University of Washington
Department of Computer Science and Engineering
CSE 321, Winter 2008

January 29, 2008

Homework 4, Due Wednesday, February 6, 2008

Problem 1:

Section 2.3 Problem 6 (Fifth edition, Section 1.8, Problem 6).

Problem 2:

Section 2.3 Problem 10 (Fifth edition, Section 1.8, Problem 10).

Problem 3:

Prove or disprove that if a, b, and c are positive integers and $a \mid bc$ than $a \mid b$ or $a \mid c$.

Problem 4:

Section 3.4 Problem 16 (Fifth edition, Section 2.4, Problem 36).

Problem 5:

How many zeros are there at the end of 100!. Determine this without computing 100!.

Problem 6:

Prove that if n is an odd positive integer, then $n^2 \equiv 1 (\text{mod } 8)$.

Problem 7:

For each $a \in \{1, \ldots, 10\}$ determine the smallest $k \geq 1$ such that $a^k \bmod 11 = 1$.

Problem 8:

Use Fermat's Little Theorem to compute $3^{302} \bmod 5$, $3^{302} \bmod 7$ and $3^{302} \bmod 11$.

Problem 9:

Prove that if p is prime, and $x^2 \equiv 1 (\text{mod } p)$ then $x \equiv 1 (\text{mod} p)$ or $x \equiv (p-1) (\text{mod } p)$.

Extra Credit 10:

Let p be an odd prime. A number $a \in \{1, \ldots, p-1\}$ is a *quadratic residue* if the equation $x^2 \equiv a (\text{mod } p)$ has a solution for x. Show that there are exactly $(p-1)/2$ quadratic residues modulo p.