Math 5248: Cryptology and Number Theory

HW 5 (Due Earth Day, Wednesday April 22nd, 2015)

Professor: Gregg Musiker

Remark: For this Problem Set, a computer algebra package such as the publically available Wolfram Alpha or Sagecell will be useful. If you have questions, let me know. You can access them from the course website for example: `http://www.math.umn.edu/~musiker/5248/`.

Remark: For problems where you use a computer algebra package for part of the exercise, please include a print-out or summary of your code/output in your assignment.

1) Problem 18.3.1 in Garrett.

2) Use Pocklington-Lehmer to prove that 42037293843489353 is prime.

   Note: For the purposes of this problem, you may use a computer algebra package to exponentiate mod p (you do not need to use successive squaring) and for computing gcd's but **do not use** the computer to check primality as this would defeat the purpose of the exercise.

   Hint: If done correctly, you will iterate Pocklington-Lehmer a few times, **your first step** will most likely involve factors of 499 and 13763, and your last step will most likely involve factoring 1470 into primes, which can be done by hand.

3) Use Proth's corollary to Pocklington-Lehmer to prove that $p = 138241$ is prime.

   Hint: Factoring $p - 1$ should be fairly straightforward in this case.

4) Problem 9.6.6 in Garrett.

5) Problem 10.5.1 in Garrett.

6) Problem 12.5.6 in Garrett.

7) Problem 12.5.7 in Garrett.

8) Consider the RSA modulus

$$n = 1079043987457248913347867451870185465017558074243010743 99$$

with encryption exponent $e = 65$.

Using $A \to 00$, $B \to 01$, $\ldots$, $Z \to 25$, and concatenating (for example, $CAT \to 020019$) create a message as a number with less than 56 digits. Then using a computer algebra package (e.g. Sage or Wolfram Alpha, etc.) encrypt your message and email it to `musiker@math.umn.edu` with the subject line 5248 Homework 5.