PRIMES IN ARITHMETIC PROGRESSIONS

> THEOREM (EUCLID): There are infinitely many primes.

(1) Prove Euclid's Theorem as follows:
By way of contradiction, suppose that there are only finitely many primes $p_1, \ldots, p_k$. Consider the number $N = p_1 p_2 \cdots p_k + 1$ and derive a contradiction. (Warning: the contradiction is *not* that N must be prime!)

(2) Modify[1] Euclid's argument to show that there are infinitely many primes p such that $p \equiv 3 \pmod{4}$.

(3) Extending your argument from (2):
   (a) Explain why your method from (2) cannot be used in the same way to show that there are infinitely many primes p such that $p \equiv 1 \pmod{4}$.
   (b) For which classes $[a] \in \mathbb{Z}_3^\times$ can your argument from (2) be modified to show that there are infinitely many primes congruent to a modulo 3? Complete these cases.
   (c) For which classes $[a] \in \mathbb{Z}_5^\times$ can your argument from (2) be used in the same way to show that there are infinitely many primes congruent to a modulo 5?

(4) In this problem we will show that there are infinitely many primes congruent to 1 modulo 4: If there are only finitely many $p_1, \ldots, p_k$, consider $N = 4(p_1 \cdots p_k)^2 + 1$. Show that if q is a prime factor of N then -1 is a quadratic residue modulo N, and conclude the proof.

(5) Show that there are infinitely many primes congruent to 1 modulo 3.
Hint: Consider $N = 3(p_1 \cdots p_k)^2 + 1$, and note that $[a]^{-1}$ is a square if and only if $[a]$ is a square.

(6) Show that there are infinitely many primes congruent to 4 modulo 5.

(7) Show that there are infinitely many primes congruent modulo 8 to 7, to 5, and to 3.

> THEOREM* (DIRICHLET): If a and n are coprime integers, with $n > 0$, then there are infinitely many primes p such that $p \equiv a \pmod{n}$.

[1] Hint: Use a different formula for N that returns a number congruent to 3 modulo 4.