Problem 1: If \( m \) and \( n \) are integers not both zero, we define their least common multiple \( \text{lcm}(m,n) \) to be the smallest positive integer \( z \) such that \( m|z \) and \( n|z \). Describe how to efficiently compute \( \text{lcm}(m,n) \), and explain why this works and why this is efficient. (Hint: Since there is no known efficient algorithm for factoring integers, there isn’t a known efficient algorithm for computing prime decompositions \( n = \prod p_i^{a_i} \) and \( m = \prod p_i^{b_i} \). Nonetheless, such decompositions exist. Consider a formula for \( \text{lcm}(m,n) \) expressed through the prime decompositions of \( m \) and \( n \): relate this to a formula for \( \gcd(m,n) \) and for \( mn \).)

Solution: Let \( p_1, p_2, p_3 \ldots \) denote the sequence of all prime numbers. Suppose the prime factorization of \( m \) is \( m = \prod_{i=1}^{\infty} p_i^{a_i} \) for the nonnegative integers \( a_1, a_2, a_3, \ldots \) (only finitely many of which are nonzero) and suppose the prime factorization of \( n \) is \( n = \prod_{i=1}^{\infty} p_i^{b_i} \) for the nonnegative integers \( b_1, b_2, b_3, \ldots \) (only finitely many of which are nonzero). Recall that \( \gcd(m,n) = \prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}} \), and it is clear that \( mn = \prod_{i=1}^{\infty} p_i^{a_i+b_i} \). Now, any integer \( z = \prod_{i=1}^{\infty} p_i^{c_i} \) is a multiple of \( m \) if and only if \( c_i \geq a_i \) for all \( i \), and is a multiple of \( n \) if and only if \( c_i \geq b_i \) for all \( i \), thus \( \text{lcm}(m,n) = \prod_{i=1}^{\infty} p_i^{\max\{a_i,b_i\}} \).

From this we see that \( \text{lcm}(m,n) = mn/\gcd(m,n) \), and we can find \( \gcd(m,n) \) efficiently via Euclid Algorithm, thus \( \text{lcm}(m,n) \) is efficiently computed as \( mn/\gcd(m,n) \).

Problem 2: Suppose \( c \) and \( d \) are positive integers. Show that if \( c^{1/d} \) is not an integer then it is irrational, i.e. it can’t be expressed as \( c^{1/d} = \frac{m}{n} \) for any integers \( m \) and \( n \). (For example, \( \sqrt{2} \) is irrational.) Hint: First characterize when an integer \( z \) is the \( d \)th power of some integer, using its prime decomposition \( z = \prod p_i^{\alpha_i} \).

Solution: Let \( p_1, p_2, p_3 \ldots \) denote the sequence of all prime numbers, let \( d \) be a positive integer. By the uniqueness of prime factorizations, any positive integer \( z \), say with prime factorization \( z = \prod_{i=1}^{\infty} p_i^{\delta_i} \), is a \( d \)th power of an integer if and only if \( d \) divides \( \delta_i \) for all \( i \). Now, suppose \( c, m, n \) are positive integers such that \( c^{1/d} = \frac{m}{n} \), and say that \( m = \prod_{i=1}^{\infty} p_i^{\alpha_i} \) and \( n = \prod_{i=1}^{\infty} p_i^{\beta_i} \), and \( c = \prod_{i=1}^{\infty} p_i^{\gamma_i} \) are each prime factorizations. Then, taking \( d \)th powers, we obtain \( c = \frac{m^d}{n^d} \), i.e. \( c \cdot n^d = m^d \), i.e. \( \prod_{i=1}^{\infty} p_i^{(d\beta_i + \gamma_i)} = \prod_{i=1}^{\infty} p_i^{d\alpha_i} \).

Thus, for all \( i \), \( d \) divides \( \gamma_i = d \cdot \alpha_i - d \cdot \beta_i \), hence \( c \) is a \( d \)th power of an integer.

Problem 3: A continued fraction of a rational number \( x \) between 0 and 1 is an expression of \( x \) as

\[
x = \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots + \frac{1}{q_j + \cdots}}}}
\]

where \( j \) is a positive integer, and \( q_1, q_2, \ldots q_j \) are positive integers. (Actually, there is a \( q_0 \) omitted for simplicity, as we assume for simplicity that \( x \) is between 0 and 1.) For example, the continued fraction
for \( \frac{1002}{2501} \) is

\[
\frac{1002}{2501} = 2 + \frac{1}{62 + \frac{1}{5}}.
\]

Explain and justify how to use the Euclid Algorithm to find a continued fraction. (Hint: If \( a, b, q, r \) are as given in the statement of the Division Lemma, simplify \( \frac{1}{q + r} \).) Use your method to compute the continued fraction of \( \frac{1337}{3501} \).

**Solution:** Suppose \( a, b, q, r \) are integers such that \( a = qb + r \), as in the division lemma. Note that

\[
\frac{1}{q + \frac{r}{b}} = \frac{1}{\frac{q + r}{b}} = \frac{b}{a}.
\]

Suppose \( m \) and \( n \) are integers such that \( n > m > 0 \), and we are interested in a continued fraction for \( \frac{m}{n} \).

Apply the Euclid algorithm to \( a_0 := n \) and \( a_1 := m \), and say the Euclid iterates are \( a_0, a_1, a_2, \ldots, a_{j+1} \) (where \( a_{j+1} = 0 \)) with quotients \( q_1, q_2, q_3, \ldots, q_j \); ie for \( i = 1, 2, \ldots, j \) it holds that \( a_{i-1} = q_ia_i + a_{i+1} \).

Iteratively applying the above,

\[
\frac{m}{n} = \frac{a_1}{a_0} = \frac{1}{q_1 + \frac{a_2}{a_1}} = \frac{1}{q_1 + \frac{1}{q_2 + \frac{a_3}{a_2}}} = \ldots = \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_j + \frac{1}{a_{j+1}}}}}}
\]

which is what is desired, since \( a_{j+1} = 0 \).

The continued fraction for \( \frac{1337}{3501} \) is

\[
\frac{1337}{3501} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}}}}}}}
\]