MAT 200 - Logic, Language and Proof

General Information

Instructor: Tom Sharland
e-mail: tjshar "*at*" math.sunysb.edu
Lectures: MW 4pm-5.20pm, ESS 079
Office hours: Monday 2-3 and Friday 11-12 in 5D148; Thursday 2.30-3.30 in MLC.

Grader: Yuhan Sun
email: yuhansun "*at*" math.sunysb.edu
Office Hours: Wednesday 2-4 in MLC.

Course outline: A basic course in the logic of mathematics, the construction of proofs and the writing of proofs. The mathematical content is primarily set theory, combinatorics and number theory. There is considerable focus on writing.

We will move from the concept of mathematics as a computational subject (focusing on *special cases*) to the notion of mathematics as a theoretical subject focusing on *general facts*, proved within a logical framework. As a brief overview (more details can be found on the syllabus page), we will start with a discussion on logic and logical connectives. We then move onto the topic of sets and functions, objects which form the building blocks of mathematics. We then use these notions to discuss cardinality of sets (very informally, how many objects they contain). After this, we make us of our new techniques and ideas to prove results in areas such as number theory.

Textbook: The course text is *An Introduction to Mathematical Reasoning* by Peter J. Eccles. The course syllabus will closely follow this book.

For further reading, many good books are available - *Foundations of Mathematics* by I. Stewart and D. Tall is aimed at a similar level, and *How to Prove it* by D. J. Velleman is a nice introductory text on writing proofs in mathematics.

Tests:

There will be two midterm exams and a final exam. Midterms will take place during classes. **The first midterm will be in class on 10/6**; here are some practice questions to help you prepare. **The second midterm will be in class on 11/3**; here are some practice questions to help you prepare.

The **Final exam** will be at **8.30-11pm** on **Tuesday 9th December** in **ESS 079**, the usual lecture room. There will be a **Review Session** in **Physics P112** at **2-4pm** (or maybe finishing later) on **Monday 8th December**. Here are some practice problems, and some guidelines for the exam. Here are some solutions to the practice exam.

Course grade is computed by the following scheme:

Midterm Test I: 25%
Midterm Test II: 25%
Final Exam: 40%

Homework: 10%

Homework assignments can be found by clicking the "Homework" link in the menubar on the left of the webpage. You are encouraged to discuss homework with your class mates, since this aids understanding of complicated concepts. However, you should write up solutions individually, to ensure you understand your own solutions. You are also encouraged to attempt non-homework problems from he textbook (or elsewhere) to check you understand the topics we are covering. Both the lecturer and the TA will be happy to discuss such problems with you if you get stuck. **Late homework will never be accepted** but an assignment may be excused if there is documented evidence as to why it was missed. Similarly, make-up exams will only be provided if documented evidence shows the exam was missed due to unforeseen circumstances. The homework grade will be calculated as your best **10** assignments.

Information for students with disabilities
If you have a physical, psychological, medical, or learning disability that may impact your course work, please contact Disability Support Services at (631) 632-6748 or http://studentaffairs.stonybrook.edu/dss/. They will determine with you what accommodations are necessary and appropriate. All information and documentation is confidential.

Students who require assistance during emergency evacuation are encouraged to discuss their needs with their professors and Disability Support Services. For procedures and information go to the following website: http://www.sunysb.edu/ehs/fire/disabilities.shtml

Academic integrity
Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another person's work as your own is always wrong. Faculty are required to report any suspected instances of academic dishonesty to the Academic Judiciary. Faculty in the Health Sciences Center (School of Health Technology & Management, Nursing, Social Welfare, Dental Medicine) and School of Medicine are required to follow their school-specific procedures. For more comprehensive

information on academic integrity, including categories of academic dishonesty, please refer to the academic judiciary website http://www.stonybrook.edu/uaa/academicjudiciary/

Critical Incident Management Statement

Stony Brook University expects students to respect the rights, privileges, and property of other people. Faculty are required to report to the Office of Judicial Affairs any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, or inhibits students' ability to learn. Faculty in the HSC Schools and the School of Medicine are required to follow their school-specific procedures.

QPS Learning objective

Learning Outcomes for "Master Quantitative Problem Solving" includes the following:

1. Interpret and draw inferences from mathematical models such as formulas, graphs, tables, or schematics.
2. Represent mathematical information symbolically, visually, numerically, and verbally.
3. Employ quantitative methods such as algebra, geometry, calculus, or statistics to solve problems.
4. Estimate and check mathematical results for reasonableness.
5. Recognize the limits of mathematical and statistical methods.

STEM+

A grade of C or better in this course ful lls the Science, Technology, Engineering, and Mathematics (STEM+) objective in the Stony Brook Curriculum.

Stony Brook University

MAT 200 - Logic, Language and Proof

Syllabus

Here is the course outline for the MAT 200 course for Fall 2014. I will try to update it regularly so that it accurately resembles where we are in class. Chapters correspond to the section in the class textbook: An Introduction to Mathematical Reasoning by Peter J. Eccles.

Week Commencing	Sections Covered	Reading
8/25	• 1. The Language of Mathematics • 2. Implications • 3. Proofs	Read pages 3-29.
9/1	• 4. Proof by Contradiction	Read pages 30-38.
9/8	• 5. The Induction Principle • 6. The Language of Set Theory	Read pages 39-65.

9/15	• 6. The Language of Set Theory • 7. Quantifiers	Read pages 65-88.
9/22	• 8. Functions • 9. Types of Functions	Read pages 89-114.
9/29	• 10. Counting Finite Sets	Read pages 123-138.
10/6	• **MIDTERM I** • 11. Properties of Finite Sets • 12. Counting Functions and Subsets	• Prepare for the midterm • Read pages 139-149.
10/13	• 12. Counting Functions and Subsets • 13. Number Systems	Read pages 149-169.
10/20	• 13. Number Systems • 14. Counting Infinite Sets	Read pages 170-181.

10/27	• 14. Counting Infinite Sets • 15. The Division Theorem	
11/3	• **MIDTERM II** • 16. The Euclidean Algorithm	
11/10	• 17. Applications of the Euclidean Algorithm • 18. Linear Diophantine Equations	
11/17	• 19. Congruence of Integers • 20. Linear Congruences	
11/24	• 21. Congruence Classes • **Eat Turkey!**	

12/1	• 22. Equivalence Relations and Partitions	

Homework Assignments

Here are the homework assignments for the MAT 200 class for Fall 2014. There will be one homework assignment per week, based on the topics covered in class that week. Homework will be posted by Wednesday each week, and will be due in class on the following Wednesday. I will try to post solutions to the assignments shortly after they are handed in. Note that it is suggested you work on problems in the book to improve your familiarity with the topics covered, since just doing the homework will probably not be sufficient practice.

- Homework 1 is due in class on 9/3.
- Homework 2 is due in class on 9/10.
- Homework 3 is due in class on 9/17.
- Homework 4 is due in class on 9/24.
- Homework 5 is due in class on 10/1.
- Homework 6 is due in class on 10/15.
- Homework 7 is due in class on 10/22.
- Homework 8 is due in class on 10/29.
- Homework 9 is due in class on 11/12.
- Homework 10 is due in class on 11/19.
- Homework 11 is due in class on 12/3.

MAT 200 - Logic, Language and Proof

Solutions

This page contains solution sets for the homework assignments and also for the practice midterm exams for the MAT200 course for Fall 2014. Please let me know if there are any mistakes in the files.

Homework Solutions

- Solutions to Homework 1.
- Solutions to Homework 2.
- Solutions to Homework 3.
- Solutions to Homework 4.
- Solutions to Homework 5.
- Solutions to Homework 6.
- Solutions to Homework 7.
- Solutions to Homework 8.
- Solutions to Homework 9.
- Solutions to Homework 10.
- Solutions to Homework 11.

Practice exam Solutions

Here are the solutions to the first practice midterm.

Here are the solutiosn to the second practice midterm.

PRACTICE QUESTIONS FOR MIDTERM I

MAT 200 - FALL 2014

Here are some practice questions for the Midterm I exam which will take place in class on 10/6. Some of these questions will be useful for the exam, others will not be (directly) useful, but an ability to tackle all of them will put you in good shape to do well on the exam. For other preparation, make sure you know all the definitions we have introduced so far, as well as understanding the results we have proven thus far in the course. Note that the best way to remember proofs is not to memorise them *verbatim*, but to understand the concepts underlying the proofs. This will allow you to apply these concepts to new problems.

Question 1. Use a truth table to show that P is equivalent to (not P) $\Rightarrow C$, where C is a contradiction.

Question 2. Use a truth table to show that $P \Rightarrow Q$ and (P or Q) $\Leftrightarrow Q$ are equivalent.

Question 3. Prove that if $x \in \mathbb{R}$ and $x^2 \geq 5x$ then $x \geq 5$ or $x \leq 0$.

Question 4. Prove that if $a \in \mathbb{R}$ then one of $\sqrt{5} - a$ and $\sqrt{5} + a$ is irrational.

Question 5. Show for all $n \in \mathbb{N}$ that

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

Question 6. Show for all $n \in \mathbb{N}$ that $n^3 - n$ is divisible by 3.

Question 7. Let A, B, C be sets. Show that $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

Question 8. Prove that if X is a universal set and $A, B \subseteq X$, then $A \subseteq B \Leftrightarrow B^c \subseteq A^c$.

Question 9. Write the negation of $\forall\, x \in \mathbb{N}, \exists\, y \in \mathbb{N}, y = x - 1$. Is the original statement true? Prove or give a counterexample.

Question 10. Let $\mathcal{C}$ be the set of circles in $\mathbb{R}^2$: that is $\mathcal{C} = \{C \subset \mathbb{R}^2 \mid C \text{ is a circle}\}$. Also, define $R\colon \mathcal{C} \to \mathbb{R}$ by $R(C) =$ "Radius of C". For each of the following statements, either prove them or give a counterexample.

(i) $\forall C_1 \in \mathcal{C}, \forall C_2 \in \mathcal{C}, C_1 \cap C_2 = \varnothing$.
(ii) $\exists x \in \mathbb{R}, \forall C \in \mathcal{C}, R(C) = x$.
(iii) $\forall C \in \mathcal{C}, \exists x \in \mathbb{Z}, R(C) = x$.

Question 11. Give an example of a map $f\colon \mathbb{N} \to \mathbb{N}$ which is an injection but not a surjection.

Question 12. Give an example of a map $f\colon \mathbb{N} \to \mathbb{N}$ which is a surjection but not an injection.

Question 13. Let $f\colon X \to Y$ and $g\colon Y \to Z$. If f is an injection and $g \circ f$ is an injection, must g be an injection? Prove or give a counterexample.

Question 14. Let $f\colon X \to Y$ and $g\colon Y \to Z$. If f is a surjection and $g \circ f$ is a surjection, must g be a surjection? Prove or give a counterexample.

PRACTICE QUESTIONS FOR MIDTERM II

MAT 200 - FALL 2014

Same deal as last time - some of these questions will be useful, others less so. Again, you will be expected to prove things in the exam, but the best method for remembering proofs is not to memorise them, but to understand the underlying concepts. Also, some of the proofs will be of new results, which will test your understanding of the material.

Question 1. Express the following recurring decimals as rational numbers.

(a) $2.71\overline{828}$
(b) $2.345\overline{67}$
(c) $1.23\overline{45} + 2.4\overline{19}$

Question 2. Show that if A and B are finite sets, then if $A \subset B$ we have

$$\min B \leq \min A$$

Question 3. Let X and Y be finite sets with $|X| < |Y|$. Show there does not exist a surjection $\phi\colon X \to Y$.

Question 4. Let $X = \{x_1, x_2, x_3, x_4\}$ and $Y = \{y_1, y_2, y_3, y_4, y_5\}$.

(a) How many maps are there $f\colon X \to Y$?
(b) How many maps are there $f\colon Y \to X$?
(c) What is $|\{f \in \mathrm{Fun}(X, Y) \mid y_4 \notin \mathrm{im} f\}|$?

Question 5. Suppose we pick 17 elements from the set $\mathbb{N}_{32}$. Show that we must have picked a pair of integers whose sum is 33.

Question 6. Four people visit a restaurant and each choose one meal from a choice of seven on the menu.

(a) How many possible combinations are there if we record who chose which dish?
(b) How many possible combinations are there if we do not record who chose which dish?
(c) How many possible combinations are there if we record who chose which dish and each person chose a different dish from everyone else?

Question 7. Suppose $X \cap Y = \varnothing$. Show that the function

$$f\colon \bigcup_{i=0}^{k} \mathcal{P}_i(X) \times \mathcal{P}_{k-i}(Y) \to \mathcal{P}_k(X \cup Y)$$

given by $f(A, B) = A \cup B$ is a bijection. From this, deduce that

$$\binom{m+n}{k} = \sum_{i=0}^{n} \binom{m}{i}\binom{n}{k-i}.$$

Question 8. Which of the following sets are countably infinite?

- $\mathbb{C}$
- $\{a\sqrt{2} + b\sqrt{3} + c\sqrt{5} \mid a, b, c \in \mathbb{Q}\}$
- $\{\pi^m + e^n \mid m, n \in \mathbb{Z}\}$
- $\mathrm{Fun}(\mathbb{N}, \{0, 1\})$
- The set of circles in the plane with rational centers and rational radii.

Question 9.

(a) Let $a < b$ and $c < d$. Show that the map $f\colon [a, b] \to [c, d]$ given by

$$f(x) = \frac{(b-x)c}{b-a} + \frac{(x-a)d}{b-a}$$

is a bijection. Deduce that any two closed intervals containing more than one point have the same cardinality.

(b) Show that all intervals containing more than one point have the same cardinality. (Hint: it is not necessary to find an explicit bijection to do this).

(c) Show that all intervals containing more than one point have the same cardinality as $\mathbb{R}$.

Question 10. By considering the map $f\colon [0, 1) \times [0, 1) \to [0, 1)$, defined by

$$f((0.a_1a_2, \ldots a_n \ldots, 0.b_1b_2 \ldots b_n \ldots)) = 0.a_1b_1a_2b_2 \ldots a_nb_n \ldots$$

(and using the expansion ending in recurring 0s if there is a choice) deduce that $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

PRACTICE QUESTIONS FOR THE FINAL EXAM

MAT 200 - FALL 2014

Here are some practice questions for the final. Here are some pointers.

- You are expected to know the basic definitions covered in class. This means you should give precise mathematical definitions; for example "f is an injection if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$" and NOT "$f$ is an injection if no two things map to the same thing in the codomain".
- There will be proofs in the exam. Again, these proofs should be made up of precise mathematical arguments, where each step logically follows from the previous one. You will be penalised for "hand-wavy" or unjustified arguments. Many of the proofs will be of results covered in class (but no proof will be very long, so as a freebie, I'll tell you that you won't have to prove the Pigeonhole principle for example).
- If you are using a result covered in class, you should explicitly state so, perhaps by summarising what the result says. If the result has a name (e.g. Pigeonhole principle), you can use that.
- The exam will be split into two parts. The first question will cover what I consider to be the "basics" of the course. This will focus on some of the simpler ideas in each section of the notes. A good perfomrance on question 1 will indicate a grasp of the basic concepts in the course, and will be rewarded with at least a C grade.
- The latter questions will involve some of the more difficult concepts, or more complicated examples than question 1. If you want to score a high grade, you should also be able to answer these questions too.
- Even if you can't work out a whole proof, outline your ideas. Showing you have an understanding of the concepts underlying the proof will get some credit.

Below are the questions. In general, I will be aiming these practice questions for the later questions on the exam, but some of the questions may also be helpful for question 1. For other practice, make sure you look back over the homework problems from the course.

Question 1. Show that
$$\prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right) = \frac{n+1}{2n}.$$

Question 2. Show that if $f\colon X \to Y$ is a surjection then there exists an injection $g\colon Y \to X$ (you may assume the axiom of choice[1]).

Question 3. Let $\mathcal{L}$ be the set of lines in the plane and let $f\colon \mathbb{R}^3 \to \mathcal{L}$ be defined so that $f(a, b, c)$ is the line with equation $ax + by = c$. Show that f is a surjection but not an injection.

Question 4. Let $C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ be the unit circle in the plane. Show that $|C| = |\mathbb{R}|$.

[1] If you don't understand this comment, feel free to be able to assume that given any set X, you are able to pick an element x from X.

Question 5. Solve the following linear diophantine equations

(i) $9m + 18n + 45p = 93$
(ii) $3m + 7n + 12p = 14$
(iii) $4m + 6n + 13p = 42$

Question 6. Solve the linear congruences.

(a) $5x \equiv 17 \mod 123$
(b) $90x \equiv 18 \mod 135$
(c) $490 \equiv 84 \mod 1428$.

Question 7. Let $\mathcal{L}$ be the set of lines in the plane and define a relation $\sim$ on $\mathcal{L}$ by $L_1 \sim L_2$ if and only if $L_1 \cap L_2 \neq \varnothing$. Is $\sim$ reflexive, symmetric or transitive? Is $\sim$ an equivalence relation?

Question 8. Let $\mathcal{L}$ be the set of lines in the plane and define a relation $\sim$ on $\mathcal{L}$ by $L_1 \sim L_2$ if and only if $L_1 \cap L_2 = \varnothing$. Is $\sim$ reflexive, symmetric or transitive? Is $\sim$ an equivalence relation?

