The Euler Totient

Definition 1 (Euler Totient)**.** *Let n be a positive integer. We define the* totient *of n, to be the cardinality of the set*

$$\mathcal{U}_n = \{a \mid 0 \leq a < n, \mathsf{gcd}(a, n) = 1\}.$$

We denote this number by $\mathsf{tot}(n)$*.*

Theorem 1.

1. *If $p > 1$ is a prime then $\mathsf{tot}(p) = p - 1$.*
2. *If $p > 1$ is a prime and $k \geq 2$, then $\mathsf{tot}(p^k) = p^k - p^{k-1}$*
3. *If a and b are positive integers with $\mathsf{gcd}(a, b) = 1$, then $\mathsf{tot}(ab) = \mathsf{tot}(a)\mathsf{tot}(b)$.*

Proof.

1. Let $0 \leq a < p$. Since $\mathsf{gcd}(a, p)$ is a proper divisor of p for $a > 0$ and p is prime, we have $\mathsf{gcd}(a, p) = 1$ if $a > 0$ and $\mathsf{gcd}(a, p) = p$ if $a = 0$.
2. Let $0 \leq a < p^k$, and consider $d = \mathsf{gcd}(a, p^k)$. Since d is a proper divisor of p^k, d is *not* 1 precisely when d, and thus a, is a multiple of p. Note that $a = pe$ is an integer with $0 \leq pe < p^k$ if and only if $0 \leq e < p^{k-1}$.
3. (to do)

□

Proposition 2. *If a, b, and c are integers such that $\mathsf{gcd}(a, c) = 1$ and $\mathsf{gcd}(b, c) = 1$, then $\mathsf{gcd}(ab, c) = 1$.*

Theorem 3 (Euler's Theorem)**.** *Let $n > 1$ and a be integers with $\mathsf{gcd}(a, n) = 1$. Then $a^{\mathsf{tot}(n)} \equiv 1 \mod n$.*