MAT331 - Project 2 - Modular arithmetic

Possible entries are

(1) congruence

(2) composite number

(3) division algorithm (done)

(4) remainder (of the division algorithm)

(5) quotient (of the the division algorithm)

(6) unit (done)

(7) multiplicative order

(8) multiplicative inverse

(9) primitive root

(10) coprime (or relatively prime)

(11) Perfect numbers.

(12) Divisor

(13) Least Common Multiple

(14) Greatest Common Divisor.

(a) Chinese Remider Theorem.

(b) Finite Field.

(c) Euler′s totient function.

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

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

(f) Ring of integers modulo n.

(g) cryptography

(h) modular arithmetic. http://www.math.rutgers.edu/ erowland/modulararithmetic.html

(i) Modular exponentiation

1 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 with remainder 10. What can you say about the difference of two numbers on your list?

(iii) List all the numbers 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.