

# UMASS AMHERST MATH 300 FALL '05, F. HAJIR

## FINAL EXAM REVIEW

Concepts we have learned throughout the course will appear on the final. However, **there will be a decided imbalance toward having more questions from the last few weeks of the course, specifically from HW 5, 6, 7 (number theory, countable and uncountable sets, complex numbers)**. Correspondingly, on this sample exam, I have included mostly questions from the last few weeks of the course. HOWEVER, you should review exams 1 and 2 as well as the sample exams to recall the material we discussed earlier in the term.

As with Exams 1 and 2, the final will have three parts: 1. Definitions, 2. Short Answer, and 3. Problems.

Be sure to memorize the definitions so you can move on to the problems section as quickly as possible. You will have 2 hours for completing the final, so this exam will be a little longer than Exams 1 and 2.

## Sample Final Exam Solutions

### 1. DEFINITIONS

[These I will leave to you to pick up from the text and my notes].

### 2. SHORT ANSWERS

a. The quantity  $\min\{x \in \mathbb{P} \mid a|x \wedge b|x\}$  is called  $\text{lcm}(a, b)$ .

b. In the above sentence, this minimum is guaranteed to exist by the WELL ORDERING Principle because the set  $S = \{x \in \mathbb{P} \mid a|x \wedge b|x\}$  is not empty ( $ab \in S$ ) hence has a least element.

c. Use the Euclidean algorithm to compute  $\text{gcd}(432, 168)$  as well as  $\text{lcm}(432, 168)$ .

$$R_1 : 432 \quad 1 \quad 0$$

$$R_2 : 168 \quad 0 \quad 1$$

$$R_3 : 96 \quad 1 \quad -2 \text{ (performing } R_1 - 2R_2)$$

$$R_4 : 72 \quad -1 \quad 3 \text{ (performing } R_2 - R_3)$$

$$R_5 : 24 \quad 2 \quad -5 \text{ (performing } R_3 - R_4)$$

$$R_6 : 0 \quad -7 \quad 18 \text{ (performing } R_4 - 3R_5)$$

Thus,  $\text{gcd}(432, 168) = 24$  and  $24 = 2(432) - 5(168)$ . We have  $\text{lcm}(432, 168) = 432 \cdot 168/24 = 7 \cdot 432 = 3024$ .

d. Sketch and shade the region in the complex plane defined by

$$R = \{z \in \mathbb{C} \mid |z - 1| < |z + 1|\}.$$

This is the set of complex numbers  $z$  which are closer to 1 than they are to  $-1$ . This is simply because  $|z - 1|$  is the distance from  $z$  to 1 and  $|z + 1| = |z - (-1)|$  is the distance

from  $z$  to  $-1$ . Thus, the set  $R$  is the set of complex numbers to the right of the  $y$ -axis, i.e. those with positive real part.

e. For  $w \in \mathbb{C}$ , define a map  $\delta_w : \mathbb{C} \rightarrow \mathbb{C}$  via  $\delta_w(z) = wz$  for all  $z \in \mathbb{C}$ . If  $w = 1 + i\sqrt{3}$ , the map  $\delta_w$  can be represented by a radial dilation by a factor  $|w| = \sqrt{4} = 2$  followed by a counterclockwise rotation around the origin of measure 60 degrees or  $\pi/3$  radians.

f. Suppose  $z, w, v$  are three complex numbers such that  $|z - w| = |z - v| + |v - w|$ . Draw a picture of what this means geometrically. What can you conclude about the geometric configuration of the complex numbers  $z, w, v$ ?

The straight-line distance from  $z$  to  $v$  plus the straight-line distance from  $v$  to  $w$  is exactly the straight-line distance from  $z$  to  $w$ , hence  $z, v, w$  must all be on a straight line. If they weren't on a straight line,  $z, v, w$  would be the vertices of a triangle and then we would have to have  $|z - w| < |z - v| + |v - w|$  because the straight line from  $z$  to  $w$  is the unique shortest path connecting these points.

g. Write the complex number  $z = (7 + 4i)/(3 - 2i)$  in polar form, i.e. find real numbers  $r, \theta$  such that  $z = re^{i\theta}$ .

