Solutions

Test I Math 287 Fall 2024

Dr Holmes

October 3, 2024

There are eight questions on this exam. Questions 1 and 2 form a pair, questions 3 and 4 form a pair and questions 5 and 6 form a pair. Your grade on a pair of questions will be seventy percent the grade on the one you do better on and thirty percent the grade on the one you do worse on. Questions 7 and 8 are free standing.

You are allowed your test paper and your writing instrument. There is no use for a calculator on this exam.

Reference sheets with axioms, propositions and definitions you need make up the last pages of the exam. You may tear them off for reference.

There is a lot more about Homework 2 logical rules than you should need: the point of that reference material is exactly to be able to look up the names of the rules.

1. (paired with 2: prop 1.11(i)) The FOIL identity you learned in school is

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

typo!

(First, Outer, Inner, Last). We supply the parentheses for precision. Show all parentheses in your calculations.

Use the axioms **only** (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, possibly applied in more than one place.

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.

$(a+b)\cdot(c+d) =$ 1.11 d comm *

$(c+d)\cdot(a+b) =$ 1.11 c dist

$(c+d)\cdot a + (c+d)\cdot b =$ 1.11 d (on a) comm *

$a\cdot(c+d) + b\cdot(c+d) =$ 1.11 c

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

□

2. (paired with 1: prop 1.14) Prove $a \cdot 0 = 0$ using **only** Proposition 1.9 and the axioms from chapter 1 in the reference sheet. Reference use of the axioms.

   Each step should use one axiom or the proposition.

$a \cdot 0 = a \cdot (0 + 0)$ id + ax 1.2

$a \cdot 0 = a \cdot 0 + 0$ id + ax 1.2

$a \cdot (0+0) = a \cdot 0 + a \cdot 0$ dist ax 1.1c

$a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$ chain of eqns

$a \cdot 0 = 0$ prop 1.9

3. (paired with 4: a Holmes-written question on homework 3) Prove using the definition of divisibility (on the reference sheet) and algebra (you may be more informal about the algebra, but pay attention to parentheses) that if $x|y$ and $y|z$, it follows that $x|z$ (divisibility is transitive).

Suppose ① $x|y$
② $y|z$

Then there is $k \in \mathbb{Z}$ such that $xk = y$ (since ①)
and there is $l \in \mathbb{Z}$ such that $yl = z$ (since ②)

So, we want to find $n \in \mathbb{Z}$ s.t. $xn = z$

$z = yl = (xk)l = x(kl)$. $kl \in \mathbb{Z}$, ~~for~~ & since
Let n be kl and we have $xn = z$ so $x|z$.

4. (paired with 3: prop 2.7(ii)) Prove, using the axioms for $\mathbf{N}$ (the set of positive integers: axiom 2.1 on the reference sheet), any additional propositions in chapter 2 that are given, and the definition of $<$ given on the reference sheet, and algebra of equations with addition, subtraction and multiplication (you may be informal about the algebra of equations (Homework 1 stuff) but be entirely formal and supply references to use of any of the other stuff) that if $x < y$ and $z < w$, $x + z < y + w$.

Assm ① $x<y$ and ② $z<w$.

so ③ $y-x \in \mathbb{N}$ def $<$

④ $w-z \in \mathbb{N}$ def $<$

so ⑤ $(y-x)+(w-z) \in \mathbb{N}$ ax 2.1i

⑥ ~~$y-x+w$~~

$(y-x)+(w-z) = (y+w)-(x+z)$ algebra

so $(y+w)-(x+z) \in \mathbb{N}$ equality

so $x+z < y+w$ (def $<$)

5. (paired with 6: prop 4.11(ii))

Prove by induction that the sum of the first n squares is $\frac{n(n+1)(2n+1)}{6}$: in symbols $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

Basis: $\sum_{i=1}^{1} i^2 = 1^2 = 1 = \frac{1(1+1)(2\cdot 1+1)}{6}$

Induction step: let $k \in \mathbb{N}$ be chosen arbitrarily

assume $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$

Then $\sum_{i=1}^{k+1} i^2 = \left(\sum_{i=1}^{k} i^2\right) + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$

$\overset{\text{def}}{=} \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \frac{(k+1)\left(k(2k+1) + 6(k+1)\right)}{6}$

$= \frac{(k+1)(2k^2 + k + 6k + 6)}{6}$

$= \frac{(k+1)(2k^2 + 7k + 6)}{6}$

$= \frac{(k+1)(2k+3)(k+2)}{6} = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$

done.

