Take-Home Test 6

Due: Thursday, December 3

Solo – No Collaboration Allowed

On this test, your work is to be your own with no consultation with any other person (in this class or not) except for the instructor. Feel free to ask me any questions. I won't give you any answers to the exercises but will be happy to try to clarify any confusion you may have, probably by asking you more questions. You may feel free to use any written references or books, just not any consultation with any persons. Be sure to acknowledge any written or internet sources you use.

As usual, you will be graded both on mathematical content and on clarity of expression. Points for this test are distributed as follows: Exercise 1 is worth a maximum of 14 points, Exercise 2 is worth a maximum of 16 points, and Exercises 3 and 4 are worth a maximum of 15 points each. Some of the questions are a bit open-ended, so be creative, make conjectures, and back up your assertions by providing proofs or counter-examples. In writing your answers, use complete sentences (with punctuation!) and be sure to say exactly what you mean. Papers will be graded on the basis of what you have written, so be sure to take the time to express yourself clearly. If you are stuck on a problem and have no idea where to begin, a good way to get started is to look at lots of specific examples and try to find a pattern.

Exercises:

(1) More fun with the Euler ϕ function.
   (a) How many positive integers are less than 3600 and relatively prime to 3600? Explain your answer.
   (b) How many positive integers are less than 7200 and relatively prime to 3600? Completely justify your answer.
   (c) Let m and n be positive integers which are relatively prime. Prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

(2) An investigative reporter came across the following message recently:

1214 0556 3545 4089 1604 1128 1631 0313 3205 1004 1490 3646

She says that she was told it was encoded using something called *RSA public key cryptography* with keys $e = 3299$ and $n = 4171$. She has no idea what this means. Can you decode it for her? Be sure to explain exactly what you did to decode the message. (To save time, it may be helpful to use a calculator or computer which can handle a large number of digits, although you can do this problem with nothing more than a TI-86. Incidentally, the 'mod' function on the TI-86 is highly erratic and may not give you the correct answer, so be careful!)

(3) Show that 3277 is a strong pseudo-prime (i.e., passes *Miller's Test*) to the base 2 but not to the base 3. Explain why this means that 3277 is composite, and find the complete prime factorization of 3277 into primes.

(4) A *Carmichael number* is a composite integer n such that $a^n \equiv a \pmod{n}$ for every integer a. The smallest Carmichael number is 561.

(a) Show that 1105 is a Carmichael number. Carefully explain your solution and quote any results you use.

(b) Suppose that for some positive integer k, the numbers $p = 6k + 1, q = 12k + 1$ and $r = 18k + 1$ are all primes. Set $n = pqr$. Show that n is a Carmichael number. Be sure to carefully justify each step of your argument.

(c) By using the result of part (b) and the integers $1, 2, \ldots, 10$ for k, how many Carmichael numbers can you construct? (Note that you can do this without having the solution to part (b); you just need the statement of part (b).)

Statement of Sources: As this was a "Solo" exam, you shouldn't have talked with anyone besides the instructor about this exam. Please write the following statement on your exam, and sign your name:

I have neither given nor received any help on this exam.

Also, if you used any references besides the class notes, list them as well.