Review for final in Math 287, Spring 2022

M. Randall Holmes

April 27, 2022

Im thinking that the description "four questions over test 1, four questions over test 2, two questions over new material" which I have given in Math 305 might have some value, but there is some pressure for three questions on new material.

You will be allowed your non-graphing calculator and one sheet of notebook paper with whatever you like written on it.

Here is the full text of the review sheet for Test I. I will highlight what I think is relevant for the final.

1. Do a couple of parts of Prop 1.11, doing every step using a single application of a single axiom.

2. Prove prop 1.13.

3. **Prove prop 1.9. Use prop 1.9 and axioms to prove that for any integer x, $x \cdot 0 = 0$. I will ask this, have it ready.**

4. **Prove that for any integers d, a, b, if $d|a$ and $d|b$ then $d|a + b$ and $d|ab$.** FINAL: Not necessarily exactly this, but something similar is likely.

5. **Using Axiom 2.1 (properties of the set of positive integers) and the definition of $<$ in terms of $\mathbb{N}$. prove props 2.2. 2,4, 2.8, all parts of 2.7. all parts of 2.12. You can use the axioms from chapter 1 implicitly, just say algebra. But you may not use familiar properties of order unless you have proved them from the given axiom and definition.** FINAL: something like this, but very likely for the reals rather than the integers. Axioms needed will be listed in an attachment.

Prove Prop 2.10 using the same resources. Prove prop 2.14.

6. Things like any part of prop 2.18 are targets.

7. I may ask something like Project 3.1, 3.2 testing reading of quantifier notation.

   Something like project 3.7 (negations of logically connected and quantified statements) can be expected. FINAL: I am thinking of asking you to say what it means for a limit statement to be false. That will apply this.

8. **I might ask a computational question about recursively defined sequences: just ask you to compute the first few terms of a sequence. But it might be paired with instructions to prove something about that sequence by induction.** FINAL: this might be more complicated induction than on Test I.

   For example, define $a_1 = 1, a_{k+1} = 2a_k + 1$. Compute the first six terms of this sequence. Then prove that $a_n = 2^n - 1$ for each natural number n, by induction.

9. Be familiar with the recursive definitions of exponentiation and factorial. Be ready to prove something like Prop 4.6 iii or another familiar property of exponentiation from algebra of addition and multiplication and the recursive definition. $(ab)^k = a^k \cdot b^k$ is another good law to prove.

   Be able to do things like prop. 4.7.

10. **Be able to do induction proofs involving summations like 4.11, 4.13.**

11. **Be ready to write the proof of 4.16ii. I will ask this.** FINAL: if I ask this, it will be the hard question in a pair. But if you can be ready for it, be ready.

12. **About the binomial theorem, some relaxed things, compute some binomial coeffients (showing hand calculations) and apply the theorem to some power of a sum.** Corollary 4.22.

    I will ask you to write down the Binomial Theorem, exactly as it appears in the book. Obviously this wont count on your take home paper.

Here is the text of the review sheet for the second test with things relevant for the final highlighted.

strong induction and Fibonacci-like recursion: Be ready for something like the induction proof about a recursive sequence which is given on p. 16 in the notes. It might involve the actual Fibonacci sequence or, as in this case, a different recursively defined sequence.

basic set axioms and definitions: I'm not going to examine you on axioms of set theory.

The second theorem on p. 20 (transitivity of the subset relation), you should be able to write.

The proof strategy for showing that two sets are equal is important to remember. I might give you a direct example (something like project 5.3), or it might show up in connection with another problem (p. 23 of the notes for the proof strategy)

In Homework 6, you will definitely see a test question like problem 3, 4 (Venn diagrams). You should be ready to give a counterexample (small finite sets) if I propose that you prove something using Venn diagrams that is not true.

I am not going to ask for a proof about Cartesian products (like problems 6,7); the test is going to be long enough without.

functions and relations: I may draw arrow diagrams and ask you whether they are pictures of functions, and if so whether they are pictures of one-to-one functions or functions onto a given set.

I may ask questions like question 1-3 in Homework 7. If I ask you how many functions there are from a set A with 10 elements to a set of 3 elements, you can't answer it by listing but you should be able to tell how many. How many functions are there from B to A in this case? FINAL: I skipped this on Test 2, I may address it on this exam.

