The Euler Totient is Even

After pondering about some stuff relating to modular matrices from a while back, I thought of a very quick, and easy to derive way of showing that the Euler totient function $\phi(n)$ is even (except in the case of $n = 2$). We'll first start with a review.

> **Definition.** The **Euler totient function** $\phi(n)$ is defined to be the number of natural numbers less than n that are relatively prime to n (that is $\gcd(n, k) = 1$ for the natural k).

While there are definitely number theory proofs of this always being even, we shall show this is true with group theory.

Let A_n denote the set, of natural numbers less than n that are relatively prime to n. We assert that this set forms a group when equipped with multiplication modulo n, and we shall denote this group by $\mathbb{Z}_n^\times$.

> **Theorem.** $\mathbb{Z}_n^\times$ forms a group.

Proof. We shall prove the three necessary conditions: associativity, the existence of an identity, and inverses for each element.

- **Associativity**: This one is obvious, as multiplication is associative and even commutative.
- **Identity element**: This condition is also obvious, as one can verify that 1 is in $\mathbb{Z}_n^\times$ and satisfies the conditions to be the identity.
- **Inverse elements**: By the Extended Euclidean algorithm, we know that for any $a \in \mathbb{Z}_n^\times$, a^{-1} exists in general. Thus, it suffices to prove that this a^{-1} is in $\mathbb{Z}_n^\times$; that is, we must prove that $\gcd(a^{-1}, n) = 1$.

  Observe that for any k, $\gcd(ka^{-1}, n) \geq \gcd(a^{-1}, n)$. If we take $k = a$, however, we see that $\gcd(ka^{-1}, n) = \gcd(1, n) = 1$, so clearly $\gcd(a^{-1}, n) = 1$.

■

This group has a direct correlation with the original problem at hand. Indeed, $|\mathbb{Z}_n^\times| =$

$|A_n| = \phi(n)$. Now that we have a group structure over the set, however, we can use some fun group theory concepts. In particular, recall Lagrange's theorem, or a certain version of it at least.

> **Theorem** (Lagrange's theorem)**.** For any subgroup H of some group G, $|H|$ divides $|G|$.

Using this we can trivially show that the Euler totient is even.

> **Theorem.** $\phi(n)$ is even for $n \geq 3$.

Proof. We have that $\mathbb{Z}_n^\times$ is a group and $|\mathbb{Z}_n^\times| = \phi(n)$. Observe, however, that $\{1, -1\} \subseteq \mathbb{Z}_n^\times$ is a subgroup of this group, and it clearly has order 2. Thus, we must have that $2 \mid \phi(n)$. ■

The only exception to this is the case of $n = 2$, where $\phi(2) = 1$. The reason that this argument fails in this case is because the subgroup is actually of order 1, as 1 is congruent to -1 modulo 2.