6. (paired with 5: prop 4.15(i))

Prove by induction that $m \cdot \sum_{i=1}^{n} x_i = \sum_{i=1}^{n}(m \cdot x_i)$, for any $n \in \mathbb{N}$, $m \in \mathbb{Z}$, and $\{x_i\}$ a sequence of integers.

Basis: $m \cdot \sum_{i=1}^{1} x_i = mx_1 = m \sum_{i=1}^{1} x_i$

Ind Step Assume

$$m \cdot \sum_{i=1}^{k} x_i = \sum_{i=1}^{k} m \cdot x_i$$

Conj: $$m \cdot \sum_{i=1}^{k+1} x_i = \sum_{i=1}^{k+1} mx_i$$

$$m \cdot \sum_{i=1}^{k+1} x_i = m \cdot \left(\sum_{i=1}^{k} x_i + x_{k+1} \right) \overset{\text{dist}}{=} m \cdot \sum_{i=1}^{k} x_i + m \cdot x_{k+1}$$

$$\overset{\text{ind hyp}}{=} \sum_{i=1}^{k} mx_i + mx_{k+1} \overset{\text{def } \Sigma}{=} \sum_{i=1}^{k+1} m \cdot x_i$$

7. (unpaired: Homework 2 problem 3)

   Prove $(A \to (B \wedge C)) \to (A \to C)$ using the formal rules used on that homework (a summary of these is provided in the reference materials).

8. (unpaired: prop 2.18(iii)) Prove by mathematical induction that for every $n \in \mathbb{N}$, $n^3 + 5n$ is divisible by 6.

Solutions

Math 287 Fall 2024, Test II

Randall Holmes

November 18, 2024

This exam will be given Tuesday Nov 19, starting at 9 am, with a ten minute warning at 1015 am. Nothing is allowed but your writing instrument and a calculator. You are required to show work using my table method or some equivalent method of hand calculation to find gcd's: using a mod function on your calculator to compute them directly does not carry credit.

1. (paired with 2) Prove using the recursive definition of summation and mathematical induction that $\sum_{i=1}^{n}(x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$.

   For reference, we state the recursive definition of indexed summation in its most general form, which you may use as a model for similar definitions needed elsewhere in the test: $\sum_{i=a}^{a} x_i = x_a$; for any $b \geq a$, $\sum_{x=a}^{b+1} x_i = (\sum_{x=a}^{b} x_i) + x_{b+1}$.

Basis ($n=1$): $\sum_{i=1}^{1}(x_i+y_i) = x_1 + y_1 = \sum_{i=1}^{1} x_i + \sum_{i=1}^{1} y_i$ ✓

Induction step: let $k \geq 1$ be chosen arbitrarily

Suppose (ind hyp) $\sum_{i=1}^{k}(x_i+y_i) = \sum_{i=1}^{k} x_i + \sum_{i=1}^{k} y_i$

$$\sum_{i=1}^{k+1}(x_i+y_i) = \sum_{i=1}^{k}(x_i+y_i) + x_{k+1} + y_{k+1}$$

$$\overset{\text{ind hyp!}}{=} \sum_{i=1}^{k} x_i + \sum_{i=1}^{k} y_i + x_{k+1} + y_{k+1}$$

$$= \left(\sum_{i=1}^{k} x_i + x_{k+1}\right) + \left(\sum_{i=1}^{k} y_i + y_{k+1}\right)$$

$$= \sum_{i=1}^{k+1} x_i + \sum_{i=1}^{k+1} y_i$$ ✓

2. (paired with 1) Prove using the recursive definition of finite product and mathematical induction that $x_a \cdot \prod_{i=a+1}^{b} x_i = \prod_{i=a}^{b} x_i$, where $\{x_i\}$ is any sequence of numbers of some familiar kind, and $a < b$ are integers.

