Infinitude of Specific Types of Primes

Lemma: All integers of the form 4 m + 3 is divisible by a prime of the same form.

Proof: There are 2 kinds of primes, primes of the form 4 n + 1 and 4 n + 3. If the number 4 m + 3's factors are solely of the form 4 n + 1, then their product which is of the form 4 k +1 will not equal 4 m + 3 for integer m and k. Therefore, there must be at least 1 prime factor of 4 m + 3 in the same form as itself.

Theorem: There are infinitely many primes of the form 4 v + 3.

Proof: If there are finitely many primes of this form, then the largest one can be called $p_k = 4 n_k + 3$. The number $4 p_k + 3$ is larger than the largest prime of this form, so it must be composite. By the above lemma, $4 p_k + 3$ must be divisible by one of these primes: $p_0 = 3$, $p_1 = 7$,…, $p_i = n_i + 3$, …, p_k. Since p_k is only prime in the list that will divide $4 p_k$ and p_0 is the only prime that will divide 3. There is no single prime in the list, that will divide both $4 p_k$ and 3. But since the lemma is true, $4 p_k + 3$ must be divisible by some prime of the form 4 v + 3. This means that there is another prime of the form 4 v + 3 that is not in the list. This contradicts that there are finitely many primes of this form, so there must be infinitely many primes of the form 4 v + 3.

Extension: If there is such an integer P so that only 1 of these (P-1), (P-2), … not including 1, is relatively prime with P, then, by using the same method, it is easy to see that there are infinitely many primes of the form Pn + R, where R is that integer that is relatively prime with P.