Rationalize

$$z = z(3 + 2i)/(3 + 2i) = (7 + 4i)(3 + 2i)/(9 + 4) = (21 + 26i - 8)/13 = (1 + 2i).$$

Thus,  $|z| = \sqrt{5}$ , and  $\tan(\theta) = 1/2$ , so with  $\theta = \tan^{-1}(0.5)$ , and  $r = \sqrt{5}$ ,  $z = re^{i\theta}$ .

h. TRUE or FALSE: If  $z_0 \in \mathbb{C}$ , then the equation  $w^5 = z_0$  has 5 distinct solutions in  $\mathbb{C}$ .

FALSE: (the key word is distinct)  $w^5 = 0$  has only the solution  $w = 0$  (repeated 5 times).

i. TRUE or FALSE: If  $X$  is a countable set, and  $\Delta$  is a partition of  $X$ , then  $\Delta$  is also a countable set.

TRUE: We have a surjective map  $X \rightarrow \Delta$ . Thus  $\Delta$  is countable if  $X$  is.

j. TRUE or FALSE: If  $x, y \in \mathbb{Z}$ , and  $3x + 17y = 2$ , then  $\gcd(x, y)$  is either 1 or 2.

TRUE. If  $d > 0$  divides  $x$  and  $y$ , then  $d$  divides  $3x + 17y$  hence  $d$  divides 2, so  $d$  is 1 or 2.

k. TRUE or FALSE: The equation  $3x + 18y = 1$  has no solution with  $x, y \in \mathbb{Q}$ .

FALSE. It has no solutions in  $\mathbb{Z}$ , but it does have solutions aplenty in  $\mathbb{Q}$ !!

l. Write down two **uncountable** sets,  $X$  and  $Y$ , which are not equivalent to each other.

$\mathbb{R}$  and  $\mathcal{P}(\mathbb{R})$  are both uncountable but cannot be equivalent by Cantor's theorem.

m. Give a bijection  $(0, 1) \rightarrow \mathbb{R}$ .

One possibility is  $f : (0, 1) \rightarrow \mathbb{R}$  given by  $f(x) = \tan(\pi x - \pi/2)$ .

n. Consider the set  $X = \{1, 2, 3, 4, 5\}$  and the map  $f : X \rightarrow \mathcal{P}(X)$  defined by  $f(1) = \{4\}$ ,  $f(2) = \{3, 4\}$ ,  $f(3) = \{2, 3, 4\}$ , and  $f(4) = \{1, 2, 3, 4\}$ . Calculate  $Y_f = \{x \in X \mid x \notin f(x)\}$ . Is  $Y_f$  in the image of  $f$ ? Are you surprised by this? Why or why not?

We have  $Y_f = \{1, 2\}$  and  $Y_f$  is not in the image of  $f$ . This is not surprising because Cantor showed that for any  $f : X \rightarrow \mathcal{P}(X)$ ,  $Y_f$  is not in the image of  $f$ .

o. Write the number 0.123 in base 5.

Let us note that  $0.125 = 125/1000 = 1/8$ , so we just have to divide 1 by 8 in base 5. Note that  $8 = (13)_5$  in base 5. Since  $(13)_5$  doesn't go into  $(1)_5$ , we spot the latter two zeros and move the decimal point to the right two spots. Now we have  $(100)_5 \div (13)_5$ . We see it goes into it 3 times, giving  $(44)_5$ . We subtract this from  $(100)_5$  and get  $(1)_5$  so we're back to where we started. Thus, now we go into an infinite repeating loop:  $(0.03030303\dots)_5$ . To double-check, we are saying that  $3/5^2 + 3/5^4 + 3/5^6 + \dots = 1/8$ . This is a geometric series  $a + ar + ar^2 + ar^3 + \dots$  where  $a = 3/25$  and  $r = 1/25$ . Since  $a + ar + ar^2 + \dots = a/(1 - r)$ , we get  $(0.\overline{03})_5 = (3/25)/(1 - 1/25) = 3/24 = 1/8$ , phew.

TRUE OR FALSE: For each statement below, Indicate whether it is True or False.

Every infinite subset of an uncountable set is uncountable.

Totally false: one could just take an infinite list of non-repeating elements in the set, which being a list, must be countable.

For *arbitrary* sets  $X, Y, Z$ , if  $|X| \leq |Y|$  and  $|Y| \leq |Z|$ , then  $|X| \leq |Z|$ .