Question 9. Let $X = \mathrm{Fun}(\mathbb{R}, \mathbb{R})$ be the set of functions $f\colon \mathbb{R} \to \mathbb{R}$. Let $\sim$ be a relation on X given by

$$f \sim g \Leftrightarrow \text{there exists a bijection } h\colon \mathbb{R} \to \mathbb{R} \text{ such that } g = h^{-1} \circ f \circ h.$$

Show that $\sim$ is an equivalence relation.

(a) What is the equivalence class of the identity function $\mathrm{id}_{\mathbb{R}}$?
(b) What is the equivalence class of the function f defined by $f(x) = 0$ for all $x \in \mathbb{R}$?

PRACTICE SOLUTIONS FOR THE FINAL EXAM

MAT 200 - FALL 2014

Question 1. *Show that*

$$\prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right)=\frac{n+1}{2n}.$$

for all $n \geq 2$.

Solution 1. We proceed by induction on n. For the base case $n = 2$, we note that

$$\prod_{i=2}^{2}\left(1-\frac{1}{i^2}\right)=1-\frac{1}{4}=\frac{3}{4}=\frac{2+1}{2\times 2}$$

so the equality holds. Now suppose that for some $k \geq 2$ we have

$$\prod_{i=2}^{k}\left(1-\frac{1}{i^2}\right)=\frac{k+1}{2k}.$$

Then now

$$\begin{aligned}
\prod_{i=2}^{k+1}\left(1-\frac{1}{i^2}\right) &= \prod_{i=2}^{k}\left(1-\frac{1}{i^2}\right)\times\left(1-\frac{1}{(k+1)^2}\right)\\
&= \frac{k+1}{2k}\times\left(1-\frac{1}{(k+1)^2}\right)\\
&= \frac{k+1}{2k}-\frac{k+1}{2k(k+1)^2}\\
&= \frac{(k+1)^3-(k+1)}{2k(k+1)^2}\\
&= \frac{(k+1)^2-1}{2k(k+1)}\\
&= \frac{k^2+2k}{2k(k+1)}\\
&= \frac{k+2}{2(k+1)} \quad = \quad \frac{(k+1)+1}{2(k+1)}
\end{aligned}$$

and so by the principle of mathematical induction, the result holds for all $n \geq 2$.

Question 2. *Show that if $f\colon X \to Y$ is a surjection then there exists an injection $g\colon Y \to X$ (you may assume the axiom of choice[1]).*

Solution 2. We know that if f is a surjection then there exists a right inverse $g\colon Y \to X$ which satisfies $f(g(y)) = y$ for all $y \in Y$ (this was proved earlier in the course - to prove this statement requires the axiom of choice). We now show that this right inverse is the required injection. Let $g(y_1) = g(y_2) = x \in X$. Then by definition of a right inverse, we must have $y_1 = f(x) = y_2$, from which it follows that g is an injection.

Question 3. *Let $\mathcal{L}$ be the set of lines in the plane and let $f\colon \mathbb{R}^3 \to \mathcal{L}$ be defined so that $f(a,b,c)$ is the line with equation $ax + by = c$. Show that f is a surjection but not an injection.*

Solution 3. The fact f is a surjection is immediate - all lines in the plane are of the form $ax+by = c$ for some choice of $(a,b,c) \in \mathbb{R}^3$. To see that f is not an injection, note that $f(1,-1,0) = f(2,-2,0)$, with both images being the line $y = x$.

Question 4. *Let $C = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ be the unit circle in the plane. Show that $|C| = |\mathbb{R}|$.*

Solution 4. Notice that the circle can be thought of as the set of points $(\cos\theta, \sin\theta)$ for $\theta \in [0, 2\pi)$. This gives a bijection $f\colon [0,2\pi) \to C$. Now we just need to show that $|\mathbb{R}| = |[0,2\pi)|$. But this follows from the arguments in the practice questions for midterm 2.

Question 5. *Solve the following linear diophantine equations*

(i) $9m + 18n + 45p = 93$
(ii) $3m + 7n + 12p = 14$
(iii) $4m + 6n + 13p = 42$

Solution 5. I just include the solutions here. The technique is similar to that found on the homework a couple of weeks ago. Of course, the given form of the solutions are not unique - you should check that the sets you give are the same as the ones given here (assuming I got the answer right, of course!).

(a) There are no solutions. The left hand side is divisible by 9, but the right hand side is not.
(b) The solution set is $(m,n,p) = (-4 - 4q - 7r, 2 + 3r, 1 + q)$.
(c) The solution set is $(m,n,p) = (4 - 5q - 3r, -3q + 2r, 2 + 2q)$.

Question 6. *Solve the linear congruences.*

(a) $5x \equiv 17 \mod 123$

[1] If you don't understand this comment, feel free to be able to assume that given any set X, you are able to pick an element x from X.

(b) $90x \equiv 18 \mod 135$
(c) $490x \equiv 84 \mod 1428$.

Solution 6. Again, I just include the solutions.

(a) There is a unique solution $x \equiv 28 \mod 123$.
(b) There are no solutions since the problem is equivalent to $5x \equiv 1 \mod 15$ which has no solutions since $\operatorname{hcf}(5, 15) = 5$.
(c) This is equivalent to solving $35x \equiv 6 \mod 102$ which is solved by $x \equiv 6 \mod 102$. There are $\operatorname{hcf}(490, 1428) = 14$ solutions modulo 1428, these are

$$x \equiv 6, 108, 210, 312, 414, 516, 618, 720, 822, 924, 1026, 1128, 1230, 1332 \mod 1428.$$

Question 7. *Let $\mathcal{L}$ be the set of lines in the plane and define a relation $\sim$ on $\mathcal{L}$ by $L_1 \sim L_2$ if and only if $L_1 \cap L_2 \neq \varnothing$. Is $\sim$ reflexive, symmetric or transitive? Is $\sim$ an equivalence relation?*

Solution 7. Clearly $\sim$ is reflexive and symmetric. However, it is not transitive. To see this, consider the lines L_1 as the line $y = x$, L_2 the line $y = -x$ and L_3 the line $y = x + 1$. Then L_1 and L_2 intersect at $(0, 0)$, and L_2 and L_3 intersect at $(-1/2, 1/2)$. However since L_1 and L_3 are parallel, they do not intersect. The relation is not an equivalence relation.

Question 8. *Let $\mathcal{L}$ be the set of lines in the plane and define a relation $\sim$ on $\mathcal{L}$ by $L_1 \sim L_2$ if and only if $L_1 \cap L_2 = \varnothing$. Is $\sim$ reflexive, symmetric or transitive? Is $\sim$ an equivalence relation?*

Solution 8. This time it is clear that $\sim$ is not reflexive but it is symmetric. It is not transitive since if L_2 is parallel to L_1 then $L_1 \sim L_2$ and $L_2 \sim L_1$ but $L_1 \nsim L_2$. The relation is not an equivalence relation. However, if we changed it to

$$L_1 \sim' L_2 \Leftrightarrow L_1 \cap L_2 = \varnothing \text{ or } L_1 = L_2$$

then this is an equivalence relation, with equivalence classes being sets of parallel lines in the plane.

Question 9. *Let $X = \operatorname{Fun}(\mathbb{R}, \mathbb{R})$ be the set of functions $f \colon \mathbb{R} \to \mathbb{R}$. Let $\sim$ be a relation on X given by*

$$f \sim g \Leftrightarrow \textit{there exists a bijection } h \colon \mathbb{R} \to \mathbb{R} \textit{ such that } g = h^{-1} \circ f \circ h.$$

Show that $\sim$ is an equivalence relation.

(a) *What is the equivalence class of the identity function $\mathrm{id}_{\mathbb{R}}$?*
(b) *What is the equivalence class of the function f defined by $f(x) = 0$ for all $x \in \mathbb{R}$?*

Solution 9. Reflexivity holds since if we set h to be the identity on $\mathbb{R}$, $f \sim f$. Clearly symmetry also holds since

$$f \sim g \quad \Leftrightarrow \quad g = h^{-1} \circ f \circ h \quad \text{for some bijection } h \qquad \Leftrightarrow \quad f = h \circ g \circ h^{-1}$$

and since h^{-1} must be a bijection, the condition holds. To check transitivity, suppose $f \sim g$ and $g \sim k$. Then there exist bijections h_1 and h_2 such that

$$g = h_1^{-1} \circ f \circ h_1 \quad \text{ and } k = h_2^{-1} \circ g \circ h_2.$$

Combining these two gives

$$k = h_2^{-1} \circ h_1^{-1} \circ f \circ h_1 \circ h_2.$$

Since $(h_1 \circ h_2)^{-1} = h_2^{-1} \circ h_1^{-1}$ and the compositions of bijections are bijections, it follows that $f \sim k$ as required and so $\sim$ is an equivalence relation.

(a) Suppose $f \in [\mathrm{id}]$. Then there exists a bijection h such that

$$f = h^{-1} \circ \mathrm{id} \circ h = h^{-1} \circ h = \mathrm{id}$$

so $f = \mathrm{id}$ and so $[\mathrm{id}] = \{\mathrm{id}\}$.

(b) Suppose $g \in [f]$. Then there exists a bijection h such that for all $x \in \mathbb{R}$

$$g(x) = h^{-1} \circ f \circ h(x) = h^{-1}(0)$$

and so g is a constant function. Hence $[f]$ is the set of constant functions on $\mathbb{R}$.

Homework 1

1. Find the contrapositive to the statement "If it quacks like a duck, it is a duck".

2. Problem 2, p53: By using truth tables prove that, for all statements P and Q, the three statements

   (a) $P \Rightarrow Q$

   (b) $(P \text{ or } Q) \Leftrightarrow Q$

   (c) $(P \text{ and } Q) \Leftrightarrow P$

   are logically equivalent.

3. (Compare Problem 3, p53) Define the logical connective $*$ by

$$(P * Q) \text{ means } ((\text{not } P) \text{ or } (\text{not } Q)).$$

   Show that

   (a) $(\text{not } P)$ means $(P * P)$

   (b) $(P \text{ or } Q)$ means $((P * P) * (Q * Q))$.

   (c) $(P \text{ and } Q)$ means $((P * Q) * (Q * P))$

   (d) $(P \Rightarrow Q)$ means $((P * (Q * Q))$.

4. Problem 6, p54: Use the properties of addition and multiplication of real numbers given in Properties 2.3.1 (pp 18-19) to deduce that, for all real numbers a and b,

   (a) $a \times 0 = 0 = 0 \times a$

   (b) $(-a)b = -ab = a(-b)$

   (c) $(-a)(-b) = ab$

   Recall that for any given x, the element $-x$ is such that $x + (-x) = 0 = (-x) + x$.

MAT 200 HOMEWORK 2

DUE IN CLASS ON 9/10

Problem 1. *Prove by contradiction that there is no largest integer. Hint: Suppose there were a largest integer* $n, \ldots$

Problem 2. *Prove by contradiction that there is no smallest postive real number.*

Problem 3. *Let* a*,* b *and* c *be positive intergers. Show that if* a *divides* b *and* a *divides* c *then* a *divides* $(b+c)$*.*

Problem 4. *Use induction to prove Bernouilli's inequality. That is, for all integers* $n \geq 1$ *and all* $x > -1$ *we have*

$$(1+x)^n \geq 1 + nx.$$

MAT 200 HOMEWORK 3

DUE IN CLASS ON 9/17

Problem 1. Prove by induction that

$$\sum_{k=1}^{n}(k \cdot k!) = 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots = (n+1)! - 1$$

for all integers $n \geq 1$.

Problem 2. Here are some attempted proofs by induction. Three are incorrect proofs of false facts. In these cases explain why the proof fails. In the remaining case, the proof is a faulty proof of a true fact. In this case you should repair the proof so that it correctly proves the stated proposition.

(a) *Proposition.* All cows are the same color.
Proof. We proceed by induction on the number of cows. First the base case: clearly one cow is the same color as itself, so the case for $n = 1$ is true. Now suppose that it is true for n cows. Consider a collection of $n+1$ cows. Removing one of them, we have n cows, which by the inductive hypothesis have the same color. Now add back in this cow and remove another one. Again, we have a collection of n cows and these are all the same color. So the cow we first removed is the same color as the other cows, which is the same color as the second cow we removed. Hence all $n+1$ cows are the same color and so we have proved the inductive step. Hence by the principle of mathematical induction, all cows are the same color.

(b) *Proposition.* $2 + 4 + \cdots + 2n = n(n+1)$.
Proof. If

$$2 + 4 + \cdots + 2n = n(n+1)$$

then

$$2 + 4 + \cdots + 2n + 2(n+1) = n(n+1) + 2(n+1) = (n+1)(n+2).$$

Hence by induction the formula is true for all n.

(c) *Proposition.* $1 + 3 + 5 + \cdots + (2n-1) = n^2 + 1$.
Proof. Assume it is true that

$$1 + 3 + 5 + \cdots + (2n-1) = n^2 + 1.$$

Then, adding $2n+1$ to both sides, we get

$$1 + 3 + 5 + \cdots + (2n-1) + (2n+1) = (n^2+1) + 2n + 1 = (n+1)^2 + 1.$$

This proves the inductive step. Hence by the principle of mathematical induction, the formula holds.

(d) *Proposition.* Suppose n straight lines are drawn on a circular disk, so that no three lines meet at the same point. Then these lines split the disk up into 2^n different regions.
Proof. Clearly, one line splits the disk into 2 regions, so the base step is true. Now suppose that the statement holds for n; that is, the n lines split the disk into 2^n regions. Then, if we add another line, this splits each region into two separate regions. Hence there are now $2 \times 2^n = 2^{n+1}$ regions. Thus, by the principle of mathematical induction, the result holds.

Problem 3. (Problem 17, p55.) For a positive integer n the number a_n is defined inductively by

$$\begin{aligned} a_1 &= 1 \\ a_{k+1} &= \frac{6a_k + 5}{a_k + 2} \qquad \text{for every positive integer } k \geq 1. \end{aligned}$$

Prove for all positive integers n that $0 < a_n < 5$.

Problem 4. (This is quite hard, so give yourself time to think about it). In this example, we use "forwards-backwards" induction. First, define the symbol

$$\prod_{i=1}^{n} x_i$$

inductively by

$$\begin{aligned} \prod_{i=1}^{1} x_i &= x_1 \\ \prod_{i=1}^{k+1} x_i &= \left(\prod_{i=1}^{k} x_i \right) \times x_{k+1} \qquad \text{for } k \geq 1. \end{aligned}$$

This means that $\prod_{i=1}^{n} x_i$ is the *product* of the numbers $x_1, \ldots, x_n$. We will prove that for all positive real numbers x_i and all $n \geq 1$

$$\frac{1}{n} \sum_{i=1}^{n} x_i \geq \left(\prod_{i=1}^{n} x_i \right)^{\frac{1}{n}}.$$

(i) Show that the statement holds for $n = 1$.
(ii) Using the fact that $(x + y)^2 \geq 0$, show that the statement holds for $n = 2$.
(iii) Show that if the statement holds for $n = 2^m$, then it also holds for $n = 2^{m+1}$ by using induction on m (*Hint*: you may need to use part (ii) at some point...). This is the forwards induction.
(iv) Show that if the statement is true for $n = k$, then it is also true for $n = k - 1$. To do this, given the numbers $x_1, \ldots, x_{k-1}$, define

$$x_k = \frac{x_1 + \cdots + x_{k-1}}{k - 1}.$$

Then, by the inductive hypothesis, we have

$$\frac{x_1 + \cdots + x_{k-1} + \frac{x_1 + \cdots + x_{k-1}}{k-1}}{k} = \sum_{i=1}^{k} x_i \geq \left(\prod_{i=1}^{k} x_i \right)^{\frac{1}{k}} = \sqrt[k]{x_1 \times \cdots \times x_{k-1} \times \frac{x_1 + \cdots x_{k-1}}{k - 1}}.$$

Proceed from here to prove the statement is true for $n = k - 1$. From this deduce that the statement is true for all $n \geq 1$.

MAT 200 HOMEWORK 4

DUE IN CLASS ON 9/24

Problem 1. Let A, B, C and D be sets.

(i) Prove that $A \cap A^c = \varnothing$.
(ii) Prove that $(A \cap B)^c = A^c \cup B^c$.
(iii) Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(iv) Prove that $A \cap (A \cup B) = A$.
(v) Prove that $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Problem 2. Let X be a set. Then, for subsets $A, B \in \mathcal{P}(X)$, define the symmetric difference of A and B to be

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Observe that $A \triangle B = B \triangle A$.

(i) Show that $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.
(ii) Show that there exists a unique $E \in \mathcal{P}(X)$ such that, for all $A \in \mathcal{P}(X)$ we have $A \triangle E = A$.
(iii) For E as above, show that for all $A \in \mathcal{P}(X)$ there exists a unique set $B \in \mathcal{P}(X)$ such that $A \triangle B = E$.
(iv) Show that, for all $A, B \in \mathcal{P}(X)$, there exists a unique $C \in \mathcal{P}(X)$ such that $A \triangle C = B$.
(v) Let $X = \mathbb{Z}$, A be the set of even integers and B be the set of multiples of 3. Describe the set $A \triangle B$.

Problem 3. Prove or give a counterexample to the following statements.

(i) $\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R}, \quad xy > 0$.
(ii) $\exists x \in \mathbb{R} \quad \forall y \in \mathbb{R}, \quad xy > 0$.
(iii) $\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R}, \quad xy \geq 0$.
(iv) $\exists x \in \mathbb{R} \quad \forall y \in \mathbb{R}, \quad xy \geq 0$.
(v) $\forall n \in \mathbb{N} \quad (n$ is even or n is odd$)$.
(vi) $(\forall n \in \mathbb{Z} \quad n$ is even$)$ or $(\forall n \in \mathbb{Z} \quad n$ is odd$)$.

