Math 2513, Spring 2005
EXAM 2—Solutions

NOTE: Most of the problems on this test can be solved in more than one way.

1. *(15 points)* Consider the implication $\mathcal{P}$: *If* $f : A \to B$ *is a surjective function then* $f : A \to B$ *has an inverse.*
(a) State the converse of $\mathcal{P}$.
(b) State the contrapositive of $\mathcal{P}$.
(c) State the inverse of $\mathcal{P}$.

(a) Converse of $\mathcal{P}$: *If* $f : A \to B$ *has an inverse then* $f : A \to B$ *is a surjective function.*
(b) Contrapositive of $\mathcal{P}$: *If* $f : A \to B$ *does not have an inverse then* $f : A \to B$ *is not a surjective function.*
(c) Inverse of $\mathcal{P}$: *If* $f : A \to B$ *is not a surjective function then* $f : A \to B$ *does not have an inverse.*

NOTE: The statements in (a) and (c) are true statements, the other two ((b) and $\mathcal{P}$ itself) are not.

2. *(15 points)* Let ℓ, m and n be positive integers.
(a) Define what 'ℓ divides m' means.
(b) Prove that if ℓ divides m and ℓ divides n then ℓ divides $3n - 5m$.
(c) Show that the converse of (b) is not true.

(a) 'ℓ divides m' means that there exists an integer k such that $m = \ell k$.
(b) Let ℓ, m and n be positive integers. Assume that ℓ divides m and that ℓ divides n. By definition of divides, this means that there are integers k_1 and k_2 such that $m = \ell k_1$ and $n = \ell k_2$. Thus

$$3n - m = 3\ell k_1 - 5\ell k_2 = \ell(3k_1 - 5k_2) \ .$$

Since $3k_1 - 5k_2$ is an integer (the product and the sum of integers is an integer) it follows that ℓ divides $3n - 5m$. □
(c) Take $n = 1$, $m = -3$ and $\ell = 2$. Then $\ell = 2$ divides $3n - 5m = 3(1) - 5(-3) = 18$ but $\ell = 2$ does not divide $n = 1$. This is just one of many possible counterexamples.

3. *(10 points)* Let A and B be sets. State the negation of each of the following propositions as directly as possible.
(a) B is a subset of A or $A \cap B = \emptyset$.
(b) If B is a subset of A then A and B are disjoint.

(a) First note that if a statement of the form "$\mathcal{P}$ or $\mathcal{Q}$" is true then either $\mathcal{P}$ is true or $\mathcal{Q}$ is true (or possibly both). So if "$\mathcal{P}$ or $\mathcal{Q}$" is false then $\mathcal{P}$ and $\mathcal{Q}$ must both be false.
So a correct answer to (a) is: *B is not a subset of A and $A \cap B \neq \emptyset$.*

(b) First note that if a statement of the form "if $\mathcal{P}$ then $\mathcal{Q}$" is false then it must be that $\mathcal{P}$ is false and $\mathcal{Q}$ is true. So a correct answer to (b) is: *B is a subset of A, and A and B are not disjoint.*

4. *(10 points)* Use a truth table to demonstrate that $(p \vee q) \wedge (\neg p \vee r)$ is not logically equivalent to $q \vee r$.

If you write out the entire truth table (which I'd rather not do here) you will discover two lines where $(p \vee q) \wedge (\neg p \vee r)$ and $q \vee r$ take different values but have the same inputs p, q and r. They are the lines where (1) $p = q = T$ and $r = F$ and where (2) $p = q = F$ and $r = T$.

5. *(15 points)* Consider the proposition '*The square of an even number is an even number*'.
(a) Describe the procedure you would use to prove the proposition with a direct proof.
(b) Describe the procedure you would use to prove the proposition with an indirect proof.
(c) Describe the procedure you would use to prove the proposition with a proof by contradiction.
(d) Prove the proposition.

(a) Assume that n is even then show using the standard principles of logical inference that n^2 is even.
(b) Assume that n^2 is not even then show that n is not even.

