1. (Multiplicative functions.) Let \( \tau(n) \) denote the number of positive divisors of \( n \). Show that the function \( \tau \) is multiplicative.

   *Hint:* You may wish to use the explicit formula for \( \tau(n) \) derived in Homework 2.

2. (Multiplicative functions.) For each positive integer \( n \), consider the function \( \sigma \) which computes the sum of all divisors of \( n \), that is

   \[ \sigma(n) = \sum_{d|n, d>0} d. \]

   (i) Show that if \((n,m) = 1\) then any divisor \( d > 0 \) of the product \( nm \) can be written uniquely as

   \[ d = d_1d_2 \]

   where \( d_1 > 0 \) is a divisor of \( n \) and \( d_2 > 0 \) is a divisor of \( m \). One way to see existence is using the prime factorization of \( n \) and \( m \).

   (ii) Using (i), conclude that \( \sigma \) is multiplicative.

   (iii) Show that for any prime \( p \) we have

   \[ \sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}. \]

   (iv) Using (ii) and (iii), write down a formula for \( \sigma(n) \) in terms of the prime factorization of \( n \).

3. (Euler’s function.) Section 3.2, solve problem 14. It may help to consider the prime factorization of \( d \) and \( n \).

4. (Systems of congruences.) Section 3.3, solve problem 1.

5. (Fermat’s theorem.) Section 3.2, solve problem 22. You may want to observe that

   \[ 11\ldots1 = \frac{1}{9} \cdot 99\ldots9 = \frac{1}{9}(10^{\ell} - 1). \]

6. (Converse to Fermat.) Section 3.2, solve part of problem 23: show that if \((a,561) = 1\) then \( a^{560} \equiv 1 \mod 561 \). Since 561 is not a prime, the converse to Fermat is false.

   *Remark:* The number 561 is an example of a Carmichael number that is, a non prime for which the converse of Fermat holds.

   *Hint:* It may help to evaluate \( a^{560} \mod 3, \mod 11, \mod 17 \) separately using Fermat and then assemble the answer \( \mod 561 \).
7. (Fermat, Chinese remainder theorem.) Using Fermat’s theorem and the Chinese remainder theorem compute

\[ 11^{193} \mod 1768. \]

*Hint: You may want to first compute the answer \( \mod 8, \mod 13, \mod 17 \) separately using Fermat, then assemble the answer \( \mod 1768. \)

8. (RSA algorithm.) This is a longer problem to read, but otherwise, it shouldn’t require much work.

The RSA encryption algorithm was described by Rivest, Shamir and Adleman; the letters RSA stand for their initials. We will describe briefly how this works.

The RSA algorithm involves three steps:

(i) key generation:
- chose \( p, q \) two prime numbers and let \( n = pq \), so that \( \phi(n) = (p - 1)(q - 1) \);
- Let \( 1 < e < \phi(n) \) be a number coprime with \( \phi(n) \) and let \( d \) be chosen such that
  \[ de \equiv 1 \mod \phi(n). \]

The number \( d \) is computed via the Euclidean algorithm. Its existence follows since \( (e, \phi(n)) = 1. \)

Then:
- the pair \( (n, e) \) is the public key;
- the pair \( (n, d) \) is the private key (or rather, \( d \) is the private key exponent).

(ii) encryption:
- Alice transmits her public key \( (n, e) \) to Bob, and keeps the private exponent \( d \) secret.
- Bob then wishes to send a message \( M \) to Alice. The message \( M \) is encoded as an integer \( 0 < m < n \) with \( (m, n) = 1 \) which is obtained via an agreed-upon reversible protocol.
- Bob computes the integer \( c \) such that \( 0 < c < n \) and
  \[ c \equiv m^e \mod n. \]

Since Bob knows the public key \( (n, e) \) as well as the message \( m \), then he can certainly calculate the integer \( c \). Bob then transmits \( c \) to Alice.

(iii) decryption: When Alice receives \( c \), the original message \( m \) is recovered by computing
  \[ c^d \equiv m \mod n. \]

While the key \( d \) is secret, \( d \) is however known to Alice, who then also can compute \( m. \)

Answer the following questions (no work is required for (b)):

(a) Explain why the decryption step (iii) works, so that Alice does recover the message \( m. \)
(b) In order to crack the code, an eavesdropper may overhear \( c \), but to find \( m \) he must must
know \( d \). Since \( de \equiv 1 \mod \phi(n) \) and \( e \) is public, finding \( d \) would be guaranteed once \( \phi(n) \)
is known. However,

\[ \phi(n) = (p - 1)(q - 1) \]

and this last step requires the prime factorization of \( n \). If the primes \( p, q \) are chosen to be
large, then cipher may be hard to break.

(c) Explicitly work out a “baby” example. You should not use a calculator for this part.

Pick \( p = 11, q = 13, e = 113 \).

- What is the public key? What is the private key?
- How would Bob transmit the message \( m = 15 \)? Here you can use Fermat’s theorem
  for the primes \( p \) and \( q \) and assemble the answer using the Chinese remainder theorem.