MAT 312/AMS 351 Midterm I

September 19, 2019 11:30am-12:50pm

Name:____________________________ **ID:**__________________

first name *first*

Recitation: R01 (Tu 1-1:53pm) R02 (W 11-11:53am) (circle yours)

DO NOT OPEN THIS EXAM YET

Instructions

(1) Fill in your name and Stony Brook ID number and circle your recitation number at the top of this cover sheet.

(2) This exam is closed-book and closed-notes; no calculators, no phones.

(3) Please write legibly to receive credit. Circle or box your final answers. If your solution to a problem does not fit on the page on which the problem is stated, please indicate on that page where in the exam to find (the rest of) your solution.

(4) You may continue your solutions on additional sheets of paper provided by the proctor. If you do so, please write your name and ID number at the top of each of them and staple them to the back of the exam (stapler available); otherwise, these sheets may get lost.

(5) Anything handed in will be graded; incorrect statements will be penalized even if they are in addition to complete and correct solutions. If you do not want something graded, please erase it or cross it out.

(6) Show your work; correct answers only will receive only partial credit (unless noted otherwise).

(7) Be careful to avoid making grievous errors that are subject to heavy penalties.

(8) If you need more blank paper, ask a proctor.

Out of fairness to others, please **stop working and close the exam as soon as the time is called**. A significant number of points will be taken off your exam score if you continue working after the time is called. You will be given a two-minute warning before the end.

1 (5pts)	2 (10pts)	3 (12pts)	4 (12pts)	5 (15pts)	6 (16pts)	Tot (70pts)

Problem 1 (5pts)

Suppose $a, b \in \mathbb{Z}^+$ are two positive integers such that

$$2a - 3b = 5.$$

(a) There are two possibilities for $\gcd(a, b)$. What are they? **Answer Only.**

$$\boxed{\gcd(a, b) = \qquad \text{or} \qquad}$$

(b) *Explain* why there are no other possibilities.

(c) Give an example of a pair (a, b) for each of the two possibilities in (a). **Answer Only.**

$$\boxed{\text{Possibility 1 in (a): } (a, b) = (\qquad , \qquad)}$$

$$\boxed{\text{Possibility 2 in (a): } (a, b) = (\qquad , \qquad)}$$

Problem 2 (10pts)

Define a sequence $a_1, a_2, a_3, \ldots$ by

$$a_1 = 1, \qquad a_2 = 2, \qquad \text{and} \qquad a_{n+2} = a_n^2 + a_{n+1} \quad \forall\, n \geq 1.$$

(a) Determine the first 5 numbers, a_n with $n = 1, \ldots, 5$, in this sequence. The answer must appear in the box below; no explanation is required for this part.

(b) Prove that every two successive terms in this sequence, a_n and a_{n+1}, are relatively prime.

Problem 3 (12pts)

Show and explain your work clearly below.

(a) Find $\gcd(11, 64)$ and express it in the form $11s+64t$ for some $s, t \in \mathbb{Z}$.

(b) Find the inverse of 11 mod 64 (the answer should be an integer between 0 and 63).

Problem 4 (12pts)

A public key code has base 85 and exponent 11, i.e. $m \equiv \beta^{11} \bmod 85$ is the message determined by a block β being encoded. The encoded message received is 81. Decode this message. *Show and explain your work clearly.*

Problem 5 (15pts)

Show and explain your work clearly below.

(a) Let p be an odd prime. How many distinct solutions $x \in \mathbb{Z}_p$ does the equation

$$x^2 = [1]_p$$

have?

(b) Let p be an odd prime. How many elements does the subset

$$\{x^2 : x \in \mathbb{Z}_p\} \subset \mathbb{Z}_p$$

contain?

(c) Let p and q be distinct odd primes. How many distinct solutions $x \in \mathbb{Z}_{pq}$ does the equation

$$x^2 = [1]_{pq}$$

have?

Problem 6 (16pts)

Solve the linear congruences and systems of congruences below. Show and explain your work clearly.

(a) $3x+5 \equiv x-3 \bmod 7$

(b) $\begin{cases} 3x+5 \equiv x-3 & \bmod 7 \\ 2x \equiv 4 & \bmod 8 \end{cases}$

(c) $\begin{cases} 3x+5 \equiv x-3 & \bmod 7 \\ 2x \equiv 4 & \bmod 8 \\ 3x \equiv 5 & \bmod 9 \end{cases}$