MATH 300 FINAL EXAM May 7, 2007

Name: _____ R. Hammack Score: _____

Directions: Prove the following statements in the space provided. To get full credit you must show all of your work. Use of calculators is **not** allowed on this test.

1. Prove that if A, B and C are nonempty sets and $A \times B = A \times C$, then $B = C$.

   Proof. Suppose A, B and C are nonempty sets and $A \times B = A \times C$.

   We need to show $B = C$, and to accomplish this we will show $B \subseteq C$ and $C \subseteq B$.

   Suppose $x \in B$. Since A is nonempty there is an element $a \in A$.
   Then $(a, x) \in A \times B$, by definition of the Cartesian product.
   Thus $(a, x) \in A \times C$, since $A \times B = A \times C$.
   Therefore $a \in A$ and $x \in C$, by definition of the Cartesian product.
   In particular, $x \in C$.
   We have shown that $x \in B$ implies $x \in C$, so $B \subseteq C$.

   Suppose $x \in C$. Since A is nonempty there is an element $a \in A$.
   Then $(a, x) \in A \times C$, by definition of the Cartesian product.
   Thus $(a, x) \in A \times B$, since $A \times B = A \times C$.
   Therefore $a \in A$ and $x \in B$, by definition of the Cartesian product.
   In particular, $x \in B$.
   We have shown that $x \in B$ implies $x \in B$, so $C \subseteq B$.

   Since $B \subseteq C$ and $C \subseteq B$, it follows that $B = C$. ■

2. Prove that if x and y are real numbers that are both greater than zero, then $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$.
   (Suggestion: consider proof by contradiction or contrapositive.)

   Proof. For the sake of contradiction, assume x and y are real numbers that are both greater than zero, but $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$. Square both sides:

$$\begin{aligned} (\sqrt{x+y})^2 &= (\sqrt{x} + \sqrt{y})^2 \\ x + y &= x + 2\sqrt{x}\sqrt{y} + y \\ 0 &= 2\sqrt{x}\sqrt{y} \\ 0 &= \sqrt{x}\sqrt{y} \\ 0^2 &= (\sqrt{x}\sqrt{y})^2 \\ 0 &= xy \end{aligned}$$

   Therefore at least one of x and y is zero, contradicting the fact that x and y are both greater than 0. ■

3. Suppose $x \in \mathbb{Z}$. Prove $7x - 3$ is even if and only if x is odd.

Proof. Suppose that $7x - 3$ is even. Thus $7x - 3 = 2a$ for some integer a.
Then $7x - 3 = x + 6x - 2 - 1 = 2a$, so $x = 2a - 6x + 2 + 1 = 2(a - 3x + 1) + 1$.
Thus $x = 2m + 1$, where m is the integer $a - 3x + 1$. Consequently, x is odd.

Conversely, suppose x is odd. Then $x = 2a + 1$ for some integer a.
Then $7x - 3 = 7(2a + 1) - 3 = 14a + 7 - 3 = 14a + 4 = 2(7a + 2)$.
Since $7x - 3 = 2(7a + 2)$, and $7a + 2$ is an integer, it follows that $7x - 3$ is even. ■

4. Prove or disprove: If A and B are nonempty sets, then $\mathscr{P}(A) \cap \mathscr{P}(B) = \mathscr{P}(A \cap B)$.

This is TRUE.

Proof. To prove $\mathscr{P}(A) \cap \mathscr{P}(B) = \mathscr{P}(A \cap B)$, we must prove $\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B)$ and $\mathscr{P}(A \cap B) \subseteq \mathscr{P}(A) \cap \mathscr{P}(B)$.

Suppose $X \in \mathscr{P}(A) \cap \mathscr{P}(B)$.
By definition of intersection, this means $X \in \mathscr{P}(A)$ and $X \in \mathscr{P}(B)$.
By the definition of power sets, this means $X \subseteq A$ and $X \subseteq B$.
Thus, any element $x \in X$ is in both A and B, so $x \in A \cap B$. Hence $X \subseteq A \cap B$, which means $X \in \mathscr{P}(A \cap B)$.
We have seen that $X \in \mathscr{P}(A) \cap \mathscr{P}(B)$ implies $X \in \mathscr{P}(A \cap B)$, so $\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B)$.