Basis ($b = a+1$):

$$x_a \cdot \prod_{i=a+1}^{a+1} x_i = x_a \cdot x_{a+1} = \left(\prod_{i=a}^{a} x_i\right) x_{a+1} = \prod_{i=a}^{a+1} x_i$$

Ind step:

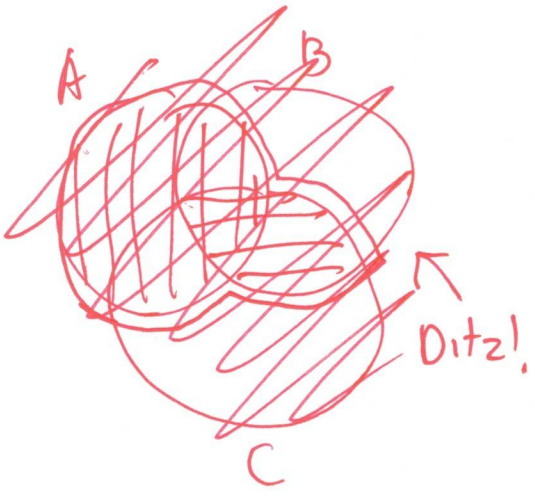
Let $k > a$ be chosen arbitrarily.

Assume $x_a \cdot \prod_{i=a+1}^{k} x_i = \prod_{i=a}^{k} x_i$

$$x_a \cdot \prod_{i=a+1}^{k+1} x_i = x_a \left(\prod_{i=a+1}^{k} x_i\right) \cdot x_{k+1} \overset{\text{ind hyp}}{=} \prod_{i=a}^{k} x_i \cdot x_{k+1}$$

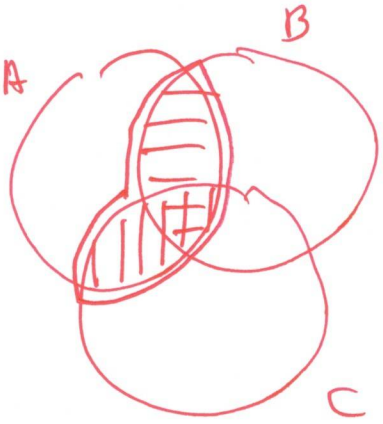
$$= \prod_{i=a}^{k+1} x_i \text{ as required} \checkmark$$

3. (paired with 4) Give a Venn diagram demonstration of the identity $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. You need to draw a diagram for each side of the equation, with appropriate shadings of sets used in the calculation, and clearly outline the result set in each diagram so a reader can see that they are the same.



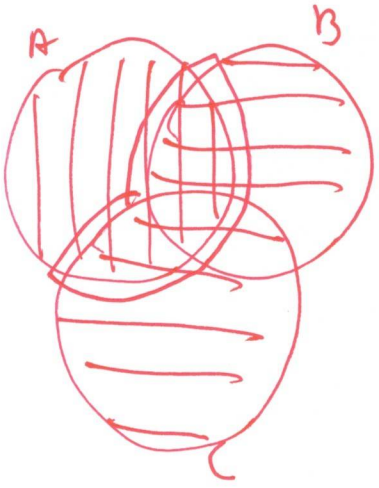
$A \cap (B \cup C)$

$\equiv A \equiv B \cup C$



$(A \cap B) \cup (A \cap C)$

$\equiv A \cap B \equiv A \cap C$



4. (paired with 3) State the recursive definition of $\bigcup_{i=a}^{b} A_i$.

   Prove by mathematical induction, using the recursive definition of indexed union notation, that $A \cap \bigcup_{i=1}^{n} B_i = \bigcup_{i=1}^{n}(A \cap B_i)$ [you can use the result of the first part].

$$\bigcup_{i=a}^{a} A_i = A_a$$

$$\bigcup_{i=a}^{b+1} A_i = \left(\bigcup_{i=a}^{b} A_i\right) \cup A_{b+1}$$

for $b \geq a$

Basis: $A \cap \bigcup_{i=1}^{1} B_i = A \cap B_1 = \bigcup_{i=1}^{1}(A \cap B_i)$

Induction: Suppose $k \in \mathbb{N}$ is chosen arbitrarily and suppose $A \cap \left(\bigcup_{i=1}^{k} B_i\right) = \bigcup_{i=1}^{k}(A \cap B_i)$

Then

$$\left(A \cap \bigcup_{i=1}^{k+1} B_i\right) = A \cap \left(\bigcup_{i=1}^{k} B_i \cup B_{k+1}\right)$$

$$= \left(A \cap \bigcup_{i=1}^{k} B_i\right) \cup \left(A \cap B_{k+1}\right) \quad \text{(first part)}$$

$$= \bigcup_{i=1}^{k}(A \cap B_i) \cup A \cap B_{k+1} \quad \text{(inductive hypothesis)}$$

$$= \bigcup_{i=1}^{k+1}\left(A \cap B_i\right) \quad \checkmark$$

5. (paired with 6) Using the extended Euclidean algorithm theorem, prove Euclid's Lemma: if p is a prime and $p|ab$, then either $p|a$ or $p|b$.

