Prop: There are infinitely many primes congruent to 3 (mod 4).

Proof We argue by contradiction. Assume that there are only finitely many such primes. In particular, suppose that

$$p_1, \_\_\_\_, p_n \quad \text{is the complete list}$$

of all primes $\equiv 3 \pmod 4$.

Each $p_i \equiv 3 \pmod 4$
$\equiv -1 \pmod 4$

Thus the product $p_1 \_\_\_ p_n \equiv (-1)^n \pmod 4$
$\equiv \pm 1 \pmod 4$.

Therefore $2(p_1 \_\_\_ p_n) \equiv \pm 2 \pmod 4$
$\equiv 2 \pmod 4$

and so the odd integer

$$M \underset{\text{def}}{=\!=} 2(p_1 \_\_ p_n) + 1 \equiv 2 + 1 \pmod 4$$
$$\equiv 3 \pmod 4$$
$$\equiv -1 \pmod 4.$$

By definition of M, $p_i \nmid M$ since there is a remainder of 1 on division by p_i.

By the fundamental th$^{\underline{m}}$, M has a prime factorization

$$M = q_1 \text{—} q_k$$

q_j all prime, $k \geq 1$ ($k = 1$ if M is prime).

Now $p_i \nmid M$ ~~and~~ $\Rightarrow$ the q_j are distinct from $p_1 \text{—} p_n$.

M odd $\Rightarrow$ each q_j is odd

$\Rightarrow q_j \equiv 1 \pmod 4$ OR $\equiv 3 \pmod 4$

$\Rightarrow q_j \equiv 1 \pmod 4$ OR $\equiv -1 \pmod 4$

Since $M \equiv -1 \pmod 4$, we conclude that at least one of the $q_j \equiv -1 \pmod 4$.

That is at least one of the primes $q_j \equiv 3 \pmod 4$.

But q_j distinct from $p_1, \text{—}, p_n \Rightarrow$ we contradicted the assumption that $p_1, \text{—}, p_n$ was <u>the complete list</u> of primes $\equiv 3 \pmod 4$, and hence the assumption that there was a finite list.

Thus, there are infinitely many such primes. $\blacksquare$