

Math 52B Brief Solutions to Practice Problems for Final Examination (3:30 pm 12/17/09)

Exam problems will be similar to some of these, but the exam will be shorter

1. SETS

- a. Define what it means to say that S is a subset of T .
 $s \in S \implies s \in T$.
- b. Show that $S = \{a \in \mathbb{Z} : a \equiv 3 \pmod{5}\}$ is a subset of $T = \{a \in \mathbb{Z} : a^2 \equiv 4 \pmod{5}\}$
By the definition of S , $a \in S \implies a \equiv 3 \pmod{5}$. By one of the rules of modular arithmetic, this implies that $a^2 \equiv 3^2 \pmod{5}$. Since $3^2 = 9 \equiv 4 \pmod{5}$, we conclude by transitivity of congruence relations that $a^2 \equiv 4 \pmod{5}$. Finally, this implies that $a \in T$, by the definition of T . We have shown $a \in S \implies a \in T$, and this is the definition of S being a subset of T .
- c. Suppose that S and W are subsets of T . Prove that $S \cap (S \cup W) = S$
Suppose $s \in S$. Then it is true that $s \in S$ or $s \in W$, because the first statement is true. Thus $s \in S \cup W$, by the definition of union. Also $s \in S$, by assumption. Thus $s \in S$ and $s \in S \cup W$, which is exactly the meaning of $s \in S \cap (S \cup W)$. We have shown that $s \in S$ implies $s \in S \cap (S \cup W)$. According to the definition of subset, this shows that $S \subset S \cap (S \cup W)$. Now suppose that $s \in S \cap (S \cup W)$. By definition of intersection, we conclude that $s \in S$ and $s \in (S \cup W)$. In particular, $s \in S$. We have shown that $s \in S \cap (S \cup W)$ implies $s \in S$. By the definition of subset, this means that $S \cap (S \cup W) \subset S$. Combined with the fact that we proved $S \subset S \cap (S \cup W)$ above, we have satisfied the definition of equality of sets, so $S = S \cap (S \cup W)$.

RELATIONS

2. In this problem, $X = \{1, 2, 3, 4\}$ and $P(X)$ is the collection of all subsets of X (called the “power set” of X).
 - a. How many subsets does X have?
 $2^{|X|} = 2^4 = 16$.
 - b. We define a relation ρ on $P(X)$, i.e. on the subsets of X . So S and T will represent two subsets of X . Remember that the number of elements in S is denoted by $|S|$. The relation is $\rho = \{(S, T) : |S| = |T|\}$. So the subset S is related to the subset T if and only if S has the same number of elements as T . Show that ρ is an equivalence relation.
Reflexivity: If S is any subset of X , then clearly S has the same number of elements as S , so S is related to S . This shows that the relation is reflexive.
Symmetry: If S is related to T , then $|S| = |T|$, so $|T| = |S|$. We see that T is related to S . This shows that the relation is symmetric.
Transitivity: If S is related to T and T is related to W , then $|S| = |T|$ and $|T| = |W|$. Combining these equalities shows that $|S| = |W|$, which means that S is related to W . This shows that the relation is transitive. Since the relation is reflexive, symmetric and transitive, it satisfies the definition of an equivalence relation.
 - c. Write out the equivalence class of $S = \{1, 3, 4\}$.
The equivalence class of S consists of everything equivalent to S . Since S has 3 elements, a subset of X will be equivalent to S iff it has 3 elements. $\{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}$
 - d. How many different equivalence classes are there? There are 5 equivalence classes: all subsets with 0 elements will be one equivalence class, all subsets with 1 element will be a second equivalence class, all subsets with 2 elements will be a third equivalence class, all subsets with 3 elements will be a fourth equivalence class, and all subsets with 4 elements will be a fifth equivalence class.
 - e. How many different equivalence classes does the subset $\{2, 4\}$ belong to?
It belongs to only one equivalence class. We know that when we have an equivalence relation,

each element belongs to one and only one equivalence class. (The equivalence classes include each element with no omissions and no repetitions.)

f. State a theorem about equivalence relations.

Theorem: The equivalence classes for an equivalence relation on a set A partition the set A into subsets that are disjoint (no overlap), and whose union is A (no omissions). Conversely, a partition of a set A into disjoint subsets whose union is A allows us to define an equivalence relation on A . Two elements will be related iff they are in the same subset created by the partition.