Suppose p is a prime and $p|ab$. ($\Rightarrow \exists h, ab = ph$)
either $p|a$ or $p \nmid a$

If $p|a$, then $p|a \vee p|b$.

If $p \nmid a$ then $\gcd(p,a) = 1$

so $\exists x, y$ s.t. $px + ay = 1$

so $b = b \cdot 1 = bpx + bay$

$= bpx + pky$

$= (bx + hy)p$

which is divisible by p.

6. (paired with 5) Make a multiplication table for mod 7 arithmetic, and a table of multiplicative inverses.

   Prove that for any modulus m, if $a \equiv_m c$ and $b \equiv_m d$, then $ab \equiv_m cd$.

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

n	n^{-1}
0	—
1	1
2	4
3	5
4	2
5	3
6	6

Suppose $a \equiv_m c$ and $b \equiv_m d$

$c - a = km$ so $c = a + km$ $\quad d - b = \ell m$ so $d = b + \ell m$

Then $\exists k, \ell$ $c = a + km$ $\quad d = b + \ell m$

so $cd = (a + km)(b + \ell m) =$

$ab + a\ell m + bkm + k\ell m^2$

$= ab + (a\ell + bk + k\ell m)m$

so $cd - ab = a\ell + b\ell + k\ell m^2 = (a\ell + bk + k\ell m)m$

which is divisible by m

7. Multiplicative inverses in modular arithmetic

(a) Find integers x and y such that $512x + 127y = \gcd(512, 127)$. Show all calculations.

(b) Find the multiplicative inverse of 127 in mod 512 arithmetic. Your answer should be a remainder mod 211.

(c) Solve the equation $127x \equiv_{512} 200$. Your answer should be a remainder mod ~~211~~ 512.

a.

	x	y	q
512	1	0	
129	0	1	
4	1	-4	4
3	-31	125	31
1	32	-129	

$\gcd(512, 129) = (32)(512) + (-129)(127)$

b. $127^{-1} \bmod 512$

$= 512 - 129 = \boxed{383}$

$127x \equiv_{512} 200$

$x \equiv_{512} (200)(383) = 76600$

$\equiv_{512} 76600 - (149)(512)$

$= \boxed{312}$

8. Do one of the two problems. Substantial extra credit may be given for doing both well.

   (a) Chinese remainder theorem

   Solve the system of equations

   $x \equiv_{31} 9$

   $x \equiv_{37} 12$

   State the smallest positive solution. State another solution. State the general form of the solution (describing all integers which are solutions).

$x = 12 + 37k$ for some k

$12 + 37k \equiv_{31} 9$

$37k \equiv_{31} 9 - 12 + 31 = 28$

find 37^{-1} mod 31

same as finding 6^{-1} mod 31

	x	y	q
31	1	0	
6	0	1	
1	1	(-5)	5

$-5 \equiv_{31} 26 = 6^{-1} \bmod 31$

$6k \equiv_{31} 28$

$k \equiv_{31} (28)(26) = 728 \equiv_{31} 728 + (23)(31) = 15$

$k = 15$

$x = 12 + (37)(15) = \boxed{567}$ ✓

$567 + 1147k$ is general, some other equivalent rule

(b) Modular exponentiation

i. Compute $31^{45} \bmod 100$ by the method of repeated squaring.

ii. Compute $22^{93} \bmod 31$. Hint: Fermat's little theorem might be useful.

45 $(561)^2 \cdot 31 = 9756351 \equiv_{1000} 351$ ← so mod 100 it is my friend

22 $831^2 = 690561 \equiv_{1000} 561$

11 $151^2 \cdot 31 = 706836 \equiv_{1000} 831$

5 $961^2 \cdot 31 = 28629151 \equiv_{1000} 151$

2 $31^2 = 961$

1 31

$22^{93} \bmod 31 \equiv_{31} 22^{93 \bmod 30} \bmod 31 = 22^3 \bmod 31$

$22^3 = 10648 \equiv_{31} 10648 - 343 \cdot 31$

$= 15$