SOLUTIONS: PROBLEM SET 25 FROM SECTION 11.2

2. $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$. Both factors are 1 if $p \equiv 1 \pmod{12}$ and both are -1 if $p \equiv -1 \pmod{12}$. If $p \equiv \pm 5 \pmod{12}$,the two factors have opposite signs so that the product is -1.

4. $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 1, 4 \pmod 5$.

6. Let $Q = 5(n!)^2 - 1$. Then 5 and $n!$ are both relatively prime to Q. Let x be a modular inverse for $n! \pmod Q$. Then $x^2 \equiv 5 \pmod Q$. It follows that 5 is a quadratic residue $\pmod Q$ and hence $\pmod p$ for every prime divisor p of Q. Hence by problem 4, every prime divisor of Q is congruent to 1 or to 4 $\pmod 5$. But $Q \equiv 4 \pmod 5$. Hence all the prime divisors of Q cannot be congruent to 1 $\pmod 5$, and at least one of them must be congruent to 4 $\pmod 5$ as desired. Moreover, all prime divisors of Q are relatively prime to $n!$, and hence larger than n. It follows that there are arbitrarily large primes congruent to 4 $\pmod 5$, and hence there are infinitely many of them.