Math 103A – Winter,2001
Professor John J Wavrik

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	**m**	**n**	
2	123456	654321	
3	**a**	**b**	**r**
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	**m**	**n**	
2	**123456**	654321	
3			
4	**=A2**	=B2	=MOD(A4,B4)
5	**=B4**	=C4	=MOD(A5,B5)
6	**=B5**	=C5	=MOD(A6,B6)
7	**=B6**	=C6	=MOD(A7,B7)
8	**=B7**	=C7	=MOD(A8,B8)
9	**=B8**	=C8	=MOD(A9,B9)
10	**=B9**	=C9	=MOD(A10,B10)
11	**=B10**	=C10	=MOD(A11,B11)
12	**=B11**	=C11	=MOD(A12,B12)
13	**=B12**	=C12	=MOD(A13,B13)
14	**=B13**	=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 3rd row and copied to the rows below.

Extended GCD algorithm

Given m,n find A,B so that 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.

	A	B	C	D	E
1					
2	*m*	*n*			
3	12345	54321			
4	*A*	*B*	*rem*		*quot*
5	1	0	=A3		
6	0	1	=B3		=INT(C5/C6)
7	=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

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

Notice that the last non-zero remainder (Column C) is 3. So 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=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 <> 0 do
% Loop invariant: $A_i m + B_i n = r_i$
q:=quot(r_0,r_1)
temp := A_0-A_1*q, A_0:=A_1, A_1:=temp;
temp := B_0-B_1*q, B_0:=B_1, B_1:=temp;
temp := r_0-r_1*q, r_0:=r_1, r_1:=temp;

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