TRUE: If  $f : X \rightarrow Y$  is injective and  $g : Y \rightarrow Z$  is injective, then  $g \circ f$  gives an injection of  $X$  into  $Z$ .

If  $X$  is an infinite set, then there is a injection  $X \rightarrow \mathbb{N}$ .

Nice try dude, but this is FALSE. It's the other way around: if  $X$  is infinite, then  $\mathbb{N}$  injects into  $X$ .

If  $|X| = \aleph_0$ , then  $|X \times X| = \aleph_0$ .

TRUE: The direct product of countably many countable sets is countable.

If  $X$  is equivalent to  $Y$ , then there is an injection  $X \hookrightarrow Y$  as well as an injection  $Y \hookrightarrow X$ .

TRUE, because there is in fact a bijection  $f : X \rightarrow Y$  whose inverse  $f^{-1}$  is then a bijection from  $Y$  to  $X$ .

If  $X$  is a countable set, then every infinite subset of  $X$  is equivalent to  $X$ .

TRUE. If  $X$  is finite, then the statement has a vacuous hypothesis hence is true trivially. Next suppose  $X$  is infinite and countable. Then  $X \sim \mathbb{N}$ . Now suppose  $Y$  is an infinite subset of  $X$ . Since the elements of  $X$  can be listed, and  $Y \subseteq X$ , the elements of  $Y$  can be listed too, hence  $Y$  is infinite countable too. Every infinite countable set is equivalent to  $\mathbb{N}$ , so  $X \sim \mathbb{N}$  and  $Y \sim \mathbb{N}$ . By the transitivity of set equivalence,  $X \sim Y$ .

### 3. PROBLEMS

A. Prove Cantor's theorem: If  $X$  is an arbitrary set, and  $f : X \rightarrow \mathcal{P}(X)$  is a map from  $X$  to the set of all subsets of  $X$ , then  $f$  is not surjective. Hint: Proof by contradiction.

Look this up in the notes.

B. Suppose  $r, s, m, n \in \mathbb{Z}$  and  $\gcd(m, n) = 1$ .

(i) Show that the set

$$\{x \in \mathbb{Z} \mid x \equiv r \pmod{m} \wedge x \equiv s \pmod{n} \wedge 0 \leq x \leq mn - 1\}$$

is a singleton. In other words, there exists a unique integer in the interval  $[0, mn - 1]$  that gives remainder  $r$  when divided by  $m$  and remainder  $s$  when divided by  $n$ .

By Bézout, we can find  $a, b$  such that  $am + bn = 1$ . Now let's try  $x' = amr + bns$ . Let's check that  $x' \equiv r \pmod{m}$ . We have  $x' - r = amr + bns - r = amr + (bn - 1)r = amr + (-am)r = m(as - ar)$  so  $x' - r$  is divisible by  $m$ , i.e.  $x' \equiv r \pmod{m}$ . Similarly,  $x' - s = (am - 1)s + bns = (-bn)s + bns = n(-bs + bs)$  so  $x' \equiv s \pmod{n}$ . So,  $x'$  satisfies two of the three needed conditions. Let's "fix" it to get the third condition: namely,  $x'$  may not be in  $[0, mn - 1]$  but its remainder when we divide by  $mn$  is in that range. To be precise, let  $x = \text{Rem}(x' \div mn)$ . On the one hand,  $0 \leq x = \text{Rem}(x' \div mn) \leq mn - 1$  and on the other hand,  $x' \equiv x \pmod{mn}$  hence  $x \equiv x' \equiv r \pmod{m}$  and  $x \equiv x' \equiv s \pmod{n}$ . This proves the existence of  $x$ . As for uniqueness, suppose  $x, y$  both satisfy the three hypotheses. Then  $x - y \equiv 0 \pmod{m}$  and  $x - y \equiv 0 \pmod{n}$ . Thus,  $x - y$  is a common multiple of  $m$  and  $n$ . Since  $\gcd(m, n) = 1$ , we have  $\text{lcm}(m, n) = mn$  so  $mn$  divides  $x - y$  (the least common multiple divides all common multiples: see the lemma called "Supremacy of the lcm and gcd" in the notes). But  $0 \leq |x - y| < mn$  since  $0 \leq x, y \leq mn - 1$ . Thus,  $|x - y| = 0$ , i.e.  $x = y$ .