MAT 200 HOMEWORK 5

DUE IN CLASS ON 10/1

Problem 1. Let X be any set. For each $A \in \mathcal{P}(X)$, define the *characteristic function* $\chi_A \colon X \to \{0, 1\}$ by

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A. \end{cases}$$

Let $A, B \in \mathcal{P}(X)$ and $x \in X$.

(i) Show that $\chi_{A \cap B}(x) = \chi_A(x)\chi_B(x)$.
(ii) Give a formula for $x \mapsto \chi_{X \setminus A}(x)$ in terms of $\chi_A(x)$.
(iii) Using the fact that $A \setminus B = A \cap B^c$ and $B^c = X \setminus B$, give a formula for $x \mapsto \chi_{A \setminus B}(x)$.
(iv) Find the set C so that $\chi_C(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x)$.

Problem 2. Show that if $f \colon X \to Y$ is an injection and $g \colon Y \to Z$ is an injection, then $g \circ f \colon X \to Z$ is an injection.

Problem 3. Show that $f \colon X \to Y$ has a right inverse if and only if it is a surjection.

Problem 4. Let $f \colon X \to Y$. Prove the following equalities hold for the induced functions $f \colon \mathcal{P}(X) \to \mathcal{P}(Y)$ and $f^{-1} \colon \mathcal{P}(Y) \to \mathcal{P}(X)$.

(i) For all $X_1, X_2 \in \mathcal{P}(X)$, $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.
(ii) For all $Y_1, Y_2 \in \mathcal{P}(Y)$, $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

MAT 200 HOMEWORK 6

DUE IN CLASS ON 10/15

Problem 1. Let A be a set containing 10 positive integers less than 100 (so that $A \subset \mathbb{N}_{100}$ and $|A| = 10$). Using the pigeonhole principle, show that there exists two disjoint subsets of A which have the same sum. Here, the sum of a set is the sum of the elements in the set.

Problem 2. Suppose X and Y are finite sets with $|X| = |Y|$. Show that a function $\phi\colon X \to Y$ is an injection if and only if it is a surjection.

Problem 3. There are 164 students in a Calculus class. Of these, 110 like differentiation, 107 like integration and 94 like differential equations. Furthermore, 18 liked only differentiation, 13 liked only integration and 4 liked only differential equations. There were 9 students who did not like any of the topics. How many students liked all three topics? (*Hint: Draw a Venn diagram representing this problem. You should have four regions of unknown cardinality. Find four equations in these unknowns and solve them to find the required solution*).

Problem 4. Using induction on n, prove the general inclusion-exclusion principle for unions of finite sets: Let $A_1, A_2, \ldots, A_n$ finite sets. For each $I = \{i_1, i_2, \ldots i_r\} \subseteq \mathbb{N}_n$, denote

$$A_I = \bigcap_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}.$$

Then

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\varnothing \neq I \subseteq \mathbb{N}_n} (-1)^{|I|-1} |A_I|$$

where the sum is taken over all non-empty subsets of $\mathbb{N}_n$.

Problem 5. Let X be a set and suppose $\phi\colon \mathbb{N} \to X$ is an injection. Prove that X is an infinite set.

MAT 200 HOMEWORK 7

DUE IN CLASS ON 10/22

Problem 1. Let $n \in \mathbb{N}$. Suppose that $A \subseteq \mathbb{N}_{2n}$ and $|A| = n + 1$. Show that A must contain a pair of integers $a \neq b$ such that a divides b.

Problem 2. Use the inclusion-exclusion principle from the last homework to show that the number of surjections from $\mathbb{N}_m$ to $\mathbb{N}_n$ is given by

$$n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \cdots + (-1)^{n-1}\binom{n}{n-1}1^m.$$

(*Hint:* In the inclusion-exclusion formula, define the set $A_i = \{f\colon \mathbb{N}_m \to \mathbb{N}_n \mid i \notin \mathrm{im}(f)\}$). From this deduce that

$$n^n - \binom{n}{1}(n-1)^n + \binom{n}{2}(n-2)^n - \cdots + (-1)^{n-1}\binom{n}{n-1}1^n = n!$$

Problem 3. Prove there does not exist a rational number whose square is 6.

Problem 4. Find the rational numbers corresponding to the following infinite decimals.

(1) $7.1032\overline{2194}$
(2) $234.915\overline{91}$
(3) $17.\overline{17}$

MAT 200 HOMEWORK 8

DUE IN CLASS ON 10/29

Problem 1. Define inequality between two fractions by

$$\frac{a_1}{b_1} < \frac{a_2}{b_2} \Leftrightarrow \begin{cases} a_1b_2 < a_2b_1 & \text{if } b_1b_2 > 0, \\ a_1b_2 > a_2b_1 & \text{if } b_1b_2 < 0. \end{cases}$$

Show that this definition is well-defined. Furthermore, show that this relation is transitive; that is.

$$\frac{a_1}{b_1} < \frac{a_2}{b_2} \text{ and } \frac{a_2}{b_2} < \frac{a_3}{b_3} \Longrightarrow \frac{a_1}{b_1} < \frac{a_3}{b_3}$$

Problem 2. Using the definition of an infinite decimal, prove that each finite decimal may be written as an infinite decimal in two different ways:

$$\begin{aligned} a_0.a_1a_2\ldots a_{n-1}a_n &= a_0.a_1a_2\ldots a_{n-1}a_n\dot{0} \\ &= a_0.a_1a_2\ldots a_{n-1}(a_n-1)\dot{9}. \end{aligned}$$

where $a_n > 0$ if $n > 0$. From this, prove that every real number is represented by a unique infinite decimal unless it is represented by a finite decimal, in which case it is represented by precisely two infinite decimals as above.

Problem 3. Show that the set of polynomials of degree n with rational coefficients is countably infinite. Using this, show that the set of algebraic numbers is countably infinite.

Problem 4. We exhibit another proof that $\mathbb{Q}$ is countably infinite. Using the map $\phi\colon \mathbb{Q} \to \mathbb{N}$, defined by

$$\phi(q) = \begin{cases} 2^a3^b & \text{if } q = \frac{a}{b}, \\ 2^a3^b5 & \text{if } q = -\frac{a}{b} \end{cases}$$

where $\frac{a}{b}$ is written in lowest terms and $a \geq 0, b > 0$, show that $|\mathbb{Q}| \leq |\mathbb{N}|$. Now show that $|\mathbb{N}| \leq |\mathbb{Q}|$ and deduce, by the Cantor-Schröder-Bernstein Theorem, that $|\mathbb{N}| = |\mathbb{Q}$.

MAT 200 HOMEWORK 9

DUE IN CLASS ON 11/12

Problem 1. Find the highest common factor of the following pairs a and b using the Euclidean algorithm.

(a) $a = 442$ and $b = 255$
(b) $a = 924$ and $b = 560$
(c) $a = 532$ and $b = 285$
(d) $a = 3960$ and $b = 2541$

Problem 2. By repeatedly using the division theorem, find the infinite decimal which represents the rational number $\frac{4}{13}$ (compare with problem 15.6 on p198).

Problem 3. Prove that every infinite decimal representing a rational number is recurring (where we consider finite decimals to be ending with recurring 0s) and furthermore that if the fraction is written in lowest terms as $\frac{a}{b}$ then the number of recurring digits is less than b.

Problem 4. Let u_n be the nth Fibonacci number. Prove that the Euclidean algorithm takes exactly n steps to prove that $\mathrm{hcf}(u_{n+1}, u_n) = 1$.

Problem 5. We define the *least common multiple* of non-zero integers a and b to be the unique positive integer m such that

(i) m is divisible by a and m is divisible by b,
(ii) If a divides n and b divides n then $m \leq n$.

We write $m = \mathrm{lcm}(a, b)$.

(a) Prove that if a divides n and b divides n then $\mathrm{lcm}(a, b)$ divides n. Deduce that $\frac{ab}{\mathrm{lcm}(a,b)}$ is an integer.
(b) Prove that $\frac{ab}{\mathrm{lcm}(a,b)}$ is a common divisor of a and b and hence $\frac{ab}{\mathrm{lcm}(a,b)} \leq \mathrm{hcf}(a, b)$.
(c) Prove that $\frac{ab}{\mathrm{hcf}(a,b)}$ is a common multiple of a and b. Now deduce that if a and b are positive, then

$$\mathrm{hcf}(a, b)\mathrm{lcm}(a, b) = ab.$$

MAT 200 HOMEWORK 10

DUE IN CLASS ON 11/19

Problem 1. Decide whether the following linear diophantine equations have a solution. If they do have a solution, find all such solutions to the equation.

(a) $442m + 255n = 17$
(b) $924m + 560n = 84$
(c) $532m + 285n = 27$
(d) $3960m + 2541n = -132$

Problem 2. Solve the linear diophantine equation

$$6m + 10n + 15p = 1.$$

by defining $x = 3m + 5n$ and solving the resulting linear diophantine equation.

Problem 3. Solve, if possible, the following linear diophantine equations.

(a) $2m + 3n + 5p = 24$
(b) $2m + 6n + 8p = 17$
(c) $3m + 6n + 11p = 13$
(d) $6m + 15n + 21p = 33$

Problem 4. Let $n > 1$. Show that if there are no non-zero integer solutions to

$$x^n + y^n = z^n$$

then there exists are no non-zero rational solutions. Hint: Maybe the contrapositive will help...

MAT 200 HOMEWORK 11

DUE IN CLASS ON 12/3

Problem 1. Solve the following linear congruences.

(a) $154x \equiv 24 \mod 819$
(b) $231x \equiv 147 \mod 598$
(c) $156x \equiv 42 \mod 252$
(d) $9x \equiv 0 \mod 21$

Problem 2.

(a) What is the final digit of 3^{2014}?
(b) What is the final digit of 73^{2014}?
(c) What is the final digit of 2^{2014}?
(d) What is the final digit of 146^{2014}?

Problem 3. Compute the inverse of 204 modulo 367. Using this, solve the following linear congruences.

(a) $204x = 4 \mod 367$
(b) $204x = 11 \mod 367$
(c) $204x = 99 \mod 367$
(d) $204x = 9 \mod 367$

Problem 4. Prove that the Fibonacci number u_n is divisible by 3 if and only if n is divisible by 4.

MAT200 SOLUTIONS 1

Problem 1. *Find the contrapositive to the statement "If it quacks like a duck, it is a duck".*

Solution 1. The contrapositive is "If it is not a duck, it does not quack like a duck".

Problem 2. *Problem 2, p53: By using truth tables prove that, for all statements P and Q, the three statements*

(i) $P \Rightarrow Q$
(ii) $(P \text{ or } Q) \Leftrightarrow Q$
(iii) $(P \text{ and } Q) \Leftrightarrow P$

are logically equivalent.

Solution 2. We first show that $P \Rightarrow Q$ is logically equivalent to $(P \text{ or } Q) \Leftrightarrow Q$.

P	Q	$P \Rightarrow Q$	P or Q	$(P \text{ or } Q) \Rightarrow Q$	$(P \text{ or } Q) \Leftarrow Q$	$(P \text{ or } Q) \Leftrightarrow Q$
T	T	***T***	T	T	T	***T***
T	F	***F***	T	F	T	***F***
F	T	***T***	T	T	T	***T***
F	F	***T***	F	T	T	***T***

The bold columns agree, which gives the required equivwlence. Now we show $P \Rightarrow Q$ is logically equivalent to $(P \text{ and } Q) \Leftrightarrow P$

P	Q	$P \Rightarrow Q$	P and Q	$(P \text{ and } Q) \Rightarrow P$	$(P \text{ and } Q) \Leftarrow P$	$(P \text{ and } Q) \Leftrightarrow Q$
T	T	***T***	T	T	T	***T***
T	F	***F***	F	T	F	***F***
F	T	***T***	F	T	T	***T***
F	F	***T***	F	T	T	***T***

Again, since the bold columns agree, the statements are logically equivalent. Since the first statement is logically equivalent to the second and third statements, the second and third statements are also logically equivalent.

Problem 3. *(Compare Problem 3, p53) Define the logical connective $*$ by*

$$(P * Q) \text{ means } ((\text{not } P) \text{ or } (\text{not } Q)).$$

Show that

(i) $(\text{not } P)$ *means* $(P * P)$
(ii) $(P \text{ or } Q)$ *means* $((P * P) * (Q * Q))$.
(iii) $(P \text{ and } Q)$ *means* $((P * Q) * (Q * P))$
(iv) $(P \Rightarrow Q)$ *means* $((P * (Q * Q))$.

Solution 3. We use the symbol $\equiv$ to mean "is logically equivalent to".

(i) $P * P \equiv \text{not } P \text{ or not } P \equiv \text{not } P$.

(ii) We'll break this down step-by-step

$$\begin{aligned}((P*P)*(Q*Q)) &\equiv (\text{not } P)*(\text{not } Q) \quad (\text{by part (i)})\\ &\equiv (\text{not (not } P)) \text{ or } (\text{not (not } Q))\\ &\equiv P \text{ or } Q.\end{aligned}$$

(iii) Again we'll do this step-by-step:

$$\begin{aligned}((P*Q)*(Q*P)) &\equiv ((\text{not } P) \text{ or } (\text{not } Q))*((\text{not } Q) \text{ or } (\text{not } P))\\ &\equiv (\text{not } ((\text{not } P) \text{ or } (\text{not } Q))) \text{ or } (\text{not } ((\text{not } Q) \text{ or } (\text{not } P)))\\ &\equiv (P \text{ and } Q) \text{ or } (Q \text{ and } P) \quad (\text{as (not } (A \text{ or } B)) \equiv (\text{not } A) \text{ and } (\text{not } B))\\ &\equiv P \text{ and } Q\end{aligned}$$

(iv) We find

$$\begin{aligned}(P*(Q*Q) &\equiv P*(\text{not } Q)\\ &\equiv (\text{not } P) \text{ or } (\text{not (not } Q))\\ &\equiv (\text{not } P) \text{ or } Q\end{aligned}$$

and we saw in class that this final line is logically equivalent to $P \Rightarrow Q$.

Problem 4. *Problem 6, p54: Use the properties of addition and multiplication of real numbers given in Properties 2.3.1 (pp 18-19) to deduce that, for all real numbers a and b,*

(i) $a \times 0 = 0 = 0 \times a$
(ii) $(-a)b = -ab = a(-b)$
(iii) $(-a)(-b) = ab$

Solution 4. We solve the properties in turn, noting which of the properties on pages 18-19 we use in parentheses.

(i)

$$\begin{aligned}a \times 0 &= a \times (0+0) && (iv)\\ &= (a \times 0) + (a \times 0) && (iii)\end{aligned}$$

We now add $-(a \times 0)$ to each side to get

$$\begin{aligned}0 = (a \times 0) + (-(a \times 0)) &= ((a \times 0) + (a \times 0)) + (-(a \times 0))\\ &= (a \times 0) + ((a \times 0) + (-(a \times 0))) && (ii)\\ &= (a \times 0) + 0 && (vi)\\ &= (a \times 0) && (iv)\\ &= (0 \times a). && (i)\end{aligned}$$

(ii)

$$\begin{aligned}ab + (-a)b &= (a + (-a))b && ((iii) \text{ and } (i))\\ &= 0 \times b && (vi)\\ &= 0. && ((\text{by part (i)})\end{aligned}$$

Hence $(-a)b = -(ab)$ by the uniqueness property in (vi) and the proof that $a(-b) = -ab$ is similar.

(iii) We will make use of the previous parts of this question.

$$\begin{aligned} (-a)(-b) + (-a)b &= (-a)(-b+b) \\ &= (-a) \times 0 \qquad \text{(by part (i))} \end{aligned}$$

This means that $(-a)(-b) = -((-a)b))$ and since $-((-a)b) = ab$ by part (ii) and (vi), we have shown that $(-a)(-b) = ab$.

MAT200 SOLUTIONS 2

Problem 1. *Prove by contradiction that there is no largest integer. Hint: Suppose there were a largest integer n,...*

Proof. Suppose, to obtain a contradiction that n is the largest integer. Since n is an integer, the number $n+1$ is also an integer. However, since $n+1$ is an integer and $n+1 > n$, this contradicts the assumption that n is the largest integer. Hence there can be no largest integer. □

Problem 2. *Prove by contradiction that there is no smallest positive real number.*

Proof. To obtain a contradiction, assume that $\varepsilon > 0$ is the smallest positive real number. Then we see that

$$0 < \frac{\varepsilon}{2} < \varepsilon$$

which means that there exists a smaller positive real number than ϵ. This contradiction means there is no smallest positive real number. □

Problem 3. *Let a, b and c be positive integers. Show that if a divides b and a divides c then a divides $(b+c)$.*

Proof. Since a divides b, there exists an integer m such that $b = am$. Similarly, since a divides c, there exists an integer n such that $c = an$. Then

$$b + c = am + an = a(m+n).$$

Since $(m+n)$ is an integer (being the sum of two integers), we see that a divides $b+c$. □

Problem 4. *Use induction to prove Bernouilli's inequality. That is, for all integers $n \geq 1$ and all $x > -1$ we have*

$$(1+x)^n \geq 1 + nx.$$

Proof. We proceed by induction. Let $P(n)$ be the statement that $(1+x)^n \geq 1+nx$. for all $x > -1$. Then for $n = 1$ (the *base case*) we have

$$(1+x)^1 = 1 + x = 1 + (1)x$$

and so the statement (in the form of equality) holds. For the inductive step, assume the inductive hypothesis $P(k)$:

$$(1+x)^k \geq 1 + kx$$

for some integer $k \geq 1$ and for all $x > -1$. Then

$$\begin{aligned}
(1+x)^{k+1} &= (1+x)^k(1+x) \\
&\geq (1+kx)(1+x) && \text{(by the inductive hypothesis and since } x > -1\text{)} \\
&= 1 + (k+1)x + kx^2 \\
&\geq 1 + (k+1)x. && \text{(since } kx^2 \geq 0\text{)}
\end{aligned}$$

This final statement is $P(k+1)$, and so by the principle of mathematical induction, $P(n)$ is true for all positive integers n. □

MAT 200 HOMEWORK 3

Problem 1. Prove by induction that

$$\sum_{k=1}^{n}(k \cdot k!) = 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots = (n+1)! - 1$$

for all integers $n \geq 1$.

