1 Problem 1

Let us prove that the following holds if and only if $\alpha$ is a primitive root.

$$\alpha^q = -1 \pmod{p}$$

(1)

If we square both sides, we find the identity,

$$\alpha^{2q} = 1 \pmod{p}$$

(2)

and

$$\alpha^{p-1} = 1 \pmod{p}$$

(3)

Working backwards,

$$\alpha^q = \pm 1 \pmod{p}$$

(4)

If $\alpha^q$ is 1, then $\alpha$ is not a primitive root, because 1 appeared early. Therefore, if $\alpha$ is a primitive root, the following will hold.

$$\alpha^q = -1 \pmod{p}$$

(5)

2 Problem 2

2.1 Primitive Roots of 15

15 Has the following exponentiation table.
A column of all ones appears at $x^4$. This means that 15 has no primitive roots, because none of the numbers act as generators. That is, no number generates all numbers relatively prime to 15.

2.2 Primitive Roots of 9

9 has the following exponentiation table.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9 has primitive roots 2, and 5. Both generate all numbers relatively prime to 9.

3 Problem 3

Let us start with an excerpt of the proof from Stinson 5.3

\[(x^b)^a = x^{\phi(n)+1} \mod n = (x^{\phi(n)})^t x \mod n\]  \(\text{(6)}\)

In order for this to be true for all $x$, Let’s try to prove that $x^{\phi(n)}$ is 1 mod $n$ for all $x$.

Let’s show that $x^{\phi(n)}$ is 1 mod $p$. 

2
\[ x^{\phi(n)} = x^{(p-1)(q-1)} \mod p \]
\[ = (x^{(p-1)})^{(q-1)} \mod p \]
\[ = (1)^{(q-1)} \mod p \]
\[ = 1 + k_1p \] 

(7)

Let’s show that \( x^{\phi(n)} \) is 1 mod q.

\[ x^{\phi(n)} = x^{(p-1)(q-1)} \mod q \]
\[ = (x^{(q-1)})^{(p-1)} \mod q \]
\[ = (1)^{(p-1)} \mod q \]
\[ = 1 + k_2q \] 

(8)

Setting these equal, we find that,

\[ 1 + k_1p = 1 + k_2q \] 

(9)

or simply,

\[ k_1p = k_2q \] 

(10)

Both \( p \) and \( q \) are prime, so \( k_1 \) must have a factor of \( q \) and \( k_2 \) must have a factor of \( p \). We can simply say substitute \( k_1 \) for a new as a multiplication of \( q \) and some other constant, \( k_3 \).

\[ k_3pq = k_2q \] 

(11)

An substituteing back in,

\[ x^{\phi(n)} = 1 + k_3pq \]
\[ = 1 \mod pq \]
\[ = 1 \mod n \] 

(12)

\[ (x^b)^a = (x^{\phi(n)})^t x \mod n \]
\[ = 1^t x \mod n \]
\[ = x \mod n \] 

(13)