Be ready to prove that $\equiv_n$ is an equivalence relation (in general, or for a specific n). Notice that the proof for $\equiv_3$ appears on pp. 32-3 of the notes without using the notation for congruence.

I might ask you whether other familiar relations are equivalence relations (you should be able to show which properties fail if they are not, by giving counterexamples).

Be ready to prove that if two equivalence classes meet, they are the same class (p. 34). Basic definitions will be provided if I ask this.

Be ready to describe the equivalence classes under a relation $\equiv_n$ or the equivalence classes under a relation given as a small finite set of ordered pairs.

division algorithm and Euclidean algorithm: Be ready to compute $a\mathtt{div}b$ and $a\mathtt{mod}b$ for values I present to you. Be sure that you know how to do this when a is negative.

Be ready to prove that the gcd of a and b is the same as the gcd of b and $a\mathtt{mod}b$. This is on p. 38 of the notes. Notice that it is a proof that two sets are equal, using the proof strategy mentioned above.

Be ready to carry out the extended Euclidean algorithm (find $\mathtt{gcd}(a, b)$ and integers x, y such that $ax + by = \mathtt{gcd}(a, b)$) in the table format i have used, using your non-graphing calculator. I strongly suggest practice. FINAL: you will need this skill to do calculations in other problems.

Modular arithmetic: As noted already, be ready to prove the theorem at the bottom of page 39, that congruence mod n is an equivalence relation.

The list of equivalence classes at the top of p. 41 is a sort of thing you should be able to produce.

Be ready to prove that if $a \equiv_n a'$ and $b \equiv_n b'$ than $ab \equiv_n a'b'$.

Be ready to compute modular addition and multiplication tables, and a table of multiplicative inverses.

Nothing like questions 6,7 in homework 8 will appear on the test. We have enough to do with the direct stuff.

You should be ready to prove Euclid's Lemma or the theorem which follows it (p. 45). FINAL: since this was abandoned in test 2, it will certainly be on this test.

You should be able to compute a multiplicative inverse in any modulus using the Euclidean algorithm, or tell me why it doesn't exist.

You should be able to solve an equation like example 2 on p. 47 of the class notes.

You should be able to do a problem like example 2 on p. 49 of the class notes.

You should be ready to do a problem like either part of problem 5, homework 9.

FINAL: These three items above fall under basic computation skills.

You should be ready to do a problem on RSA encryption and decryption. I reserve the right to ask you to carry out the entire process (encode a message, find decryption exponent, decode the message). I'll try to have nice numbers, and I may ask questions about RSA which ask you to do only part of the process or supply you with useful information to help you do it more efficiently. FINAL: this will incorporate other computational procedures from modular arithmetic.

I strongly suggest practice on RSA. I point out that you can create examples yourself, and you can tell if you are doing it right, if the decryption recovers your original message. It would be natural to work in pairs on such practice; each student make a key, tell the other student their public key, and then each student send the other a coded message, which the receiver can then decode...

Here is the text of Test I, highlighting problems you need to be ready to on the final.

1. (paired with 1) The FOIL identity you learned in school is

$$(a + b) \cdot (c + d) = (a \cdot c + a \cdot d) + (b \cdot c + a \cdot d)$$

(First, Outer, Inner, Last). We supply the parentheses for precision.

Use the axioms (parts of Axiom 1.1, listed in the attachments to the paper, which you may tear off for reference) to give a detailed step by step proof of FOIL.

Each step should be justified by a single axiom.

You may use references to parts of the axiom using the exact phrases I give, and be aware that the phrase distributive law refers to exactly the form in the axioms: you need to change things to apply it on the other side.

$(a+b)\cdot(c+d) = (c+d)\cdot(a+b)$ comm *

$= (c+d)a + (c+d)b$ dist (distributivity has to be $x(y+z) = xy + xz$)

$= a(c+d) + b(c+d)$ comm * (in two places)

$= (ac+ad) + (bc+bd)$ dist (in two places)

If one applies distributivity to the original form, before commutativity, one gets a form in which the terms have to be reordered using commutativity and associativity of addition.