Solution 1. *Proof.* Clearly the statement holds for $n = 1$, since

$$1 \cdot 1! = 1 = 2 - 1 = 2! - 1.$$

Now suppose the proposition holds for $n = k$. Then we have

$$\sum_{i=1}^{k}(i \cdot i!) = (k+1)! - 1.$$

Hence we get

$$\begin{aligned}
\sum_{i=1}^{k+1}(i \cdot i!) &= \sum_{i=1}^{k}(i \cdot i!) + ((k+1) \cdot (k+1)!) \\
&= ((k+1)! - 1) + ((k+1) \cdot (k+1)!) \\
&= ((k+1)!)(1 + (k+1)) - 1 \\
&= (k+2)! - 1
\end{aligned}$$

Hence, by the principle of mathematical induction, the proposition is true for all $n \geq 1$. $\square$

Problem 2. Here are some attempted proofs by induction. Three are incorrect proofs of false facts. In these cases explain why the proof fails. In the remaining case, the proof is a faulty proof of a true fact. In this case you should repair the proof so that it correctly proves the stated proposition.

(a) *Proposition.* All cows are the same color.
Proof. We proceed by induction on the number of cows. First the base case: clearly one cow is the same color as itself, so the case for $n = 1$ is true. Now suppose that it is true for n cows. Consider a collection of $n+1$ cows. Removing one of them, we have n cows, which by the inductive hypothesis have the same color. Now add back in this cow and remove another one. Again, we have a collection of n cows and these are all the same color. So the cow we first removed is the same color as the other cows, which is the same color as the second cow we removed. Hence all $n+1$ cows are the same color and so we have proved the inductive step. Hence by the principle of mathematical induction, all cows are the same color.

(b) *Proposition.* $2 + 4 + \cdots + 2n = n(n+1)$.
Proof. If

$$2 + 4 + \cdots + 2n = n(n+1)$$

then

$$2 + 4 + \cdots + 2n + 2(n+1) = n(n+1) + 2(n+1) = (n+1)(n+2).$$

Hence by induction the formula is true for all n.

(c) *Proposition.* $1 + 3 + 5 + \cdots + (2n-1) = n^2 + 1$.
Proof. Assume it is true that

$$1 + 3 + 5 + \cdots + (2n-1) = n^2 + 1.$$

Then, adding $2n+1$ to both sides, we get

$$1 + 3 + 5 + \cdots + (2n-1) + (2n+1) = (n^2+1) + 2n + 1 = (n+1)^2 + 1.$$

This proves the inductive step. Hence by the principle of mathematical induction, the formula holds.

(d) *Proposition.* Suppose n straight lines are drawn on a circular disk, so that no three lines meet at the same point. Then these lines split the disk up into 2^n different regions.
Proof. Clearly, one line splits the disk into 2 regions, so the base step is true. Now suppose that the statement holds for n; that is, the n lines split the disk into 2^n regions. Then, if we add another line, this splits each region into two separate regions. Hence there are now $2 \times 2^n = 2^{n+1}$ regions. Thus, by the principle of mathematical induction, the result holds.

Solution 2. (a) The inductive step does not work for the case $n = 1$. This is because, when there are only two cows, the collections of cows under consideration do not have any cows in common (they each contain only one cow). Since there are no common elements, we cannot assert the cows all have the same color.

(b) This is almost correct. It just needs cleaning up and the base step needs adding.

Proof. The claim holds for $n = 1$ since

$$2 = 1 \times 2$$

Now suppose it holds for $n = k$. Then we get

$$\begin{aligned} 2 + 4 + \cdots + 2n + 2(n+1) &= n(n+1) + 2(n+1) && \text{(by the inductive hypothesis)} \\ &= (n+2)(n+1). \end{aligned}$$

Hence by induction, the proposition holds for all $n \geq 1$. □

(c) This is similar to the previous problem, except this time the base case is false! This is easily checked as for $n = 1$, we have $1 \neq 2 = 1^2 + 1$.

(d) Here, the logic in the inductive step is faulty. You can check this by attempting to go from the step $n = 2$ to $n = 3$; it is not true that the new line drawn must intersect each of the previous regions (indeed, it is impossible), and so the proof is not correct.

Problem 3. (Problem 17, p55.) For a positive integer n the number a_n is defined inductively by

$$\begin{aligned} a_1 &= 1 \\ a_{k+1} &= \frac{6a_k + 5}{a_k + 2} \qquad \text{for every positive integer } k \geq 1. \end{aligned}$$

Prove for all positive integers n that $0 < a_n < 5$.

Solution 3. *Proof.* Clearly the proposition holds for $n = 1$. To prove the inductive step, assume that $0 < a_k < 5$. We write

$$a_{k+1} = \frac{6a_k + 5}{a_k + 2} = \frac{6(a_k + 2) - 7}{a_k + 2} = 6 - \frac{7}{a_k + 2}.$$

By the inductive hypothesis, we get

$$0 < \frac{5}{2} = 6 - \frac{7}{2} < a_{k+1} < 6 - \frac{7}{7} = 5.$$

Hence by induction, the proposition holds. $\square$

Problem 4. (This is quite hard, so give yourself time to think about it). In this example, we use "forwards-backwards" induction. First, define the symbol

$$\prod_{i=1}^{n} x_i$$

inductively by

$$\begin{aligned} \prod_{i=1}^{1} x_i &= x_1 \\ \prod_{i=1}^{k+1} x_i &= \left(\prod_{i=1}^{k} x_i\right) \times x_{k+1} \qquad \text{for } k \geq 1. \end{aligned}$$

This means that $\prod_{i=1}^{n} x_i$ is the *product* of the numbers $x_1, \ldots, x_n$. We will prove that for all positive real numbers x_i and all $n \geq 1$

$$\frac{1}{n}\sum_{i=1}^{n} x_i \geq \left(\prod_{i=1}^{n} x_i\right)^{\frac{1}{n}}.$$

(i) Show that the statement holds for $n = 1$.
(ii) Using the fact that $(x + y)^2 \geq 0$, show that the statement holds for $n = 2$.
(iii) Show that if the statement holds for $n = 2^m$, then it also holds for $n = 2^{m+1}$ by using induction on m (*Hint*: you may need to use part (ii) at some point...). This is the forwards induction.
(iv) Show that if the statement is true for $n = k$, then it is also true for $n = k - 1$. To do this, given the numbers $x_1, \ldots, x_{k-1}$, define

$$x_k = \frac{x_1 + \cdots + x_{k-1}}{k - 1}.$$

Then, by the inductive hypothesis, we have

$$\frac{x_1 + \cdots + x_{k-1} + \frac{x_1 + \cdots + x_{k-1}}{k-1}}{k} = \sum_{i=1}^{k} x_i \geq \left(\prod_{i=1}^{k} x_i\right)^{\frac{1}{k}} = \sqrt[k]{x_1 \times \cdots \times x_{k-1} \times \frac{x_1 + \cdots x_{k-1}}{k - 1}}.$$

Proceed from here to prove the statement is true for $n = k - 1$. From this deduce that the statement is true for all $n \geq 1$.

Solution 4.

(i) This step is easy since both sides are equal to x_1.

(ii) Now, using the hint, we get (replacing y by $-x_2$)

$$0 \leq (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2$$

which means that

$$(x_1 + x_2)^2 = x_1^2 + 2x_1x_2 + x_2^2 \geq 4x_1x_2.$$

Taking square roots and rearranging this gives

$$\frac{x_1 + x_2}{2} \geq \sqrt{x_1x_2}$$

which is the statement for $n = 2$.

(iii) Assume the proposition holds for $n = 2^m$, so that

$$\frac{1}{2^m}\sum_{i=1}^{2^m} x_i \geq \left(\prod_{i=1}^{2^m} x_i\right)^{\frac{1}{2^m}}.$$

Then

$$\begin{aligned}
\frac{1}{2^{m+1}}\sum_{i=1}^{2^{m+1}} x_i &= \frac{1}{2^{m+1}}\left(\sum_{i=1}^{2^m} x_i + \sum_{i=1}^{2^m} x_{2^m+i}\right) \\
&= \frac{1}{2}\left(\frac{\sum_{i=1}^{2^m} x_i}{2^m} + \frac{\sum_{i=1}^{2^m} x_{2^m+i}}{2^m}\right) \\
\text{(inductive step)} \qquad &\geq \frac{1}{2}\left(\left(\prod_{i=1}^{2^m} x_i\right)^{\frac{1}{2^m}} + \left(\prod_{i=1}^{2^m} x_{2^m+i}\right)^{\frac{1}{2^m}}\right) \\
\text{(from the case } n=2\text{)} \qquad &\geq \sqrt{\left(\prod_{i=1}^{2^m} x_i\right)^{\frac{1}{2^m}}\left(\prod_{i=1}^{2^m} x_{2^m+i}\right)^{\frac{1}{2^m}}} \\
&= \left(\prod_{i=1}^{2^{m+1}} x_i\right)^{\frac{1}{2^{m+1}}}.
\end{aligned}$$

This proves the inductive step.

(iv) Suppose the statement is true for $n = k$. Following the hint, given the numbers $x_1, \ldots, x_{k-1}$, we define $x_k = \frac{x_1+\cdots+x_{k-1}}{k-1}$. Then

$$\frac{x_1 + \cdots + x_{k-1} + \frac{x_1+\cdots+x_{k-1}}{k-1}}{k} \geq \sqrt[k]{x_1 \cdots x_{k-1}\frac{x_1 + \cdots x_{k-1}}{k-1}}$$

Rewriting the left hand side, this becomes

$$\begin{aligned}
& \frac{x_1 + \cdots + x_{k-1}}{k-1} \geq \sqrt[k]{x_1 \cdots x_{k-1} \frac{x_1 + \cdots x_{k-1}}{k-1}} \\
\Leftrightarrow \quad & \left(\frac{x_1 + \cdots + x_{k-1}}{k-1}\right)^k \geq x_1 \cdots x_{k-1} \frac{x_1 + \cdots x_{k-1}}{k-1} \\
\Leftrightarrow \quad & \left(\frac{x_1 + \cdots + x_{k-1}}{k-1}\right)^{k-1} \geq x_1 \cdots x_{k-1} \\
\Leftrightarrow \quad & \frac{x_1 + \cdots + x_{k-1}}{k-1} \geq \sqrt[k-1]{x_1 \cdots x_{k-1}}.
\end{aligned}$$

This final line is

$$\frac{1}{k-1} \sum_{i=1}^{k-1} x_i \geq \left(\prod_{i=1}^{k-1} x_i\right)^{\frac{1}{k-1}}$$

which completes the proof.

MAT 200 HOMEWORK 4

Problem 1. Let A, B, C and D be sets.

(i) Prove that $A \cap A^c = \varnothing$.
(ii) Prove that $(A \cap B)^c = A^c \cup B^c$.
(iii) Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(iv) Prove that $A \cap (A \cup B) = A$.
(v) Prove that $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Solution 1.

Proof.

(i) Suppose that $x \in A \cap A^c$. Then $x \in A$ and $x \in A^c$. But this is impossible, so no such x can exist. Hence $A \cap A^c = \varnothing$.

(ii) *Proof of* $\subseteq$: Let $x \in (A \cap B)^c$. Then $x \notin A \cap B$ and so $x \notin A$ or $x \notin B$. This means that $x \in A^c$ or $x \in B^c$ and so $x \in A^c \cup B^c$.
Proof of $\supseteq$: Let $x \in A^c \cup B^c$. Then $x \in A^c$ or $x \in B^c$, and so $x \notin A$ or $x \notin B$. Hence $x \notin A \cap B$ and so $x \in (A \cap B)^c$.

(iii) *Proof of* $\subseteq$: Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B$ or C. This means that $x \in A$ and either $x \in B$ or $x \in C$, hence $x \in A$ and $x \in B$ or $x \in A$ and $x \in C$. But this means that $x \in (A \cap B) \cup (A \cap C)$.
Proof of $\supseteq$: Now suppose $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$, which means that either $x \in A$ and $x \in B$ or $x \in A$ and $x \in C$. Hence $x \in A$ and either $x \in B$ or $x \in C$, thus $x \in A$ and $x \in B \cup C$. It follows that $x \in A \cap (B \cup C)$.

(iv) From part (iii), we see that $A \cap (A \cup B) = (A \cap A) \cup (A \cap B) = A \cup (A \cap B)$. Clearly $A \subseteq A \cup (A \cap B)$. Now suppose that $x \in A \cup (A \cap B)$. Then $x \in A$ or $x \in A$ and $x \in B$. Hence $x \in A$ and $x \in B$; in particular, $x \in A$. Thus $A \cup (A \cap B) \subseteq A$ and so $A \cap (A \cup B) = A \cup (A \cap B) = A$.

(v)

$$\begin{aligned}
(x, y) \in (A \times B) \cap (C \times D) \quad &\Leftrightarrow \quad (x, y) \in A \times B \text{ and } (x, y) \in C \times D \\
&\Leftrightarrow \quad x \in A \text{ and } y \in B \text{ and } x \in C \text{ and } y \in D \\
&\Leftrightarrow \quad x \in A \text{ and } x \in C \text{ and } y \in B \text{ and } y \in D \\
&\Leftrightarrow \quad x \in A \cap C \text{ and } y \in B \cap D \\
&\Leftrightarrow \quad (x, y) \in (A \cap C) \times (B \cap D).
\end{aligned}$$

□

Problem 2. Let X be a set. Then, for subsets A, $B \in \mathcal{P}(X)$, define the symmetric difference of A and B to be

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Observe that $A \triangle B = B \triangle A$.

(i) Show that $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

(ii) Show that there exists a unique $E \in \mathcal{P}(X)$ such that, for all $A \in \mathcal{P}(X)$ we have $A \triangle E = A$.
(iii) For E as above, show that for all $A \in \mathcal{P}(X)$ there exists a unique set $B \in \mathcal{P}(X)$ such that $A \triangle B = E$.
(iv) Show that, for all A, $B \in \mathcal{P}(X)$, there exists a unique $C \in \mathcal{P}(X)$ such that $A \triangle C = B$.
(v) Let $X = \mathbb{Z}$, A be the set of even integers and B be the set of multiples of 3. Describe the set $A \triangle B$.

Solution 2.

(i) This is quite tricky, and perhaps the clearest way to see it is true is to use a truth table. Note that $x \in A \triangle B$ means that x is in exactly one of the two sets A and B. Then we can construct the table below.

$x \in A$	$x \in B$	$x \in C$	$x \in A \triangle B$	$x \in (A \triangle B) \triangle C$	$x \in B \triangle C$	$x \in A \triangle (B \triangle C)$
T	T	T	F	$\boldsymbol{T}$	F	$\boldsymbol{T}$
T	F	T	T	$\boldsymbol{F}$	T	$\boldsymbol{F}$
T	T	F	F	$\boldsymbol{F}$	T	$\boldsymbol{F}$
T	F	F	T	$\boldsymbol{T}$	F	$\boldsymbol{T}$
F	T	T	T	$\boldsymbol{F}$	F	$\boldsymbol{F}$
F	F	T	F	$\boldsymbol{T}$	T	$\boldsymbol{T}$
F	T	F	T	$\boldsymbol{T}$	T	$\boldsymbol{T}$
F	F	F	F	$\boldsymbol{F}$	F	$\boldsymbol{F}$

Since the two bold rows agree, the sets are equal.

(ii) Take $E = \varnothing$. Then for all $A \in \mathcal{P}(X)$ we have $A \triangle \varnothing = (A \setminus \varnothing) \cup (\varnothing \setminus A) = A \cup \varnothing = A$.
(iii) For every $A \in \mathcal{P}(X)$, we have $A \triangle A = (A \setminus A) \cup (A \setminus A) = \varnothing \cup \varnothing = \varnothing$.
(iv) Take $C = A \triangle B$. Then using parts (i), (ii) and (iii), we get

$$\begin{aligned} A \triangle C &= A \triangle (A \triangle B) \\ &= (A \triangle A) \triangle B \\ &= \varnothing \triangle B \\ &= B. \end{aligned}$$

(v) $A \triangle B$ is the set of all integers which are either multiples of 2 or multiples of 3 but which are not multiples of 6.

Problem 3. Prove or give a counterexample to the following statements.

(i) $\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R}, \quad xy > 0$.
(ii) $\exists x \in \mathbb{R} \quad \forall y \in \mathbb{R}, \quad xy > 0$.
(iii) $\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R}, \quad xy \geq 0$.
(iv) $\exists x \in \mathbb{R} \quad \forall y \in \mathbb{R}, \quad xy \geq 0$.
(v) $\forall n \in \mathbb{N} \quad (n$ is even or n is odd).
(vi) $(\forall n \in \mathbb{Z} \quad n$ is even) or $(\forall n \in \mathbb{Z} \quad n$ is odd).

