# A proof outline of the Euler's totient product theorem, Math 311w, 2018

Assume $p$ and $q$ are positive relatively prime integers.

**Lemma 1.** $\forall s, t \in \mathbb{Z}$, $\gcd(s, q) = \gcd(t, p) = 1 \Leftrightarrow \gcd(sp + tq, pq)$.

**Lemma 2.** $\forall s, t \in \mathbb{Z}$, $[s]_q$ *and* $[t]_p$ *are invertible if and only if* $[sp + tq]_{pq}$ *is invertible.*

*Proof.* Use Lemma 1. □

Let $Q = \{0, 1, ...q - 1\}$, $P = \{0, 1, ...p - 1\}$, and $W = \{0, 1, ...pq - 1\}$. Define the function $f : Q \times P \to W$ such that $f(s, t) = (sp + tq)\%(pq)$.

**Lemma 3.** *The function* $f$ *is a bijection between it's domain and codomain.*

The same thing works, if we switch from talking about integers to talking about congruence classes. Define the function $h : \mathbb{Z}_q \times \mathbb{Z}_p \to \mathbb{Z}_{pq}$ such that $h([s]_q, [t]_p) = [f(s, t)]_{pq}$.

**Lemma 4.** *The function* $h$ *is a bijection between it's domain and codomain.*

*Proof.* Use Lemma 3. □

**Theorem 5.** $\phi(pq) = \phi(p)\phi(q)$

*Proof.* We start with our bijection $h$ between $\mathbb{Z}_q \times \mathbb{Z}_p$ and $\mathbb{Z}_{pq}$ from Lemma 4. Since $\mathbb{Z}_q^\times \times \mathbb{Z}_p^\times \subseteq \mathbb{Z}_q \times \mathbb{Z}_p$, we can create a restricted function $h^* : \mathbb{Z}_q^\times \times \mathbb{Z}_p^\times \to \mathbb{Z}_{pq}$ that is the same as $h$ but whose domain is only pairs of invertible elements from $\mathbb{Z}_q \times \mathbb{Z}_p$. Now, by Lemma 2, if $[s]_q$ and $[t]_p$ are invertible, then so is $h^*([s]_q, [t]_p) = [sp + tq]_{pq}$, so $\text{Image}(h^*) \subseteq \mathbb{Z}_{pq}^\times$. And by the same Lemma 2, if $[sp + tq]_{pq}$ is invertible then so are both $[s]_q$ and $[t]_p$, so $\mathbb{Z}_{pq}^\times \subseteq \text{Image}(h^*)$. So, by the weak antisymmetry property of the subset partial ordering, $\mathbb{Z}_{pq}^\times = \text{Image}(h^*)$. Since $h$ is injective (Lemma 4), $h^*$ is also injective. Since, for every injective function, the domain and image have the same cardinality, $|\mathbb{Z}_q^\times \times \mathbb{Z}_p^\times| = |\mathbb{Z}_{pq}^\times|$. Final, ... □