250 MIDTERM TWO

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 7 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:	
Prob 7:	
TOTAL	

1.

2. (10 points) Give a Context Free Grammar for the language

$$\{a^{2n}b^{3n} : n \in \mathsf{N}\}.$$

3. (15 points) $P(n)$ is a sentence about the rationals (positive and negative). The following are known:

   $P(-7)$ is true.

   For all rationals q, if $P(q)$ is true then $P(q + \frac{1}{2})$ is true.

   Describe the set of rationals q for which we know $P(q)$ is true.

   You may use either set notation or DOT-DOT-DOT notation but in any case your answer should be clear!

4. (10 points) Give a 2-coloring of the edges of K_5 so that there is no monochromatic triangle.

5. (20 points) Alice and Bob are going to use the Diffie-Helman key exchange to obtain a shared secret key. They use $p = 11$ and $g = 6$ and the TABLE on the next page (It is provided so you don't have to do much computation. It may be INCORRECT but this does not matter for the problem.)

   (a) If Alice picks $a = 1$ and Bob picks $b = 8$ then what is their shared secret key?

   (b) Is it a bad idea to use $a = 1$? Explain your answer.

   (c) If Alice picks $a = 2$ and Bob picks $b = 8$ then what is their shared secret key?

i	$g^i \pmod{11}$
0	1
1	6
2	3
3	7
4	9
5	10
6	5
7	8
8	4
9	2
10	1

6. (20 points) Prove that $6^{1/4}$ is irrational. You MAY NOT use the Unique Factorization Theorem. You WILL have to come up with, and prove, a lemma about congruence.

7. (20 points) YOU are a professor trying to make up an exam. You want to give the students the following problem (but you don't know how to set the parameter B).

> T is defined as follows:
>
> $T(1) = 5$
>
> $T(2) = 20$
>
> $T(3) = 24$
>
> $(\forall n \geq 4)[T(n) = Bn + T(n/3) + T(n/4)]$.
>
> By constructive induction find a constant a such that:
>
> $(\forall n \geq 1)[T(n) \leq an]$.

You WANT the answer to come out that $a = 15$.

FIND the value of B such that if the students do this problem correctly by construction induction they will deduce that $a = 15$. (You may actually deduce that $a \geq 15$ but the class knows that you want to take the minimal value of a.)

(You may ignore floor-ceiling issues with the $n/3$ and $n/4$.)

Scratch Paper