CS 173: Discrete Structures, Fall 2009
Homework 4 Solutions

This homework contains 6 problems worth a total of 50 regular points plus 5 bonus points.

Starting with this homework, we will take one point off your homework score if your name and the day and time of your section are not clearly visible on the top sheet of your homework.

---

1. **[16 points] Sets**

   Define the following sets

$$\begin{aligned} A &= \{\{\text{Elm}\}, \{\text{Pine}\}\} \\ B &= \{\text{Elm}, \text{Oak}, \text{Maple}\} \\ C &= \{\text{Elm}, \text{Vine}, \text{Birch}, \text{Maple}\} \\ D &= \{\text{Tree}, \text{Disease}, \text{Street}\} \end{aligned}$$

   For each of the following expressions, list the elements of the set or calculate the value (as appropriate).

   (a) $\{(x, y) \in \mathbb{Z}^2 \mid x \geq 0 \text{ and } y \geq 0 \text{ and } x + y = 3\}$
   Answer: $\{(0, 3), (1, 2), (2, 1), (3, 0)\}$

   (b) $\{x \in \mathbb{Z} \mid -20 \leq x \leq 20 \text{ and } x \equiv 2 \pmod 7\}$
   Answer: $\{-19, -12, -5, 2, 9, 16\}$

   (c) $\{X \in \mathbb{P}(C) \ : \ |X| \text{ is even}\}$
   Answer: $\{\emptyset, \{\text{Elm}, \text{Vine}\}, \{\text{Elm}, \text{Birch}\}, \{\text{Elm}, \text{Maple}\}, \{\text{Vine}, \text{Birch}\}, \{\text{Vine}, \text{Maple}\}, \{\text{Birch}, \text{Maple}\}, C\}$

   (d) $A \cap B$
   Answer: $\emptyset$

   (e) $A \cap \mathbb{P}(B \cap C)$
   Answer: $\{\{\text{Elm}\}\}$

   (f) $(B \cap C) \times D$
   Answer: $\{(\text{Elm}, \text{Tree}), (\text{Elm}, \text{Disease}), (\text{Elm}, \text{Street}), (\text{Maple}, \text{Tree}), (\text{Maple}, \text{Disease}), (\text{Maple}, \text{Street})\}$

   (g) $|\mathbb{P}(C \times D)|$
   Answer: Notice that $|C \times D| = |C||D| = 3 \cdot 4 = 12$. Since the size of the power set is 2 to the size of the set, we have $2^{12} = 4096$

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

Answer: Since $B \cap D$ is empty, the power set of the empty set is $\{\emptyset\}$, which has size $2^0 = 1$.

2. [**8 points**] **Euclidean algorithm**

(a) Trace the execution of the Euclidean algorithm (lecture 10 or p 229 in Rosen) on the inputs 391 and 2380. 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.

[**Answer:**]

x	**y**	**r**
391	2380	391
2380	391	34
391	34	17
34	17	0
17	0	

Thus, the algorithm outputs $\gcd(391, 2380) = 17$. (Note the first algorithm on the lecture slides terminates when $y = 0$, not when $r = 0$, so there will be a last row in the table that is $(17, 0, \text{blank})$).

(b) The pseudo code for the Euclidean algorithm presented in lecture handles only positive number inputs, despite the fact that the definition of GCD also works if the inputs are negative or (in some cases) zero. Modify the recursive version of the pseudocode so that it can take any two integers as input. Your pseudocode should output an answer that follows our mathematical definition of GCD. The pseudocode can signal errors (e.g. illegal inputs) using the error command, e.g.

```
if (excessive_pressure)
   error ‘‘Please don’t squeeze the tomatoes.’’
```

[**Answer:**]

```
procedure gcd(a,b: integers)
    if (b = 0 and a = 0) error ‘‘0 mod 0 is undefined’’
    else if (b = 0) return a
    else if (a = 0) return b

    else
       begin
       a := |a|
       b := |b|
       r := a mod b
       return gcd(b,r)
       end
```

3. [**8 points**] Pseudocode

I found the following uncommented pseudocode in Professor Snape's lab notebook.

```
procedure foo(n,m:  natural numbers)
   if (m = 0) return 1
   else return n*foo(n,m-1)

procedure bar(n: natural number)
   p := 0
   for i := 0 to n
       p := p + foo(n,3)
   return p
```

(a) Describe the output of foo, as a (simple) function of the inputs n and m.

[**Answer:**]

Note that foo multiplies n by itself m times, so we get:

$$foo(n,m) = n^m$$

(b) Describe the output of bar, as a function of the input n. Give your answer as a summation and also in closed form (equation that doesn't involve a summation).

