Fermat's Little Theorem

Fermat's Little Theorem:

$\forall p \in \mathbb{P}\ \forall x \in \mathbb{Z}\ (p \nmid x \rightarrow x^{p-1} \equiv 1 \pmod p)$

Examples:

$4^4 = 256 \quad 256 \equiv 1 \bmod 5$ as $256 = 51 \cdot 5 + 1$

$3^6 = 729 \quad 729 \equiv 1 \bmod 7$ as $729 = 104 \cdot 7 + 1$

$2^{10} = 1024 \quad 1024 \equiv 1 \bmod 11$ as $1024 = 93 \cdot 11 + 1$

Fermat's Little Theorem is very useful for computing exponents modulo p when p is prime.

Example:

$3^{100} \bmod 13 = 3^{(100 \bmod 12)} \bmod 13 = 3^4 \bmod 13 = 81 \bmod 13$

$= 3$ as $81 = 6 \cdot 13 + 3$

Proof of Fermat's Little Theorem

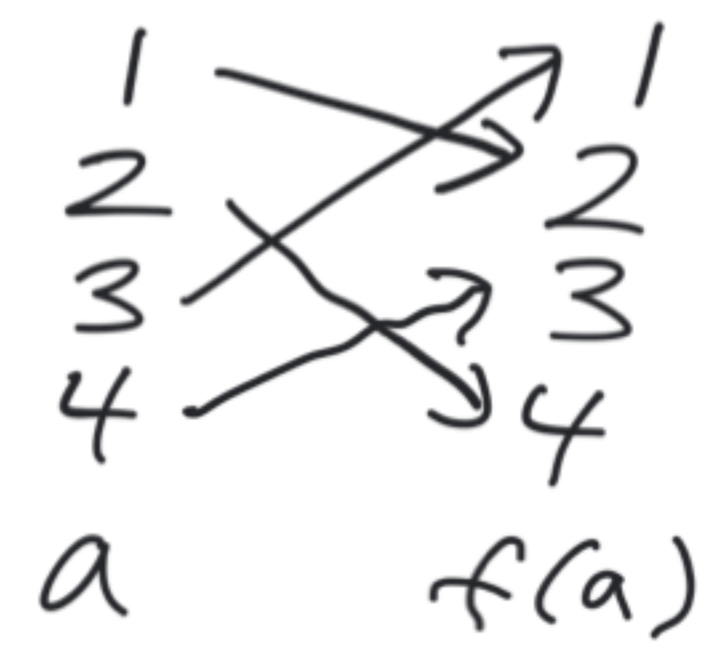
Fermat's Little Theorem:

$\forall p \in \mathbb{P}\ \forall x \in \mathbb{Z}\ (p \nmid x \rightarrow x^{p-1} \equiv 1 \pmod p)$

Proof:

Key idea: If $p \nmid x$ then $f(a) = xa \bmod p$ gives a bijection from $[p-1]$ to itself.

Example: If $p=5$ and $x=2$,



To see why this is a bijection, observe that if we take $f^{-1}(a) = x^{-1}a \bmod p$ (where x^{-1} is the inverse of x in $\mathbb{Z}_p$ then $\forall a \in [p-1]\ (f^{-1}(f(a)) = a \wedge f(f^{-1}(a)) = a)$.

Trick: Let $P = \prod_{j=1}^{p-1} j$ and consider $\prod_{j=1}^{p-1}(xj)$ in $\mathbb{Z}_p$. On the one hand, $\prod_{j=1}^{p-1}(xj) = x^{p-1}\prod_{j=1}^{p-1} j = x^{p-1} \cdot P$. On the other hand, in $\mathbb{Z}_p$, $\prod_{j=1}^{p-1}(xj) = \prod_{j=1}^{p-1} j = P$. In $\mathbb{Z}_p$, $x^{p-1} \cdot P = P$. Multiplying both sides by P^{-1}, $x^{p-1} = 1$ in $\mathbb{Z}_p$ so $x^{p-1} \equiv 1 \bmod p$.