15-451 Algorithms, Fall 2004

Mini # 5 **due: midnight December 2, 2004**

This mini is due via email to your TA, by midnight Thursday December 2. Please use the subject line "15-451 MINI #5" in your email.

1. Number theory practice.

   (a) What is 4^{-1} mod 17?

   (b) For an element $a \in Z_N^*$, define $\langle a \rangle = \{1, a, a^2, \ldots\}$ (multiplication is done mod N and notice this has to eventually loop back to 1). A *generator* for Z_N^* is a number $a \in Z_N^*$ such that $\langle a \rangle = Z_N^*$. That is, a is a generator if any number in Z_N^* can be written as a power of a. (These notions can also be defined more generally for any group G.)

   For $N = 7$, what are the sets $\langle a \rangle$ for each $a \in Z_7^*$? For instance, $\langle 1 \rangle = \{1\}$ and $\langle 2 \rangle = \{1, 2, 4\}$. Which a's are generators for Z_7^*?

2. Linear equations mod 2.

   (a) Solve the following set of linear equations mod 2 (they're lined up to make the problem easier to think about):

```
x + y         = 1 (mod 2)
    y + z     = 0 (mod 2)
    y +     w = 1 (mod 2)
x +     z + w = 0 (mod 2)
```

   (b) What is a general procedure for solving linear equations mod 2?

ps. This may help on homework 7.