[**Answer:**]

The inner loop of bar runs $n+1$ times, and each time it adds another call to $foo(n,3)$, which we know is n^3. Thus we have the following:

$$bar(n) = \sum_{i=0}^{n} n^3 = (n+1)n^3$$

Notice that the call to foo uses n, not i.

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 x, y, p, q and m, with $m > 0$, if $x \equiv p \pmod{m}$ and $y \equiv q \pmod{m}$, then $x^2 + xy \equiv p^2 + pq \pmod{m}$.

[**Answer:**]

Let $x, y, p, q, m \in \mathbb{Z}$ such that $m > 0$, $x \equiv p \pmod{m}$, and $y \equiv q \pmod{m}$. By definition, $x = p + km$ and $y = q + \ell m$ for $k, \ell \in \mathbb{Z}$. Squaring the first equation yields $x^2 = (p + km)^2 = p^2 + 2kmp + (km)^2$, and multiplying the first equation times the second yields $xy = (p + km)(q + \ell m) = pq + kmq + p\ell m + km^2$.

If we add the equations for x^2 and xy together, we get the following:

$$x^2 + xy = p^2 + pq + m(kq + p\ell + km + 2kp + k^2m)$$

which is of the form $x^2 + xy = p^2 + pq + am$ for some integer a, and the result holds.

[Alternate answer:]

First note the following: if $x \equiv p \pmod{m}$ and $y \equiv q \pmod{m}$, then $xy \equiv pq \pmod{m}$. To see this, let $k, \ell \in \mathbb{Z}$ such that $x = p + km$ and $y = q + \ell m$ (by definition of modular equivalence). Multiplying these equations together yields $xy = am + pq$, (where $a = k\ell m + p\ell + k\ell$), which implies that $xy \equiv pq \pmod{m}$.

Next, note that it is equivalent to show that $x^2 - p^2 + xy - pq \equiv 0 \pmod{m}$, or that $(x+p)(x-p) + xy - pq = tm$ for some integer t. Since (by definition) $x - p = km$ and $xy - pq = am$, we can let $t = (x+p)k + a$, and the theorem is proved.

5. **[8 points] Proof using inequalities**

Prove the following claims using direct proof.

(a) For any integers m and k, if $0 < \frac{1}{k} < m$ then $\frac{m}{m^2+1} < k$.

[Answer:]

Multiplying the given inequality by m yields $\frac{m}{k} < m^2 < m^2 + 1$. Inverting and multiplying by m gives the result (all numbers are positive, we switch the sign on the inequality):

$$\frac{k}{m} > \frac{1}{m^2+1}$$

$$k > \frac{m}{m^2+1}$$

(b) For any integers m and k, if $k \leq 7$ and $0 < m - 3 \leq \frac{k}{7}$, then $m^2 - 9 \leq k$.

[Answer:]

It is equivalent to show that $(m+3)(m-3) \leq k$. Note that $(m+3)(m-3) \leq (m+3)\frac{k}{7}$, from our assumption. Also note that if $m - 3 \leq \frac{k}{7}$, adding 6 to both sides shows that $m + 3 \leq \frac{k}{7} + 6 \leq \frac{7}{7} + 6 = 7$, since $k \leq 7$. Thus, we have that $(m+3)(m-3) \leq (m+3)\frac{k}{7} \leq 7\frac{k}{7} = k$.

6. **[5 points] Bonus proof**

(This is a bonus problem. That is, if you have time to do it, it will add a few bonus points to your homework average. But it's OK to skip it if you have run out of time or interest.)

Show that if x, y and m are integers with $m \geq 2$, then if $x \equiv y \pmod{m}$ then $gcd(x, m) = gcd(y, m)$.

[Answer:]

By definition, $x = km + y$ for some integer k. Let $d = \text{gcd}(x, m)$. By definition, $d|x$, which implies that $d|km + y$. Since d also divides m, we note that $d|y$. Now suppose there is some larger d' such that $d'|y$ and $d'|m$. However, since $y = x - km$, this would imply that $d'|x$ as well, contradicting the fact that d is the GCD of x and m.

[**Alternate answer:**]

Suppose d is a common divisor of x and m (**not** necessarily the greatest common divisor). Then $d|km+y$, and since d divides m, d must also divide y. In other words, any common divisor of x and y is a common divisor of y and m. Identical reasoning shows that any common divisor of y and m divides x. Therefore, the set of common divisors of x and y is the same as the set of common divisors of y and m, which in particular means that they share the greatest common divisor.