11. The Euler’s Theorem

**Definition 1.** Let \( m \geq 2 \) be an integer. We define \( \phi(m) \) to be the number of integers \( a \) in the range \( 1 \leq a \leq m \) such that \( \gcd(a, m) = 1 \). The function \( \phi \) is called the Euler \( \phi \)-function.

The following table gives the \( \phi(m) \) for small values of \( m \):

<table>
<thead>
<tr>
<th>( m )</th>
<th>( a ) with ( 1 \leq a \leq m ) such that ( \gcd(a, m) = 1 )</th>
<th>( \phi(m) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1,2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1,3</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>1,2,3,4</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>1,5</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>1,2,3,4,5,6</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>1,3,5,7</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>1,2,4,5,7,8</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>1,3,7,9</td>
<td>4</td>
</tr>
</tbody>
</table>

It should be clear that if \( p \) is prime, then \( \phi(p) = p - 1 \). This is because every integer from 1 to \( p \) except for \( p \) is relatively prime to \( p \). What is not clear is what \( \phi(m) \) is when \( m \) is not prime. We’ll find a formula for \( \phi(m) \) on the next worksheet.

For an integer \( m \geq 2 \), we let \( S_m^* \) be the set of integers between 1 and \( m - 1 \) which are relatively prime to \( m \). For example, we have:

\[
S_4^* = \{1, 3\} \\
S_5^* = \{1, 3, 5, 7\} \\
S_9^* = \{1, 2, 4, 5, 7, 8\} \\
S_{10}^* = \{1, 3, 7, 9\}
\]

We note that \( S_m^* \) has \( \phi(m) \) elements, by definition of the Euler \( \phi \)-function.

**Lemma 2.** Suppose \( \gcd(a, m) = 1 \) and \( b \in S_m^* \). Prove that \( \lnr(ab, m) \in S_m^* \).

**Proof.** Homework. \( \square \)

If \( \gcd(a, m) = 1 \), we can define a function \( f_m^a : S_m^* \rightarrow S_m^* \) by \( f_m^a(x) = \lnr(ax, m) \) for each \( x \in S_m \). Here is an example with \( m = 9 \). We have \( S_9^* = \{1, 2, 4, 5, 7, 8\} \). Let’s choose \( a = 4 \). Then

\[
\begin{align*}
f_9^4(1) &= \lnr(4 \cdot 1, 9) = 4 \\
f_9^4(2) &= \lnr(4 \cdot 2, 9) = 8 \\
f_9^4(4) &= \lnr(4 \cdot 4, 9) = 7 \\
f_9^4(5) &= \lnr(4 \cdot 5, 9) = 2 \\
f_9^4(7) &= \lnr(4 \cdot 7, 9) = 1 \\
f_9^4(8) &= \lnr(4 \cdot 8, 9) = 5
\end{align*}
\]

Notice that, just as with the case \( m = p \) is prime (which we did before on Worksheet #9), every element in \( S_9^* \) was ‘hit’; that is, the map is *onto*. We want to prove this is always the case:
Proposition 3. Suppose \( m \) is prime and \( \gcd(a,m) = 1 \). Then the map \( f_m^a : S_m^* \to S_m^* \) is one-to-one and onto.

Proof. We first prove \( f_m^a \) is one-to-one. Suppose \( f_m^a(x) = f_m^a(y) \) for some \( x, y \in S_m^* \). Then \( \lnr(ax,m) = \lnr/ay,m) \). Thus, \( ax \equiv ay \pmod{m} \). Since \( a \in S_m^* \), \( \gcd(a,m) = 1 \). Thus, we can cancel \( a \) from both sides of this congruence equation and obtain \( x \equiv y \pmod{m} \). That is, \( m \) divides \( x - y \). But since \( 1 \leq x, y \leq m - 1 \), this must mean \( x = y \). Hence, \( f_m^a \) is one-to-one. Since \( f_m^a \) is a one-to-one function from a finite set to itself, \( f_m^a \) must be onto as well.

By mimicking the proof for Fermat’s theorem, we can obtain a more general version of it called Euler’s Theorem:

Theorem 4. (Euler’s Theorem) Let \( m \geq 2 \) be an integer and \( a \) an integer such that \( \gcd(a,m) = 1 \). Then \( a^{\phi(m)} \equiv 1 \pmod{m} \).

Proof. By the theorem above, \( f_m^a : S_m^* \to S_m^* \) is one-to-one and onto, we have

\[
S_m^* = \{x_1, x_2, \ldots, x_{\phi(m)}\} = \{f_m^a(x_1), f_m^a(x_2), \ldots, f_m^a(x_{\phi(m)})\} = \{\lnr(ax_1, m), \lnr(ax_2, m), \ldots, \lnr(ax_{\phi(m)}, m)\}.
\]

Thus,

\[
x_1 x_2 \cdots x_{\phi(m)} \equiv (ax_1)(ax_2) \cdots (ax_{\phi(m)}) \pmod{m} \\
\equiv x_1 x_2 \cdots x_{\phi(m)} a^{\phi(m)} \pmod{m}
\]

Since each \( x_i \) is relatively prime to \( m \), we can cancel it from both sides of the modular equation. (Equivalently, we could multiply both sides of the equation by the inverse of \( x_i \).) Doing this for all \( x_i \), we obtain:

\[
1 \equiv a^{\phi(m)} \pmod{m}.
\]

Homework:

1. Prove Lemma 2.

2. We’ll show on the next worksheet that \( \phi(1000) = 400 \). Use this fact to find \( \lnr((21)^{800}, 1000) \).