2. (paired with 2) **Prove $a \cdot 0 = 0$ using Proposition 1.9 and the axioms from chapter 1 in the reference sheet.**

   Each step should use one axiom or the proposition.

   The application of 1.9 will take something of the form $X + a0 = X + 0$ to the desired $a0 = 0$.

   The right X is $a0$. Here is the actual proof:

   (1) $a0 + a0 = a(0+0)$ **dist**

   $= a0$

   (2) $a0 + 0 = a0$ **identity property of addition**

   (3) $a0 + a0 = a0 + 0$ **(1), (2) things equal to the same thing are equal to each other**

   $a0 = 0$ **prop 1.9 applied to (3)**

3. (paired with 4) **Prove using the definition of divisibility (on the reference sheet) and algebra (you may be more informal about the algebra) that if $d|a$ and $d|b$, it follows that $d|(a+b)$.**

   Your proof will start: Let a, b, d be integers and assume that $d|a$ and $d|b$...because $d|a$, there is an integer x such that $a = d \cdot x$...carry on from there.

   Let a, b, d be integers and assume that $d|a$ and $d|b$.

Because $d|a$ there is an integer x such that $a = dx$. (def of divisibility)

Because $d|b$ there is an integer y such that $b = dy$. (def of divisibility)

To show $d|(a+b)$ we need to find an integer z such that $a+b = dz$.

Now $a + b = dx + dy = d(x + y)$: setting $z = x + y$ we have found an integer z such that $dz = a + b$, so $d|(a + b)$.

4. (paired with 3) **Prove, using the axioms for N (the set of positive integers: axiom 2.1 on the reference sheet) and the definition of $<$ given on the reference sheet and algebra of equations with addition, subtraction and multiplication (about which you may be informal but be quite formal about applying the axioms for the positive integers (referencing the correct part of axiom 2.1) and the definition of $<$) that if $x < y$ and $0 < z$, $x \cdot z < y \cdot z$.**

   Your proof will begin "Let x, y, z be integers. Suppose that $x < y$ and $0 < z$. It follows that $y - x \in$ N, by the definition of $<$ and...(carry on from there).

   Let x, y, z be integers. Suppose that $x < y$ and $0 < z$.

   It follows that $y - x \in$ N and $z - 0 \in$ N (and so since $z = z - 0$, $z \in$ N).

   It then follows by Ax 2.1 b that $(y - x)z \in$ N.

   By algebra, $yz - xz \in$ N, since $yz - xz = (y - x)z$.

   By def $<$, $xz < yz$ follows.

5. (paired with 6)

   Prove by induction that the sum of the first n integers is $\frac{n(n+1)}{2}$: in symbols $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

   Basis: $\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$. check

   Induction Step: Let k be chosen arbitrarily.

   Assume (ind hyp) that $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

   Goal: show that $\sum_{i=1}^{k+1} i = \frac{(k+1)((k+1)+1)}{2} = \frac{(k+1)(k+2)}{2}$

Proof of induction step: $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$ **recursive definition of summation**

$= \frac{k(k+1)}{2} + (k+1)$ **ind hyp**

$= \frac{k(k+1)+2(k+1)}{2}$ **common denominator**

$= \frac{(k+2)(k+1)}{2}$ **dist**

$= \frac{(k+1)(k+2)}{2}$ **comm ***

6. (paired with 5)

   A sequence a_1 is defined recursively: $a_1 = 1$, $a_{k+1} = 2a_k + 1$.

   Compute the first six terms of this sequence. $1, 3, 7, 15, 31, 63$

   Prove by induction that for each natural number n, $a_n = 2^n - 1$.

   Basis: $a_1 = 1 = 2^1 - 1$ check

   Induction step: Fix a natural number k, chosen arbitrarily.

   Assume (ind hyp) $a_k = 2^k - 1$

   Goal: $a_{k+1} = 2^{k+1} - 1$

   Proof of goal: $a_{k+1} = 2a_k + 1$ def of sequence a

   $= 2(2^k - 1) + 1$ ind hyp

   $= 2^{k+1} - 2 + 1 = 2^{k+1} - 1$, which is what we want.

