MATH 371 – Homework assignment 3 – September 13, 2013

An unusual assignment

This week, rather than the standard problem set, I've got a programming project for you to do. You'll be able to use the Maple I wrote as a template for parts of it (let me know if you would like me to put an html version of the Maple on my webpage so you can see t, in case you don't have access to Maple). But you'll have to do some additional programming and maybe a little adaptation.

You may use any computer language you like – we'll want to see the program code and the output (we can at least check the output).

There are two problems we'd like you to solve using your programs:

1. (a) Write a program to test whether a number N is a strong pseudoprime (i.e., a Miller-Rabin liar) relative to a base b). This is essentially what the procedure called "MR" in my Maple worksheet does. Make sure to use the second version (and write the subroutine that calculates $b^u \bmod N$ the smart way, so you can use your program on very large numbers. Use it to test whether the number 1234567890123456789012345678901234567890 is a strong pseudoprime relative to the base 1357913579.

(b) Implement the full Miller-Rabin test (that chooses a bunch of random bases to test a number N for primality), which is called "MRtest" in my Maple worksheet. Use your program to find the first prime number bigger than 1234567890123456789012345678901234567890. (You might automate the searching process, while you're at it).

2. (a) Write a program that uses the Euclidean algorithm to find the gcd of two numbers.

(b) Use the programs from 1(a) and 2(a) and the characterization of Carmichael numbers given in the notes to find a Carmichael number bigger than 10^6. Bonus points for finding one bigger than 10^9.

And two regular problems:

These are from Brett's problem sheet from Wednesday:

3. Prove that $\lim_{n\to\infty} \varphi(n) = \infty$ by proving that for each m there are only finitely many n with $\varphi(n) = m$.

4. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Prove that, given any integer a, we can find integers $a_1, a_2, \ldots, a_r$ so that $\frac{a}{n} = \frac{a_1}{p_1^{e_1}} + \frac{a_2}{p_1^{e_2}} + \cdots + \frac{a_r}{p_1^{e_r}}$. The analogous statement for polynomials is the partial fraction decomposition you learned in calculus.