CS311:	**Homework 2**	Due in class Tuesday, Sep. 16, 2008

Number-Theoretic Algorithms

Problems:

1. [25 pts.] p. 39, problem 1.8: Justify the correctness and analysis of the recursive division algorithm on page 15.
2. [25 pts.] [cf. 1.9, p. 39] Show from the definition of $x \equiv y \pmod N$ that

$$x \equiv x' \pmod N \ \&\ y \equiv y' \pmod N \ \Rightarrow\ x + y \equiv x' + y' \pmod N$$

3. [10 pts.] Do problem 1.18, p. 40 and also compute x, y such that $210x+588y = \text{gcd}(210, 588)$.
4. [15 pts.] Do problem 1.27, p. 40; please show your work.
5. [25 pts.] CRT: 1.37, p. 42, do parts (a) through (c).