Generalization of Fermat's Little Theorem

Recall Euler's totient function

$\phi(n) = |\{x \in [n] : \gcd(x,n) = 1\}|$

Generalization of Fermat's Little Theorem:

$\forall n \in \mathbb{N}\ \forall x \in \mathbb{Z}\ (\gcd(x,n) = 1 \rightarrow x^{\phi(n)} \equiv 1 \bmod n)$

Example:

$\phi(9) = 6$

$2^6 = 64 \quad 64 \equiv 1 \bmod 9 \quad \text{as} \quad 64 = 7 \cdot 9 + 1.$

This theorem is very useful for computing exponents modulo n.

Example: $\phi(64) = 2^5(2-1) = 32$

$3^{100} \bmod 64 = 3^{(100 \bmod 32)} \bmod 64 = 3^4 \bmod 64 = 81 \bmod 64 = 17$

Generalization of Fermat's Little Theorem Proof

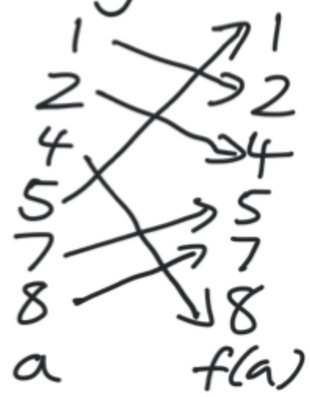
Theorem: $\forall n \in \mathbb{N}\, \forall x \in \mathbb{Z}\, (\gcd(x,n)=1 \rightarrow x^{\phi(n)} \equiv 1 \bmod n)$

Definition: Define $\mathbb{Z}_n^\times = \{a \in [n-1] : \gcd(a,n)=1\}$.

Note: For all $n>1$, $\mathbb{Z}_n^\times$ is the group of invertible elements in $\mathbb{Z}_n$.

Proof: Observe that if $\gcd(x,n)=1$ then the function $f(a) = xa \bmod n$ gives a bijection from $\mathbb{Z}_n^\times$ to itself.

Example: If $n=9$ and $x=2$



To show this is a bijection, take $f^{-1}(a) = x^{-1} \cdot a \bmod n$ where x^{-1} is the inverse of x in $\mathbb{Z}_n$ and observe that $\forall a \in \mathbb{Z}_n^\times\, (f^{-1}(f(a)) = a \wedge f(f^{-1}(a)) = a)$

Trick: Take $P = \prod_{a \in \mathbb{Z}_n^*} a$ and consider $\prod_{a \in \mathbb{Z}_n^*} (xa)$ in $\mathbb{Z}_n$. On the one hand, $\prod_{a \in \mathbb{Z}_n^*} (xa) = x^{\phi(n)} \prod_{a \in \mathbb{Z}_n^*} a = x^{\phi(n)} P$. On the other hand, in $\mathbb{Z}_n$, $\prod_{a \in \mathbb{Z}_n^*} (xa) = \prod_{a \in \mathbb{Z}_n^*} a = P$. Thus, $x^{\phi(n)} P = P$ in $\mathbb{Z}_n$. Multiplying both sides by P^{-1}, $x^{\phi(n)} = 1$ in $\mathbb{Z}_n$ so $x^{\phi(n)} \equiv 1 \bmod n$.