Homework 4, 550.371 Cryptology and Coding, Spring 2017

Important Instructions: You may discuss this homework with students currently in the class, with the TAs, and with me, up until the time that you do your write-up; but the solutions and code that you submit should be entirely your own. At no time may you consult any existing written solutions; this would be in violation of the homework rules and, in addition, would be plagiarism if sources are not cited.

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.)

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 cant 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 dth power of some integer, using its prime decomposition $z = \prod p_i^{a_i}$.

Problem 3: A continued fraction expansion of a number x is an expression of x as

$$x = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots \cfrac{1}{q_{j-1} + \cfrac{1}{q_j}}}}}$$

where j is a positive integer, and $q_1, q_2, \ldots q_j$ are positive integers. (Actually, there is a q_0 which I omitted for simplicity.) For example, the continued fraction expansion for $\frac{1002}{2501}$ is

$$\frac{1002}{2501} = \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{62 + \frac{1}{8}}}}.$$

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