**Homework #11.** Due Tue 11/6.

#1 – Suppose $N$ is to be factored. You know $a$ and its order mod $N$. The order of $a$ is even. What do you do next?

#2 – (programming required) Let $N = 31 \times 41$. How many $a$ in the range $1 \leq a < N$ satisfy $(a, N) = 1$? Of these, how many have odd order, and how many have even order? Of those with even order, how many lead to a successful discovery of a nontrivial factor of $N$?

#3 – Let $\omega = e^{2\pi i/Q}$, and consider the sum

$$\text{Sum}(y) = \sum_{x=0}^{Q-1} \omega^{xy}.$$  

Prove that for $1 \leq y < Q$ this sum is 0. Hint 1: Look at your class notes from long ago. Hint 2: What happens when you multiply the sum by $\omega^y$?

#4 – In the previous problem, what is $\text{Sum}(0)$?

#5 – Suppose that $N = p \times q$ where $p$ and $q$ are distinct primes. Show that the number of $a$ in the range $1 \leq a < N$ which satisfy $(a, N) = 1$ is $(p - 1)(q - 1)$.

**Eleventh week summary**

Tue 10/23. We covered the number theoretic background to Shor’s algorithm. There was an “unofficial” handout on this material. One key idea is that the quantum portion of factoring consists of finding the order of a randomly chosen $a$. The order of $a$ (with respect to $N$) is the smallest positive exponent $j$ such that

$$a^j = 1 \mod N.$$
(The notation means that the difference \( a^j - 1 \) is divisible by \( N \).) Every \( a \) which is relatively prime to \( N \) has an order.

The second key idea from number theory is that if the order \( j \) is EVEN, then we have

\[
a^j - 1 = (a^{j/2} + 1)(a^{j/2} - 1).
\]

Thus, we have a product of two numbers which is divisible by \( N \). The \( \gcd (a^{j/2} - 1, N) \) might yield a nontrivial factor. (It could yield only the trivial factors 1, \( N \) also; some good luck is needed.)

Wed 10/24. We went over the quantum part of Shor’s algorithm. In a nutshell, the machine is put into the following state

\[
\frac{1}{Q} \sum_{y=0}^{Q-1} |y\rangle \otimes \left[ \sum_{x=0}^{Q-1} \omega^{xy} |F(x)\rangle \right]
\]

where \( \omega = e^{2\pi i/Q} \), and \( F \) is the function

\[
F : \{0, 1\}^q \rightarrow \{0, 1\}^q
\]

defined by

\[
F(x) = a^x \mod N.
\]

From the above, we see that the circuit contains a certain \( U_F \), and also the Fourier transform \( \mathcal{F}_Q \). The circuit is, in fact, identical to Simon’s circuit except that the second occurrence of \( H^\otimes n \) in Simon is replaced by \( \mathcal{F}_Q \).

Thu 10/25. Today we reported on some further experiments with Shor’s order finding circuit.

**Twelfth week topics**

Tue 10/30. Jay will talk about Chapter 9, sections 1,2: classical cryptography, and BB84 quantum key exchange protocol.

Wed 10/31. James will talk about Chapter 10, sections 1,2: Shannon Entropy, and von Neumann Entropy.

Thu 11/1. Joey will talk about Chapter 10, section 3: classical and quantum data compression.