MAT331 - Project 2 - Modular arithmetic

If you add to numbers or multiply two numbers, whether or not the answer is even or odd only depends on whether the numbers you started with are respectively even or odd. This leads into "periodic" or modular arithmetic, which is the topic of this project.

You can divide your work into an annotated worksheet and a spreadsheet (the spreadsheet must contain one sheet for question, for instance, one sheet for the multiplication table of p, another sheet for the multiplication table of n.). Some parts of this project are easier to do in Maple (like i or ii) but the multiplication and addition tables require a spreadsheet. You should choose the most appropriated format in each case. Remember that it is not necessary to write down Maple explanations, only mathematics explanations.

1 The wiki

(Extra credit but *strongly encouraged* to work on it): You can add or edit one aspect of one relevant entry to the wiki. An aspect of an entry might be the definition, examples, proofs, applications... Don't be shy and write! Make sure that you write about something you understand in your own words. Mathematical formulae can be added by using "Equation editor" which can be found by click the $\sum$ symbol in the right of the panel, next to the smiling face. (You start by click *view* in the wiki, and then *edit* on the right. Do not forget to save your work at the end.)

Possible entries are

(1) prime number

(2) composite number

(3) division algorithm

(4) remainder (of the division algorithm)

(5) quotient (of the the division algorithm)

(6) cryptography

(7) modular arithmetic

(8) unit

(9) multiplicative order

(10) multiplicative inverse

(11) primitive root

(12) coprime (or relatively prime)

(13) Multiplicative group of integers modulo n, where n is a positive integer

(14) Additive group of integers modulo n, where n is a positive integer.

(15) Ring of integers modulo n.

(16) Perfect numbers.

2 The project

You are given (in Blackboard) two numbers, n and p.

(i) Divide n into $1, 2, \ldots\ldots$ and 150, but just write down the remainder in each case. Is there a pattern? (You can use the maple command to compute remainders but perform the step by step computation on 150, 60 and 6). Note: You have to write down the reminders of dividing 1 by n, 2 by $n \ldots$,150 by n.

(ii) List all the numbers between 0 and 150 with remainder 10. What can you say about the difference of two numbers on your list?

(iii) List all the numbers between 0 and 150 with remainder 3. What can you say about the difference of two numbers on your list?

(iv) Can you generalize the results for the list of numbers with remainder 3 and the list of numbers with reminder 10 to list of numbers with any remainders? Justify your generalization.

(v) Add each of the numbers with remainder 10 by each of the numbers with remainder 3. Compute the remainder of dividing each of the sums by n. Explain the result. (Use the spreadsheet command to compute reminders, but again, give a step by step explanation of two or three particular cases in your Maple worksheet.)

(vi) Multiply each of the numbers with remainder 10 by each of the numbers with remainder 3. Compute the remainder of dividing each of the products by n. Explain the result. (Use the spreadsheet command to compute reminders, but again, give a step by step explanation of three particular cases in your Maple worksheet.)

(vii) The addition and multiplication above can be generalized to lists of numbers with other remainders. Explain how to do it with some examples. Extra credit: Explain it in general.

(viii) For $\mathbb{Z}/n\mathbb{Z}$ (that is for all possible remainders of dividing by n),

   (a) compute the addition tables,

   (b) multiplications tables,

   (c) a list of the units, (see http://mathworld.wolfram.com/Unit.html, Wikipedia or our Wiki for definition of unit. Make sure you understand what a "multiplicative inverse" means)

   (d) the (multiplicative) order of the elements, (look for definition as in (c))

   (e) some equations with no solutions and some equations with solutions. (Example, in $\mathbb{Z}/6\mathbb{Z}$, $3x \equiv 1 \pmod 6$ has no solution and $x^2 \equiv -2 \pmod 6$ has solution)

(ix) For each number a between 0 and n, compute the remainder of dividing a^n by n. Describe and explain any pattern you found.

(x) For each number a between 0 and n, compute the remainder of dividing a^{n-1} by n. Describe and explain any pattern you found.

(xi) Repeat (i) to (x) of the above replacing n by p.

Extra credit: Work even more in the Wiki. If you started working on the topics I posted earlier, you are welcome to continue (let me know what are you working on so there will be no overlap with Project 3). If you did not start, just concentrate in the wiki for extra credit.