Solution 3.

(i) This is false. If we take $x = 0$ then clearly for all $y \in \mathbb{R}$ we have $xy = 0$.
(ii) This is false. Given $x \in \mathbb{R}$, take $y = -x$. Then $xy = -x^2 \leq 0$.
(iii) This is true. Indeed, given $x \in \mathbb{R}$, we can take $y = x$. Then $xy = x^2 \geq 0$.
(iv) This is true. Take $x = 0$. Then for any choice of $y \in \mathbb{R}$ we have $xy = 0 \geq 0$.

(v) This is true, since if $n \in \mathbb{N}$ then either n is a multiple of 2 (in which case it is even) or it is not a multiple of 2 (in which case it is odd).

(vi) This is false. Notice this is of the form P or Q. The first statement is false since there exists an odd natural number (for example, 17). The second statement is false since there exists an even natural number (for example, 378). Hence the statement is false.

MAT 200 HOMEWORK 5

DUE IN CLASS ON 10/1

Problem 1. *Let X be a set. For each $A \in \mathcal{P}(X)$, define $\chi_A \colon X \to \{0,1\}$ by*

$$\chi_A(x) = \begin{cases} 0 & \text{if } x \notin A \\ 1 & \text{if } x \in A. \end{cases}$$

Suppose that $A, B \in \mathcal{P}(X)$.

(i) *Show that $\chi_A(x)\chi_B(x) = \chi_{A\cap B}(x)$*
(ii) *Show that $\chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x) = \chi_{A\cup B}(x)$.*
(iii) *Using the fact that $A \setminus B = A \cap B^c$ and $B^c = X \setminus B$, give a formula for $x \mapsto \chi_{A\setminus B}(x)$.*
(iv) *Find the set C so that $\chi_C(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x)$.*

Solution 1.

(i) By computing the four cases we get

$$\chi_A(x)\chi_B(x) = \begin{cases} 0 \times 0 = 0 & \text{if } x \notin A \text{ and } x \notin B \\ 1 \times 0 = 0 & \text{if } x \in A \text{ and } x \notin B \\ 0 \times 1 = 0 & \text{if } x \notin A \text{ and } x \in B \\ 1 \times 1 = 1 & \text{if } x \in A \text{ and } x \in B. \end{cases}$$

Thus $\chi_A(x)\chi_B(x) = 1$ if and only if $x \in A \cap B$, thus the required equality holds.

(ii) Notice that if $\chi_A(x) = 1$ then $\chi_{X\setminus A}(x) = 0$ and if $\chi_A(x) = 0$ then $\chi_{X\setminus A}(x) = 1$. Thus we get

$$\chi_{X\setminus A}(x) = 1 - \chi_A(x).$$

(iii) We make use of the previous two answers. We notice that since $A \setminus B = A \cap (X \setminus B)$, we get

$$\chi_{A\setminus B}(x) = \chi_{A\cap(X\setminus B)}(x) = \chi_A(x)\chi_{X\setminus B}(x) = \chi_A(x)(1 - \chi_B(x)).$$

(iv) We claim the set $C = A \cup B$. Again, computing the four cases

$$\chi_C(x) = \begin{cases} 0 + 0 - (0 \times 0) = 0 & \text{if } x \notin A \text{ and } x \notin B \\ 1 + 0 - (1 \times 0) = 1 & \text{if } x \in A \text{ and } x \notin B \\ 0 + 1 - (0 \times 1) = 1 & \text{if } x \notin A \text{ and } x \in B \\ 1 + 1 - (1 \times 1) = 1 & \text{if } x \in A \text{ and } x \in B. \end{cases}$$

Thus we see that $\chi_C(x) = 1$ if and only if $x \in A \cup B$, and so $C = A \cup B$.

Problem 2. *Let $f \colon X \to Y$ and $g \colon Y \to Z$. Prove that if f is injective and g is injective, then $g \circ f$ is injective.*

Solution 2.

Proof. We need to show that for $x_1, x_2 \in X$, then if $g(f(x_1)) = g(f(x_2))$ then $x_1 = x_2$. So suppose $g(f(x_1)) = g(f(x_2))$. By injectivity of g, this means that $f(x_1) = f(x_2)$. Moreover, the injectivity of f means that $x_1 = x_2$. Thus $g \circ f$ is injective. □

Problem 3. *Let $f\colon X \to Y$. Prove that f has a right inverse if and only if it is surjective.*

Solution 3.

Proof. Proof of $\Rightarrow$: Suppose f has a right inverse $g\colon Y \to X$ and let $y \in Y$. Consider the element $x_0 = g(y) \in X$. Then since g is a right inverse to f, we have $f(x_0) = f(g(y)) = y$. Thus there exists $x \in X$ such that $f(x) = y$. Since y was arbitrary, f is surjective.
Proof of $\Leftarrow$*:* Now suppose f is surjective. Then given $y \in Y$, there exists $x_0 \in X$ such that $f(x) = y$. So define $g(y) = x_0$. Then we get $f(g(y)) = f(x_0) = y$, and so g is a right inverse. □

Problem 4. *Let $f\colon X \to Y$. Show that for all $X_1, X_2 \in \mathcal{P}(X)$ and all $Y_1, Y_2 \in \mathcal{P}(X)$*

(i) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.
(ii) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

Solution 4.

(i) *Proof of* $\subseteq$: Let $y \in f(X_1 \cup X_2)$. Then there exists $x \in X_1 \cup X_2$ such that $f(x) = y$. So there exists $x \in X_1$ such that $f(x) = y$ or there exists $x \in X_2$ such that $f(x) = y$. Thus we have $y \in f(X_1)$ or $y \in f(X_2)$, and so $y \in f(X_1) \cup f(X_2)$.
Proof of $\supseteq$: Let $y \in f(X_1) \cup f(X_2)$. Then there exists $x \in X_1$ such that $f(x) = y$ or there exists $x \in X_2$ such that $f(x) = y$. Hence there exists $x \in X_1 \cup X_2$ such that $f(x) = y$ and so $y \in f(X_1 \cup X_2)$.

(ii)
$$\begin{aligned} x \in f^{-1}(Y_1 \cap Y_2) \quad &\Leftrightarrow \quad f(x) \in Y_1 \cap Y_2 \\ &\Leftrightarrow \quad f(x) \in Y_1 \text{ and } f(x) \in Y_2 \\ &\Leftrightarrow \quad x \in f^{-1}(Y_1) \text{ and } x \in f^{-1}(Y_2) \\ &\Leftrightarrow \quad x \in f^{-1}(Y_1) \cap f^{-1}(Y_2). \end{aligned}$$

MAT200 SOLUTIONS 6

Problem 1. *Let A be a set containing 10 positive integers less than 100 (so that $A \subset \mathbb{N}_{100}$ and $|A| = 10$). Using the pigeonhole principle, show that there exists two disjoint subsets of A which have the same sum. Here, the sum of a set is the sum of the elements in the set.*

Solution 1. Given 10 elements of $\mathbb{N}_{100}$, the largest possible sum for a subset is $91 + 92 + \cdots + 99 + 100 = 955$. Clearly, the smallest possible sum is 0 (the sum of the empty set). Hence there are at most 956 possible sums. However, the cardinality of $\mathcal{P}(A)$ is $2^{10} = 1024$, so there are 1024 subset sums. By the pigeonhole principle, there must be some sum which is obtained more than once (since $1024 > 956$). To show that we can pick the subsets to be disjoint, suppose there exists two subsets, X and Y with the same sum. Write $Z = X \cap Y$. Then $X \setminus Z$ and $Y \setminus Z$ will have the same sum, and by construction will be disjoint.

Problem 2. *Suppose X and Y are finite sets with $|X| = |Y|$. Show that a function $\phi\colon X \to Y$ is an injection if and only if it is a surjection.*

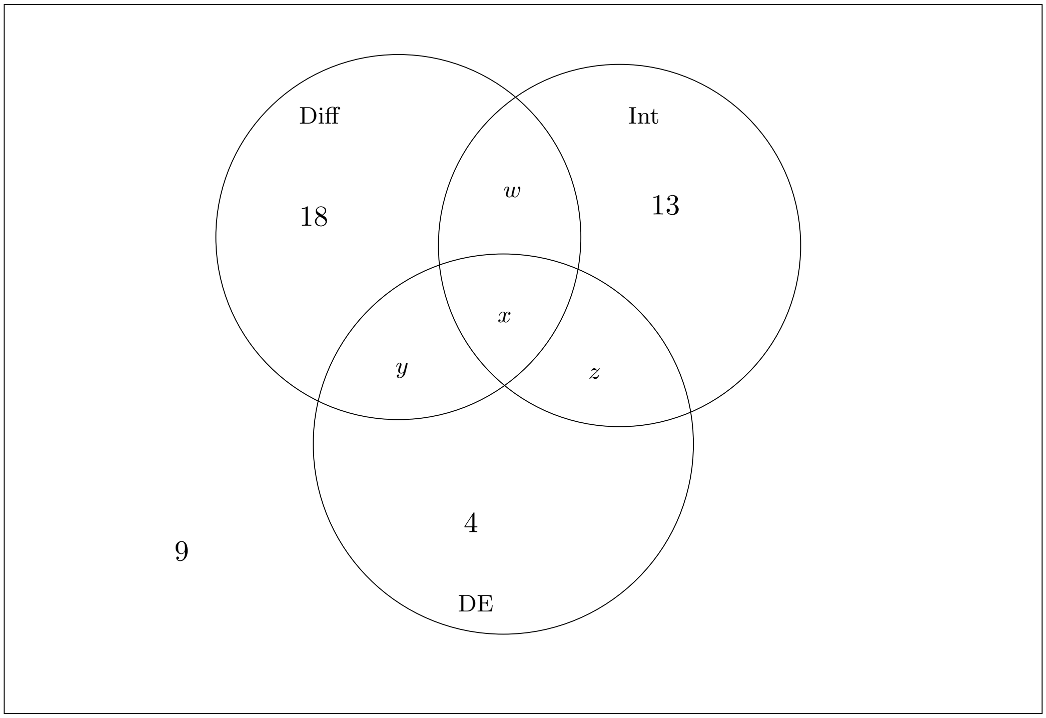
Solution 2. Suppose ϕ is an injection but not a surjection. Then there exists $y \in Y$ such that there is no $x \in X$ with $\phi(x) = y$. But then $\operatorname{im}(\phi) \subset Y$ and so $|\operatorname{im}(\phi)| < |Y| = |X|$. But by the pigeonhole principle, if $|\operatorname{im}(\phi)| < |X|$, there cannot be an injection $\phi\colon X \to \operatorname{im}$. This is a contradiction, so ϕ is a surjection.

Now suppose ϕ is a surjection but not an injection. Then there exists $x_1 \neq x_2$ in X such that $\phi(x_1) = \phi(x_2)$. Then we must have $|\operatorname{im}(\phi)| \leq |X| - 1 < |X| = |Y|$. But that must mean that $\operatorname{im}(\phi) \neq Y$ and so ϕ is not a surjection. This is a contradiction, so ϕ must be an injection.

Problem 3. *There are 164 students in a Calculus class. Of these, 110 like differentiation, 107 like integration and 94 like differential equations. Furthermore, 18 liked only differentiation, 13 liked only integration and 4 liked only differential equations. There were 9 students who did not like any of the topics. How many students liked all three topics? (*Hint: Draw a Venn diagram representing this problem. You should have four regions of unknown cardinality. Find four equations in these unknowns and solve them to find the required solution*).*

Solution 3. First we look at the suggested Venn diagram, labelling the unknown regions (see next page). Now, using the addition principle, and the information in the question, we get the following system of equations.

$$\begin{array}{rcccccccccl}
18 & + & w & + & x & + & y & & & = & 110 \\
13 & + & w & + & x & & & + & z & = & 107 \\
4 & + & & & x & + & y & + & z & = & 94 \\
(9+18+13+4) & + & w & + & x & + & y & + & z & = & 164
\end{array}$$



which simplifies to

$$\begin{array}{ccccccccc} w & + & x & + & y & & & = & 92 \\ w & + & x & & & + & z & = & 94 \\ & & x & + & y & + & z & = & 90 \\ w & + & x & + & y & + & z & = & 120 \end{array}$$

Using standard techniques, this solves to $w = 30$, $x = 26$, $y = 26$, $z = 28$. Since x represents the students who like all three topics, we see that 26 students like all three topics.

Problem 4. *Using induction on n, prove the general inclusion-exclusion principle for unions of finite sets: Let $A_1, A_2, \ldots, A_n$ finite sets. For each $I = \{i_1, i_2, \ldots i_r\} \subseteq \mathbb{N}_n$, denote*

$$A_I = \bigcap_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}.$$

Then

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\varnothing \neq I \subseteq \mathbb{N}_n} (-1)^{|I|-1} |A_I|$$

where the sum is taken over all non-empty subsets of $\mathbb{N}_n$.

Solution 4. *Proof.* For the base case $n = 1$, we just note that

$$\left| \bigcup_{i=1}^{1} A_i \right| = |A_1| = \sum_{I = \{1\}} (-1)^{|I|-1} |A_I|$$

Also, recall for $n = 2$, the inclusion-exclusion principle says that

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Now, for the inductive step, suppose that the formula holds for some $n = k$. Then we have

$$\left|\bigcup_{i=1}^{k} A_i\right| = \sum_{\varnothing \neq I \subseteq \mathbb{N}_k} (-1)^{|I|-1} |A_I|$$

where the sum is taken over all non-empty subsets of $\mathbb{N}_k$.

So now consider the union of $k+1$ sets, and make use of the case for the union of two sets:

$$\begin{aligned}
\left|\bigcup_{i=1}^{k+1} A_i\right| &= \left|\bigcup_{i=1}^{k} A_i \cup A_{k+1}\right| \\
&= \left|\bigcup_{i=1}^{k} A_i\right| + |A_{k+1}| - \left|\left(\bigcup_{i=1}^{k} A_i\right) \cap A_{k+1}\right|.
\end{aligned}$$

We consider this final term. First by the distributivity rule, we can write

$$\left|\left(\bigcup_{i=1}^{k} A_i\right) \cap A_{k+1}\right| = \left|\bigcup_{i=1}^{k} (A_i \cap A_{k+1})\right|.$$

Notice this is a union of k sets, and furthermore for $I = \{i_1, i_2, \ldots, i_r\}$

$$\bigcap_{i \in I} A_i \cap A_{k+1} = (A_{i_1} \cap A_{k+1}) \cap (A_{i_2} \cap A_{k+1}) \cap \cdots \cap (A_{i_r} \cap A_{k+1}) = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r} \cap A_{k+1} = A_I \cap A_{k+1}.$$

So we may use the inductive hypothesis

$$\left|\bigcup_{i=1}^{k} (A_i \cap A_{k+1})\right| = \sum_{\varnothing \neq I \subseteq \mathbb{N}_k} (-1)^{|I|-1} |A_I \cap A_{k+1}|.$$

This leads us to

$$\begin{aligned}
\left|\bigcup_{i=1}^{k+1} A_i\right| &= \left|\bigcup_{i=1}^{k} A_i \cup A_{k+1}\right| \\
&= \left|\bigcup_{i=1}^{k} A_i\right| + |A_{k+1}| - \left|\left(\bigcup_{i=1}^{k} A_i\right) \cap A_{k+1}\right| \\
&= \sum_{\varnothing \neq I \subseteq \mathbb{N}_k} (-1)^{|I|-1} |A_I| + |A_{k+1}| - \sum_{\varnothing \neq I \subseteq \mathbb{N}_k} (-1)^{|I|-1} |A_I \cap A_{k+1}| \\
&= \sum_{\varnothing \neq I \subseteq \mathbb{N}_k} (-1)^{|I|-1} |A_I| + |A_{k+1}| + \sum_{\varnothing \neq I \subseteq \mathbb{N}_k} (-1)^{|I|} |A_I \cap A_{k+1}|
\end{aligned}$$

Looking at this final expression, we see that the first term concerns intersections of all (non-empty) subsets of $\mathbb{N}_{k+1}$ which do not contain $k+1$ and the final two terms concern all (non-empty) subsets of $\mathbb{N}_{k+1}$ which contain $k+1$. So we are summing over all such subsets and so we get

$$\left|\bigcup_{i=1}^{k+1} A_i\right| = \sum_{\varnothing \neq I \subseteq \mathbb{N}_{k+1}} (-1)^{|I|-1} |A_I|$$

and so by the principle of mathematical induction, the result holds. $\square$

Problem 5. *Let X be a set and suppose $\phi\colon \mathbb{N} \to X$ is an injection. Prove that X is an infinite set.*

Solution 5. *Proof.* We assume X is finite and obtain a contradiction. Since X is finite, there exists $n \in \mathbb{N}$ for which there is a bijection $\psi\colon \mathbb{N}_n \to X$. Consider the map $\phi|_{\mathbb{N}_{n+1}}$. Since ϕ is an injection, so is $\phi|_{\mathbb{N}_{n+1}}$. Then the map $\psi^{-1} \circ \phi|_{\mathbb{N}_{n+1}} : \mathbb{N}_{n+1} \to \mathbb{N}_n$ is a composition of injections and so also an injection. But this is a contradiction of the pigeonhole principle, and so X must be infinite. $\square$

MAT200 SOLUTIONS 7

Problem 1. *Let $n \in \mathbb{N}$. Suppose that $A \subseteq \mathbb{N}_{2n}$ and $|A| = n+1$. Show that A must contain a pair of integers $a \neq b$ such that a divides b.*

Solution 1. Define the function $f\colon A \to \{1, 3, \ldots, 2n-1\}$ by defining $f(a)$ to be the largest odd divisor of a. Note that if $f(a) = m$ then $a = 2^k m$ for some $k \geq 0$. We note that the codomain has cardinality n, and so by the pigeonhole principle, there exists some value r such that there are $a < b$ in A with $f(a) = r = f(b)$. By the above remark, we have that there exists $k, j \geq 0$ such that $a = 2^k r$ and $b = 2^j r$. But then $b = (2^{j-k})a$, and so a divides b as required.