(c) Assume that n is even and that n^2 is not even then derive a contradiction.
(d) I'll use a direct proof: Let n be an integer. Assume that n is even. This means that $n = 2k$ for some integer k (definition of "even"). Therefore

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2) .$$

Since $2k^2$ is an integer (because it can be expressed as the product of three integers 2, k and k), we conclude that n^2 is even (by the definition of "even"). □

6. *(15 points)* Let A and B be sets. Show that $A \subseteq B$ if and only if $A - B = \emptyset$. Break the proof into two separate parts, one for each implication.

($\Rightarrow$) Let A and B be sets. Assume that A is a subset of B and that $A - B \neq \emptyset$. Let x be an element of $A - B$ (which exists since we know that $A - B$ is not the empty set). This means that $x \in A$ and $x \notin B$. Since $x \in A$ and $A \subseteq B$, it follows from the definition of subset that $x \in B$. Thus $x \in B$ and $x \notin B$ which is a contradiction. This shows that $A \subseteq B$ implies $A - B = \emptyset$ using proof by contradiction.

($\Leftarrow$) Let A and B be sets. Assume that A is not a subset of B. Therefore there is an element x such that $x \in A$ and $x \notin B$ (by definition of subset). By the definition of set difference, x is an element of $A - B$. Since $A - B$ has at least one element it cannot equal the empty set; that is, $A - B \neq \emptyset$. This shows (by an indeirect proof) that if $A - B = \emptyset$ then $A \subseteq B$. □

7. *(10 points)* Let n and m be integers.
(a) What does $m \equiv n \pmod 5$ mean? (State the definition.)s
(b) Find three different values of n which satisfy the equation $n + 1 \equiv 0 \pmod 5$.
(c) Does the equation $n^2 + 1 \equiv 0 \pmod 5$ have any solutions? If so how many?
(d) Does the equation $n^4 + 1 \equiv 0 \pmod 5$ have any solutions? If so how many?

(a) $m \equiv n \pmod 5$ means that $m - n$ is divisible by 5. In other words, there is an integer k so that $m - n = 5k$ or so that $m = 5k + n$.
(b) If $n + 1 \equiv 0 \pmod 5$ then $n + 1 = (n + 1) - 0$ must be divisible by 5 by part (a). This means that $n + 1 = 5k$ or that $n = 5k - 1$ for some integer k. Take three different values for k to give specific answers for (b).
(c) Note that $n = 2$ and $n = 3$ are solutions to the equation $n^2 + 1 \equiv 0 \pmod 5$. Any integer which is congruent to 2 or 3 modulo 5 will also satisfy the equation. In other words, all integers of the form $5k + 2$ and $5k + 3$ where k is an integer will satisfy the equation. Therefore the equation has infinitely many solutions.
(d) By direct checking we see that the equation $n^4 + 1 \equiv 0 \pmod 5$ has no solution between 0 and 4 (because $0^4 + 1 = 1$, $1^4 + 1 = 2$, $2^4 + 1 = 17$,$3^4 + 1 = 82$ and $4^4 + 1 = 257$ none of which are divisible by 5). If n was a solution to the equation then $5k + n$ would also be a solution, and this means that there would have to be at least one solution where n is between 0 and 4, which we have seen to be impossible. We conclude that the equation in (d) has no solutions.

8. *(10 points)* Let m and n be positive integer larger than 1.
(a) Describe the prime factorization of n^2 in terms of the prime factorization of n.
(b) Explain how to use your answer to part (a) to determine whether or not the integer 288 is a perfect square.
(c) Show that it is not always true that $\gcd(n^2, m^3) = \gcd(n, m)^2$.

(a) If n has the prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ (where the p_i's are distinct primes and each a_i is a positive integer) then the prime factorization of n^2 is $n^2 = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k}$.
(b) By part (a) an integer n which is a perfect square would have to have a prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where each a_i is even. Since the prime factorization of 288 is $288 = 2^5 3^2$ we see that 288 is not a perfect square (as the power of 2 is an odd number).
(c) It is true that $\gcd(n, m)^2$ divides $gcd(n^2, m^3)$, but they are not always equal. One counterexample occurs when $n = 25$ and $m = 5$, but many others can be found as well.