1. Proof of rsa.

We want to show that

$$(m^e)^d \equiv m \pmod{n}$$

where $n=pq$, p and q are distinct prime numbers, and e and d are positive integers satisfying $ed \equiv 1 \bmod (p-1)(q-1)$. The fact $ed \equiv 1 \bmod (p-1)(q-1)$ implies ed is divisible by $(p-1)$ and $(q-1)$. We can thus write

$$ed-1 = h(p-1) = k(q-1).$$

for some nonnegative integers h & k.

We will check that $m^{ed} \equiv m \bmod pq$ by checking $m^{ed} \equiv m \bmod p$ and $m^{ed} \equiv m \bmod q$ separately.

i) show $m^{ed} \equiv m \bmod p$

Case 1: $m \equiv 0 \bmod p$. Then $m^{ed} \equiv 0 \equiv m \bmod p$.

Case 2: $m \not\equiv 0 \bmod p$. Then

$$m^{ed} = m^{ed-1}m = m^{h(p-1)}m = (m^{p-1})^h m \equiv 1^h m \equiv m \bmod p$$

since $m^{p-1} \equiv 1 \bmod p$ by fermat's little theorem.

Note that we can make an analogous argument $\bmod q$, using the fact that $(m^{q-1})^k \equiv 1 \bmod q$. Hence $m^{ed} \equiv m \bmod q$.

We have shown that $m^{ed} \equiv m \bmod p$ and $m^{ed} \equiv m \bmod q$.
Hence $m^{ed} \equiv m \bmod pq$, or equivalently,

$$m^{ed} \equiv m \bmod n.$$