Group Exploration 1: Euler's Totient Function

Throughout this worksheet, m and n stand for positive integers. Our goal is to prove the following

Theorem: If m and n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.

In what follows, we will refer to this as the *Main Theorem* of this worksheet. We start with a few definitions.

Definition: $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is the set of all pairs whose first entry is an integer, considered modulo m, and whose second entry is an integer, considered modulo n. In other words,

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \{(a \bmod m, b \bmod n) : a, b \in \mathbb{Z}\}.$$

We call this set the *product* of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

In our proof, we will need to compare the product of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ with the set $\mathbb{Z}/mn\mathbb{Z}$. This will be done through the function Δ, whose definition appears below.

Definition: The function $\Delta : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is the function whose domain is $\mathbb{Z}/mn\mathbb{Z}$, whose target is $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, and that is defined by

$$\Delta(x) = (x, x).$$

Note: The first time x appears in this formula, it is taken modulo mn, the second time, modulo m, and the third time, modulo n.

Warmup.

(1) How many elements are there in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/mn\mathbb{Z}$?
(2) Explicitly describe the function Δ when $m = 4$ and $n = 6$ by filling out the table

x	$\Delta(x)$
0	$\Delta(0)$
1	$\Delta(1)$
$\vdots$	$\vdots$
23	$\Delta(23)$

In the right-hand column, simplify so that the first entry of $\Delta(x)$ is between 0 and 3, and the second between 0 and 5. Also indicate which entries of the left-hand column are units.
(3) Repeat the same calculation, except with the choice of $m = 3$ and $n = 8$.
(4) Compare and contrast these two examples. For instance, is Δ onto, or one-to-one? Is there a connection between the units of the left-hand column, and the pairs in the right-hand column whose entries are both units?

Step 1. We will start by establishing the following theorem.

Theorem: If m and n are relatively prime, then Δ is a *bijection*, i.e., Δ is an *invertible function*, i.e., Δ is both $1-1$ and onto.

This result is also sometimes referred to as the Chinese Remainder Theorem. Below, we will see how to translate the CRT, as stated in class, into the above form.

(1) Write the expression $\Delta(x) = (a, b)$ in terms of a system of two congruences.
(2) State what it means for Δ to be $1-1$, and onto.

(3) Consider the situation when $m = 51$ and $n = 74$. If the theorem stated immediately above is true, which it is, then there must be an x between 0 and 3773 (note that $mn = 3774$ in this case) such that $\Delta(x) = (18, 31)$. Find such an x. If the theorem is correct, which it is, how many such x can there be?
(4) State the CRT, as presented in class, separating the statement into two parts.
(5) Explain why the first part of the CRT presented in class shows that Δ is onto, and why the second part shows that Δ is $1-1$. This proves the theorem above.

Step 2. Our goal here is to prove the following

> **Lemma**: If m and n are relatively prime, then x is a unit modulo mn if and only if the first entry of $\Delta(x)$ is a unit modulo m, and the second entry is a unit modulo n.

(1) Return to the problem from the Warm-up with $m = 3$ and $n = 8$, and verify that the above lemma is true in this case. There is no need to write anything, besides affirming that you checked it in this case. But please do check it!
(2) We start the "easy" implication: Prove that if x is a unit modulo mn, then each entry of $\Delta(x)$ is a unit modulo the respective moduli. **Hint**: If u is the inverse of x modulo mn, then write out what this means, and apply Δ. **Note**: You shouldn't need to use that $\gcd(m, n) = 1$ for this direction.
(3) Next, the "harder" implication: Prove that if both coordinates of $\Delta(x)$ are units, then x must be a unit modulo mn. **Hint**: If y, z are the inverses of the entries of $\Delta(x)$, then invoke the fact that Δ is onto to hit $(y, z) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then, invoke the fact that Δ is $1-1$.

Step 3.

(1) Explain how to use Steps 1 and 2 to prove the Main Theorem.

A cool application. Our final goal is to prove the following vague theorem.

> **Theorem**: If the prime factorization of n is known, then one can explicitly compute $\varphi(n)$. That is, if we write $n = p_1^{e_1} \cdots p_t^{e_t}$, where each p_i is prime, $p_i \neq p_j$ if $i \neq j$, and each exponent e_i is positive, then there is an explicit formula for $\varphi(n)$ in terms of the p_i and e_i.

(1) In class, we saw that $\phi(p) = p - 1$ when p is prime. Generalize this to obtain a formula for $\phi(p^e)$ when p is prime, and e is a positive integer. **Hint**: What happens when $p = 2$ and $e = 4$? What about when $p = 3$ and $e = 3$?
(2) Produce the "explicit formula" that is asserted to exist in the previous theorem.
Hint: Apply our Main Theorem repeatedly to the prime factorization of n.