MATH 2590 - ASSIGNMENT 4

NOVEMBER 9, 2010

It is easy to make a multiplication table from modular arithmetic using a spreadsheet. If you want an easy to use spreadsheet program go to “Google Documents” (GD) and create a new spreadsheet document. Now to create a multiplication table say $(mod\ 13)$ (1) make sure that the first row isn’t blocked off as a header (for GD, go to Tools → Freeze Rows → No frozen rows) (2) in the A1 cell enter the formula “`=mod( row(A1)*column(A1), 13)`” (3) copy this formula (4) highlight a 13×13 square and paste.
If you are using Excel or Open Office or something similar you should (3) highlight the A1 cell and 12 cells below then select “Fill Down” from the edit menu and (4) then highlight a 13×13 square and then “Fill Right” from the edit menu.

(1) Make multiplication tables $(mod\ 13)$, $(mod\ 14)$, $(mod\ 15)$, $(mod\ 16)$, $(mod\ 17)$. You might want to do this on a new ‘sheet’ or ‘tab’ on your spreadsheet document. Make sixteen observations about patterns that you see in these tables. Try to make those observations as general as possible and apply to as many of the tables as possible. How do the $(mod\ 13)$ and $(mod\ 17)$ tables (which are prime numbers) differ from $(mod\ 14)$, $(mod\ 15)$, $(mod\ 16)$ (which are composite)?

(2) We say that the order of an a number a $(mod\ m)$ is the number of times you have to multiply a by itself $(mod\ m)$ in order to get to 1. Find the following orders of elements:
   (a) Order of 2 $(mod\ 13)$
   (b) Order of 3 $(mod\ 13)$
   (c) Order of 5 $(mod\ 13)$
   (d) Order of 3 $(mod\ 14)$
   (e) Order of 5 $(mod\ 14)$
   (f) Order of 2 $(mod\ 17)$
   (g) Order of 3 $(mod\ 17)$
   (h) Order of 5 $(mod\ 17)$
   (i) what patterns do you observe in this question?

(3) In last question I didn’t ask (for instance) for the order of 2 $(mod\ 14)$ or the order of 3 $(mod\ 15)$. Explain what goes wrong and why.

(4) Say that true is 1 and 0 is false. Recall that in the first homework I asked you to do a few calculations with the operations of AND, OR, XOR and $IMPL$ and NOT. They had the following truth tables (which I am stating now with 1’s and 0’s).

Date: due November 23, 2010.

A	B	A AND B	A OR B	A IMPL B	A XOR B	NOT A
1	1	1	1	1	0	0
1	0	0	1	0	1	0
0	1	0	1	1	1	1
0	0	0	0	1	0	1

Find a formula for A AND B, A OR B, A IMPL B, A XOR B, and NOT A in terms of A, B, ×, + $(\mathit{mod}\ 2)$. Example: A AND B $\equiv$ A × B $(\mathit{mod}\ 2)$.

(5) Calculate 17^{33} $(\mathit{mod}\ 113)$ using your spreadsheet. What problems do you have doing this? Why? How do you fix it?

(6) A bank IBAN number can be easily 28 digits or more. Bank programs do this using simple properties of modular arithmetic to simplify their calculations and they use nothing more sophisticated than a spreadsheet. Use your spreadsheet to calculate the following:

(a) 12938749582374593845 $(\mathit{mod}\ 97)$
(b) 12938749528374593845 $(\mathit{mod}\ 97)$
(c) 349503840529334502394 $(\mathit{mod}\ 97)$
(d) 349503840529384502394 $(\mathit{mod}\ 97)$
(e) 349587239457230495872394587239457 $(\mathit{mod}\ 97)$
(f) 349587239457234095872394587239457 $(\mathit{mod}\ 97)$