Now suppose $X \in \mathscr{P}(A \cap B)$.
By definition of the power set, this means $X \subseteq A \cap B$.
Thus any element $x \in X$ is in $A \cap B$, so $x \in A$ and $x \in B$. Hence $X \subseteq A$ and $X \subseteq B$.
Thus $X \in \mathscr{P}(A)$ and $X \in \mathscr{P}(B)$, so $X \in \mathscr{P}(A) \cap \mathscr{P}(B)$, by definition of intersection.
We have seen that $X \in \mathscr{P}(A \cap B)$ implies $X \in \mathscr{P}(A) \cap \mathscr{P}(B)$, so $\mathscr{P}(A \cap B) \subseteq \mathscr{P}(A) \cap \mathscr{P}(B)$.

The previous two paragraphs imply $\mathscr{P}(A) \cap \mathscr{P}(B) = \mathscr{P}(A \cap B)$. ■

5. Prove or disprove: If A and B are sets with $A \neq B$, and $A \subseteq B$, then $|A| < |B|$.

This is FALSE. Here is a counterexample.
Let $A = \mathbb{N}$ and $A = \mathbb{Z}$.
Then $A \neq B$, and $A \subseteq B$, but $|A| = \aleph_0 = |B|$.

6. Prove or disprove: If an equivalence relation on a set A has finitely many equivalence classes, then A is finite.

This is FALSE. Here is a counterexample.
Let $A = \mathbb{Z}$ and R be the equivalence relation mRn if and only if $m \equiv n \pmod 2$.
This equivalence relation has just two equivalence classes [0] and [1], yet A is infinite.

7. Suppose a, b and c are integers. Prove that if $a|b$ and $a|(b+c)$, then $a|c$.

Proof. Suppose $a|b$ and $a|(b+c)$.
By definition of divisibility, this means $b = am$ and $b + c = an$ for some $m, n \in \mathbb{Z}$.
Then $c = (b+c) - b = an - am = a(n-m)$.
Thus $c = ak$ where k is the integer $n - m$.
Thus $a|c$, by definition of divisibility. ■

8. Suppose A and B are sets. Use the technique of contrapositive proof to prove the following:
If $A \times B = \emptyset$, then $A = \emptyset$ or $B = \emptyset$.

Proof. (Contrapositive) Suppose it is not true that $A = \emptyset$ or $B = \emptyset$.
Then $A \neq \emptyset$ and $B \neq \emptyset$.
Since A and B are nonempty, there are elements $a \in A$ and $b \in B$.
Then $(a, b) \in A \times B$, by definition of the Cartesian product.
Thus $A \times B$ is not the empty set. ■

9. Prove that if $a \equiv 1 \pmod 5$, then $a^2 \equiv 1 \pmod 5$.

Proof. Suppose $a \equiv 1 \pmod 5$.
By definition of congruence modulo 5, this means $5|(a-1)$.
In turn, by definition of divisibility, *this* means $a - 1 = 5k$ for some integer k.
Then $a = 5k + 1$, and squaring both sides produces $a^2 = (5k+1)^2 = 25k^2 + 10k + 1$.
From this, $a^2 - 1 = 25k^2 + 10k$, hence $a^2 - 1 = 5(5k^2 + 2k)$.
Then $5|(a^2 - 1)$, by definition of divisibility.
And so $a \equiv 1 \pmod 5$, by definition of congruence modulo 5. ■

10. Prove that $\sqrt{2}$ is irrational.

Proof. Suppose to the contrary that $\sqrt{2}$ is rational. Then there exists $a, b \in \mathbb{N}$ for which $\sqrt{2} = \dfrac{a}{b}$.
We may assume that the fraction $\dfrac{a}{b}$ is reduced, **so a and b are not both even.**
From $\sqrt{2} = \dfrac{a}{b}$, we get $2 = \left(\dfrac{a}{b}\right)^2 = \dfrac{a^2}{b^2}$, so $a^2 = 2b^2$, so a^2 is even, and hence a is even.
Since a and b are not both even, it follows that b **is odd**.
Since a is even, $a = 2k$ for some integer k. The equation $a^2 = 2b^2$ then yields $(2k)^2 = 2b^2$ or $4k^2 = 2b^2$, which implies $2k^2 = b^2$. Consequently b^2 is even, so **so b is even**.
We have therefore deduced that b is even and b is odd. This contradiction proves the theorem. ■

11. Suppose R is a transitive relation on a set A, and $x \not R\, x$ for all $x \in A$. Show that if xRy, then $y \not R\, x$.

