Math 55 Spring 2016 Practice Midterm 1 Solutions

Nikhil Srivastava

80 minutes, closed book, closed notes

1. (3 pts each) True or False (and provide a brief one or two sentence explanation):

   (a) The compound propositions
   $$\neg p \to q$$
   and
   $$\neg p \vee \neg q$$
   are logically equivalent.

   Solution: False, the first expression is equivalent to $p \vee q$, which is different from the second expression (for instance, when p and q are both false).

   (b) The compound proposition
   $$(p \to F) \vee (p \to T)$$
   is a tautology, where T and F are true and false.

   Solution: This is a tautology, because the conditional $p \to T$ is always true, and so its disjunction with any other proposition is also true.

   (c) Every subset of the integers has a least element.

   Solution: False. $\mathbb{Z}$ itself does not.

   (d) If A and B are uncountable then $A \cup B$ is also uncountable.

   Solution: True. Here is a proof of the contrapositive: suppose there is a bijection $f : \mathbb{Z}^+ \to A \cup B$. Then consider the function $g : \mathbb{Z}^+ \to A$ where $g(n)$ is the n^{th} element of the sequence $f(1), f(2), \ldots$ which is an element of A. It is then easy to check that g is a bijection so A must be countable, so in particular it is not the case that A and B are uncountable.

   (A similar argument can be used to show that B is also countable, and this establishes the stronger statement that if $A \cup B$ is countable then both A and B must be countable.)

2. (7 pts) Suppose A, B, and C are sets such that $A \cap C = B \cap C$ and $A \cup C = B \cup C$. Can you conclude that $A = B$? Give a proof or a counterexample.

   Solution: Yes, you can.

Proof. We will first show that $A \subseteq B$. Assume $x \in A$. If $x \in C$ then $x \in A \cap C$ so $x \in B \cap C$ and consequently $x \in B$. On the other hand, if $x \notin C$ then since $x \in A \cup C$ and $A \cup C = B \cup C$ we have $x \in B \cup C$, so x must be an element of B or C, but since we have assumed $x \notin C$ we must have $x \in B$. Since $x \in B$ in both cases, we conclude that $A \subseteq B$.

A completely analogous argument shows that $B \subseteq A$, so $A = B$. $\square$

3. (7 pts) Suppose A, B, and C are sets and $f : A \to B$ and $g : B \to C$ are functions such that $g \circ f : A \to C$ is injective. Can you conclude that both f and g are injective? Give a proof or a counterexample.

   Solution: No. For a counterexample, consider $A = C = \{0, 1\}$, $B = \{0, 1, 2\}$, $f : A \to B$ by $f(x) = x$, and $g : B \to C$ by $g(0) = 0, g(1) = 1, g(2) = 1$. Then g is not injective but the composition $g \circ f$ is injective.

4. (7 pts) Prove that if x and y are integers and p is a prime such that xy and $x + y$ are both divisible by p, then both x and y must be divisible by p.

   Proof. Since $p|xy$, we know by Euclid's lemma that either $p|x$ or $p|y$. If p divides x, then since p divides $x + y$, we can conclude that p must also divide $x + y - x = y$. Thus, p divides both x and y, as desired. The case $p|y$ is completely analogous. $\square$

   Note: instead of using "completely analogous", I could also have begun the proof by saying "assume without loss of generality that $p|x$", since the problem is completely symmetric in x and y, and I can assume I have named the numbers in a way that x is always divisible by p. See page 95 of the book for a more detailed discussion.

5. (7 pts) Prove that if n is an integer then $n^2 \equiv 0$ or $1 (\text{mod } 4)$. Use this to show that if $m = 4k + 3$ for some integer k then m cannot be written as the sum of the squares of two integers.

   Proof. We will first show that $n^2 \equiv 0$ or $1 (\text{mod } 4)$. If n is even then there exists an integer k such that $n = 2k$. In this case, $n^2 = 4k^2$, which is always divisible by 4, so $n^2 \equiv 0 (\text{mod } 4)$. If n is odd then there exists an integer k such that $n = 2k + 1$, in which case $n^2 = 4k^2 + 4k + 1$. Since the first two terms are divisible by 4 we have $n^2 \equiv 1 (\text{mod } 4)$ in this case.

   For the second part, let $m = 4k + 3$ and assume for contradiction that m can be written as the sum of two squares, i.e.,

$$m = a^2 + b^2$$

   for some integers a, b. By the first part of the question, we have[1]

$$a^2 + b^2 \equiv (a^2 \ \mathbf{mod}\ 4) + (b^2 \ \mathbf{mod}\ 4) \equiv \ 0 \text{ or } 1 \text{ or } 2 \ \not\equiv 3 (\text{mod } 4),$$

[1]For clarity I will use the boldface **mod** to denote the remainder operation.

which is absurd since $m \equiv 3 \pmod 4$. Thus, our assumption is false, and m cannot be written as the sum of two squares. $\square$

6. (5 pts each) (a) Find an inverse of 5 modulo 13. (b) Compute the remainder when 3^{16} is divided by 11.

Solution:

(a) We use the Euclidean algorithm to compute $gcd(13, 5)$:

$$\begin{aligned} 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Reversing these equalities, we can express 1 as an integer linear combination of 5 and 13:

$$1 = 3 - 1 \cdot 2 = 3 - (5 - 1 \cdot 3) = 2 \cdot 3 - 5 = 2 \cdot (13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5.$$

The inverse of 5 modulo 13 must be the coefficient of 5 in this linear combination, which is $-5 \equiv 8 \pmod{13}$.

Note that since 13 is prime it is also possible to calculate this inverse by appealing to Fermat's Little Theorem, which tells us it must be congruent to 5^{11} modulo 13.

(b) Since 11 is prime and $11 \nmid 3$, Fermat's Little Theorem tells us that

$$3^{10} \equiv 1 \pmod{11}.$$

Thus,

$$3^{16} \equiv 3^{10} \cdot 3^6 \equiv 1 \cdot 9^3 \equiv (-2)^3 \equiv -8 \equiv 3 \pmod{11}.$$