MATH 114

Solution to problem 3.1 #30

What goes wrong when you try to adapt the proof that there are infinitely many primes to show that there are infinitely many primes of the form $4k+1$?

The first two columns below are theorems with proofs given in the book (make sure that you understand every step in these proofs) and the third column is an attempt to modify the proofs.

Theorem	**Theorem**	**Conjecture**
There are infinitely many primes.	There are infinitely many primes of the form $4k+3$.	There are infinitely many primes of the form $4k+1$.
Proof	**Proof**	**Attempt to modify proof**
Suppose there are finitely many primes: $p_1,\ p_2,\ \ldots, p_n$.	Suppose there are finitely many primes of the form $4k+3$: $p_1,\ p_2,\ \ldots, p_n$.	Suppose there are finitely many primes of the form $4k+1$: $p_1,\ p_2,\ \ldots, p_n$.
Consider $Q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.	Consider $Q = 4p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1$.	Consider $Q = 4p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
	Q is of the form $4k+3$.	Q is of the form $4k+1$.
<u>Case I.</u> Q is prime But $Q > p_i$ for all i, so Q is not one of the primes listed above. We get a contradiction.	<u>Case I.</u> Q is prime But $Q > p_i$ for all i, so Q is not one of the primes listed above. We get a contradiction.	<u>Case I.</u> Q is prime But $Q > p_i$ for all i, so Q is not one of the primes listed above. We get a contradiction.
<u>Case II.</u> Q is composite Q has a prime factorization.	<u>Case II.</u> Q is composite Q has a prime factorization.	<u>Case II.</u> Q is composite Q has a prime factorization.
	The only even prime is 2, and odd primes are either of the form $4k+1$ or of the form $4k+3$.	The only even prime is 2, and odd primes are either of the form $4k+1$ or of the form $4k+3$.
Let the first prime in the factorization be p_i (for some i). Then p_i divides both Q and $p_1 \cdot p_2 \cdot \ldots p_n$, therefore p_i divides their difference which is 1. This is impossible.	The factorization cannot contain 2 because Q is odd. It cannot contain a prime of the form $4k+3$ because then it would have to be p_i for some i. Then p_i would divide both Q and $4p_1 \cdot p_2 \cdot \ldots p_n$ and therefefore would divide their difference which is -1. This is impossible.	The factorization cannot contain 2 because Q is odd. It cannot contain a prime of the form $4k+1$ because then it would have to be p_i for some i. Then p_i would divide both Q and $4p_1 \cdot p_2 \cdot \ldots p_n$ and therefefore would divide their difference which is 1. This is impossible.
	Therefore the prime factorization only contains primes of the form $4k+1$. But a product of numbers of the form $4k+1$ is of the form $4k+1$ while Q is of the form $4k+3$. (If $q \equiv 1 (\text{mod } 4)$ and $r \equiv 1 (\text{mod } 4)$ then $qr \equiv 1 (\text{mod } 4)$.)	Therefore the prime factorization only contains primes of the form $4k+3$. *And the product of numbers of the form $4k+3$ can be of the form $4k+1$...* *(If $q \equiv 3 (\text{mod } 4)$ and $r \equiv 3 (\text{mod } 4)$ then $qr \equiv 9 \equiv 1 (\text{mod } 4)$.)*
We get a contradiction again, which means that the assumption that there are finitely many primes was false.	We get a contradiction again, which means that the assumption that there are finitely many primes of the form $4k+3$ was false.	*We do not get a contradiction, so this modification does not work.*