2.38 Theorem. (Infinitude of $4k+3$ Primes Theorem) There are infinitely many prime numbers that are congruent to 3 modulo 4.

Proof. Suppose not. That is, suppose there is a finite set $S = \{p_1, p_2, ..., p_m\}$ such that each p_i is congruent to 3 modulo 4. Let a natural number (not in S) $n = 2p_1p_2...p_m + 1$. We know this number to be odd (by letting $p_1p_2...p_m = k$ such that $2k+1$) and no p_i divides n. Thus, $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$. Suppose $n \equiv 1 \pmod 4$. By definition, $4k = n - 1$. Substituting for n,

$$\begin{aligned} 4k &= (2p_1p_2...p_m + 1) - 1 \\ &= 2p_1p_2...p_m. \end{aligned}$$

This implies $4|2p_1p_2...p_m$, which is not true since $p_1p_2...p_m$ is odd. Thus, $n \equiv 3 \pmod 4$. By FTA, n has a prime factorization such that $n = r_1r_2...r_t$. We want to show that one of these prime factors are congruent to 3 modulo 4 (there may be more, but we only need to show one) and that it is not in S. Since $n \equiv 3 \pmod 4$, we can write $r_1r_2...r_m \equiv 3 \pmod 4$. By Theorem 2.37, we know that one of these prime factors is not congruent 1 modulo 4, else $n \equiv 1 \pmod 4$. Thus, at least one of these primes must be congruent 3 modulo 4. This contradicts our initial assumption because none of n's primes are in set S. Therefore, there are infinitely many prime numbers that are congruent to 3 modulo 4. $\square$