

$5n^2 - 1 = N$ divisible by p ✓
 $\Rightarrow 5n^2 - 1 \equiv 0 \pmod{p} \Rightarrow 5n^2 \equiv 1 \pmod{p}$ ✓
 so $(5/p)(n^2/p) = (1/p)$ ✓

but $(n^2/p) = (1/p) = 1 \therefore (5/p) \cdot 1 = 1 \Rightarrow (5/p) = 1$ ✓

You'll never know how much agony this question caused me.

quadratic residue of 5. Any no. can be expressed as

$$\begin{aligned}
 &5k \\
 &5k+1 \\
 &5k+2 \\
 &5k+3 \\
 &5k+4
 \end{aligned}$$

Taken modulo 5, these become

$$\begin{aligned}
 &0 \\
 &1 \\
 &2 \\
 &3 \\
 &4
 \end{aligned}$$

5 has $(5-1)/2 = 2$ quadratic residues:

1 since $1 = 1^2 \pmod{5}$

4 since $4 = 2^2 \pmod{5}$ ✓

and

$$(5k+3)^2 = 5(5k^2 + 6k + 1) + 4 = 4 \pmod{5}$$

$$(5k+4)^2 = 5(5k^2 + 8k + 3) + 1 = 1 \pmod{5}$$

$\therefore p$ has one of the forms $5k+1$ or $5k+4$ ✓

iii) Suppose that all the primes which divide p have form $5k+1$ (since N is odd, from part ii), all the primes which divide N have form $5k+1$ or $5k+4$. The product of any two of these primes will be of the form $5k+1$ ✓

$$(5m+1)(5n+1) = 5(5m+n+1) + 1$$

and the product of any no. of primes