Math 210

Third Hour Exam

Name ______________________________

Notes:

1. Show your work. Answers given without indication of how you got the answer may not receive credit.
2. Calculators are permitted on this exam. In problems involving calculating a number, however, it is sufficient to leave the calculation in a form in which it can be entered into a calculator (**except where a number is called for in the problem**). If you do use a calculator, you should include this “pre-calculator” expression as part of your answer.

Friday, April 8
100 pts.

I. Some RSA stuff.

1. (5 pts. each) Without using your calculator (and being sure to show your work or a theorem which justifies your calculation), calculate

   a. $3^{16} \bmod 17$

   b. $3^{10} \bmod 13$

2. (5 pts.) Bob has (secretly) picked two primes, 13 and 31, and has set e = 53 as his private key, publishing 13*31 (=403) and 53 as his public key. What must be true for 197 to be the private key?

I. (5 pts. each) Consider the statement

If I study I will pass the exam.

a. Write the **converse** of this statement

b. Write the **contrapositive** of this statement

c. Which of the above two (converse and contrapositive) is equivalent to the original statement?

d. What is the **sufficient** condition in this statement?

e. What is the **necessary** condition in this statement?

II. Truth tables and digital circuitry

1. (15 pts.) Complete the following truth table

p	q	$\neg p$	$\neg p \vee q$	$p \wedge (\neg p \vee q)$
T	T			
T	F			
F	T			
F	F			

2. (5 pts). Write the circuit diagram for $\neg p \vee q$

III. Some questions on predicate logic and proof.

1. (5 pts.) Simplify (by moving negations inwards) $\neg \forall x(p(x) \Rightarrow q(x))$

(problem III continued)

2. Some definitions (5 pts. each): Define or briefly describe

a. Modus Ponens

b. Modus Tolens

c. Direct proof

d. Proof by contradiction

IV. (15 pts.) Mathematical induction. Following the following steps, prove that

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

a. State and prove the **base case**.

b. State the **inductive step**. What is the **inductive hypothesis** in this case?

c. Prove the inductive step.