Problem Set 5

CSCE 440/640

Due dates: Electronic submission of the pdf file of this homework is due on **10/14/2016 before 2:50pm** on ecampus.tamu.edu, a signed paper copy of the pdf file is due on **10/14/2014** at the beginning of class.

Name: (put your name here)

Resources. (All people, books, articles, web pages, etc. that have been consulted when producing your answers to this homework)

On my honor, as an Aggie, I have neither given nor received any unauthorized aid on any portion of the academic work included in this assignment. Furthermore, I have disclosed all resources (people, books, web sites, etc.) that have been used to prepare this homework.

Signature: ____________________________

Problem 1. (20 points)
(a) Find the multiplicative order r of 13 modulo 8633, that is, the smallest exponent r such that $13^r \equiv 1 \pmod{8633}$.
(b) Determine one or more factors of 8633 by calculating

$$\gcd(13^{r/2} \pm 1, 8633).$$

Solution.

Problem 2. (10 points) Show that the order r of a positive integer a modulo N cannot exceed N assuming that $\gcd(a, N) = 1$. In other words, show that the smallest positive integer exponent r such that $a^r \equiv 1 \pmod{N}$ is bounded by $r \leq N$.

Solution.

Problem 3. (10 points) Calculate the convergents of 91/256.

Solution.

Problem 4. (10 points) Recall that the convergents p_k/q_k of a simple continued fraction satisfy the relation

$$p_{k-1}q_k - q_{k-1}p_k = (-1)^k.$$

Deduce that the rational number p_k/q_k is in reduced form, so $\gcd(p_k, q_k) = 1$.

Solution.

Problem 5. (20 points)
(a) Work out the steps of Shor's algorithm as given in the box on page 139-140 in our textbook assuming that you want to factor $N = 129$ using $n = 8$ qubits for $a = 14$. Values such as m_b should be determined. Typeset all the steps.
(b) Assuming the quantum part of Shor's algorithm would give you 6/256. Could you determine the period r of $a = 14$ modulo 129 from this observation. If so, how?

Solution.

Problem 6. (30 points)
(a) Read Shor's paper on perusall.com and make at least 5 insightful comments.
(b) Study Shor's explanation of the probability to observe a given state starting from the state given in (5.4) until just before (5.11) on pages 17–18. Summarize this explanation in your own words. Be sure to capture the intution as well as the technical details.

Solution.

Checklist:

□ Did you add your name?
□ Did you disclose all resources that you have used?
(This includes all people, books, websites, etc. that you have consulted)

□ Did you sign that you followed the Aggie honor code?

□ Did you solve all problems?

□ Did you submit the pdf file resulting from your latex source file on ecampus?

□ Did you submit a hardcopy of the pdf file in class?