Problem Set 3

Due in class on Tuesday, February 22, 2005.

This is a "mini" problem set to give you some practice before the midterm exam with some of the recently-covered number theory. I encourage you to finish these problems by the due date above, but I will give an automatic extension until class time on Thursday to anybody who requests it.

Problem 8: Chinese remainder theorem

Solve the following system of equations for x:

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{17} \end{aligned}$$

Use the method of Section 9 of the week 5 lecture notes. Do *not* do an exhaustive search for x on the computer, although you are welcome to use a computer or calculator to evaluate arithmetic formulas.

Problem 9: Primitive roots

(a) Give a formula for the number of primitive roots of p when p is prime, and evaluate this formula for $p = 11$ and $p = 23$.

(b) Find all primitive roots of p, for $p = 11$ and $p = 23$. You may use a computer.

Problem 10: Square roots

Find all square roots of 1 modulo 77. Again, you may use the computer.