(ii) How many integers in the interval  $[0, 5000]$  give remainder 73 when divided by 100 and remainder 1 when divided by 37? What is the least such integer?

Since  $\gcd(100, 37) = 1$ , by (i), in the interval  $[0, 37 \cdot 100 - 1] = [0, 3699]$  has exactly one such integer in it. Since  $10m - 27n = 1$  where  $m = 100$  and  $n = 37$ , we try  $x' = 10ms - 27nr$  where  $r = 73$  and  $s = 1$  according to the recipe in the proof of part (i). We get  $x' = 1000 - 27 \cdot 37 \cdot 73 = -71927$ . The remainder of  $x'$  when divide by 3700 is 2073; this is our  $x$ . The next such  $x$  is  $2073 + 3700 = 5773$  which is bigger than 5000, so there is exactly one  $x$  in the range  $[0, 5000]$ , namely  $x = 2073$ . We check  $2073 = 56 \cdot 37 + 1$ .

C. Let  $p$  be a prime number. Let  $X = \mathbb{Z}$  be the set of integers, and for  $x, y \in \mathbb{Z}$ , write  $x \sim y$  if and only if  $\widetilde{x} \equiv y \pmod{p}$ , i.e. if and only if  $p|(x - y)$ . Thus, the set  $\widetilde{X}$  has  $p$  elements, namely  $\widetilde{0}, \widetilde{1}, \dots, \widetilde{p-1}$ . On the set  $\widetilde{X}$ , let us define two operations,  $+$ ,  $\times$  as follows:

$$\widetilde{a} + \widetilde{b} := \widetilde{a + b}, \quad \widetilde{a}\widetilde{b} := \widetilde{ab}.$$

Show that if  $\widetilde{a} \neq \widetilde{0}$ , then there exists  $b \in \mathbb{Z}$  such that  $\widetilde{a}b = \widetilde{1}$ .

Since  $\widetilde{a} \neq \widetilde{0}$ ,  $a$  is not a multiple of  $p$ . Since  $p$  is a prime, we have  $\gcd(a, p) = 1$ , hence, by Bézout, there exist integers  $x, y$  such that  $ax + py = 1$ . Thus,  $ax \sim 1$ , i.e.  $\widetilde{ax} = \widetilde{ax} = \widetilde{1}$ .

D. Describe a bijection  $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ , thereby proving that  $\mathbb{N}$  is countable. (Drawing a picture is a good idea, but it should be accompanied by a careful description of the map you are constructing).

We use the weaving argument. For each  $(a, b) \in \mathbb{N} \times \mathbb{N}$ , let  $s(a, b) = a + b$  be their “coordinate-sum”. For each integer  $x \in \mathbb{N}$ , there exist a finite number of elements  $(a, b)$  of  $\mathbb{N} \times \mathbb{N}$  such that  $s(a, b) = x$ , namely there are  $x + 1$  such elements, we can list them as  $(0, x), (1, x - 1), (2, x - 2), \dots, (x - 1, 1), (x, 0)$ . So now we list all the elements of  $\mathbb{N} \times \mathbb{N}$  with coordinate-sum 0, then all the elements with coordinate-sum 1, then all the elements of coordinate-sum 2, etc. Since each element of  $\mathbb{N} \times \mathbb{N}$  has finite coordinate-sum, each will eventually be listed. Thus,  $\mathbb{N} \times \mathbb{N}$  is countable.

E. State the triangle inequality, then use it to prove that for  $u, v \in \mathbb{C}$ ,

$$|u| - |v| \leq |u - v|.$$

The triangle inequality states: If  $z, w \in \mathbb{C}$ , then  $|z + w| \leq |z| + |w|$ . Suppose we are given  $u, v$  in  $\mathbb{C}$ . Let  $w = v$  and put  $z = u - v$ . Then  $|z + w| = |z + v| = |u| \leq |z| + |w|$  by the triangle inequality. Subtracting  $|w|$ , which is just  $|v|$  from both sides, we get  $|u| - |v| \leq |u - v|$ .

F. Find six complex roots of the equation  $z^6 + z^3 + 1 = 0$ . Hint: let  $w = z^3$  so that  $w^2 + w + 1 = 0$ . Solve for  $w$  and put the solutions  $w_1, w_2$  in  $re^{i\theta}$  form, then solve  $z^3 = w_1$  and  $z^3 = w_2$ .

