

DISCRETE MATHEMATICS
HOMEWORK 9

1. Suppose we turn letters into numbers by just using the position of the letter in the alphabet, with a leading 0 if the position is less than 10. Thus,

$$\begin{aligned}A &\rightarrow 01 \\B &\rightarrow 02 \\C &\rightarrow 03 \\&\vdots \\Z &\rightarrow 26.\end{aligned}$$

We then group pairs of letters to form 4-digit numbers. For example, the word “code” becomes

$$\text{code} \rightarrow 0315\ 0405.$$

Encode this message to me using RSA encryption with $n = 10961$ and $e = 5$. To do the encoding, encode each block of 2 letters separately and send me 2 numbers.

2. Suppose you intercept the message “7849”, and you know that it was encoded using RSA encryption with $n = 10961$ and $e = 4301$. Can you, as an enemy agent (sorry, this is Earlham, “Can you, as a foreign neighbor”) crack the code and read the message? Hint: to save you some work, $10961 = 97 \cdot 113$. Another hint: the message should be a familiar 2-character string.
3. Using among other things the theorem that if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$, try to construct an argument that every positive integer factors into primes in exactly one way. This argument will have two parts.
- (a) First, prove that every integer factors into primes.
 - (b) Then prove that if

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$$

are two factorizations of a into primes, then $n = m$ and the primes p_1, p_2, \dots, p_n are a rearrangement of the primes q_1, q_2, \dots, q_m . It is this second part of the proof that will need the theorem mentioned above.

4. Show inductively that the number of subsets of a set with n elements is 2^n . *Hint:* The subsets of $\{1, 2, 3, \dots, n, n + 1\}$ are of two types:
- (a) Subsets of $\{1, 2, 3, \dots, n\}$.
 - (b) Subsets of $\{1, 2, 3, \dots, n\}$ with the element $n + 1$ thrown in as well.

5. In doing this problem, you may want to refer back to what we did on Homework 3 about $\phi(n)$.
- (a) How many integers k with $1 \leq k \leq 840$ have $\gcd(k, 840) = 1$?
 - (b) How many integers k with $1 \leq k \leq 840$ have $\gcd(k, 840) = 3$?
 - (c) How many integers k with $1 \leq k \leq 840$ have $\gcd(k, 840) = 2$?
 - (d) How many integers k with $1 \leq k \leq 840$ have $\gcd(k, 840) = 35$?