Problem 2. *Use the inclusion-exclusion principle from the last homework to show that the number of surjections from $\mathbb{N}_m$ to $\mathbb{N}_n$ is given by*

$$n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \cdots + (-1)^{n-1}\binom{n}{n-1}1^m.$$

*(*Hint*: In the inclusion-exclusion formula, define the set $A_i = \{f\colon \mathbb{N}_m \to \mathbb{N}_n \mid i \notin \mathrm{im}(f)\}$). From this, deduce that*

$$n^n - \binom{n}{1}(n-1)^n + \binom{n}{2}(n-2)^n - \cdots + (-1)^{n-1}\binom{n}{n-1}1^n = n!.$$

Solution 2. Take A_i as defined in the hint. Then if S is the set of surjections $f\colon \mathbb{N}_m \to \mathbb{N}_n$, we have

$$S = \mathrm{Fun}(\mathbb{N}_m, \mathbb{N}_n) \setminus \left(\bigcup_{i=1}^{n} A_i\right).$$

So we have $|S| = |\mathrm{Fun}(\mathbb{N}_m, \mathbb{N}_n)| - |\bigcup_{i=1}^n A_i|$. From the class, we know that $|\mathrm{Fun}(\mathbb{N}_m, \mathbb{N}_n)| = n^m$. To deal with the other term, we use the inclusion-exclusion principle. We have (see previous homework for the notation)

$$\begin{aligned}
\left|\bigcup_{i=1}^{n} A_i\right| &= \sum_{\varnothing \neq I \subseteq \mathbb{N}_n} (-1)^{|I|-1}|A_I| \\
&= \sum_{1 \leq i_1 \leq n} |A_{i_1}| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| \\
&\quad + \cdots + (-1)^{n-2} \sum_{1 \leq i_1 < \cdots < i_{n-1} \leq n} |A_{i_1} \cap \cdots \cap A_{i_{n-1}}| \quad + (-1)^{n-1} \quad |A_1 \cap \cdots \cap A_n|
\end{aligned}$$

Now notice that

$$A_{i_1} \cap \cdots \cap A_{i_r} = \{f \in \mathrm{Fun}(\mathbb{N}_m, \mathbb{N}_n) \mid \{i_1, \ldots, i_r\} \cap \mathrm{im}(f) = \varnothing\}.$$

So this is a set of maps from a set of cardinality m to a set of cardinality $(n-r)$, and so has cardinality $(n-r)^m$. Furthermore, the set $\{i_1, \ldots, i_r\} \subseteq \mathbb{N}_n$ is an r-subset: by definition there are

$\binom{n}{r}$ such subsets. Hence the sum above containing r intersections is equal to $\binom{n}{r}(n-r)^m$. Putting all this together gives

$$\left|\bigcup_{i=1}^{n} A_i\right| = \binom{n}{1}(n-1)^m - \binom{n}{2}(n-2)^m + \cdots + (-1)^{n-2}\binom{n}{n-2}(2)^m + (-1)^{n-1}\binom{n}{n-1}(1)^m.$$

Thus we have

$$|S| = n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \cdots + (-1)^{n-1}\binom{n}{n-1}1^m$$

as required.

To solve the second part, note that we already showed that the number of bijections $\phi\colon \mathbb{N}_n \to \mathbb{N}_n$ is $n!$. Furthermore, this is equal to the number of surjections from $\mathbb{N}_n$ to $\mathbb{N}_n$. Hence, by replacing m by n in the formula for $|S|$, we get

$$n^n - \binom{n}{1}(n-1)^n + \binom{n}{2}(n-2)^n - \cdots + (-1)^{n-1}\binom{n}{n-1}1^n = n!$$

Problem 3. *Prove there does not exist a rational number whose square is 6.*

Solution 3. Suppose that there is a rational number such that $x^2 = 6$, where $x = \frac{p}{q}$ when written in lowest terms . Then we have

$$6 = x^2 = \frac{p^2}{q^2}$$

and so we have

$$p^2 = 6q^2.$$

Since p^2 is a multiple of 6, it is in particular a multiple of 2, and so is even. Thus $p = 2r$ for some integer r. Hence we can now rewrite the second displayed equation as

$$4r^2 = 6q^2 \quad \text{and so} \quad 2r^2 = 3q^2.$$

In this final equation, the left hand side is clearly even, and so the right hand side must also be even. It follows that q^2 is even, and so q must also be even. But we have shown that both p and q are even, and so $x = \frac{p}{q}$ could not have been in the lowest terms. This contradiction shows that there is no rational whose square is 6.

Problem 4. *Find the rational numbers corresponding to the following infinite decimals.*

(1) $7.1032\overline{2194}$
(2) $234.915\overline{91}$
(3) $17.\overline{17}$

Solution 4.

(1) We split this number into an initial part and a recurring part:

$$a = 7.1032\overline{2194} = 7.1032 + 0.0000\overline{2194}.$$

Since the recurring string has length 4, we multiply a by 10^4 to get

$$10^4 a = 71032.2194 + 0.0000\overline{2194}.$$

Since $10^4 a$ and a have the same recurring part, we can subtract the latter from the former to get a finite decimal, which is a rational number. That is

$$9999a = 10^4 a - a = 71032.2194 - 7.1032 = 71025.1162 = \frac{710251162}{10000}.$$

Hence

$$a = \frac{710251162}{99990000} = \frac{355125581}{49995000}.$$

(2) We again split the number into initial and recurring parts:

$$b = 234.915 + 0.000\overline{91}.$$

The recurring string is length 2, so we multipy by 10^2 to get

$$100b = 23491.591 + 0.000\overline{91}$$

which yields

$$99b = 23491.591 - 234.915 = 23256.676 = \frac{23256676}{1000}.$$

Hence

$$b = \frac{23256676}{99000} = \frac{581469}{24750}.$$

(3) We follow the same method as before, so first we write (note it is best to avoid putting the integer part in the recurring part)

$$c = 17 + 0.\overline{17}$$

and so

$$100c = 1717 + 0.\overline{17}$$

which gives us

$$c = \frac{1700}{99}.$$

MAT200 SOLUTIONS 8

Problem 1. *Define inequality between two fractions by*

$$\frac{a_1}{b_1} < \frac{a_2}{b_2} \Leftrightarrow \begin{cases} a_1b_2 < a_2b_1 & \text{if } b_1b_2 > 0, \\ a_1b_2 > a_2b_1 & \text{if } b_1b_2 < 0. \end{cases}$$

Show that this definition is well-defined. Furthermore, show that this relation is transitive; that is

$$\frac{a_1}{b_1} < \frac{a_2}{b_2} \text{ and } \frac{a_2}{b_2} < \frac{a_3}{b_3} \Longrightarrow \frac{a_1}{b_1} < a_3b_3$$

Solution 1. Suppose that $\frac{a_1}{b_1}$ and $\frac{c_1}{d_1}$ represent the same rational number, and that $\frac{a_2}{b_2}$ and $\frac{c_2}{d_2}$. We need to show

$$\frac{a_1}{b_1} < \frac{a_2}{b_2} \Leftrightarrow \frac{c_1}{d_1} < \frac{c_2}{d_2}.$$

By assumption, we have

$$a_1d_1 = b_1c_1 \quad \text{and} \quad a_2d_2 = b_2c_2.$$

There are four cases here, depending on whether b_1b_2 and d_1d_2 are positive or negative. I outline a couple of the cases below, the other two are similar.

$b_1b_2 > 0, d_1d_2 > 0$. We get

$$\begin{aligned} \frac{a_1}{b_1} < \frac{a_2}{b_2} \quad &\Leftrightarrow \quad a_1b_2 < a_2b_1 \\ &\Leftrightarrow \quad a_1b_2d_1d_2 < a_2b_1d_1d_2 \\ &\Leftrightarrow \quad (a_1d_1)b_2d_2 < (a_2d_2)b_1d_1 \\ &\Leftrightarrow \quad (b_1c_1)b_2d_2 < (b_2c_2)b_1d_1 \\ &\Leftrightarrow \quad c_1d_2 < c_2d_1 \\ &\Leftrightarrow \quad \frac{c_1}{d_1} < \frac{c_2}{d_2}. \end{aligned}$$

$b_1b_2 < 0, d_1d_2 > 0$. We get

$$\begin{aligned} \frac{a_1}{b_1} < \frac{a_2}{b_2} \quad &\Leftrightarrow \quad a_1b_2 > a_2b_1 \\ &\Leftrightarrow \quad a_1b_2d_1d_2 > a_2b_1d_1d_2 \\ &\Leftrightarrow \quad (a_1d_1)b_2d_2 > (a_2d_2)b_1d_1 \\ &\Leftrightarrow \quad (b_1c_1)b_2d_2 > (b_2c_2)b_1d_1 \\ &\Leftrightarrow \quad c_1d_2 < c_2d_1 \\ &\Leftrightarrow \quad \frac{c_1}{d_1} < \frac{c_2}{d_2}. \end{aligned}$$

To show transitivity, we need to split into eight cases, depending on whether b_1, b_2 and b_3 are positive or negative. Below I consider the case where they are all positive; suitable amendments deal with the other cases. Assume $b_1, b_2, b_3 > 0$. Then since $\frac{a_1}{b_1} < \frac{a_2}{b_2}$ we have

$$a1b_2 < a_2b_1.$$

Similarly, since $\frac{a_2}{b_2} < \frac{a_3}{b_3}$ we have

$$a_2 b_3 < a_3 b_2.$$

This gives

$$a_1 b_2 < a_2 b_1 \quad \Rightarrow \quad a_1 b_2 b_3 < a_2 b_1 b_3 < a_3 b_2 b_1$$

from which it follows that

$$a_1 b_3 < a_3 b_1$$

and so $\frac{a_1}{b_1} < \frac{a_3}{b_3}$.

Problem 2. *Using the definition of an infinite decimal, prove that each finite decimal may be written as an infinite decimal in two different ways:*

$$\begin{aligned} a_0.a_1 a_2 \ldots a_{n-1} a_n &= a_0.a_1 a_2 \ldots a_{n-1} a_n \dot{0} \\ &= a_0.a_1 a_2 \ldots a_{n-1}(a_n - 1)\dot{9} \end{aligned}$$

where $a_n > 0$ if $n > 0$. From this, prove that every real number is represented by a unique infinite decimal unless it is represented by a finite decimal, in which case it is represented by precisely two infinite decimals as above.

Solution 2. Let $a = a_0.a_1 a_2 \ldots a_{n-1} a_n$ be a finite decimal and let $b_0.b_1 \ldots b_k \ldots$ be an infinite decimal representing a. By definition of an infinite decimal representing a, we must have for each k

$$b_0.b_1 \ldots b_k \le a_0.a_1 \ldots a_n \le b_0.b_1 \ldots b_k + \frac{1}{10^k}.$$

It follows from this that $b_i = a_i$ for $i = 0, \ldots n-1$.

Clearly the infinite decimal $a = a_0.a_1 a_2 \ldots a_{n-1} a_n \dot{0}$ represents a, since for each k we have

$$a_0.a_1 \ldots a_n \overbrace{0 \ldots 0}^{k \text{ zeroes}} \le a = a_0.a_1 \ldots a_n \le a_0.a_1 \ldots a_n \overbrace{0 \ldots 0}^{k \text{ zeroes}} + \frac{1}{10^{n+k}}.$$

Now consider the infinite decimal $a_0.a_1 \ldots a_{n-1}(a_n - 1)\dot{9}$. We clearly have for each k that

$$a_0.a_1 \ldots a_{n-1}(a_n - 1)\overbrace{9 \ldots 9}^{k \text{ nines}} \le a = a_0.a_1 \ldots a_n \le a_0.a_1 \ldots a_{n-1}(a_n - 1)\overbrace{9 \ldots 9}^{k \text{ nines}} + \frac{1}{10^{n+k}}$$

which means the decimal representation with recurring 9s must also represent a. Now suppose that $a_0.a_1 \ldots a_{n-1} c_n \ldots c_k \ldots$ is any other infinite decimal, then there will exist an integer $k > n$ such that

$$|a - a_0.a_1 \ldots a_{n-1} c_n \ldots c_k| > \frac{1}{10^k}.$$

For example, if $c_n = a_n$ and $c_{k-1} \neq 0$, the above must hold. A similar consideration takes care of the decimal ending in recurring 9s.

Now suppose that a is not represented by a finite decimal and that the two infinite decimals $a_0.a_1 \ldots a_n \ldots$ and $b_0.b_1 \ldots b_n \ldots$ both represent a. We prove by induction that $a_k = b_k$ for all k. For the base case, we note that since a does not have a finite representation, we must have $a_0 = b_0$. For the inductive step, suppose that for some $k \ge 0$ we have shown that $a_i = b_i$ for all $0 \le i \le k$. Suppose that $a_{k+1} < b_{k+1}$. Then

$$a_0.a_1 \ldots a_k a_{k+1} + \frac{1}{10^{k+1}} \le a_0.a_1 \ldots a_k b_{k+1}$$

But we must also have

$$a_0.a_1 \dots a_k a_{k+1} \leq a \leq a_0.a_1 \dots a_k a_{k+1} + \frac{1}{10^{k+1}}$$

and

$$a_0.a_1 \dots a_k b_{k+1} \leq a \leq b_0.b_1 \dots a_k b_{k+1} + \frac{1}{10^{k+1}}$$

This means that $a = a_0.a_1 \dots a_k(a_{k+1}+1)$. But this is a finite decimal, and this is a contradiction. Hence $a_{k+1} = b_{k+1}$. Hence by induction, both the infinite expansions agree.

Problem 3. *Show that the set of polynomials of degree n with rational coefficients is countably infinite. Using this, show that the set of algebraic numbers is countably infinite.*

Solution 3. First, we note that the set of polynomials of degree n is clearly infinite. To see that it is countable, note that the map

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n \mapsto (a_0, a_1, \dots, a_{n-1}, a_n) \in \mathbb{Q}^n$$

maps the set of polynomials of degree n with rational coefficients to a subset of the countably infinite set $\mathbb{Q}^n$ (we need to consider polynomials in the lowest terms, so this is not quite a bijection, but the above is enough). Hence the set of polynomials of degree n with rational coefficients is countably infinite. Now the union over all n is a countable union of countably infinite sets, and so is countably infinite.

For the algebraic numbers, note that such a number is the root of some polynomial with rational coefficients. Since each polynomial has finitely many roots, and there are countably infinite many such polynomials, it follows there are countably infinite many algebraic numbers.

Problem 4. *We exhibit another proof that $\mathbb{Q}$ is countably infinite. Using the map $\phi\colon \mathbb{Q} \to \mathbb{N}$, defined by*

$$\phi(q) = \begin{cases} 2^a 3^b & \text{if } q = \frac{a}{b}, \\ 2^a 3^b 5 & \text{if } q = -\frac{a}{b} \end{cases}$$

where $\frac{a}{b}$ is written in lowest terms and $a \geq 0$, $b > 0$, show that $|\mathbb{Q}| \leq |\mathbb{N}|$. Now show that $|\mathbb{N}| \leq |\mathbb{Q}|$ and deduce, by the Cantor-Schröder-Bernstein Theorem, that $|\mathbb{N}| = |\mathbb{Q}|$.

Solution 4. We first show that ϕ is an injection. Suppose $\phi(q_1) = \phi(q_2)$. Then $\frac{\phi(q_1)}{\phi(q_2)} = 1$, so they have the same factors, so that $\phi(q_1)$ is divisible by 2^a if and only if $\phi(q_2)$ is divisible by 2^a. The same holds for divisibility by 3^b and by 5. Hence if $\phi(q) = 2^a 3^b 5^c$ ($c \in \{0,1\}$) if and only if $q = (-1)^c \frac{a}{b}$. Thus we must have $q_1 = q_2$. This means $|\mathbb{Q}| \leq |\mathbb{N}|$. Moreover, the inclusion $\iota\colon \mathbb{N} \to \mathbb{Q}$ is an injection, and so $|\mathbb{N}| \leq |\mathbb{Q}|$. By the Cantor-Schröder-Bernstein Theorem, $|\mathbb{N}| = |\mathbb{Q}|$.

MAT200 SOLUTIONS 9

Problem 1. *Find the highest common factor of the following pairs a and b using the Euclidean algorithm.*

(a) $a = 442$ *and* $b = 255$
(b) $a = 924$ *and* $b = 560$
(c) $a = 532$ *and* $b = 285$
(d) $a = 3960$ *and* $b = 2541$

Solution 1.

(a) We repeatedly use the division algorithm to get

$$\begin{aligned}
442 &= (255 \times 1) + 187 \\
255 &= (187 \times 1) + 68 \\
187 &= (68 \times 2) + 51 \\
68 &= (51 \times 1) + 17 \\
51 &= (17 \times 3)
\end{aligned}$$

and so $\text{hcf}(442, 255) = 17$.

