1 For which positive integers \( n \) that are relatively prime to 15 does the Jacobi symbol \( \left( \frac{15}{n} \right) \) equal 1?

**Solution** : First note that for the Jacobi symbol to be defined, we require that \( n \) is odd. Suppose first that \( n \equiv 1 \pmod{4} \). Then
\[
\left( \frac{15}{n} \right) = \left( \frac{3}{n} \right) \left( \frac{5}{n} \right) = \left( \frac{n}{3} \right) \left( \frac{n}{5} \right)
\]
and so to have \( \left( \frac{15}{n} \right) = 1 \), we require that either
\[
\left( \frac{n}{3} \right) = \left( \frac{n}{5} \right) = 1 \quad \text{or} \quad \left( \frac{n}{3} \right) = \left( \frac{n}{5} \right) = -1.
\]
The first of these occurs when
\[
n \equiv 1 \pmod{3} \quad \text{and} \quad n \equiv 1, 4 \pmod{5},
\]
while the second corresponds to
\[
n \equiv 2 \pmod{3} \quad \text{and} \quad n \equiv 2, 3 \pmod{5}.
\]
Similarly, if \( n \equiv 3 \pmod{4} \), we have
\[
\left( \frac{15}{n} \right) = \left( \frac{3}{n} \right) \left( \frac{5}{n} \right) = - \left( \frac{n}{3} \right) \left( \frac{n}{5} \right)
\]
and so to have \( \left( \frac{15}{n} \right) = 1 \), we require that either
\[
\left( \frac{n}{3} \right) = 1, \left( \frac{n}{5} \right) = -1 \quad \text{or} \quad \left( \frac{n}{3} \right) = -1, \left( \frac{n}{5} \right) = 1.
\]
The first of these occurs when
\[
n \equiv 1 \pmod{3} \quad \text{and} \quad n \equiv 2, 3 \pmod{5},
\]
while the second corresponds to
\[
n \equiv 2 \pmod{3} \quad \text{and} \quad n \equiv 1, 4 \pmod{5}.
\]
In summary, we find, via the Chinese Remainder Theorem, that there are precisely 8 residue classes for \( n \) modulo 60 for which \( \left( \frac{15}{n} \right) = 1 \). They are (after a little work) given by
\[
n \equiv 1, 7, 11, 17, 43, 49, 53, 59 \pmod{60}.
\]

2 Show that there exist infinitely many primes \( p \equiv 1 \pmod{4} \). Hint : recall Assignment 1; you may assume without proof, if \( p \) is an odd prime, that there exists an integer \( x \) such that \( x^2 \equiv -1 \pmod{p} \) iff \( p \equiv 1 \pmod{4} \)
Solution: There are several ways to approach this problem. Let us suppose that there are only finitely many primes congruent to 1 modulo 4, say
\[ p_1 < p_2 < \cdots < p_k. \]
Set
\[ N = (p_k!)^2 + 1. \]
Then we have that \( N \) is odd and (arguing as in Euclid’s proof) not divisible by any of the primes \( p_1, p_2, \ldots, p_k \). But \( N \) must have an odd prime divisor, say \( q \), so that
\[ (p_k!)^2 \equiv -1 \pmod{q}, \]
and so
\[ \left( \frac{-1}{q} \right) = 1. \]
It follows that \( q \equiv 1 \pmod{4} \), contradicting our initial assumption. We conclude that there exist infinitely many primes congruent to 1 modulo 4.

3 We calculate the continued fraction expansion of \( e \) as
\[ e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots]. \]
Find the first 5 convergents to \( e \).

Solution: We have
\[ C_0 = [2] = 2, \quad C_1 = [2; 1] = 2 + \frac{1}{1} = 3, \]
\[ C_2 = [2; 1, 2] = 2 + \frac{1}{1 + \frac{1}{2}} = 2 + \frac{2}{3} = \frac{8}{3}, \]
\[ C_3 = [2; 1, 2, 1] = 2 + \frac{1}{1 + \frac{1}{\frac{1}{2} + \frac{1}{3}}} = 2 + \frac{3}{4} = \frac{11}{4} \]
and
\[ C_4 = [2; 1, 2, 1, 1] = 2 + \frac{1}{1 + \frac{1}{\frac{1}{2} + \frac{1}{\frac{1}{1} + \frac{1}{3}}}} = 2 + \frac{5}{7} = \frac{19}{7}. \]

4 Suppose that
\[ \alpha = [a_0; a_1, \ldots, a_n], \]
where \( a_i \in \mathbb{Z} \) for each \( i \) and we have that \( a_i \geq 2 \) for \( i \geq 1 \). If we write \( C_k = p_k/q_k \) for the \( k \)th convergent, prove that \( q_k \geq 2^k \).

Solution: We proceed by induction upon \( k \). We have that
\[ q_0 = 1 = 2^0 \quad \text{and} \quad q_1 = a_1 \geq 2 = 2^1. \]
For \( k \geq 2 \), we have that
\[ q_k = a_k q_{k-1} + q_{k-2}. \]
Given $k \geq 2$, suppose that we have, for each $i \leq k$, $q_i \geq 2^i$. It follows that
\[ q_{k+1} = a_{k+1}q_k + q_{k-1} \geq 2 \cdot q_k + q_{k-1} \geq 2 \cdot 2^k + 2^{k-1} > 2^{k+1}, \]
which, by the principle of mathematical induction, implies the desired claim.

5 Prove that if $p \geq 7$ is prime, then there are always at least two consecutive quadratic residues, say $a$ and $a + 1$, modulo $p$.

Solution: We been by observing that
\[ 1 = \left( \frac{10}{p} \right)^2 = \left( \frac{10}{p} \right) \left( \frac{10}{p} \right) = \left( \frac{10}{p} \right) \left( \frac{2}{p} \right) \left( \frac{5}{p} \right). \]
It follows that we cannot have
\[ \left( \frac{10}{p} \right) = \left( \frac{2}{p} \right) = \left( \frac{5}{p} \right) = -1 \]
and so
\[ \left( \frac{a}{p} \right) = \left( \frac{a + 1}{p} \right) = 1 \]
for one of $a \in \{1, 4, 9\}$. 