3. Two triangles T_1 and T_2 are similar if you can multiply the lengths of the sides of T_1 by a positive real number r and get the lengths of the sides of T_2 .

a. Show that similarity is an equivalence relation on the set of all triangles.

Reflexivity: If T is any triangle, then you can multiply the lengths of the sides of T by 1 to get the lengths of the sides of T . Thus T is similar to T according to the definition. This shows that the relation of similarity is reflexive.

Symmetry: If T_1 is similar to T_2 , then there is a positive real number r with the property that you can multiply the lengths of the sides of T_1 by r and get the lengths of the sides of T_2 . Then you can multiply the lengths of the sides of T_2 by $1/r$ to get back to the lengths of the sides of T_1 . Since $1/r$ is also a positive real number, this shows that T_2 is similar to T_1 . So similarity is symmetric.

Transitivity: If T_1 is similar to T_2 and T_2 is similar to T_3 , then there is a positive integer r_1 and a positive integer r_2 so that multiplying the lengths of the sides of T_1 by r_1 gives the lengths of the sides of T_2 , and multiplying the lengths of the sides of T_2 by r_2 gives the lengths of the sides of T_3 . From this, it follows that multiplying the lengths of the sides of T_1 by $r = r_1 r_2$ gives the lengths of the sides of T_3 . Thus T_1 and T_3 are similar. So similarity is transitive. Since it is reflexive, symmetric and transitive, it is an equivalence relation.

b. Show that all equilateral triangles are in the same equivalence class for the equivalence relation in part (a).

An equilateral triangle has three sides of the same length. Let T_0 be the equilateral triangle with three sides of length 1. Suppose T_1 is any equilateral triangle at all. It has three sides of equal length a_1 . We can take $r = a_1$, and find that T_0 is similar to T_1 . This shows that any equilateral triangle is similar to T_0 , so it is in the equivalence class of T_0 , by the definition of equivalence class. So all equilateral triangles are in the equivalence class of T_0 .

c. Show that there are infinitely many different equivalence classes of isosceles triangles.

If c is any real number between 0 and 2, we can create an isosceles triangle T_c with sides of length 1, 1, and c . Similarly T_d will be a triangle with sides of length 1, 1, and d . If T_c is similar to T_d , then there is a positive number r so that the lengths of the sides of T_d are r times the lengths of the sides of T_c , namely r , r , and rc . But the lengths of the sides of T_d are 1, 1, and d . So r must equal 1 in order for the first two lengths to match. Then in order for the last number to match when $r = 1$, we see that $c = d$. This means that if we take $c \neq d$, we will get that T_c is not similar to T_d . Since we can take infinitely many different choices of c between 0 and 2 (for instance, $1/2$, $1/3$, $1/4$, $1/5$...) we can find infinitely many different triangles T_c that are not similar to any of the others (for instance, $T_{1/2}$, $T_{1/3}$, ...). So each one of these triangle is in a different equivalence class, and there must be infinitely many equivalence classes.

4. INDUCTION

a. Prove by induction that if $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$ for every positive integer n .

The proof is by induction on n . Assume that $a \equiv b \pmod{m}$ Then $P(n)$ will be the statement that $a^n \equiv b^n \pmod{m}$.

Basis step: If $n = 1$ the statement $P(1)$ says that $a^1 \equiv b^1 \pmod{m}$. Since we have assumed that $a \equiv b \pmod{m}$, it is clear that $P(1)$ is true.

Inductive step: We may assume that $P(N)$ is true. So $a^N \equiv b^N \pmod{m}$. We also know by our original assumption that $a \equiv b \pmod{m}$. By the rules of modular arithmetic for multiplication of congruences, we can conclude that $a^N a \equiv b^N b \pmod{m}$. Now using rules for exponents, this becomes $a^{N+1} \equiv b^{N+1} \pmod{m}$. We have proved that $P(N+1)$ follows from $P(N)$. By the principle of mathematical induction, we may conclude that $P(n)$ holds true for all n , that is $a^n \equiv b^n \pmod{m}$.

- b. A sequence is defined by $a_1 = 3$, $a_2 = 3$, and $a_{n+1} = a_n + 2a_{n-1}$ for $n \geq 1$. Prove by complete induction that $a_n = (2)^n - (-1)^n$ for all positive integers n .