(b) As above, we compute

$$\begin{aligned}
924 &= (560 \times 1) + 364 \\
560 &= (364 \times 1) + 196 \\
364 &= (196 \times 1) + 168 \\
196 &= (168 \times 1) + 28 \\
168 &= (28 \times 6)
\end{aligned}$$

and so $\text{hcf}(924, 560) = 28$.

(c) The Euclidean algorithm gives

$$\begin{aligned}
532 &= (285 \times 1) + 247 \\
285 &= (247 \times 1) + 38 \\
247 &= (38 \times 6) + 19 \\
38 &= (19 \times 2)
\end{aligned}$$

and so $\text{hcf}(532, 285) = 19$.

(d) Finally, we compute

$$
\begin{aligned}
3960 &= (2541 \times 1) + 1419 \\
2541 &= (1419 \times 1) + 1122 \\
1419 &= (1122 \times 1) + 297 \\
1122 &= (297 \times 3) + 231 \\
297 &= (231 \times 1) + 66 \\
231 &= (66 \times 3) + 33 \\
66 &= (33 \times 2)
\end{aligned}
$$

and so $\mathrm{hcf}(3960, 2541) = 33$.

Problem 2. *By repeatedly using the division theorem, find the infinite decimal which represents the rational number* $\frac{4}{13}$ *(compare with problem 15.6 on p198).*

Solution 2. We use the division theorem to work out the decimals in the expansion of $\frac{4}{13}$. To find the first decimal place, note that $40 = (3 \times 13) + 1$, and so our first decimal place a_1 is $a_1 = 3$. We continue in this way to get

$$
\begin{aligned}
40 &= (3 \times 13) + 1 && \Rightarrow a_1 = 3 \\
10 &= (0 \times 13) + 10 && \Rightarrow a_2 = 0 \\
100 &= (7 \times 13) + 9 && \Rightarrow a_3 = 7 \\
90 &= (6 \times 13) + 12 && \Rightarrow a_4 = 6 \\
120 &= (9 \times 13) + 3 && \Rightarrow a_5 = 9 \\
30 &= (2 \times 13) + 4 && \Rightarrow a_6 = 2.
\end{aligned}
$$

The final remainder is 4, which means the next step will see us return to the same computation as the first step. Since this will then mean we repeat the pattern again, we see that $\frac{4}{13} = 0.\overline{307692}$.

Problem 3. *Prove that every infinite decimal representing a rational number is recurring (where we consider finite decimals to be ending with recurring* 0*s) and furthermore that if the fraction is written in lowest terms as* $\frac{a}{b}$ *then the number of recurring digits is less than* b.

Solution 3. Suppose we follow the same method as above. Then each application of the division theorem leaves some remainder r with $0 \leq r < b$. If $r = 0$ then we will ahve a finite decimal ending in recurring 0s. Otherwise, suppose that at each step $0 < r < b$ - and there are precisely $b - 1$ possible remainders. After b iterations of the above method, by the pigeonhole principle some remainder must have appeared twice, and so the pattern will be repeating. Since it is already repeating by the bth step, the total number of recurring digits must be strictly smaller than b.

Problem 4. *Let* u_n *be the* n*th Fibonacci number. Prove that the Euclidean algorithm takes exactly* n *steps to prove that* $\mathrm{hcf}(u_{n+1}, u_n) = 1$.

Solution 4. We proceed by induction. For the base case, note that the Euclidean algorithm takes one step to show that $\mathrm{hcf}(u_2, u_1) = \mathrm{hcf}(1, 1) = 1$. For the inductive step, suppose that for some $k \geq 1$ the Euclidean algorithm takes k steps to prove that $\mathrm{hcf}(u_{k+1}, u_k) = 1$. Then since

$$u_{k+2} = u_{k+1} + u_k$$

we see by the Division Theorem that $\mathrm{hcf}(u_{k+2}, u_{k+1}) = \mathrm{hcf}(u_{k+1}, u_k)$. Then, by the inductive hypothesis it takes k steps to prove $\mathrm{hcf}(u_{k+1}, u_k) = 1$. Hence we have seen it takes $k + 1$ steps to prove $\mathrm{hcf}(u_{k+2}, u_{k+1}) = 1$. This proofs the statement by induction.

Problem 5. *We define the* least common multiple *of non-zero integers a and b to be the unique positive integer m such that*

(i) *m is divisible by a and m is divisible by b,*
(ii) *If a divides n and b divides n then $m \leq n$.*

We write $m = \mathrm{lcm}(a, b)$.

(a) *Prove that if a divides n and b divides n then $\mathrm{lcm}(a, b)$ divides n. Deduce that $\frac{ab}{\mathrm{lcm}(a,b)}$ is an integer.*
(b) *Prove that $\frac{ab}{\mathrm{lcm}(a,b)}$ is a common divisor of a and b and hence $\frac{ab}{\mathrm{lcm}(a,b)} \leq \mathrm{hcf}(a, b)$.*
(c) *Prove that $\frac{ab}{\mathrm{hcf}(a,b)}$ is a common multiple of a and b. Now deduce that if a and b are positive, then*

$$\mathrm{hcf}(a, b)\mathrm{lcm}(a, b) = ab.$$

Solution 5.

(a) Suppose to obtain a contradiction that a divides n and b divides n but $\mathrm{lcm}(a, b)$ does not divide n. Then by the Division Theorem there exists integers q and r with $0 < r < \mathrm{lcm}(a, b)$ such that

$$n = \mathrm{lcm}(a, b) \times q + r.$$

By assumption a divides n and by definition a divides $\mathrm{lcm}(a, b)$, from which it follows that a divides r. Similarly, we can see that b divides r. This means that r is a common multiple of a and b. However, $r < \mathrm{lcm}(a, b)$, which is a contradiction since by definition $\mathrm{lcm}(a, b)$ is the least common multiple. Hence we see that $\mathrm{lcm}(a, b)$ divides n. In particular ab is a common multiple of a and b, and so the proposition applies to ab. Hence ab is divisible by $\mathrm{lcm}(a, b)$ and so $\frac{ab}{\mathrm{lcm}(a,b)}$ is an integer.

(b) We will show that

$$\frac{a}{\frac{ab}{\mathrm{lcm}(a,b)}}$$

is an integer. But this is easy since

$$\frac{a}{\frac{ab}{\mathrm{lcm}(a,b)}} = \frac{\mathrm{lcm}(a, b)}{b}$$

and clearly b divides $\mathrm{lcm}(a, b)$ by definition, so this final term is an integer and so $\frac{ab}{\mathrm{lcm}(a,b)}$ divides a. Similarly $\frac{ab}{\mathrm{lcm}(a,b)}$ divides b. Hence $\frac{ab}{\mathrm{lcm}(a,b)}$ is a common factor of a and b, so by definition $\frac{ab}{\mathrm{lcm}(a,b)} \leq \mathrm{hcf}(a, b)$, or equivalently $ab \leq \mathrm{lcm}(a, b)\mathrm{hcf}(a, b)$.

(c) Since $\mathrm{hcf}(a,b)$ is a factor of b, we see that

$$\frac{b}{\mathrm{hcf}(a,b)}$$

is an integer, and so

$$\frac{ab}{\mathrm{hcf}(a,b)} = a\frac{b}{\mathrm{hcf}(a,b)}$$

is a multiple of a, with a similar argument showing it is also a multiple of b. It follows that

$$\frac{ab}{\mathrm{hcf}(a,b)} \geq \mathrm{lcm}(a,b)$$

or equivalently

$$ab \geq \mathrm{lcm}(a,b)\mathrm{hcf}(a,b).$$

It follows from the results of parts (b) and (c) that

$$ab = \mathrm{lcm}(a,b)\mathrm{hcf}(a,b).$$

MAT200 SOLUTIONS 10

Problem 1. *Decide whether the following linear diophantine equations have a solution. If they do have a solution, find all such solutions to the equation.*

(a) $442m + 255n = 17$
(b) $924m + 560n = 84$
(c) $532m + 285n = 27$
(d) $3960m + 2541n = -132$

Solution 1.

(a) From the previous homework we know that $\mathrm{hcf}(442, 255) = 17$, and so the equation has a solution. To find a particular solution, we reverse the Euclidean algorithm:

$$\begin{aligned} 17 &= 68 - (51 \times 1) \\ &= 68 - ((187 - (68 \times 2)) \times 1) \\ &= (68 \times 3) - 187 \\ &= (((255 - (187 \times 1)) \times 3) - 187 \\ &= (255 \times 3) - (187 \times 4) \\ &= (255 \times 3) - ((442 - (255 \times 1)) \times 4) \\ &= (255 \times 7) - (442 \times 4). \end{aligned}$$

To now find all solutions, we need to solve the homogenous equation $442m + 255n = 0$. Dividing through by $\mathrm{hcf}(442, 255) = 17$, this means we need to solve

$$26m + 15n = 0,$$

which rearranges to

$$26m = -15n$$

Since 26 and 15 are coprime, we see that if n solves this equation then $n = 26q$ for some $q \in \mathbb{Z}$. Replacing this into the equation, it follows then that $m = -15q$ for the same $q \in \mathbb{Z}$. Hence the solutions of the homogenous equation are of the form

$$(m, n) = (-15q, 26q) \qquad \text{for some } q \in \mathbb{Z}.$$

Combining this with our particular solution above, our total set of solutions is the set of pairs (m, n)

$$(m, n) = (-4 - 15q, 7 + 26q) \qquad \text{for some } q \in \mathbb{Z}.$$

(b) This time we know that $\mathrm{hcf}(924, 560) = 28$ and since 28 divides 84, the equation has a solution. Again we can unpack the Euclidean algorithm to get

$$\begin{aligned}
28 &= 196 - 168 \\
&= 196 - (364 - 196) \\
&= (196 \times 2) - 364 \\
&= ((560 - 364) \times 2) - 364 \\
&= (560 \times 2) - (364 \times 3) \\
&= (560 \times 2) - ((924 - 560) \times 3) \\
&= (560 \times 5) - (924 \times 3).
\end{aligned}$$

So a particular solution to $924m + 560n = 84$ is

$$924 \times (-9) + 560 \times 15 = 84.$$

We now solve the homogenous equation which, after dividing through by $28 = \mathrm{hcf}(924, 560)$ is

$$33m + 20n = 0.$$

The set of solutions to this equation is given by pairs $(m, n) = (-20q, 33q)$ where $q \in \mathbb{Z}$. Hence our solution set is

$$S = \{(-9 - 20q, 5 + 33q) \mid q \in \mathbb{Z}\}.$$

(c) We know that $\mathrm{hcf}(532, 285) = 19$. Since 19 does not divide 27, this linear diophantine equation has no solutions.

(d) We computed $\mathrm{hcf}(3960, 2541) = 33$ and since $-132 = 33 \times (-4)$, a solution exists. Using our calculations in the Euclidean algorithm, we end up with the particular solution

$$3960 \times (-34) + 2541 \times 53 = 33$$

and so a solution to the original equation is

$$3960 \times 136 + 2541 \times (-212) = -132.$$

We solve the (simplified) homogenous equation to get

$$120m + 77n = 0 \quad \Leftrightarrow \quad (m, n) = (-77q, 120q) \text{ for some } q \in \mathbb{Z}.$$

It follows that our solution set is

$$S = \{(m, n) \in \mathbb{Z}^2 \mid m = 136 - 77q \text{ and } n = -212 + 120q \text{ for some } q \in \mathbb{Z}\}.$$

Problem 2. *Solve the linear diophantine equation*

$$6m + 10n + 15p = 1.$$

by defining $x = 3m + 5n$ and solving the resulting linear diophantine equation.

Solution 2. Using $x = 3m + 5n$, the equation becomes

$$2x + 15p = 1$$

We use the Euclidean algorithm on the pair $(15, 2)$ to get

$$\begin{aligned} 15 &= 2 \times 7 + 1 \\ 2 &= 1 \times 2 \end{aligned}$$

so that $\mathrm{hcf}(15, 2) = 1$. Undoing this gives a particular solution

$$(x, p) = (-7, 1)$$

We now solve the homogenous equation $2x + 15p = 0$, which is easily solved by $(x, p) = (-15q, 2q)$ for some $q \in \mathbb{Z}$. So the full set of solutions to $2x + 15p = 1$ is $(x, p) = (-7 - 15q, 1 + 2q)$ for some $q \in \mathbb{Z}$. We now need to solve the equation

$$3m + 5n = x = -7 - 15q$$

for some $q \in \mathbb{Z}$. In actual fact, we first solve $3m + 5n = -7$, and then solve $3m + 5n = -15q$. So again we apply the Euclidean algorith to get

$$\begin{aligned} 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + 1 \\ 2 &= 2 \times 1 \end{aligned}$$

from which we see (not that we didn't know this before!) that $\mathrm{hcf}(5, 3) = 1$, and this gives us a particular solution

$$3 \times (-14) + 5 \times (7) = -7.$$

We now solve the equation $3m+5n = -15q$. We could use our previous work on finding $\mathrm{hcf}(5, 3) = 1$ to write down the solution

$$3 \times (-30q) + 5 \times (15q) = -15q$$

but perhaps it is easier to notice that a solution is given by

$$3 \times (-5q) + 5 \times (0q) = -15q.$$

We now solve the homogenous equation to see that

$$3m + 5n = 0 \quad \Leftrightarrow \quad (m, n) = (-5r, 3r) \text{ for some } r \in \mathbb{Z}.$$

Hence the solution set to $3m + 5n = -7 - 15q$ is given by

$$(m, n) = (-14 - 5q - 5r, 7 + 3r).$$

Combining this with our previous solution gives the solutions to $6m + 10n + 15p = 1$ as the triples

$$(m, n, p) = (-14 - 5q - 5r, 7 + 3r, 1 + 2q)$$

for integers $q, r \in \mathbb{Z}$.

Problem 3. *Solve, if possible, the following linear diophantine equations.*

(a) $2m + 3n + 5p = 24$
(b) $2m + 6n + 8p = 17$
(c) $3m + 6n + 11p = 13$
(d) $6m + 15n + 21p = 33$

Solution 3. We use the same method as in Problem 2 to solve each of these equations. There are other equally good methods.

(a) First we define $x = 2m + 3n$ and so we need to solve $x + 5p = 24$. We apply the Euclidean algorithm to get $\mathrm{hcf}(5, 1) = 1$ (this takes only one step). We can write down the particular solution (this is not the only one of course)

$$(x, p) = (-1, 5).$$

We now solve the homogenous equation $x + 5p = 0$, which has solutions $(x, p) = (-5q, q)$ for $q \in \mathbb{Z}$, giving the general solution $(x, p) = (-1-5q, 5+q)$. We now need to solve in turn the equations $2m + 3n = -1$ and $2m + 3n = -5q$. Again $\mathrm{hcf}(3, 2) = 1$ and we can write down the respective particular solutions $(m, n) = (1, -1)$ and $(m, n) = (-q, -q)$, giving the solution set $(m, n) = (1 - q, -1 - q)$. The homogenous equation $2m + 3n = 0$ is solved by $(m, n) = (-3r, 2r)$ for some $r \in \mathbb{Z}$. Putting all this together means that we get the solution set for $2m + 3n = -1 - 5q$ is (for example)

$$(m, n) = (1 - q - 3r, -1 - q + 2r)$$

and so the solutions to the original equation are of the form

$$(m, n, p) = (1 - q - 3r, -1 - q + 2r, 5 + q)$$

for $q, r \in \mathbb{Z}$.

(b) The highest common factor of 2, 6 and 8 is 2, but this does not divide 17. Hence there are no solutions to this equation.

(c) Set $x = m + 2n$, so the new equation is $3x + 11p = 13$. The Euclidean algorithm yields

$$\begin{aligned} 11 &= 3 \times 3 + 2 \\ 3 &= 2 \times 1 + 1 \\ 2 &= 1 \times 2 \end{aligned}$$

and so $\mathrm{hcf}(11, 3) = 1$. Undoing the algorithm gives the particular solution $(x, p) = (-13, 52)$ (maybe you spotted the simpler solution $(2, -3)$ — it is perfectly fine if you did) and the homogenous equation is solved by $(x, p) = (-11q, 3q)$ for some $q \in \mathbb{Z}$. So we have the general solution

$$(x, p) = (-13 - 11q, 52 + 3q).$$

We now solve the equation $m + 2n = x = -13 - 11q$. Using the Euclidean algorithm (or another method) we find the solution $(m, n) = (-1-q, -6-5q)$. The homogenous equation is solved by $(m, n) = (-2r, r)$ for $r \in \mathbb{Z}$, giving the solution $(m, n) = (-1-q-2r, -6-5q+r)$ for $q, r \in \mathbb{Z}$. Now we can write down the solution set for the original equation as

$$S = \{(-1 - q - 2r, -6 - 5q + r, 52 + 3q) \mid q, r \in \mathbb{Z}\}.$$

(d) We write $x = 2m + 5n$. This gives us $3x + 21p = 33$ which we may simplify to $x + 7p = 11$. Using our favourite method we find the solution $(x, p) = (-3, 2)$ and the homogenous equation is solved by $(x, p) = (-7q, q)$, giving a general solution $(x, p) = (-3 - 7q, 2 + q)$. We now solve $2m + 5n = x = (-3 - 7q)$, which yields a general solution $(m, n) = (1 - q - 5r, -1 - q + 2r)$. Hence the general solution is

$$(m, n, p) = (1 - q - 5r, -1 - q + 2r, 2 + q)$$

for $q, r \in \mathbb{Z}$.