Proof. Suppose R is a transitive relation on A, and $x \not R\, x$ for all $x \in A$.
Assume xRy for $x, y \in A$. We need to show $y \not R\, x$.
Suppose for the sake of contradiction that yRx.
Then we have xRy and yRx, from which transitivity implies xRx, contradicting $x \not R\, x$.
Consequently, if xRy, then it cannot be the case that yRx, so $y \not R\, x$. ■

The questions on this page involve the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined as $f((x, y)) = (x + y, x)$

12. Prove that f is injective.

Proof. Suppose $f((a, b)) = f((c, d))$.
Then the definition of f implies $(a + b, a) = (c + d, c)$.
Since these ordered pairs are equal, it must be that $a + b = c + d$ and $a = c$.
From $a + b = c + d$ and $a = c$, it follows $a + b = a + d$, so $b = d$.
Therefore we have $a = c$ and $b = d$, so $(a, b) = (c, d)$.
It follows that f is injective. ■

13. Prove that f is surjective.

Proof. Take an arbitrary element (a, b) in the codomain $\mathbb{Z} \times \mathbb{Z}$.
Then certainly $(b, a - b)$ is in the domain $\mathbb{Z} \times \mathbb{Z}$.
Observe that $f((b, a - b)) = (a - b + b, b) = (a, b)$.
This shows that f is surjective. ■

14. Find a formula for f^{-1}.

Notice that $f(f^{-1}((a, b))) = (a, b)$.
What should $f^{-1}((a, b))$ be, so that taking f if it produces (a, b)?
The solution of Problems 13 suggests that $f^{-1}((a, b)) = (b, a - b)$.

Therefore, try $f^{-1}((x, y)) = (y, x - y)$.
Then $f(f^{-1}((x, y))) = f((y, x - y)) = (y + x - y, y) = (x, y)$ for all $(x, y) \in \mathbb{Z} \times \mathbb{Z}$
And $f^{-1}(f((x, y))) = f^{-1}((x + y, x)) = (x, x + y - x) = (x, y)$ for all $(x, y) \in \mathbb{Z} \times \mathbb{Z}$

Therefore $f^{-1}((x, y)) = (y, x - y)$.

15. Use mathematical induction to prove $1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$ for all $n \in \mathbb{N}$.

Proof. For the basis step, notice that when $n = 1$ the statement is $1^3 = \frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$, which is true.

Now assume the statement is true for some integer $n = k \geq 1$, that is assume
$1^3 + 2^3 + 3^3 + 4^3 + \cdots + k^3 = \dfrac{k^2(k+1)^2}{4}$.

Observe that this implies the statement is true for $n = k + 1$.

$$\begin{aligned}
1^3 + 2^3 + 3^3 + 4^3 + \cdots + k^3 + (k+1)^3 &= (1^3 + 2^3 + 3^3 + 4^3 + \cdots + k^3) + (k+1)^3 \\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\
&= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\
&= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\
&= \frac{(k+1)^2(k^2 + 4(k+1)^1)}{4} \\
&= \frac{(k+1)^2(k^2 + 4k + 4)}{4} \\
&= \frac{(k+1)^2(k+2)^2}{4} \\
&= \frac{(k+1)^2((k+1)+1)^2}{4}
\end{aligned}$$

Therefore $1^3 + 2^3 + 3^3 + 4^3 + \cdots + k^3 + (k+1)^3 = \dfrac{(k+1)^2((k+1)+1)^2}{4}$, which means the statement is true for $n = k + 1$. Thus the result follows by mathematical induction. ■

16. Use mathematical induction to prove $4|(5^n - 1)$ for every $n \in \mathbb{N}$.

Proof. For the basis step, note that if $n = 1$, the statement $4|(5^1 - 1)$ is $4|4$, which is true.