7. (unpaired)

   (a) Write the negation of the sentence "I like coffee and I don't like tea" in natural English (the negation moved all the way in and applied to the verb). answer: "I don't like coffee **or** I like tea"

   (b) Write the negation of the sentence in logical notation

   $$(\exists x \in \mathbf{N} : (\forall y \in \mathbf{N} : x \geq y)),$$

   in a form which doesn't involve negation at all (move the negation all the way to the right and replace the order relation with its negation).

   answer:

   $$(\forall x \in \mathbf{N} : (\exists y \in \mathbf{N} : x < y)),$$

which is all you needed to write, but here is step by step justification:

$$\neg(\exists x \in \mathbf{N} : (\forall y \in \mathbf{N} : x \geq y))$$

is equivalent to

$$(\forall x \in \mathbf{N} : \neg(\forall y \in \mathbf{N} : x \geq y))$$

which is equivalent to

$$(\forall x \in \mathbf{N} : (\exists y \in \mathbf{N} : \neg x \geq y))$$

which is equivalent to

$$(\forall x \in \mathbf{N} : (\exists y \in \mathbf{N} : x < y))$$

(c) Say in English what the sentences

$$(\exists x \in \mathbf{N} : (\forall y \in \mathbf{N} : x > y))$$

and

$$(\forall y \in \mathbf{N} : (\exists x \in \mathbf{N} : x > y))$$

mean. Which one is true?

The first sentence says that there is a fixed natural number x which is greater than every natural number (this would include itself!). This is false.

The second sentence says that for any natural number, there is a greater natural number. This is true.

FINAL: this is relevant as applied to the definition of limit.

8. (unpaired)

State the Binomial Theorem using notation for binomial coefficients and summation notation.

State it for the exponent 4 and write the sum out in full, eliminating the summation notation and evaluating all the binomial coefficients (in other words, expand out $(x + y)^4$ using the theorem).

The theorem: for any natural number n, $(x+y)^n = \sum_{i=0}^{k} \left(\begin{array}{c} n \\ i \end{array} \right) x^{n-i}y^i$

For $n = 4$, $(x+y)^4 = \sum_{i=0}^{4} \left(\begin{array}{c} n \\ i \end{array} \right) x^{n-i}y^i$

$= \left(\begin{array}{c} 4 \\ 0 \end{array} \right) x^4 + \left(\begin{array}{c} 4 \\ 1 \end{array} \right) x^3y + \left(\begin{array}{c} 4 \\ 2 \end{array} \right) x^2y^2 + \left(\begin{array}{c} 4 \\ 3 \end{array} \right) xy^3 + \left(\begin{array}{c} 4 \\ 4 \end{array} \right) y^4$

$= x^4 + 4xy^3 + 6x^2y^2 + 4xy^3 + y^4$

I didnt require the step by step development but I was pleased to see it on many papers.

1 Reference sheet

Axiom 1.1. If m, n, and p are integers, then

(a) m + n = n + m . (commutativity of addition)

(b) (m + n) + p = m + (n + p) . (associativity of addition)

(c) m · (n + p) = m · n + m · p . (distributivity)

(d) m · n = n · m . (commutativity of multiplication)

(e) (m · n) · p = m · (n · p) . (associativity of multiplication)

Axiom 1.2. There exists an integer 0 such that whenever m ∈ Z, m + 0 = m. (identity element for addition)

Axiom 1.3. There exists an integer 1 such that 1 ≠ 0 and whenever m ∈ Z, m · 1 = m . (identity element for multiplication)

Axiom 1.4. For each m ∈ Z, there exists an integer, denoted by −m , such that m + (−m) = 0. (additive inverse)

Axiom 1.5. Let m , n, and p be integers. If m · n = m · p and m ≠ 0, then n = p. (cancellation).

Proposition 1.9. Let m, n, and p be integers. If m + n = m + p, then n = p

Axiom 2.1. There exists a subset N ⊆ Z with the following properties:

(a) If m, n ∈ N then m + n ∈ N.

(b) If m, n ∈ N then mn ∈ N.

(c) 0 ∉ N.

(d) For every m ∈ Z, we have m ∈ N or m = 0 or −m ∈ N.

Definition: The statements m < n (m is less than n) and n > m (n is greater than m) both mean that n − m ∈ N .

