Problem 1. a) Prove that any natural number n such that $n \equiv 3 \pmod 4$ has a prime divisor p such that $p \equiv 3 \pmod 4$ (hint: note that every odd prime number q either satisfies $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$; what can you say about product of primes of the first type?)

b) Prove that $n! - 1 \equiv 3 \pmod 4$ for any $n > 3$.

c) Prove that every prime divisor of $n! - 1$ is bigger than n.

d) Conclude that there are infinitely many primes q such that $q \equiv 3 \pmod 4$.

Solution: a) Note that for every odd integer m either $m \equiv 1 \pmod 4$ or $m \equiv 3 \pmod 4$. Also, iff $a_1, ..., a_s$ are integers satisfying $a_i \equiv 1 \pmod 4$ for $i = 1, 2, ..., s$ then by multiplying these congruences we see that $a_1 a_2 ... a_s \equiv 1 \pmod 4$.

Consider now a positive integer $n \equiv 3 \pmod 4$. Note that n is odd, so all its prime divisors are odd. We know that n is a product of prime numbers. If each of these prime numbers were $\equiv 1 \pmod 4$, then according to our remark above, also their product n would be $\equiv 1 \pmod 4$, which is false. Thus n must have a prime divisor $p \equiv 3 \pmod 4$.

b) If $n > 3$ then $n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot n$ is divisible by 4. Thus $n! \equiv 0 \pmod 4$ and $n! - 1 \equiv -1 \equiv 3 \pmod 4$.

c) If $p \leq n$ then p divides $n!$ and therefore does not divide $n! - 1$. It follows that any divisor of $n! - 1$ is larger than n.

d) Let $n > 3$. By a) and b) there is a prime number $q \equiv 3 \pmod 4$ which divides $n! - 1$ and $q > n$ by c). Thus there are arbitrarily large primes $\equiv 3 \pmod 4$, so the set of such primes is infinite.

Problem 2. Prove that every composite number n has a prime divisor not larger than $\sqrt{n}$.

Solution: Since n is composite, we may factor n as $n = ab$, where $1 < a \leq b$. Thus $n = ab \geq a^2$ and $\sqrt{n} \geq a$. Any prime divisor of a is a prime divisor of n and it is $\leq \sqrt{n}$.

Problem 3. The numbers n, $n+2$, $n+4$ are prime. What is n? Prove your answer. (Hint: consider these numbers modulo 3).

Solution: Note that one of the congruences $n \equiv 0 \pmod 3$, $n \equiv 1 \pmod 3$, $n \equiv 2 \pmod 3$ holds. If $n \equiv 0 \pmod 3$ then $3|n$. Since n is a prime, we must have $n = 3$ and then indeed $n+2 = 5$, $n+4 = 7$ are primes.

If $n \equiv 1 \pmod 3$ then $n+2 \equiv 3 \equiv 0 \pmod 3$, i.e. $3|n+2$. Since $n+2$ is a prime, we must have $3 = n+2$, i.e. $n = 1$. Hovewer, $n = 1$ is not a prime, so this case is not possible.

If $n \equiv 2 \pmod 3$ then $n+4 \equiv 6 \equiv 0 \pmod 3$, i.e. $3|n+4$. Again, since $n+4$ is prime, we have $n+4 = 3$, i.e. $n = -1$, which is not possible.

Thus $n = 3$ is the only solution.