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: Paul Gustafson

Resources. Wikipedia entry for continued fractions.

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. (a) I wrote a small python script to calculate this. The result was $r = 1056$.
(b) The results of the gcd calculations were 97 and 89, which are factors of 8633.

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. I claim that a is multiplicatively invertible mod N. Since $\gcd(a, N)$, there exist integers x, y. $ax + Ny = 1$. Hence, $a^{-1} = x$.

I also claim that $(a^k)_{k=0}^{r-1}$ are disjoint mod N. Suppose not. Then there exist $0 \leq j < k < r$ such that $a^j = a^k \pmod{N}$. Hence, since a is invertible, $a^{k-j} = 1$. Since $k - j < r$, this contradicts the assumption that r is the order of a.

Since there are only N possible choices for the a^k modulo N, this implies that $r \leq N$.

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

Solution. The convergents are $\frac{0}{1}, \frac{1}{2}, \frac{1}{3}, \frac{5}{14}, \frac{11}{31}, \frac{16}{45}, \frac{91}{256}$.

Here's a python script to calculate them:

```
a = 91
b = 256

#continued fraction expansion
def cfExp(p,q, cfE):
    if q == 0 :
        cfE = [p];
    else:
        cfExp(q, p - q*(p/q), cfE)
        cfE.insert(0, p/q)

cfE = []
cfExp(a, b, cfE)
print cfE

#Old convergents, initial conditions
p2 = 0
```

```
q2 = 1
p1 = 1
q1 = 0


for a in cfE:
    p = a*p1 + p2
    q = a*q1 + q2
    print("\\frac{" + str(p) + "}{"  + str(q) + "}, ")
    p2 = p1
    q2 = q1
    p1 = p
    q1 = q
```

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. The number $\gcd(a, b)$ is the least positive integer k such that there exist integers x, y such that $ax + by = k$. Multiply the given relation by ± 1 to get the desired equality.

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. 1. Create the state

$$|\psi_0\rangle = \sum_{x=0}^{255} \frac{1}{\sqrt{2^n}} |x\rangle |14^x \pmod{129}\rangle.$$

We can rewrite the above state as

$$|\psi_0\rangle = \sum_{b=0}^{41} \frac{1}{\sqrt{2^n}} \sum_{z=0}^{m_b - 1} |42z + b\rangle |14^x \pmod{129}\rangle,$$

where

$$m_b = \left\lfloor \frac{255 - b}{42} \right\rfloor + 1 = \begin{cases} 7 & b \leq 3 \\ 6 & b > 3 \end{cases}$$

2. Measure the second register. We measure $14^b \pmod{129}$ where b is chosen almost uniformly at random from $\{0, 1, \ldots, r-1\}$. Let's say the random value was $b = 29$. Then our measurement would be 74, and $m_b = 6$, and the first register is in a superposition

$$\frac{1}{\sqrt{6}} \sum_{z=0}^{5} |42z + 29\rangle.$$

3. We apply $\mathrm{QFT}_{2^n}^{-1}$ to the first register, and then measure a value x.
4. The output is $x/256$.

Assuming the output was $6/256$, we know that there is a relatively high probability that $\left|\frac{6}{256} - \frac{j}{r}\right| \leq \frac{1}{512}$ for some integer $0 \leq j \leq r-1$. So, one checks for values of r from the denominators of the convergents of 256. The second convergent of $6/256$ is $1/42$, which would give you the correct value of r.

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. Background

The inputs are positive integers x and n. The problem is to find the least r such that $x^r = 1 \pmod{n}$. Let $q = 2^N$ be the least power of 2 that is greater than or equal to n^2. We requre $2N$ qubits. The first N qubits are grouped together into the first register, and the second N qubits are the second register. Assume all qubits are initialized into the state $|0\rangle$

We apply Hadamards to each qubit in the first register to put it into a uniform superposition of all the standard basis vectors, leaving the second register alone. We then calculate $x^a \pmod{n}$ for each vector $|a\rangle \otimes |0\rangle$ in the superposition and put the result in the second register. This is a reversible operation since the only non-hardcoded input is a for each vector in the superposition, and a is left alone. We then apply the discrete Fourier transform on the first register, giving us a superposition of states $\exp(2\pi iac/q)|c\rangle \otimes |x^a \pmod{n}\rangle$, where a, c range over all integers from 0 to $2^N - 1$.

Summary of Shor's explanation from (5.4) to (5.11)

We then take a measurement of all the qubits. The probability of measuring $|c\rangle \otimes |x^a \pmod{n}\rangle$, for some $0 \leq a < r$, is

$$\left| \frac{1}{q} \sum_{k : x^k = x^a \pmod{n}} \exp(2\pi ikc/q) \right|^2.$$

Since r is the multplicative order of x, those k are parametrized by $k = a + br$ for nonnegative integers b. Thus, the above probability is equal to

$$\left| \frac{1}{q} \sum_{b:a+br<q} \exp(2\pi i brc/q) \right|^2 .$$

Let $\{rc\}_q$ denote the representative of rc mod q such that $-q/2 \leq \{rc\}_q \leq q/2$. When $\{rc\}_q \leq r/2$, this sum is well-approximated (i.e. error with $O(1/q)$) by the integral

$$\begin{aligned} \frac{1}{q} \int_{b:0\leq a+br<q} \exp(2\pi i b\{rc\}_q/q)\, db &= \frac{1}{r} \int_{u:0\leq a+qu<q} \exp(2\pi i u\{rc\}_q/r)\, du \\ &\approx \frac{1}{r} \int_{u:0\leq u<1} \exp(2\pi i u\{rc\}_q/r)\, du, \end{aligned}$$

where the error in the last approximation is again $O(1/q)$.

Letting $\{rc\}_q$ vary between $-r/2$ to $r/2$, the last absolute value of the last integral is minimized at the endpoints $\pm r/2$ at a value of $2/(\pi r)$. Thus, if $|\{rc\}_q| \leq r/2$, the probability of measuring $|c\rangle \otimes |x^a \pmod N\rangle$ is $\frac{4}{\pi^2 r^2} + O(1/n^2)$. Hence for sufficiently large n, this probability is greater than $\frac{1}{3r^2}$.

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?