Proof. Theorem 3.9 implies that if $\gcd(m,n)=1$ then

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times,$$

and the result follows.

For the second part of the theorem notice that if p is prime and $k>0$ then among the numbers $1,2,\ldots,p^k$ all multiples of p and only those are not coprime to p^k. There are p^{k-1} many such numbers. Therefore $\varphi(p^k) = p^k - p^{k-1}$. □

Proposition 3.15. $\sum_{d|n}\varphi(d)=n$.

Proof 1. For a divisor d of n denote $A_d := \{a : 1\le a\le n : \gcd(n,a)=d\}$. Then $\{1,\ldots,n\}$ is the disjoint union of $(A_d)_{d|n}$ and $|A_d|=\varphi(n/d)$. □

Proof 2. Since φ is multiplicative, $\sum_{d|n}\varphi(d)$ is also multiplicative. So it suffices to establish the equality for $n=p^k$ where p is a prime. In this case

$$\sum_{d|n}\varphi(d)=\sum_{i=0}^{k}\varphi(p^i)=1+(p-1)+(p^2-p)+\cdots+(p^k-p^{k-1})=p^k.$$

□

3.6 Euler's theorem

Theorem 3.16 (Euler)**.** *If* $\gcd(a,m)=1$ *then* $a^{\varphi(m)}\equiv 1 \mod m$.

Proof 1. Denote $k:=\varphi(m)$ and let $m_1,\ldots,m_k$ be a *reduced residue system* modulo m, that is, $\gcd(m_i,m)=1$ for all i and $m_i\not\equiv m_j \mod m$ for $i\neq j$. In other words, $(\mathbb{Z}/m\mathbb{Z})^\times=\{m_1,\ldots,m_k\}$.

Observe that $am_1,\ldots,am_k$ is again a reduced residue system mod m and hence it is a permutation of $m_1,\ldots,m_k \bmod m$. Therefore

$$\prod_i m_i \equiv \prod_i am_i = a^k\prod_i m_i.$$

Since $\gcd\left(\prod_i m_i, m\right)=1$, we can deduce that $a^k\equiv 1 \mod m$. □

Proof 2. Consider the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ and its subgroup (a) generated by a. If the latter has order (cardinality) n then $a^n=1$. By Lagrange's theorem n divides the order of the group $(\mathbb{Z}/m\mathbb{Z})^\times$ which is $\varphi(m)$. Thus, $a^{\varphi(m)}=1$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ and we are done. □

Corollary 3.17 (Fermat's little theorem)**.** *If* p *is prime and* $p\nmid a$ *then* $a^{p-1}\equiv 1 \mod p$.

Proof. When p is prime, $\varphi(p)=p-1$. □