The proof is by complete induction on n . We are given that $a_1 = 3$, $a_2 = 3$, and $a_{n+1} = a_n + 2a_{n-1}$ for $n \geq 1$. We let $P(n)$ denote the statement that $a_n = (2)^n - (-1)^n$.

Basis step: First, $P(1)$ states that $a_1 = 2^1 - (-1)^1$, which simplifies to $a_1 = 3$. Since we were given that $a_1 = 3$, we know that $P(1)$ is true. Second, $P(2)$ states that $a_2 = 2^2 - (-1)^2$, which simplifies to $a_2 = 3$. Since we were given that $a_2 = 3$, we know that $P(2)$ is true.

Inductive step: We may assume that $P(N)$ and $P(N-1)$ are true. So $a_N = (2)^N - (-1)^N$ and $a_{N-1} = (2)^{N-1} - (-1)^{N-1}$. We use the definition with $n = N$ to get $a_{N+1} = a_N + 2a_{N-1}$. Now substituting in the values we have just written for a_N and a_{N-1} , we get

$$a_{N+1} = (2)^N - (-1)^N + 2[(2)^{N-1} - (-1)^{N-1}] = 2^N + 2^N - (-1)^N(1 - 2) = 2^{N+1} - (-1)^{N+1}.$$

This proves $P(N+1)$ and the proof is done by complete induction.

5. THE EUCLIDEAN ALGORITHM

- a. Describe the Extended Euclidean algorithm, what it is used for, and what the steps in the algorithm are.

See the textbook for a description.

- b. Suppose that a and b are two positive integers, and their greatest common divisor is g . Show that if d is a positive integer such that $d|a$ and $d|b$, then $d|g$.

A consequence of the Extended Euclidean algorithm is that there exist integers x and y such that $ax + by = g$. Now if $d|a$ and $d|b$, this means that $a = dk$ and $b = dj$ for some integers k and j . Substituting these in and using the distributive law, we get

$$g = ax + by = dkx + djy = d(kx + jy),$$

which shows that $d|g$.

- c. Show how to use the Euclidean algorithm to solve for x and y such that $37x + 99y = 1$.

$$99 - 37(2) = 25$$

$$37 - 25(1) = 12$$

$$25 - 12(2) = 1$$

$$1 = 25 - 12(2) = 25 - [37 - 25](2) = 25(3) - 37(2) = [99 - 37(2)](3) - 37(2) = 99(3) - 37(8)$$

$$\text{So } x = -8 \text{ and } y = 3$$

- d. Use part (c) to find $37^{-1} \pmod{99}$.

$$37^{-1} \pmod{99} \equiv -8 \pmod{99} \equiv 91 \pmod{99}.$$

- e. Use your answers above to solve for z such that $37z \equiv 10 \pmod{99}$.

$$\text{Multiplying by } 37^{-1} \pmod{99} \equiv -8 \pmod{99}, \text{ we get } z \equiv -80 \pmod{99} \equiv 19 \pmod{99}.$$

6. LOGIC

- a. Define what it means for two logical statements to be equivalent.
They are equivalent if they have the same truth table.
- b. If A and B are two statements, show that the statement $\neg A \wedge (A \vee B)$ is equivalent to the statement $B \wedge \neg A$.

A	B	$\neg A$	$A \vee B$	$\neg A \wedge (A \vee B)$	$B \wedge \neg A$
T	T	F	T	F	F
T	F	F	T	F	F
F	T	T	T	T	T
F	F	T	F	F	F

The columns for $\neg A \wedge (A \vee B)$ and for $B \wedge \neg A$ are the same. This shows that the two statements are equivalent.

- c. Write the converse and the contrapositive of the statement “If you ace Math 52, then you understand modular arithmetic and you understand equivalence relations.” Which of these is equivalent to the original statement?

Converse: “If you understand modular arithmetic and you understand equivalence relations, then you ace Math 52.”

Contrapositive: If you do not understand modular arithmetic or you do not understand equivalence relations, then you do not ace Math 52.

The contrapositive is equivalent to the original statement.

