CS 173: Discrete Structures, Spring 2010
Homework 4

This homework contains 5 problems worth a total of 50 points. It is due on Friday, 19 February at 4pm.

---

1. **Set Operations [16 points]**

   Suppose you were given the following sets:

   $$\begin{aligned}\mathbf{A} &= \{\text{Piano}, \{\text{Violin}, \text{Viola}, \text{Cello}\}, \text{Guitar}\}\\ \mathbf{B} &= \{\{\text{Flute, Piccolo}\}, \text{Cymbals}\}\\ \mathbf{C} &= \{\text{Piano}, \text{Flute}\}\\ \mathbf{D} &= \{\{\text{Violin, Viola, Cello}\}, \{\text{Flute, Piccolo}\}\}\end{aligned}$$

   List the elements of the set for the following expressions:

   (a) $A \cup D$

   (b) $B \cap C$

   (c) $A - (B - C)$

   (d) $A \cap \mathbb{P}(B \cap C)$

   (e) $(B \cap D) \times C$

   (f) $| \mathbb{P}(B \cap D) |$

   (g) $\{X \in \mathbb{P}(A) \ : \ |X| \text{ is not prime}\}$

   (h) $\{X \in (\mathbb{P}(A) \cup \mathbb{P}(B)) \ : \ |X| \equiv 3 \pmod 2\}$

2. **Euclidean algorithm [4 points]**

   Trace the execution of the Euclidean algorithm (lecture 10 or p 229 in Rosen) on the inputs $a = 837$ and $b = 2015$. That is, give a table showing the values of the main variables (x, y, r) for each pass through the loop. Explicitly indicate what the output value is.

3. **Pseudocode [10 points]**

```
procedure func(a, b: natural numbers)
  if (b = 0) return 1
  if (b = 1) return a
  m := func(a, floor(b/2))
  p := func(a, (b mod 2))
  return m * m * p
```

(a) Trace the execution of func(2, 5). That is, give a table showing the values of the main variables (a, b, m, p) and the return value for each call to func. *Note*: To fill in the value of m for a given row, it may be necessary to look up the return value of another row.

(b) Give a brief explanation of what `func(a, b)` computes.

4. **[10 points] Direct Proof Using Congruence mod k**

In the book, you will find several equivalent ways to define congruence mod k. For this problem, use the following definition: for any integers x and y and any positive integer m, $x \equiv y \pmod{m}$ if there is an integer k such that $x = y + km$.

Using this definition prove that, for all integers a, b, c, p, q where p and q are positive, if $a \equiv b \pmod{p}$ and $c \equiv b \pmod{q}$ and $q|p$, then $a - 2c \equiv (-b) \pmod{p}$.

5. **[10 points] Computations With Congruence mod k**

It's not hard to show that (for any integers a, b, c, d, m where m is positive) if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. (See Rosen for proof.) ¿From this, it follows that if $a \equiv b \pmod{m}$, then $a^2 \equiv b^2 \pmod{m}$.

(a) Use this fact about squaring to compute the value of 6^k mod 13 for $k = 0, 1, 2, 4, 8, 16, 32, 64$. Show your work.

(b) Using your result from part (a), compute the value of 6^{82} mod 13 (showing your work).

(c) Show that, for every integer n, n^2 is congruent to either 0, 1, or 4, mod 5. That is, show that $n^2 \equiv 0 \pmod{5}$ or $n^2 \equiv 1 \pmod{5}$ or $n^2 \equiv 4 \pmod{5}$. Hint: n mod 5 doesn't have very many possible values. Consider each one separately.