CS 103X: Discrete Structures
Homework Assignment 3

Due February 3, 2006

Exercise 1 (Reading Assignment)**.** Read pages 43–44 in Lehman-Leighton.

Exercise 2. Warm-up:

(a) Two integers a, b are said to be *coprime* if $\gcd(a, b) = 1$. If a and b are coprime, prove that the *linear Diophantine equation* $ax + by = c$ always has an integer solution x, y. Conclude that the equation has infinitely many solutions.

(b) For integers $a, b \neq 0$, and any integer $m > 0$, show that $\gcd(ma, mb) = m \cdot \gcd(a, b)$.

Exercise 3. Some prime facts:

(a) Prove that for every positive integer n, there exist at least n consecutive composite numbers.

(b) Prove that if an integer $n \geq 2$ is such that there is no prime $p \leq \sqrt{n}$ that divides n, then n is a prime.

Exercise 4. Fun with coprime numbers:

(a) Prove that a and b are coprime if and only if every integer is a linear combination of a and b.

(b) Prove that $a/\gcd(a, b)$, $b/\gcd(a, b)$ are coprime.

(c) Let a and b be coprime. Prove:

i. If $a|c$ and $b|c$ then $ab|c$

ii. If $a|bc$ then $a|c$

Is the assumption that a and b are coprime necessary? (Substantiate.)

Exercise 5. Even more irrational roots:

(a) Use the Fundamental Theorem of Arithmetic to prove that for $n \in \mathbb{N}$, $\sqrt{n}$ is irrational unless n is a perfect square, that is, unless there exists $a \in \mathbb{N}$ for which $n = a^2$.

(b) Prove more generally that for any $k \in \mathbb{N}$, $\sqrt[k]{n}$ is irrational unless $n = a^k$ for some $a \in \mathbb{N}$.

(c) Prove that if p and q are distinct primes, $\sqrt{pq}$ and $\sqrt{p/q}$ are irrational.

(d) Suppose $a, b, c \in \mathbb{Q}$. Prove that if

$$a\sqrt{2} + b\sqrt{3} + c\sqrt{5} = 0$$

then

$$a = b = c = 0.$$

Exercise 6. EXTRA CREDIT:

For $a, b \in \mathbb{Z}$, m is said to be a *common multiple* of a and b if and only if $a|m$ and $b|m$. If $a, b \neq 0$, they have positive common multiples (such as $|ab|$) and, by the well-ordering principle, a smallest positive common multiple, called the *least common multiple*, or $\mathrm{lcm}(a, b)$. This is the integer m that satisfies the following two criteria:

- $a|m$ and $b|m$.
- If $a|n$ and $b|n$ then $m \leq n$.

For example, $\mathrm{lcm}(10, 15) = 30$.

(a) For positive integers a and b, let $d = \gcd(a, b)$ and $m = \mathrm{lcm}(a, b)$. Prove that $dm = ab$. Use this to calculate $\mathrm{lcm}(9524, 8692)$.

(b) Show that s is a common multiple of a and b if and only if $m|s$, where $m = \mathrm{lcm}(a, b)$.