Q34 Let p and q be two distinct odd primes such that $p-1 \mid q-1$. If $\gcd(n, pq) = 1$, show that

$n^{q-1} \equiv 1 \pmod{pq}$.

Sol: We will remember first: Little Fermat's theorem: If p is a prime number and a is a natural number, then $a^p \equiv a \pmod{p}$.

Also remember the Chinese Remainder Theorem: Let r and s be positive integers which are relatively prime and let a and b be any two integers. Then there is an integer N such that $N \equiv a \pmod{r}$ and $N \equiv b \pmod{s}$. Moreover, N is uniquely determined modulo rs. } In this problem: $p-1 \mid q-1 \Rightarrow \exists k \in \mathbb{Z}$:

$q-1 = k(p-1)$ By L.F.T. we have: $n^p \equiv n \pmod{p}$

$\Rightarrow n^p - n \equiv 0 \pmod{p} \Rightarrow n(n^{p-1}-1) \equiv 0 \pmod{p}$

$\Rightarrow n^{p-1} - 1 \equiv 0 \pmod{p}$ (because $\gcd(n,p) = 1$)

$\Rightarrow n^{p-1} \equiv 1 \pmod{p} \Rightarrow 1 \equiv 1^k \equiv (n^{p-1})^k \equiv n^{q-1} \pmod{p}$

So we have. ~~$n^{p-1} \equiv 1 \pmod{p}$~~ $n^{q-1} \equiv 1 \pmod{p}$

and $n^{q-1} \equiv 1 \pmod{q}$ (by F.L.T.) And by the Chinese Remainder Theorem, we know that n^{q-1} is uniquely determined modulo $pq \Rightarrow n^{q-1} \equiv 1 \pmod{pq}$ ▨