QUESTION

(i) Prove that any prime $p > 3$ is either of the form $6k+1$ or of the form $6k+5$ for some integer k.

(ii) Prove that the product of any two integers of the form $6k+1$ is of that same form.

(iii) Adapt the proof of Theorem 2.7 to prove that there are infinitely many primes of the form $6k+5$.

ANSWER

(i) By the division algorithm, any integer can be written in one of the forms $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$. Of these, $6k, 6k+2$ and $6k+4$ are even, and $6k+3$ is divisible by 3. Thus none of these can represent a prime > 3. Thus p must be of the form $6k+1$ or $6k+5$.

(ii) $(6k+1)(6l+1) = 36kl + 6k + 6l + 1 = 6(6kl + k + l) + 1$.

Thus the product of two integers of the form $6n+1$ is again of the form $6n+1$

(iii) Suppose there are only finitely many primes of the form $6k+5$. Let them be $p_1, \ldots p_n$, and consider $N = 6(p_1 \ldots p_n) - 1$

Now $N = 6((p_i \ldots p_n) - 1) + 5$, so N is of the form $6k+5$. Thus neither 2 nor 3 divides N, so by (i) the prime divisors of N are either of the form $6k+1$ or $6k+5$. Suppose every prime dividing N is of the form $6k+1$. Then, by repeated use of (ii), N would also be of that form- but we have seen that this is not the case.

Thus N has a prime divisor, p say, of form $6k+5$. By assumption, $p_1, \ldots, p_n$ are the only such primes, so $p = p_i$ for some i, and in particular $p | p_1 \ldots p_n$. But $p|N$, so by theorem 1.3(4), $p | 6(p_1 \ldots p_n) - N$, i.e. $p|1$- but this contradicts p prime, as all primes are > 1.

This contradiction shows our original assumption was wrong, so there are infinitely many primes of the form $6k+5$.