CSC 5451, Professor E. Gethner
Assignment 5 (last one!)
5 November 2015
Quiz 5 is in class on Thursday 19 November 2015

Please feel free to collaborate with one another on this assignment. Consider writing up the solutions on your own for quiz practice. **Important information regarding the quiz: be neat, write complete sentences, and show all of your work. The way you communicate the solution to your answer is as important as the answer itself.**

1. **(Decipher this Secret Message)** $4_2 5_2 2_1 7_3 7_1 4_1 7_1 4_3 9_3 8_3 8_1 4_3 4_2 6_2 2_1 4_2 6_2$ (No hints will be given)

2. Suppose p and q are distinct odd primes and assume with have an implementation of RSA with public key (n, e), where $n = pq$. Let the encryption function be denoted by E. A block b of the RSA message is said to be fixed by E if $E(b) = b$. How many blocks are fixed by RSA when $p = 3$, $q > 3$, and $e = 3$? Hint: learn and use the Chinese Remainder Theorem. Show all of your work.

3. **(RSA)** The message

   $$19 \quad 14 \quad 3$$

   was encrypted using the RSA cryptosystem with public key $n = 118$ and $e = 39$. Decrypt the message and give the corresponding plaintext message (using $A = 10$, $B = 11, \ldots$, $Z = 35$, and BLANK$= 99$). Show all of your work.

4. **(Number Theory)** Use only the following tools: pen, paper, and your friends.

   (a) Prove that $x^{97} - x + 1 \equiv 0 \pmod{97}$ has no solutions. Show all of your work.

   (b) Prove that if $2^n - 1$ is prime then n must be prime. Show all of your work.

   (c) Suppose p and $p + 2$ are both primes such that $p > 3$. Prove that $6|(p + 1)$. Show all of your work.

   (d) Find the last digit of 7^{355}. Show all of your work.

5. **(Quantum Factorization)** Let $N = 899$ and suppose $y = 4$ (y was chosen at random, but that does not affect how you proceed with this problem.) Use the technique given in class to factor N. Show all of your work.

6. **(Secret Sharing)** For this problem you will need to read the Mathematica notebook on Shamir's Secret Sharing Scheme. You have each been given one share in Shamir's secret sharing scheme. You will all need to cooperate to determine the final answer. What number represents the secret message? A successful completion of this problem will result in 20 points added to each student's total quiz score for the semester.