HW 07 CMSC/MATH/ENEE 456. Morally DUE Nov 9

1. (0 points but you MUST hand this in)
   (a) What DAY and TIME are the TIMED FINAL?
   (b) IF that DAY/TIME is not good for you then EMAIL ME.
   (c) We are NOT meeting the Tuesday of Thankgiving. When is the make-up lecture?

GOTO NEXT PAGE

2. (25 points) Let a_1, a_2, a_3 be such that every pair a_i, a_j are relatively prime. Show that

$$\phi(a_1 a_2 a_3) = \phi(a_1)\phi(a_2)\phi(a_3).$$

(You may use that if a, b are rel prime then $\phi(ab) = \phi(a)\phi(b)$.)

GOTO NEXT PAGE

3. (25 points) Let p be a prime and $a \geq 1$. Find and prove a formula for $\phi(p^a)$.

GOTO NEXT PAGE

4. (25 points) Using the answers to the last two problems, compute by hand:

$$\phi(3528).$$

(You can use a calculator for mult, division and addition only. The key thing is you have to show work and show how you are using the last two problems.)

GOTO NEXT PAGE

5. (25 points) In this problem we will use a version of Pollards $p-1$ suitable for hand calculation to factor 143. (You CAN use a calculator or Wolfram Alpha or write a program or use a slide rule or an abacus or your fingers or your fingers and toes.)

   For $(x,y) = (0,1),(1,0),(0,2),(1,1),(2,0),(0,3),(1,2),(2,1),(3,0),\ldots$

   (a) Compute $M = 2^x 3^y$.

   (b) Compute $d = GCD(2^M - 1 \bmod 143, 143)$. (This is new for you. In class we just used $GCD(2^M - 1, N)$ to factor N; however, $2^M - 1$ can get very large, and $GCD(a,b) = GCD(a \pmod b, b)$ so we mod down to keep the numbers small. I have NOW included this in the slides on Pollard $p-1$.)

   (c) If $d \neq 1$ and $d \neq 143$ then output d (it should be a factor of 143) and BREAK OUT of the for loop.

   Your answer should show all work, even work that didn't give a factor. So the line for (1,2) looks like this:

   $(x,y) = (1,2)$: $M = 2^1 \times 3^2 = 18$. $d = GCD(2^{18} - 1 \pmod{143}, 143) = GCD(24, 143) = 1$. Didn't get a factor. Darn!

   Wolfram Alpha Tip If you type in, for example,

   $$GCD(2^{23} - 1, 143)$$

   it will think you mean

   $GCD(2^{23} - 1143)$ and return 8387465 which I assume IS $2^{23} - 1143$.

   So you need to type in

   $$GCD(2^{23} - 1, 143)$$

   where there is a space after the comma.