MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #2

Problems

Problem 1. Compute $357 \cdot 862 \cdot 193$ modulo 943.

Problem 2. Let $m \geq 1$ be an integer and suppose that

$$a_1 \equiv a_2 \pmod{m} \quad \text{and} \quad b_1 \equiv b_2 \pmod{m}.$$

Prove that

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \quad \text{and} \quad a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

Problem 3. Let $m \in \mathbb{Z}$ be odd and $a \in \mathbb{Z}$. Prove that $2m + a^2$ is never a perfect square.

Date: Due Friday, 10 September 2010.