The best way to prepare for the final is to be sure that you know how to do all the homework problems and all the problems that were on the two exams. If you can do all of those problems, then you are in good shape for the final.

Here are some other problems to look at. Parts of Chapter 8 will be covered in class on Wednesday and Thursday. This sheet does not include Chapter 8, even though topics covered in class from that chapter may be on the final.

1. Consider the proposition $(\neg p \vee q) \rightarrow r$.

   a) Give the truth table for this proposition.

   b) Give the negation of this proposition and simplify it so no compound proposition is negated.

2. Use truth tables to verify that $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are logically equivalent.

3. Let $D(x)$ be the proposition that x is in Denton, $U(x)$ the proposition that x is at UNT, and $B(x)$ the proposition that x has been to Beth Marie's. Use logic symbols to write the statement "Someone at UNT has not been to Beth Marie's, but everyone who has been to Beth Marie's is in Denton." Give the negation of this proposition both in symbols and as a sentence.

4. Show that $((p \vee q) \wedge \neg p) \rightarrow q$ is a tautology by first using a truth table and then using the logical equivalences on page 24.

5. Let $f : A \rightarrow B$ and $g : B \rightarrow C$. Prove or give a counterexample to each.

   a) If f is one-to-one and g is onto, then $g \circ f$ is one-to-one.

   b) If f is one-to-one and g is one-to-one, then $g \circ f$ is one-to-one.

   c) If f is onto and g is one-to-one, then $g \circ f$ is onto.

   d) If f is onto and g is onto, then $g \circ f$ is onto.

   e) If $g \circ f$ is one-to-one and g is one-to-one, then f is one-to-one.

   f) If $g \circ f$ is onto and g is onto, then $g \circ f$ is onto.

6. Prove that for any integer n, $4 \nmid (n^2+1)$.

7. Prove that $3|n$ if and only if $3 \nmid (n^2-1)$.

8. Prove that if x^3 is irrational, then x is irrational.

9. Prove or give a counterexample.

   a) For all real numbers x and y, $\lfloor x \rfloor + \lceil y \rceil = \lceil x \rceil + \lfloor y \rfloor$.

   b) For any positive integer x, $\lfloor \frac{x-1}{8} \rfloor = \lceil \frac{x}{8} \rceil - 1$.

   c) For any rational number r, $r \geq 3\lfloor \frac{r}{3} \rfloor$.

10. Give an algorithm asked for on exam 2 problem 2 different from the one you gave on the exam. Determine the order of the worst case complexity of your algorithm.

11. Find the order for each of the functions. Express your answers as θ of a standard function.

    a) $(n^2+2)(3n^3+5n^2-7)$
    b) $(n+1)^3-(n-1)^3$
    c) $1^2+2^2+3^2+\ldots+n^2$
    d) $\log n!$
    e) $1+a+a^2+a^3+a^4+\ldots+a^n$ (Here, a is a fixed positive number and n is the variable. Your answer should have three cases, $a<1$, $a=1$, and $a>1$.)

12. Give an example of a problem that is NP-complete.

13. How many zeros are at the end of the number 9873! when written in the usual base 10?

14. What is the largest power of 2 that divides 947!

15. Use the Euclidean algorithm to find gcd(32088, 6216).

16. Find the multiplicative inverse of $a \pmod n$ or show that it does not exist.

    a) $a=14$, $n=49$
    b) $a=28$, $n=37$
    c) $a=7994$, 2669

17. The public keys in a simple RSA encryption are $n=221$ and $e=5$.

    a) Encrypt the message 10.
    b) Compute the private keys p, q, d.
    c) Decrypt the encrypted message 7.

18. Prove that an integer is divisible by 9 if and only if the sum of it's digits is divisible by 9.

19. Prove that if $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then

    a) $a+c \equiv b+d \pmod n$.
    b) $ac \equiv bd \pmod n$.
    c) Use parts a) and b) to explain why one can replace the number 7 with the number 0 when computing $g(7)$ mod 7 if g is a polynomial with integer coefficients.

20. Show that if $a \equiv b \pmod p$ and $a \equiv b \pmod q$ where p and q are distinct primes, then $a \equiv b \pmod{pq}$. Give an example to show that the assumption that p and q are prime cannot be dropped from the statement.

21. Show that the system of congruences $x \equiv 2 \pmod 6$ and $x \equiv 3 \pmod 9$ has no solution.

22. Show that if the denomination of coins are $c^0, c^1, c^2, c^3, \ldots, c^k$, where c and k are positive integers, then the greedy algorithm produces change using the fewest number of coins.

23. Prove $\sqrt{5}$ is irrational.

24. Show there is no integer solution of $x^4+y^4=1000$.

25. Prove $1^3 + 3^3 + 5^3 + \ldots + (2n+1)^3 = (n+1)^2(2n^2+4n+1)$ for any positive integer n.

26. Prove that $\frac{1}{1(3)} + \frac{1}{3(5)} + \frac{1}{5(7)} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$ for any positive integer n.

27. Let $g(x) = xe^x$. By computing a few derivatives, make a conjecture for a formula for the n^{th} derivatives of $g(x)$. Prove your conjecture.

28. By looking at the first few Fibonacci numbers, determine for which n, f_n is even and for which n f_n is odd. Prove you conjecture using induction.

29. Use bubble sort to sort the list $8, 1, 5, 3, 9, 4, 7, 2$. Show all intermediate lists obtained during the sort.

30. Prove that if n and $a \geq 3$ are positive integers and either $n \geq 2$ or $a - 1$ is not a prime number, then $a^n - 1$ is not a prime number.

31. Compute $7^{3370} \bmod 23$.

32. Give an algorithm that computes $\gcd(a, b)$ recursively.

33. The set B of *balanced strings of parentheses* is defined recursively by

    Basis Step: $\lambda \in B$, where λ is the empty string.

    Recursive Step: $(x) \in B$ and $xy \in B$ if $x, y \in B$.

    a) Show that a balanced string of parentheses has the same number of left and right parentheses.
    b) Show that $(()())$ is a balanced string of parentheses.
    c) Show that $((()())$ is not a balanced string of parentheses.
    d) Find all balanced string of parentheses with four or fewer parentheses.

34. Let S be the set of all strings of English letters. Determine whether these relations are reflexive, symmetric, antisymmetric, or transitive.

    a) $R_1 = \{(a, b) | a$ and b have no letters in common.$\}$
    b) $R_2 = \{(a, b) | a$ and b have the same number of letters.$\}$
    c) $R_3 = \{(a, b) | a$ is longer than $b\}$

35. Suppose that R_1 and R_2 are both reflexive relations on a set A. Is $R_1 \cup R_2$ reflexive? Is $R_1 \cap R_2$ reflexive? Prove or give a counterexample for each.

36. Which of these are equivalence relations on the set of all people?

    a) $\{(x, y) |$ x and y have the same sign of the zodiac.$\}$
    b) $\{(x, y) |$ x and y were born in the same year. $\}$
    c) $\{(x, y) |$ x and y were born within a year of each other.$\}$