CSE191, Fall 2013 **Assignment 7** **Due Fri. 11/8**

Reading: From Sections 4.4–4.6 we will "cover" only the following subsections: Linear Congruences and Theorem 1 on pages 275–277, Fermat's Little Theorem on page 281, and Hashing in Section 4.5 on pages 287–288. The rest including all of Section 4.6 is skim/FYI.

The main focus this month will fall on Chapter 5. Please read sections 5.1–5.2 for next week. Lectures will make one stylistic change that I feel is important: doing induction "$k-1$ to k" rather than "k to $k+1$." For one example of why, consider the code:

```
int sqr(int n) {
   if (n <= 1) { return n; } else { return 2*n - 1 + sqr(n-1); }
}
```

We don't actually program "`int sqr(int n+1)`," so the natural way to think about the program is that if the call `sqr(n-1)` returns the correct value $(n-1)^2$, then `sqr(n)` will get the right answer. A second is that it better reflects the way C/C++/Java/etc. number things $0 \ldots k-1$. A third is that the goal of the induction is often simpler when expressed via "n" than via "$n+1$." A fourth is that "strong induction" is easier to inderstand when it separates "everything less than n" from "n." So it is a good self-study aid to try out some of the text's examples with this notation change, which has the benefit of reinforcing your understanding of it, and some of them will of course be covered in lecture.

(1) Rosen, page 244 in section 4.1, exercise 14, (b,c,e) only. Show where you did any "eager modding" in your scratchwork, or if you did "lazy modding" only at the end. ($3 \times 3 = 9 pts.$)

(2) Rosen, page 244, exercise 22, (b,c) only. Show the unique "$a = qm + r$" representation—never minding that lecture wrote "$n = am + b$" or etc. ($6 + 3 = 9$ pts.)

(3) Rosen, page 245, exercise 40. You should cite the equivalence of "eager" and "lazy" modding to say your calculations amount to a complete proof. (9 pts.)

(4) Rosen, page 255, exercises 8 and 12 taken together, doing only "BAD" for the former. ($3 + 6 = 9$ pts.)

(5) Rosen, page 255, exercise 24, (b) only. ($3 + 6 = 9$ pts.)

(6) Rosen, page 272, exercise 16, all parts (15 pts. total, the extra 3 being for finding one that is "no").

(7) Rosen, page 273, exercise 30 (12 pts.)

(8) Rosen, page 273, exercise 40, (a,b,e) only ($3 + 6 + 9 = 18$ pts., for 87 total on the set).