Mathematics 243, section 3 – Algebraic Structures
Problem Set 6
due: October 26, 2012

'A' Section

1. Solve each of the following congruences for $x \in \mathbb{Z}$, with $0 \leq x < n$. Note that in each case it is possible to rewrite the given congruence in the form $ax \equiv b \pmod{n}$ with $\gcd(a, n) = 1$.

   a. $7x \equiv 13 \pmod{24}$

   b. $14x + 25 \equiv 3 \pmod{393}$

2. What is the ones digit in 43^{15}? Hint: consider $43^{15} \pmod{10}$ and use Theorem 2.22 in the text, or problem B 4 below.

3. Find a positive integer x that satisfies the two simultaneous congruences

$$\begin{aligned} 2x + 1 &\equiv 5 \pmod{9} \\ 3x + 4 &\equiv 8 \pmod{10} \end{aligned}$$

   Explain your method.

'B' Section

1. A *least common multiple*, or *lcm*, of two nonzero integers a, b is a positive integer m such that

   - $a|m$ and $b|m$, and
   - $a|c$ and $b|c$ imply $m|c$.

   Part a below will show that lcm's always exist, and part b asks you to derive a method for computing them via prime factorizations.

   a. Show that if $a, b > 0$ and $d = \gcd(a, b)$ with $a = da_0$ and $b = db_0$, then $m = da_0b_0$ is a least common multiple of a, b.

   b. Deduce from part a that $md = ab$.

   c. Describe a method for computing a least common multiple of a, b from their standard form factorizations as on page 92 of the text.

2. In this problem, you will derive another result first found by the Pythagorean philosophers in ancient Greece. Let a, b be relatively prime integers.

   a. Arguing by contradiction, use the fact that 2 is a prime number and Euclid's Lemma to show that it is never the case that $a^2 = 2b^2$.

   b. Explain why the result of part a shows that $\sqrt{2} \in \mathbb{R}$ is *not a rational number*.

Comment: A possibly fictional story runs that Hippasus of Metapontum (one of the Pythagoreans) was murdered by his colleagues for divulging this terrible secret(!) At the time, only rational numbers were accepted as valid objects for mathematical reasoning.

3. Let $b > 1$ be an integer. Show that every positive integer n can be written in the form

$$n = d_0 + d_1 b + d_2 b^2 + \cdots + d_m b^m$$

where $0 \leq d_i < b$ for all i. (The resulting expansion is called the *base-b expansion* of n, and the d_i are called the base-b digits of n. The usual choice for us is $b = 10$, but any other base $b > 1$ works just as well.) Hints: Let m be the largest non-negative integer such that $b^m \leq n$, and divide b^m into n. If you are clever you can then apply an induction hypothesis to finish the proof.

4. Give a direct proof (i.e. one *not* appealing to Theorem 2.22 in the text) of the following statements: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

5. Show that if m is any integer, then exactly one of the following statements is true: $m^2 \equiv 0 \pmod{8}$, $m^2 \equiv 1 \pmod{8}$, or $m^2 \equiv 4 \pmod{8}$.