MAT 311 Spring 2011 Midterm 1

Name: ________________________________ SB ID number: ______________________

Problem 1:	__________	/15
Problem 2:	__________	/25
Problem 3:	__________	/30
Problem 4:	__________	/30
Total:	__________	/100

Instructions: *Please write your name at the top of every page of the exam.* This exam is closed book, closed notes, calculators are not allowed, and all cellphones and other electronic devices must be turned off for the duration of the exam. Electronic language translators may be approved by the proctor for ESL students, but the student must identify himself or herself to the proctor so that the translator may be approved prior to using the translator.

You will have approximately 80 minutes for this exam. The point value of each problem is written next to the problem – use your time wisely. Please show all work, unless instructed otherwise. Partial credit will be given only for work shown.

You may use either pencil or ink. If you have a question, need extra paper, need to use the restroom, etc., raise your hand.

Name: ______________________________________ **Problem 1**: ________________ /15

Problem 1(15 points) Let a, b and n be positive integers. Assume that $\gcd(a, n)$ equals $\gcd(b, n)$. Prove that there exist integers x and y such that $\gcd(x, n) = \gcd(y, n) = 1$ and such that

$$ax \equiv b (\text{mod } n),$$

$$by \equiv a (\text{mod } n).$$

Name: ______________________________ **Problem 2**: ______________ /25

Problem 2(25 points) Let a, b and c be positive integers such that $c = ab$. If each of b and c is a sum of two square integers, is also a a sum of two square integers? If so, explain why. If not, give a counterexample.

Name: ______________________________ **Problem 3**: ______________ /30

Problem 3(30 points) Find all solutions modulo $63 = 3^2 \cdot 7$ of the following congruence,

$$x^3 - x + 3 \equiv 0 (\text{mod } 63).$$

Name: ____________________ **Problem 4**: __________ /30

Problem 4(30 points) Let $p > 3$ be a prime integer. Find a necessary and sufficient condition on p so that the following holds: for every integer g which is a primitive root modulo p, also g^3 is a primitive root modulo p.