1. (a) Use Euclid’s algorithm to compute the gcd of 495 and 210. Write out the steps.
\[ \gcd(495, 210) = \gcd(495 - 210, 210) \]
\[ = \gcd(285, 210) = \gcd(285 - 210, 210) \]
\[ = \gcd(75, 210) = \gcd(210 - 75, 75) \]
\[ = \gcd(75, 135) = \gcd(135 - 75, 75) \]
\[ = \gcd(75, 60) = \gcd(60, 75 - 60) \]
\[ = \gcd(15, 60) = 15 \]

(b) What is the prime factorization of 495 and of 210?
\[ 495 = 3 \cdot 3 \cdot 5 \cdot 11 \]
\[ 210 = 2 \cdot 3 \cdot 5 \cdot 7 \]

(c) Is your answer to part (a) correct?
Yes.

2. Prove the following theorem

**Theorem:** If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \) then

(a) \( a + c \equiv b + d \pmod{m} \)

*Proof.* If \( a \equiv b \pmod{m} \), then \( a = b + im \), for some integer \( i \). Similarly, \( c = d + jm \). Now:
\[ a + c = b + im + d + jm \]
\[ = b + d + (i + j)m \]
\[ \equiv b + d + (i + j)m \pmod{m} \]
\[ \equiv b + d \pmod{m} \]

(b) \( ac \equiv bd \pmod{m} \)

*Proof.* If \( a \equiv b \pmod{m} \), then \( a = b + im \), for some integer \( i \). Similarly, \( c = d + jm \). Now:
\[ ac = (b + im)(d + jm) \]
\[ = bd + dim + bjm + im^2 \]
\[ \equiv bd + dim + bjm + im^2 \pmod{m} \]
\[ \equiv bd \pmod{m} \]
Note: If \(a = q_am + r_a\) and \(b = q_bm + r_b\) where \(r_a < m\) and \(r_b < m\) it is possible that \(r_a + r_b \geq m\).

3. Construct the multiplication table for arithmetic mod 7.

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
1 & 2 & 3 & 4 & 5 & 6 & 0 \\
2 & 4 & 1 & 3 & 5 & 0 & 0 \\
3 & 2 & 5 & 1 & 4 & 0 & 0 \\
4 & 2 & 6 & 3 & 0 & 6 & 0 \\
5 & 4 & 2 & 0 & 0 & 4 & 0 \\
6 & 1 & 0 & 0 & 0 & 4 & 0 \\
7 & 0 & 6 & 3 & 0 & 6 & 3 \\
\end{array}
\]

4. (Extended Euclidean Algorithm) What is multiplicative inverse of 400 mod 997? The answer is 167.

We can find this by completing Euclid’s Algorithm:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>quotient</th>
<th>remainder</th>
</tr>
</thead>
<tbody>
<tr>
<td>997</td>
<td>400</td>
<td>2</td>
<td>197</td>
</tr>
<tr>
<td>400</td>
<td>197</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>197</td>
<td>6</td>
<td>32</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Now at each stage the remainder = \(a - \text{quotient} \times b\). Using a recursive back substitution:

\[
1 = 6 - 5 \\
= 33 \times 6 - 197 \\
= 33 \times 400 - 67 \times 197 \\
1 = 167 \times 400 - 67 \times 997
\]

Hence, this implies the modular inverse of 400 in \(\mod 997\) is 167.

5. Prove for relatively prime \(a\) and \(b\) that if \(a\) divides \(bc\), then \(a\) divides \(c\).

**Hint:** First show that there exist \(s\) and \(t\) such that \( sac + tbc = c\) and then argue that \(a\) divides \(c\).

Give counter example when \(a\) and \(b\) are not relatively prime.

The answer is taken from lecture:

**Lemma 1.** If \(a\) and \(b\) are relatively prime and \(a\) divides \(bc\), then \(a\) divides \(c\).

Note, you may use the math guide for understanding relatively prime and gcd.

We start the proof with an example to gain some intuition. If \(a = 2 \times 3\), \(b = 2 \times 2\), and \(c = 3 \times 3\), then \(a = 6\) does divide \(bc = 36\). However, \(a = 10\) does not divide \(c = 9\), because a portion of what \(a\) was dividing in \(bc\) was in \(b\). However, our lemma only holds if \(a\) and \(b\) are relatively prime. In our example \(gcd(a, b) = 2\), hence \(a\) and \(b\) were not relatively prime. The idea is that if \(a\) divides \(bc\) and \(a\) and \(b\) are relatively prime, then all of what \(a\) is dividing in \(bc\) is in \(c\).

**Proof.** Since \(a\) and \(b\) are relatively prime, there exist, \((\exists)\), integers \(s\) and \(t\) such that \(as + bt = 1\). Now:

\[
\frac{asc + btc}{a} = \frac{c}{a}
\]

\[
s + t \left( \frac{bc}{a} \right) = \frac{c}{a}
\]

The lemma states \(a\) divides \(bc\). Hence, \(\frac{c}{a}\) is the sum of multiples of integers. Hence, \(\frac{c}{a}\) is an integer.

Hence, \(a\) divides \(c\). \(\square\)