For the inductive hypothesis, assume that $4|(5^k - 1)$ is true for some integer $k \geq 1$.
Now we will show this implies $4|(5^{k+1} - 1)$ is true.
Since $4|(5^k - 1)$, there is an integer c for which $5^k - 1 = 4c$.
Multiply both sides of this equation by 5 to get $5^{k+1} - 5 = 20c$.
Now subtract 4 from both sides and we have $5^{k+1} - 1 = 20c - 4 = 4(5c - 1)$.
Since $5c - 1$ is an integer, the equation on the previous line yields $4|(5^{k+1} - 1)$.

Therefore, by the Principle of Mathematical Induction it follows that $4|(5^n - 1)$ for every $n \geq 0$. ■

17. Use mathematical induction to prove $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1$ for every $n \in \mathbb{N}$.

Proof. For the basis step, notice that when $n = 1$ the statement is $1 \cdot 1! = (1+1)! - 1$, or $1 = 1$, which is true.

Now assume the statement is true for some integer $n = k \geq 1$, that is assume
$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + k \cdot k! = (k+1)! - 1$.

Observe that this implies the statement is true for $n = k + 1$.

$$\begin{aligned}
1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + k \cdot k! + (k+1) \cdot (k+1)! &= (1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + k \cdot k!) + (k+1) \cdot (k+1)! \\
&= (k+1)! - 1 + (k+1) \cdot (k+1)! \\
&= (k+1)! + (k+1) \cdot (k+1)! - 1 \\
&= (1 + (k+1))(k+1)! - 1 \\
&= (k+2)(k+1)! - 1 \\
&= (k+2)! - 1 \\
&= ((k+1)+1)! - 1
\end{aligned}$$

Therefore $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + k \cdot k! + (k+1) \cdot (k+1)! = ((k+1)+1)! - 1$, which means the statement is true for $n = k + 1$. Thus the result follows by mathematical induction. ■

18. Let $\mathbb{R}^+ = \{x \in \mathbb{R} \ : \ x > 0\}$. Prove that $|\mathbb{R}^+| = |\mathbb{R}|$.
(Suggestion: use the definition of what it means for two sets to have the same cardinality, combined with your knowledge of algebra and functions)

Proof. From calculus, you are familiar with the function $\ln : \mathbb{R}^+ \to \mathbb{R}$.
Now, ln is injective, for given $x, y \in \mathbb{R}^+$ with $\ln(x) = \ln(y)$, then $e^{\ln(x)} = e^{\ln(y)}$, so $x = y$.
And ln is surjective, for given a real number $y \in \mathbb{R}$, the number e^y is in $\mathbb{R}^+$, and $\ln(e^y) = y$.
Thus we have a bijection $\ln : \mathbb{R}^+ \to \mathbb{R}$, which means $|\mathbb{R}^+| = |\mathbb{R}|$ by definition of what it means for two sets to have the same cardinality. ■

19. This problem concerns 4-letter codes that can be made from the letters A,B,C,D,E, …, Z of the English Alphabet.

    (a) How many such codes can be made? Answer: $26 \cdot 26 \cdot 26 \cdot 26 = \mathbf{456976}$

    (b) How many such codes are there that have no two consecutive letters the same?

    To answer this we use the Multiplication Principle. There are 26 choices for the first letter. The second letter can't be the same as the first letter, so there are only 25 choices for it. The third letter can't be the same as the second letter, so there are only 25 choices for it. The fourth letter can't be the same as the third letter, so there are only 25 choices for it. **Thus there are $\mathbf{26 \cdot 25 \cdot 25 \cdot 25 = 406,250}$ codes with no two consecutive letters the same.**

20. How many 9-digit numbers can be made from the digits $1, 2, 3, 4, 5, 6, 7, 8, 9$ if repetition is not allowed and all the odd digits occur first (on the left) followed by all the even digits? (i.e. 1375980264 is such a number, but 0123456789 is not.)

    Answer: $4!5! = 2880$.