(m,n)$  and  $Am+Bn=g$

**Initialization:**  $A_0:=1, B_0:=0; r_0:=m$   
 $A_1:=0, B_1:=1; r_1:=n$

While  $r_1 \neq 0$  do  
 % Loop invariant:  $A_i m + B_i n = r_i$   
 $q:=\text{quot}(r_0,r_1)$   
 $\text{temp} := A_0 - A_1 * q, A_0:=A_1, A_1:=\text{temp};$   
 $\text{temp} := B_0 - B_1 * q, B_0:=B_1, B_1:=\text{temp};$   
 $\text{temp} := r_0 - r_1 * q, r_0:=r_1, r_1:=\text{temp};$

Return  $A:=A_0, B:=B_0, g:=r_0$