$\boxed{Q34}$ 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: $n^{q-1} \equiv 1 \pmod p$

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

$\boxed{Q32}$ If $2q+1$ is an odd prime, prove that $(q!)^2+(-1)^q \equiv_{2q+1} 0$.

Sol. Remember Wilson's Theorem: The integer p is prime iff

$(p-1)! \equiv -1 \pmod p$. Then: $((2q+1)-1)! \equiv -1 \pmod{2q+1}$

$1 \times 2 \cdot 3 \times \dots \cdot q \times (q+1) \cdot (q+2) \cdot \dots \cdot (2q) \equiv -1 \pmod{2q+1}$

$q! \times [(2q+1)-(q)][(2q+1)-(q-1)] \times \dots \times [(2q+1)-1] \equiv -1 \pmod{2q+1}$

$q!(-q)(-(q-1))(-(q-2))\dots(-1) \equiv -1 \pmod{2q+1}$

$q!(-1)^q q! \equiv -1 \pmod{2q+1} \Rightarrow (-1)^q (q!)^2 + 1 \equiv 0 \pmod{2q+1}$

We now multiply by $(-1)^q$: $(q!)^2 + (-1)^q \equiv 0 \pmod{2q+1}$ ∎

$\boxed{Q31}$ Prove Wilson's Theorem. Sol:

Remember Lagrange's theorem (number theory): If p is a prime number and $f(x) \in \mathbb{Z}[x]$ is a polynomial with integer coefficients, then either: (i) every coefficient of $f(x)$ is divisible by p, or (ii) $f(x) \equiv 0 \pmod p$ has at most $\deg(f(x))$ incongruent solutions.

If the modulus is not prime (probably p in this case) then it is possible for there to be more than $\deg f(x)$ solutions.

Proof of Wilson's thm: The result is trivial when $p=2$, so assume p is an odd prime $p \geq 3$. Since the residue classes $\pmod p$ are a field, every nonzero a has a unique multiplicative inverse, a^{-1}.