250 MIDTERM

Do not open this exam until you are told.

READ THE INSTRUCTIONS

1. This is a closed book exam, though ONE sheet of notes is allowed. **No calculators, or other aids are allowed**. If you have a question during the exam, please raise your hand.
2. There are 6 problems which add up to 100 points. The exam is 2 hours. (You shouldn't need that much.)
3. For each question show all of your work and **write legibly**. **Clearly indicate** your answers. No credit for illegible answers.
4. After the last page there is paper for scratch work. If you need extra scratch paper **after** you have filled these areas up, please raise your hand. Scratch paper must be turned in with your exam, with your name and ID number written on it, but scratch paper **will not** be graded.
5. Please write out the following statement: "*I pledge on my honor that I will not give or receive any unauthorized assistance on this examination.*"
6. Fill in the following:

NAME :
SIGNATURE :
SID :
SECTION NUMBER :

SCORES ON PROBLEMS

Prob 1:	
Prob 2:	
Prob 3:	
Prob 4:	
Prob 5:	
Prob 6:	
TOTAL	

Below there is a list of numbers mod 26 that have inverses and what the inverses are. It may or may not be useful. That is a tautology.

Number	1	3	5	7	9	11	15	17	19	21	23	25
Inverse of Number	1	9	21	15	3	19	7	23	11	5	17	25

1. (10 points) The Unlucks use a 13 letter alphabet.

   (a) How many shift ciphers can they have?

   (b) How many affine ciphers can they have?

2. (10 points) For each of the following sentences

   - Give an infinite domain where it is TRUE OR prove there is no infinite domain where it is TRUE.
   - Give an finite domain with **at least three elements** where it is TRUE OR prove there is no finite domain with at least three elements where it is TRUE.

   All symbols have their usual meaning. A domain is a subset of R.

   (a) $(\forall x)(\exists y)[x + y = 0]$.

   (b) $(\forall x)(\exists y)[xy = 1]$.

   (a) $(\forall x)(\exists y)[x + y = 0]$.
   INFINITE DOMAINS WHERE TRUE: Q, R, Z.
   FINITE DOMAIN WHERE TRUE: $\{-1, 0, 1\}$. Can make bigger: $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$.

   (b) $(\forall x)(\exists y)[xy = 1]$.
   INFINITE DOMAINS WHERE TRUE: Q $- \{0\}$, R $- \{0\}$
   FINITE DOMAINS WHERE TRUE: $\{\frac{1}{2}, 1, 2\}$. Can make bigger: $\{\frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1, 2, 3, 4, 5\}$

3. (20 points) Consider the following arithmetic function:

$$f(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = \begin{cases} 0 & \text{if exactly ONE of the inputs is 0} \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

(a) How many rows are in the TT for f?

(b) Do you want to do the TT for f (hint: The answer is NO!!!!) Explain how you can avoid doing that.

(c) Based on your observation from part (c), describe a way to build the circuit for f WITHOUT doing the TT for f.

(d) Use your method to construct the circuit for f. (That is, DRAW IT.)

(e) You used a trick to avoid writing down that TT. Name a function $g(x_1, \ldots, x_n)$ where the trick would save you LOTS of time.

(f) Name a function $h(x_1, \ldots, x_n)$ where the trick would NOT save LOTS of time. Explain why.

NOTE: both of the functions for part (e) and (f) must be defined on n input variables, i.e. a function $g(x_1, \ldots, x_8)$ would not work.

4. (20 points) In this problem the domain is the natural numbers and the language has the usual logical symbols and arithmetic operations.

   (a) A number is *cool* if it can be written as the sum of ≤ 3 cubes. Let $COOL(x)$ mean that x is cool. Write a formula for $COOL(x)$.

   (b) (You may use $COOL(x)$ in this problem.) Write a sentence to express the following: *There exists an infinite number of numbers that are NOT cool*

   (c) Give 2 examples of cool numbers. Prove that they are cool.

   (d) Give 2 examples of numbers that are not cool. Prove that they are not cool.

5. (20 points)

(a) Find a set X such that the following is true (and prove it).

- $X \subseteq \{0,1,2,3,4,5,6,7,8\}$
- For all $n \in \mathsf{N}$, there exists $a \in X$ such that $n^3 \equiv a \pmod 9$.
- For all $a \in X$, there exists $n \in \mathsf{N}$ such that $n^3 \equiv a \pmod 9$.

(b) Show that there exists an infinite number of numbers n such that n CANNOT be written as the sum of ≤ 3 cubes. (In the language of the last problem, there are an infinite number of numbers that are NOT cool.) HINT: Use the results of the last problem.

How to determine X? Take cube mod 9 of all numbers in $\{0,\ldots,8\}$

$0^3 \equiv 0$

$1^3 \equiv 1$

$2^3 \equiv 8$

$3^3 \equiv 27 \equiv 0$

$4^3 \equiv 16 \times 4 \equiv 7 \times 4 \equiv 28 \equiv 1$

$5^3 \equiv 25 \times 5 \equiv 7 \times 5 \equiv 35 \equiv 8$

$6^3 \equiv 36 \times 6 \equiv 0$

$7^3 \equiv 49 \times 7 \equiv 4 \times 7 \equiv 1$

$8^3 \equiv (-1)^3 \equiv -1 \times 8$

So $X = \{0,1,8\}$. We will prefer to see this as $\{0,1,-1\}$

To prepare for the next problem lets see which numbers mod 9 can be written as a sum of $0, 1, -1$. Or better- lets just find a number that cannot be written.

There are not $a, b, c \in X$ with $a + b + c \equiv 4 \pmod 9$.

PROOF:

If do not use 0 then can only have sums of 1's and -1's so can only get

$-1 + -1 + -1 = -3 \equiv 6$

$-1 + -1 + 1 = -1 \equiv 8$

$-1 + 1 + 1 \equiv 1$

$1 + 1 + 1 \equiv 3$

NOT 4.

If do not use -1 then can only have sums of 1's and 0's. This will be $\{0, 1, 2, 3\}$ so not 4.

If do not use 1 then can only have sums of -1's and 0's. This will be $\{0, 6, 7, 8, \}$ so not 4.

If use all three then get 0, not 4

So CANNOT get any number that is $\equiv 4 \pmod 9$.

SO our infinite set is $\{n \mid n \equiv 4 \pmod 9\}$.

6. NOTE FOR SPRING 2019 CLASS- WE DID NOT COVER THIS MATERIAL SO YOU CAN IGNORE. (20 points) Alice is using an affine cipher $f(x) = ax + b$ to send messages to Bob. Eve intercepts a very long text T that Alice sent to Bob.

   (a) Eve thinks that $(a, b) = (5, 2)$. Explain in English an algorithm Eve would use to determine if she is right. Also give pseudeocode. (DO NOT use part (b) of this problem.) (She does NOT decode and LOOK AT the text to see if it LOOKS like English.)

   (b) Eve has no idea what (a, b) is. Explain in English an algorithm Eve would use to determine (a, b). Also write pseudo-code.

Scratch Paper