First recall that to solve  $z^3 = u$ , for any  $u$ , if we find one solution  $z_0 = u^{1/3}$ , then the other two solutions are  $z'_0 = z_0 e^{2\pi i/3}$  and  $z''_0 = z_0 e^{4\pi i/3}$ .

It's easy to solve  $w^2 + w + 1 = 0$ , say using the quadratic formula: its two solutions are  $w_1 = (-1 + i\sqrt{3})/2$  and  $w_2 = (-1 - i\sqrt{3})/2$ . Now these are just the cube roots of unity  $w_1 = e^{2\pi i/3}$  and  $e^{4\pi i/3}$ . Now  $z^3 = w_1$  is the equation  $z^3 = e^{i\theta_1}$  with  $\theta_1 = 2\pi/3$ , so the solutions are  $z = e^{i\theta/3}$ ,  $e^{i(\theta+2\pi)/3}$ , and  $e^{i(\theta+4\pi)/3}$ . Similarly for  $z^3 = e^{i\theta_2}$ , where  $\theta_2 = 2\theta_1$ . Thus, the set

of all solutions is  $e^{i\alpha}$  as  $\alpha$  runs over the set

$$\{2\pi/9, 2\pi/9 + 2\pi/3, 2\pi/9 + 4\pi/3, 4\pi/9, 4\pi/9 + 2\pi/3, 4\pi/9 + 4\pi/3\}.$$

G. (i) Suppose  $z_0, z_1 \in \mathbb{C}$  and  $z_0 \neq z_1$ . Consider a map  $z : [0, 1] \rightarrow \mathbb{C}$  defined by  $z(t) = tz_1 + (1-t)z_0$  for  $0 \leq t \leq 1$ . Note that  $z(0) = z_0$  and  $z(1) = z_1$ . Thinking of this map as a path in the complex plane, describe (geometrically) what this path is.

This path is just a straight line from  $z_0$  to  $z_1$ . One can check this rigorously by showing that the slope of the line from  $z(t)$  to  $z_0$  is a constant independent of  $t$ .

(ii) Let  $B = \{z \in \mathbb{C} \mid |z| < 1\}$  be the inside of the unit circle; it's called the unit disc. Use the triangle inequality to show that, given two distinct points  $z_0, z_1 \in B$ , every point of the line segment joining  $z_0$  to  $z_1$  is inside  $B$  also. (This is clear geometrically, I am asking for an "algebraic" proof). You have just shown that the unit disc is *convex*.

By (i), if  $z$  is a point of the line segment joining  $z_0$  and  $z_1$ , then  $z = tz_0 + (1-t)z_1$  for some  $t \in [0, 1]$ . By the triangle inequality,  $|z| \leq t|z_0| + (1-t)|z_1|$ . But  $|z_0| < 1$  and  $|z_1| < 1$ ; so  $|z| < t + (1-t) = 1$  thus  $z$  is in  $B$ .

H. Use strong induction to prove that if  $n \geq 2$  is an integer, then there exists a prime number  $p$  such that  $p|n$ . (Do not use the fact that integers factor into products of prime powers).

Let  $P(n)$  be the statement that there exists a prime  $p$  such that  $n$  is divisible by  $p$ . For  $n = 2$ ,  $P(2)$  holds since 2 is a prime and  $2|2$ . Suppose  $k \geq 2$  is an integer and that  $P(t)$  holds for all integers  $t$  in the range  $2 \leq t \leq k$ . We claim that then  $P(k+1)$  holds. For if  $k+1$  is itself prime, then clearly  $P(k+1)$  holds, whereas if  $k+1$  is not prime, then by definition, there exist integers  $a, b$  in the range  $2 \leq a, b < k+1$  such that  $k+1 = ab$ . By the strong induction hypothesis,  $P(a)$  and  $P(b)$  both hold, thus  $a$ , say, is divisible by some prime  $p$ , and then  $k+1$  is divisible by  $p$  also. This shows that  $P(2), P(3), \dots, P(k)$  imply  $P(k+1)$ . By complete (or strong) induction, we are done.

#### 4. EXTRA CREDIT

A. Suppose  $n \geq 2$  is an integer. Write down an explicit formula for a non-identity 2 by 2 matrix  $M$  with real entries such that  $M^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .