QUESTION

(i) Prove that there are infinitely many primes congruent to 3 mod 8.

[Hint: Suppose $p_1, p_2 \ldots, p_n$ are the only such primes. Consider $N = (p_1 p_2 \ldots p_n)^2 + 2$, and use the result of question 5.]

(ii) Prove that there are infinitely many primes congruent to 1 mod 6.

[Hint: Suppose $p_1, p_2 \ldots, p_n$ are the only such primes. Consider $(2p_1 p_2 \ldots p_n)^2 + 2$ and use the result of question 5.]

ANSWER

(i) Following the hint, suppose $p_1, p_2 \ldots p_n$ are the only primes $\equiv 3 \bmod 8$. (The list is non-empty- $p_1 = 3, p_2 = 11$, etc.) Set $N = (p_1 p_2 \ldots p_n)^2 + 2$. Now each p_I is odd, so N is odd, and hence all prime divisors of N ore odd. Let p be a prime divisor of N. Then $N \equiv 0 \bmod p$, so that $(p_1 p_2 \ldots p_n)^2 \equiv -2 \bmod p$. This shows that -2 is a square mod p, so that $\left(\frac{-2}{p}\right) = 1$. Thus we may use question 5(i) to deduce that $p \equiv 1$ or 3 mod 8.

Now identify $(8k+1)(8l+1) = 8(8kl + k + l) + 1$ shows that if every prime dividing N is $\equiv 1 \bmod 8$, then N is also $\equiv 1 \bmod 8$. But $N = (p_1 p_2 \ldots p_n)^2 + 2 = p_1^2 p_2^2 \ldots p_n^2 + 2$, and as each $p_i \equiv 3 \bmod 8$, each $p_I^2 \equiv 9 \equiv 1 \bmod 8$. Thus $p_1^2 p_2^2 \ldots p_n^2 \equiv 1 \bmod 8$, so $N \equiv 1 + 2 \equiv 3 \bmod 8$. Thus N has at least one prime divisor $p \equiv 3 \bmod 8$. As $p_1, p_2, \ldots, p_n$ are the only primes $\equiv 3 \bmod 8$, $p = p_i$ for some i. Thus $p | p_1 p_2 \ldots p_n$. But $p|N$. Hence $p | N - (p_1 p_2 \ldots p_n)^2 = 2$. But we have already remarked that every prime divisor of N is odd, so $p \neq 2$. This contradiction shows that our original assumption was wrong, so there are infinitely many primes congruent to 3 mod 8.

(ii) Suppose $p_1, p_2, \ldots, p_n$ are the only primes$\equiv 1 \bmod 6$. (The list is non-empty, e.g. $p_1 = 7$) Set $N = (2p_1 p_2 \ldots p_n)^2 + 3$. We note that as $3 \not| p_i$ for each i, $3 \not| N$. Also N is odd, so each prime divisor of N is odd.

Let p be a prime divisor of N. Then $N \equiv 0 \bmod p$, so $(2p_1 p_2 \ldots p_n)^2 \equiv -3 \bmod p$, and so $\left(\frac{-3}{p}\right) = 1$, Thus by question 5(ii), $p \equiv 1 \bmod 6$. But by assumption, $p_1, p_2 \ldots p_n$ are the only primes $\equiv 1 \bmod 6$. Thus $p = p_i$ for some i, and hence $p | (2p_1 p_2 \ldots p_n)$. But $p|N$, so $p | N - (2p_1 p_2 \ldots p_n)^2 = 3$. But we have already seen $3 \not| N$, so $p \neq 3$. This contradiction shows that our original assumption was wrong, and so there are infinitely many primes $\not\equiv 1 \bmod 6$.