7. FUNCTIONS

- a. According to our formal definition, what is a function?
A function f from S to T is a relation f so that for each $s \in S$, there is one and only one $t \in T$ for which $(s, t) \in f$.
- b. Let $S = \{2, 4, 6\}$ and $T = \{7, 8, 9, 10\}$. Define a relation σ from S to T by $\sigma = \{(2, 8), (4, 7), (6, 8)\}$. Show that σ is a function from S to T .
The set S consists of three elements: 2, 4, and 6. For $s = 2$, the one and only value of $t \in T$ for which $(2, t) \in \sigma$ is $t = 8$. For $s = 4$, the one and only value of $t \in T$ for which $(4, t) \in \sigma$ is $t = 7$. For $s = 6$, the one and only value of $t \in T$ for which $(6, t) \in \sigma$ is $t = 8$. This shows that σ is a function from S to T .
- c. What is the definition of one-to-one?
A function f is one-to-one if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$.
- d. Show that σ is not one-to-one.
Since $\sigma(2) = 8 = \sigma(6)$, σ is not one-to-one.
- e. What is the definition of onto?
A function f is onto if every $t \in T$ is an output of the function for some input s , so $f(s) = t$.
- f. Show that σ is not onto.
Notice that $9 \in T$, but 9 is not an output of the function: we do not have $\sigma(s) = 9$ for any $s \in S$.
- g. What is the range of σ ? Write out this set. The range is the set of all outputs of the function: $\{7, 8\}$.
- h. Does σ have an inverse function? Does σ have an inverse relation? Why or why not?
The function σ has no inverse function because it is not one-to-one. We also know it has no inverse function because it is not onto. It has an inverse relation because every relation has an inverse. In this case $\sigma^{-1} = \{(8, 2), (7, 4), (8, 6)\}$.
- i. Suppose that f is a function from X to Y and g is a function from Y to Z . If f and g are onto, prove that $g \circ f$ is onto.
See solutions to Test II, problem 1e for the solution to this problem.

- j. If f and g have inverse functions, prove that $g \circ f$ has an inverse, namely $f^{-1} \circ g^{-1}$.
See the solution to problem 1h on the solutions to Practice Test II for the solution.

8. MODULAR ARITHMETIC

- a. Write the table for multiplication in $\mathbb{Z}/7\mathbb{Z}$.
See homework on section 3.2.
- b. Suppose that p is a prime number greater than 2. Show that 2 has an inverse modulo p .
Since p is prime, its only factors are 1 and p , by definition. Since 2 is less than p , it does not have a factor of p , so the only common factor between p and 2 is 1. This shows that $GCD(2, p) = 1$, so 2 and p are relatively prime. There is a theorem that says a has an inverse $(\text{mod } m)$ if and only if $GCD(a, m) = 1$. Using that theorem, we see that 2 has an inverse modulo p .
- c. Let $b = 2^{-1} \pmod{p}$. Define a function $f : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ by $f(x) = 2x \pmod{p}$ and define $g(y) = by \pmod{p}$. Show that g is the inverse function of f .
By the definition of b , we have $2b \equiv 1 \pmod{p}$, so

$$f(g(y)) \equiv 2g(y) \equiv 2(by) \equiv (2b)y \equiv (1)y \equiv y \pmod{p}$$

by the rules of modular arithmetic. This shows that $f(g(y)) = y$, since they are congruent modulo p and both between 0 and $p - 1$ inclusive. A similar computation shows that $g(f(x)) = x$. This shows that g is the inverse function of f .

- d. Show that f is a bijection.
We have shown that f has an inverse function. This is equivalent to the statement that f is a bijection (one-to-one and onto).
- e. Use part (d) to show that

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \equiv (2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdots (2 \cdot (p-2))(2 \cdot (p-1)) = 2^{p-1}(p-1)! \pmod{p}.$$

Since f is a bijection from $\mathbb{Z}/p\mathbb{Z}$ to itself, the numbers $f(1), f(2), \dots, f(p-1)$ are just a rearrangement of the numbers $1, 2, \dots, p-1$. (We are leaving out $f(0) = 0$.) So the product is the same either way. Using the definition of f , we get

$$1 \cdot 2 \cdots (p-1) \pmod{p} = (2 \cdot 1)(2 \cdot 2) \cdots (2 \cdot (p-1)) \pmod{p}.$$

This gives the congruence we want. The equality comes from combining all of the factors of 2 together.

