$\boxed{Q\,3\,4}$ Let p and q be two distinct odd primes such that $p-1 \mid q-1$. If $\gcd(n,pq)=1$, show that $n^{q-1} \equiv 1 \pmod{pq}$.

<u>Sol</u>: 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 $pq \Rightarrow n^{q-1} \equiv 1 \pmod{pq}$ ▨

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

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

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

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

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

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

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}.

Lagrange's theorem implies that the congruence $a^2 \equiv 1$ can have at most two roots (mod p), therefore the only values for which $a = a^{-1}$ ~~$a \equiv 1$~~ (mod p) are $a \equiv \pm 1$ (mod p). Thus, with the exception of ± 1, the factors of $(p-1)!$ can be arranged in unequal pairs, where the product of each pair is $\equiv 1$ (mod p). ▨

Proof using Fermat's little Theorem: Result is trivial for $p=2$, so suppose $p \geq 3$. Consider the polynomial $g(x) = (x-1)(x-2)\dots(x-(p-1))$.

The polynomial g has degree $(p-1)$, leading term x^{p-1}, and constant term $(-1)^{p-1}(p-1)! = (p-1)!$. Its $p-1$ roots are $1, 2, \dots, p-1$. Now consider $h(x) = x^{p-1} - 1$. The polynomial h has leading term x^{p-1}, degree $(p-1)$, and, modulo p, Fermat's little Theorem says it also has the roots $1, 2, \dots (p-1)$. Finally consider $f(x) = h(x) - g(x)$. The polynomial f has degree ~~of~~ at most $(p-2)$, because the leading terms cancel. Modulo p, it has the same roots $1 \dots (p-1)$, but Lagrange's theorem says it cannot have more than $(p-2)$ roots modulo p. Therefore f must vanish identically (is identically zero), so its constant term $(p-1)! + 1 \equiv 0 \pmod p$

$\boxed{Q30}$ Prove that $5n^3 + 7n^5 \equiv 0 \pmod{12}$ $\forall n \in \mathbb{Z}$. Sol:

$f(n) \equiv 5n^3 + 7n^5 \equiv 5n^3 + (-5)n^5 \equiv 5(n^3 - n^5) \equiv 5(n^5 - n^3) = n^3(n^2 - 1) \pmod{12}$

Remember Euler's theorem (Fermat-Euler theorem or Euler's totient theorem): If a and n are coprime positive integers, then $a^{\varphi(n)} \equiv 1 \pmod{n}$ where $\varphi(n)$ is Euler's totient function. Remember: $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ where the product is over the distinct prime numbers dividing n. (Rk: Euler's theorem is generalized by Carmichael's theorem.). Now:

$f(n) \equiv (n-1)n^3(n+1) \pmod{12}$ and $g(n) = (n-1)n^3(n+1)$

The factorization of g includes the product of three consecutive numbers, thus $g(n) \equiv 0 \pmod{3}$. Case 1: $n = 1, 3, 5, 7, 9, 11$

The number n is coprime with 4, that is: $\gcd(n, 4) = 1$.

Applying Euler's theorem: $n^{\varphi(4)} = n^{2^{2-1}(2-1)} = n^2 \equiv 1 \pmod{4}$

$\Rightarrow n^2 - 1 \equiv 0 \pmod{4} \Rightarrow (n-1)n^3(n+1) \equiv 0 \pmod{4} \Rightarrow g(n) \equiv 0 \pmod{4}$

We apply the Chinese Remainder Theorem (C.R.T.) to the following two ~~expr~~ expressions: $g(n) \equiv 0 \pmod{3} \wedge g(n) \equiv 0 \pmod{4}$

$\Rightarrow g(n) \equiv 0 \pmod{12} \Rightarrow f(n) \equiv 0 \pmod{12}$. ... (I)

Case 2: $n = 0, 2, 4, 6, 8, 10 \Rightarrow n^2 \equiv 0 \pmod{4} \Rightarrow g(n) \equiv 0 \pmod{4}$

By C.R.T.: $g(n) \equiv 0 \pmod{12} \Rightarrow f(n) = 0 \pmod{12}$ ... (II)

Joining (I) and (II): $f(n) \equiv 0 \pmod{12}$ $\forall n \in \mathbb{Z}$ (Because, mod 12, every integer is congruent with either a value in case 1 or in case 2)

$\blacksquare$