Definition: When m and n are integers, we say m is divisible by n (or alternatively, n divides m) Do not confuse this with the notations n m and n/m for fractions. if there exists j ∈ Z such that m = jn. We use the notation n | m.

Here is the text of Test 2. Stuff that is relevant will be highlighted.

1. **Define** $a_1 = 6; a_2 = 20; a_{k+2} = 6a_{k+1} - 8a_k$**.**

   Compute the terms of this sequence up to a_6**.**

   Prove by strong induction that $a_n = 2^n + 4^n$ **for each natural number** n**.** FINAL: this is relevant.

2. **Give a Venn diagram demonstration of the identity** $A - (B \cap C) = A - B \cup A - C$**.**

   You should shade sets of interest informatively in each of the two pictures, provide a key to the shadings, and clearly outline the set which is the result of the computation. FINAL: this represents fairly easy points....

3. Do one of the two proofs. If you do both, the best one will count; if you do well on both extra credit is possible.

   (a) Prove that the relation $x \equiv_n y$ is an equivalence relation.
   Recall that for any $n > 1$, $x \equiv_n y$ is defined as $n|(x - y)$.

(b) **Prove that if $a \equiv_n a'$ and $b \equiv_n b'$, then $ab \equiv_n a'b'$.** FINAL: I might ask about this, or the corresponding theorem about addition. You did fine on part a, and I don't think I am likely ask it again.

4. **Construct addition and multiplication tables for mod 7 arithmetic, and make a table of multiplicative inverses.** FINAL: easy points which I might or might not do.

5. **Prove Euclid's Lemma: if p is prime and $p|ab$ then either $p|a$ or $p|b$.**

   The proof depends on the extended Euclidean algorithm theorem, which I remind you says that for any a, b not both equal to zero there are integers x, y such that $ax + by = \texttt{gcd}(a, b)$. FINAL: this WILL be asked, or else the theorem which follows it immediately in the class notes.

6. **Each of the parts in this problem provides information for the next one.**

   (a) **Find integers** x, y **such that** $137x + 15y = 1$ **using the extended Euclidean algorithm (my table format).**

   Tell me clearly what x **and** y **are and show a check that this is the case.**

   (b) **Compute** $15^{-1}\texttt{mod}137$**.**

   (c) **Solve the equation** $15x \equiv_{137} 16$ **for** x**.**

   FINAL: Something like this is likely.

7. Compute $23^{72} \texttt{mod} 100$ using the method of repeated squaring. Show all work. FINAL: this is covered by the RSA question.

8. Simplification of modular exponentiation.

   (a) **Use Fermat's Little Theorem to simplify the calculation of** $2^{927} \mathtt{mod} 23$

   (b) Use Euler's Theorem to simplify the computation of $5^{1282} \mathtt{mod} 55$ **(notice that 55 is of the form** pq **with** p **and** q **prime).** FINAL: this might be asked independently.

9. **My public key has $N = 55, r = 3$.**

   Encrypt the message 42 to me.

   My secret, which you can't possibly guess, is that $N = (5)(11)$.

   Determine my decryption exponent s.

   Carry out the calculation I will do to decrypt your message.

   (The numbers here are wonderfully small; of course the cryptographic security is zip!) FINAL: I am likely to ask an RSA question like this. If I don't you will have questions covering both calculations with modular inverses and exponentiation by repeated squaring.

NEW MATERIAL:

1. **There will be a limit question about a linear function, like** $\texttt{lim}_{x \to 4} 3x - 2 = 9$

2. **There will be a limit question like** $\texttt{lim}_{x \to 3} x^2 = 9$ **or** $\texttt{lim}_{x \to 3} \frac{1}{x} = \frac{1}{3}$

3. **There will be a limit theorem question (the sum or constant multiple rule): this will be the hard part of a paired question.**

4. **I might ask for the proof that the square root of two is irrational.**

5. **There might be a question about least upper bounds and greatest lower bounds of specific sets, and possibly a hard paired part with a simple piece of reasoning about least upper bounds.**

6. **Logical methods for negation of quantified sentences might be applied in the context of asking you to state what it means for a given limit statement be false.**

AND this adds up to too many questions on the new material, so I will not ask all of this...some selection will appear, or you will be allowed to choose.