CS5319 Advanced Discrete Structure

Homework 5
Due: December 27, 2021 (11:59pm)
Exam 3: January 11, 2022

1. Compute $\phi(1720)$.

2. In this question, we want to show that $2^n \not\equiv 1 \pmod{n}$ for all $n > 1$.

   (a) Prove that if $n^j \equiv 1 \pmod{m}$ and $n^k \equiv 1 \pmod{m}$, then

   $$n^{\gcd(j,k)} \equiv 1 \pmod{m}$$

   Hint: Properties of GCD.

   (b) Assume for the sake of contradiction that $2^n \equiv 1 \pmod{n}$ for some $n > 1$. Using the result of part (a), show that

   $$2^{\gcd(p-1,n)} \equiv 1 \pmod{p}$$

   where p is the smallest prime factor of n.

   (c) By the choice of p, what is the value of $\gcd(p-1, n)$? Show that there exists a contraction, and hence $2^n \not\equiv 1 \pmod{n}$ for all $n > 1$.

3. A number n is a perfect number if the sum of all the proper divisors of n (i.e., all divisors excluding n itself) is exactly n. For instance, 6 and 28 are both perfect numbers, because

   $$\begin{array}{lcll} \text{sum of proper divisors of } 6 & = & 1+2+3 & = 6, \text{ and} \\ \text{sum of proper divisors of } 28 & = & 1+2+4+7+14 & = 28. \end{array}$$

   In the following, we shall show an interesting result by Euler:

   Theorem 1. *An even number n is a perfect number if and only if $n = 2^m(2^{m+1}-1)$ and $2^{m+1}-1$ is prime.*

   (a) Prove that if $n = 2^m(2^{m+1}-1)$ and $2^{m+1}-1$ is a prime, then n is a perfect number.

   (b) Suppose n is an even number, so that we can express n as $2^m Q$ for some odd integer Q. Also, suppose $\sigma(Q)$ denotes the sum of all divisors of Q (i.e., including itself). Show that if n is a perfect number, then

   $$2^{m+1}Q = 2n = (2^{m+1}-1)\sigma(Q).$$

   (c) Continuing with part (b), show that Q is a multiple of $2^{m+1}-1$.

   (d) Continuing with parts (b) and (c), suppose that $Q = (2^{m+1}-1)q$. Show that the following is true:

   $$2^{m+1}q = \sigma(Q) \geq q + Q = 2^{m+1}q.$$

   (e) Continuing with parts (b), (c), and (d), show that Q must be a prime and $Q = 2^{m+1}-1$. In other words, $n = 2^m Q = 2^m(2^{m+1}-1)$ for some prime $Q = 2^{m+1}-1$.

4. Decrypt the ciphertext

   1040 1182 1075 741 2366 1495

   that was encrypted using the RSA algorithm with key $(e, n) = (211, 2419)$.

   Remark: Use a calculator to help.

5. Consider a deck with $2n$ cards, with cards labeled by $1, 2, \ldots, 2n$ from top to bottom. A *perfect shuffle* is special kind of shuffle, where we divide the deck into two halves (the top n cards and the bottom n cards), and then reproduce a deck by repeatedly picking a card, one from the bottom half and one from the top half, until no cards are left. Note that cards are always picked from top to bottom.

   For example, suppose that $n = 3$, so that the original deck contains $1, 2, 3, 4, 5, 6$ from top to bottom. When we divide the deck into two halves, the top n cards are $1, 2, 3$ and the bottom n cards are $4, 5, 6$. The new deck is formed by picking a card from the bottom half (which is 4) and then a card from the top half (which is 1), and the procedure is repeated until we do not have cards left. Thus, in the end, the new deck contains $4, 1, 5, 2, 6, 3$ from top to bottom.

   (a) Argue that when we perform perfect shuffle enough number of times, the cards within deck will resume the initial ordering, that is, $1, 2, 3, \ldots, 2n$ from top to bottom.

   (b) Let x be the minimum number of perfect shuffles to resume the initial ordering. What is the relationship between x and n?