- f. Show that $1 \equiv 2^{p-1} \pmod{p}$.
All of the prime factors of $(p-1)!$ are less than p , so $(p-1)!$ is relatively prime to p . Thus $(p-1)!$ has an inverse modulo p . Multiplying the congruence $(p-1)! \equiv 2^{p-1}(p-1)! \pmod{p}$ in part (e) by this inverse gives $2^{p-1} \equiv 1 \pmod{p}$.
Congratulations, you have proved Fermat's Little Theorem again. (This same argument works for any number from 1 to $p-1$ in place of 2).
- g. If $A \equiv a \pmod{mn}$, show that $A \equiv a \pmod{m}$ and $A \equiv a \pmod{n}$. Show that the converse is not always true, but it is true if $GCD(m, n) = 1$.
If $A \equiv a \pmod{mn}$, then $A = a + mnk$ for some integer k , by one of the equivalent definitions of congruence. Hence $A = a + m(nk) = a + mk_1$ and $A = a + n(mk) = a + nk_2$. The first equality shows that $A \equiv a \pmod{m}$, since $k_1 = nk$ is an integer. Similarly, the second equality shows that $A \equiv a \pmod{n}$.
If $GCD(m, n) = 1$, we prove the converse. That is, suppose $A \equiv a \pmod{m}$, and $A \equiv a$

(mod n). Then $A - a = mt$ for some integer t and $n|(A - a)$, so $n|mt$. We have seen (Theorem 3.5 in our text) as a corollary of the extended Euclidean algorithm that if $n|mt$ and $GCD(n, m) = 1$, then $n|t$. So $t = ns$ for some integer s . Substituting this in for t , we have $A - a = mns$. This can be rewritten as $A = a + mns$, which shows that $A \equiv a \pmod{mn}$.

We give a counterexample when $GCD(m, n) \neq 1$. Take $A = 4$, $a = 0$, $m = 2$ and $n = 4$. Notice that $4 \equiv 0 \pmod{2}$ and $4 \equiv 0 \pmod{4}$, but $4 \not\equiv 0 \pmod{8}$

- h. Use Fermat's Little Theorem to prove that if a is not a multiple of 13 or 5 or 7, then $a^{12} \equiv 1 \pmod{13}$ and $a^{12} \equiv 1 \pmod{7}$ and $a^{12} \equiv 1 \pmod{5}$, so $a^{12} \equiv 1 \pmod{5 \cdot 7 \cdot 13}$.

Fermat's Little theorem says that if p is a prime and a is not a multiple of p , then $a^{p-1} \equiv a \pmod{p}$. When $p = 13$, it says that $a^{12} \equiv 1 \pmod{13}$. When, $p = 7$, it says $a^6 \equiv 1 \pmod{7}$. From this we can use the rules of modular arithmetic and square both sides to get $a^{12} \equiv 1 \pmod{7}$. When $p = 5$, it says $a^4 \equiv 1 \pmod{5}$. Using the rules of modular arithmetic, we can cube both sides to get $a^{12} \equiv 1 \pmod{5}$. Now we know that $a^{12} \equiv 1 \pmod{13}$ and $a^{12} \equiv 1 \pmod{7}$ and $a^{12} \equiv 1 \pmod{5}$. Since 13 and 7 are relatively prime, we can apply part (g) to conclude that $a^{12} \equiv 1 \pmod{7 \cdot 13}$. Then since $7 \cdot 13$ and 5 are relatively prime, we can apply part (g) again to conclude that $a^{12} \equiv 1 \pmod{5 \cdot 7 \cdot 13}$

- i. Find the smallest positive integer A such that $A \equiv 7 \pmod{31}$ and $A \equiv 10 \pmod{35}$.

By the Extended Euclidean algorithm, we find that $mx + ny = 31(-9) + 35(8) = 1$. By the any-bmx form of the Chinese Remainder Theorem, we get $A \equiv any + bmx = 7(35)(8) + 10(31)(-9) \pmod{31 \times 35}$. This says $A \equiv -830 \pmod{1085}$, so the minimal positive answer is $A = -830 + 1085 = 255$. You can check that this answer is correct: $255 \pmod{31} = 7$ and $255 \pmod{35} = 10$.

9. MATHEMATICAL WRITING

Summarize how one of the following topics (your choice) unfolded in this course: Logic, Sets, Relations, Functions, or Modular Arithmetic. Include statements of important definitions and theorems in a logical order, and at least one proof. Follow the guidelines for clear mathematical writing.

Practice this on your own!