As a side note, you can ponder how you may solve a diophantine equation with 4 variables, or indeed a diophantine equation with n variables. How many free variabes would you expect if a solution exists?

Problem 4. *Let $n > 1$. Show that if there are no non-zero integer solutions to*

$$x^n + y^n = z^n$$

then there exists are no non-zero rational solutions. Hint: Maybe the contrapositive will help...

Solution 4. Suppose there exists a non-zero rational solution

$$(x, y, z) = \left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}\right).$$

Then we have

$$\left(\frac{a_1}{b_1}\right)^n + \left(\frac{a_2}{b_2}\right)^n = \left(\frac{a_3}{b_3}\right)^n.$$

Multiplying through to get a common denominator, we get

$$\left(\frac{a_1 b_2 b_3}{b_1 b_2 b_3}\right)^n + \left(\frac{a_2 b_1 b_3}{b_1 b_2 b_3}\right)^n = \left(\frac{a_3 b_1 b_2}{b_1 b_2 b_3}\right)^n$$

from which it follows that

$$(a_1 b_2 b_3)^n + (a_2 b_1 b_3)^n = (a_3 b_1 b_2)^n$$

is a non-zero integer solution to the problem.

Problem 4 concerns a very famous result you may have seen before, referred to as *Fermat's Last Theorem*. We of course know that (infinitely many) solutions exist when $n = 2$, and we call these Pythagorean triples. But it was an open problem whether any non-trivial integer solutions exist for $n > 2$. It was finally shown by Andrew Wiles in the late 20th Century that no solutions exist. The simplicity of the statement and the difficulty of the proof is just one of the many intriguing facets of mathematics!

MAT 200 HOMEWORK 11

DUE IN CLASS ON 12/3

Problem 1. *Solve the following linear congruences.*

(a) $154x \equiv 24 \mod 819$
(b) $231x \equiv 147 \mod 598$
(c) $156x \equiv 42 \mod 252$
(d) $9x \equiv 0 \mod 21$

Solution 1.

(a) By using the Euclidean Algorithm, we see that $\mathrm{hcf}(154, 819) = 7$. Since 7 does not divide 24, there are no solutions.

(b) First note that 231 and 147 are divisible by 3 and 3 does not divide 598, we can reduce this problem to

$$77x \equiv 49 \mod 598.$$

We now use the Euclidean Algorithm to compute $\mathrm{hcf}(77, 598)$:

$$\begin{aligned} 598 &= (77 \times 7) + 59 \\ 77 &= (59 \times 1) + 18 \\ 59 &= (18 \times 3) + 5 \\ 18 &= (5 \times 3) + 3 \\ 5 &= (3 \times 1) + 2 \\ 3 &= (2 \times 1) + 1 \end{aligned}$$

which gives $\mathrm{hcf}(77, 598) = 1$, and the equation certainly has a (unique!) solution. Now we unpack the algorithm to get

$$233 \times 77 - 30 \times 598 = 1$$

which gives the solution $x = 233$ to the linear congruence $77x \equiv 1 \mod 598$. Hence the solution to $77x \equiv 49 \mod 598$ is $x \equiv 233 * 49 \equiv 55 \mod 598$. So our solution is $x \equiv 55 \mod 598$.

(c) First we can reduce by dividing through by 6, which means we are looking for solutions to

$$26x \equiv 7 \mod 42.$$

However, notice that $\mathrm{hcf}(26, 42) = 2$, but this does not divide 7. Hence there are no solutions to this linear congruence.

(d) The congruence can be reduced to

$$3x \equiv 0 \mod 7$$

and then

$$x \equiv 0 \mod 7$$

which yields the solutions $x \equiv 0 \mod 21$, $x \equiv 7 \mod 21$ and $x \equiv 14 \mod 21$.

Problem 2.

(a) *What is the final digit of* 3^{2014}*?*
(b) *What is the final digit of* 73^{2014}*?*
(c) *What is the final digit of* 2^{2014}*?*
(d) *What is the final digit of* 146^{2014}*?*

Solution 2.

(a) It is easy to check that $3^4 \equiv 1 \mod 10$, and so it follows that

$$3^{2014} \equiv 3^{2012} \times 3^2 \equiv (3^4)^{503} \times 3^2 \equiv 1^{503} \times 9 \equiv 9 \mod 10.$$

(b) Since $3 \equiv 73 \mod 10$, the solution is the same as the above: $73^{2014} \equiv 9 \mod 10$.

(c) This time, we note that we have the following sequence

$$2^1 \equiv 2 \mod 10,\ 2^2 \equiv 4 \mod 10,\ 2^3 \equiv 8 \mod 10,\ 2^4 \equiv 6 \mod 10,\ 2^5 \equiv 2 \mod 10, \ldots$$

and the pattern repeats, so that $2^{4n+1} \equiv 2 \mod 10$. Then we can compute

$$2^{2014} \equiv 2^{2013} \times 2 \equiv 2^{(4\times 503)+1} \times 2 \equiv 2 \times 2 \equiv 4 \mod 10.$$

(d) $146^{2014} \equiv (2 \times 3)^{2014} \equiv 2^{2014} \times 3^{2014} \equiv 4 \times 9 \equiv 36 \equiv 6 \mod 10$.

Problem 3. *Compute the inverse of* 204 *modulo* 367*. Using this, solve the following linear congruences.*

(a) $204x \equiv 4 \mod 367$
(b) $204x \equiv 11 \mod 367$
(c) $204x \equiv 99 \mod 367$
(d) $204x \equiv 9 \mod 367$

Solution 3. We begin by finding the inverse of 204 modulo 367, which requires us to solve $204x \equiv 1 \mod 367$. To do this, we use the method of linear diophantine equations to convert the problem to finding $x, y \in \mathbb{Z}$ solving

$$204x + 367y = 1.$$

Of course, we use the Euclidean Algorithm to first find $\text{hcf}(204, 367)$.

$$\begin{aligned}
367 &= (204 \times 1) + 163 \\
204 &= (163 \times 1) + 41 \\
163 &= (41 \times 3) + 40 \\
41 &= (40 \times 1) + 1
\end{aligned}$$

Hence $\text{hcf}(204, 367) = 1$ (as the question implied, since otherwise an inverse would not exist). We now unpack the algorithm to find x, which will be the inverse of 204. The solution we find is $x = 9$ (and $y = 5$, but this is not important for the linear congruence case). We can now solve the linear congruences in the question.

(a) $204x \equiv 4 \mod 367 \Leftrightarrow 9 \times 204x \equiv 9 \times 4 \mod 367 \Leftrightarrow x \equiv 36 \mod 367.$
(b) $204x \equiv 11 \mod 367 \Leftrightarrow 9 \times 204x \equiv 9 \times 11 \mod 367 \Leftrightarrow x \equiv 99 \mod 367.$
(c) $204x \equiv 99 \mod 367 \Leftrightarrow 9 \times 204x \equiv 9 \times 99 \mod 367 \Leftrightarrow x \equiv 891 \equiv 157 \mod 367.$
(d) $204x \equiv 4 \mod 367 \Leftrightarrow 9 \times 204x \equiv 9 \times 9 \mod 367 \Leftrightarrow x \equiv 81 \mod 367.$

Problem 4. *Prove that the Fibonacci number u_n is divisible by 3 if and only if n is divisible by 4.*

Solution 4. We consider the first few terms in the Fibonacci sequence.

$$\begin{aligned}
1 &\equiv 1 \mod 3 \\
1 &\equiv 1 \mod 3 \\
2 &\equiv 2 \mod 3 \\
3 &\equiv 0 \mod 3 \\
5 &\equiv 2 \mod 3 \\
8 &\equiv 2 \mod 3 \\
13 &\equiv 1 \mod 3 \\
21 &\equiv 0 \mod 3 \\
34 &\equiv 1 \mod 3 \\
55 &\equiv 1 \mod 3
\end{aligned}$$

We see that in general, since the pattern will repeat, $u_{k+8n} \equiv u_k \mod 3$ for $1 \leq k \leq 8$ (this can be checked by a simple but laborious induction argument on n). Since $u_4 \equiv 0 \mod 3$ and $u_8 \equiv 0 \mod 3$, but $u_k \not\equiv 0 \mod 3$ for $k = 1, 2, 3, 5, 6, 7$, the statement follows.

PRACTICE QUESTIONS FOR MIDTERM I - SOLUTIONS

MAT 200 - FALL 2014

Question 1. *Use a truth table to show that P is equivalent to (not P) $\Rightarrow C$, where C is a contradiction.*

Solution 1. Note that the contradiction C is always false, by definition.

P	(not P)	C	(not P) $\Rightarrow C$
$\boldsymbol{T}$	F	F	$\boldsymbol{T}$
$\boldsymbol{F}$	T	F	$\boldsymbol{F}$

Since the bold rows agree, the two statements are logically equivalent.

Question 2. *Use a truth table to show that $P \Rightarrow Q$ and $(P$ or $Q) \Leftrightarrow Q$ are equivalent.*

Solution 2.

P	Q	$P \Rightarrow Q$	(P or Q)	(P or Q) $\Rightarrow Q$	(P or Q) $\Leftarrow Q$	(P or Q) $\Leftrightarrow Q$
T	T	$\boldsymbol{T}$	T	T	T	$\boldsymbol{T}$
T	F	$\boldsymbol{F}$	T	F	T	$\boldsymbol{F}$
F	T	$\boldsymbol{T}$	T	T	T	$\boldsymbol{T}$
F	F	$\boldsymbol{T}$	F	T	T	$\boldsymbol{T}$

Again, since the bold columns agree, the two statements are logically equivalent.

Question 3. *Prove that if $x \in \mathbb{R}$ and $x^2 \geq 5x$ then $x \geq 5$ or $x \leq 0$.*

Solution 3. *Proof.* Suppose $x^2 \geq 5x$ and assume $x > 0$ (if $x \leq 0$ we are done). Since $x > 0$, we can multiply both sides of the first inequality to get $x \geq 5$. □

Question 4. *Prove that if $a \in \mathbb{R}$ then one of $\sqrt{5} - a$ and $\sqrt{5} + a$ is irrational.*

Solution 4. Let $a \in \mathbb{R}$. Suppose, to obtain a contradiction, that both $\sqrt{5} - a$ and $\sqrt{5} + a$ are rational. Then the sum $(\sqrt{5} - a) + (\sqrt{5} + a) = \sqrt{5}$ is a sum of rational numbers and so is rational. But $\sqrt{5}$ is irrational. This is a contradiction, so we conclude one of $\sqrt{5} - a$ and $\sqrt{5} + a$ must be irrational.

Question 5. *Show for all $n \in \mathbb{N}$ that*

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

Solution 5. *Proof.* We proceed by induction on n. First the base case. If $n = 1$ then we get

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

Now, for the inductive step, suppose the formula holds for some $k \geq 1$. Then

$$\begin{aligned}
\sum_{i=1}^{k+1} \frac{1}{i(i+1)} &= \sum_{i=1}^{k} \frac{1}{i(i+1)} + \frac{1}{(k+1)(k+2)} \\
&= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\
&= \frac{k(k+2)+1}{(k+1)(k+2)} \\
&= \frac{(k+1)^2}{(k+1)(k+2)} \\
&= \frac{k+1}{k+2}
\end{aligned}$$

Hence, the formula holds by induction. □

Question 6. *Show for all $n \in \mathbb{N}$ that $n^3 - n$ is divisible by 3.*

Solution 6. *Proof.* We proceed by induction on n. First, note that for $n = 1$, we have $n^3 - n = 1^3 - 1 = 0$, and 0 is divisible by 3. Now for the inductive step, assume that for some $k \geq 1$, the statement holds. So now consider

$$(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = n^3 + 3n^2 + 2n = (n^3 - n) + 3(n^2 + n)$$

This last expression is the sum of two things which are divisible by 3, and so is divisible by 3. Hence the statement holds by induction. □

Question 7. *Let A, B, C be sets. Show that $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.*

Solution 7. *Proof.*

$$\begin{aligned}
A \setminus (B \setminus C) &= A \cap (B \setminus C)^c \\
&= A \cap (B \cap C^c)^c \\
&= A \cap (B^c \cup C) \\
&= (A \cap B^c) \cup (A \cap C) \\
&= (A \setminus B) \cup (A \cap C).
\end{aligned}$$

□

Question 8. *Prove that if X is a universal set and $A, B \subseteq X$, then $A \subseteq B \Leftrightarrow B^c \subseteq A^c$.*

Solution 8. *Proof.* This is actually very simple. Recall that $A \subseteq B$ means

$$x \in A \quad \Longrightarrow \quad x \in B.$$

Now, this is equivalent to its contrapositive, which is

$$x \notin B \quad \Longrightarrow \quad x \notin A$$

which is the statement $B^c \subseteq A^c$. $\square$

Question 9. *Write the negation of $\forall\, x \in \mathbb{N}, \exists\, y \in \mathbb{N}, y = x - 1$. Is the original statement true? Prove or give a counterexample.*

Solution 9. The negation to this statement is

$$\exists\, x \in \mathbb{N}, \forall\, y \in \mathbb{N}, y \neq x - 1.$$

The original statement is false (and so the negation is true). To see this, take $x = 1 \in \mathbb{N}$. Then there is no element y of $\mathbb{N}$ such that $y = x - 1$, since 1 is the smallest element of $\mathbb{N}$.

Question 10. *Let $\mathcal{C}$ be the set of circles in $\mathbb{R}^2$: that is $\mathcal{C} = \{C \subset \mathbb{R}^2 \mid C \text{ is a circle}\}$. Also, define $R\colon \mathcal{C} \to \mathbb{R}$ by $R(C) =$ "Radius of C". For each of the following statements, either prove them or give a counterexample.*

(i) $\forall C_1 \in \mathcal{C}, \forall C_2 \in \mathcal{C}, C_1 \cap C_2 = \varnothing$.
(ii) $\exists x \in \mathbb{R}, \forall C \in \mathcal{C}, R(C) = x$.
(iii) $\forall C \in \mathcal{C}, \exists x \in \mathbb{Z}, R(C) = x$.

Solution 10.

(i) This is false. Consider the circle C_1 with equation $x^2 + y^2 = 1$ and the circle C_2 with equation $(x-2)^2 + y^2 = 1$. Then $(1, 0) \in C_1 \cap C_2$.
(ii) This is false. Let $x \in \mathbb{R}$. Then for $r \neq x$, consider the circle C given by the equation $x^2 + y^2 = r^2$. Then $R(C) = r \neq x$.
(iii) This is false. Consider the circle C with equation $x^2 + y^2 = \pi^2$. Then $R(C) = \pi \notin \mathbb{Z}$.

Question 11. *Give an example of a map $f\colon \mathbb{N} \to \mathbb{N}$ which is an injection but not a surjection.*

Solution 11. There are many options here. For example, $f(n) = 2n$ is an injection but not a surjection. To show this, note that if $f(n) = r = f(m)$, then $2n = r = 2m$, and so $n = m$. Furthermore, there does not exist n such that $f(n) = 3$, since 3 is odd.

Question 12. *Give an example of a map $f\colon \mathbb{N} \to \mathbb{N}$ which is a surjection but not an injection.*

Solution 12. Again, there are many options here. For example, define

$$f(n) = \begin{cases} 5 & \text{if } n = 1 \\ n - 1 & \text{if } n > 1 \end{cases}$$

Then f is a surjection since for all $n \in \mathbb{N}$, we have $f(n+1) = n$. However, it is not an injection since $f(1) = 5 = f(6)$.

Question 13. *Let $f\colon X \to Y$ and $g\colon Y \to Z$. If f is an injection and $g \circ f$ is an injection, must g be an injection? Prove or give a counterexample.*

Solution 13. This is false. Let $X = \{1, \}, Y = \{a, b\}$ and $Z = \{z\}$. Now define f by $f(1) = a$, and g by $g(a) = g(b) = z$. Clearly f is an injection (since X contains only one element) and $g \circ f\colon X \to Z$ is defined by $g \circ f(1) = z$, so is also an injection. However, g is not an injection, since $g(a) = g(b)$.

Question 14. *Let $f\colon X \to Y$ and $g\colon Y \to Z$. If f is a surjection and $g \circ f$ is a surjection, must g be a surjection? Prove or give a counterexample.*

Solution 14. This is true. Indeed, we don't actually need the condition on f being a surjection!

Proof. Suppose g is not a surjection. Then there exists $z \in Z$ such that there is no $y \in Y$ with $g(y) = y$. But then there cannot exists $x \in X$ such that $g(f(x)) = z$, since otherwise $f(x) \in Y$ and so cannot map to z by our assumption. Hence our assumption that g was not a surjection is false and so g must be a surjection. $\square$

Please let me know if you find any mistakes in this document! Best of luck to everyone for the Midterm!

PRACTICE QUESTIONS FOR MIDTERM II - SOLUTIONS

MAT 200 - FALL 2014

Question 1. Express the following recurring decimals as rational numbers.

(a) $2.71\overline{828}$
(b) $2.345\overline{67}$
(c) $1.23\overline{45} + 2.4\overline{19}$

Solution 1.

(a) We have

$$a = 2.71\overline{828} = 2.71 + 0.00\overline{828}$$

and so

$$1000a = 2718.28 + 0.00\overline{828}.$$

Hence

$$999a = 2715.57 = \frac{271557}{100}$$

and so

$$a = \frac{271557}{99900}.$$

(b) We have

$$b = 2.345\overline{67} = 2.345 + 0.000\overline{67}$$

and so

$$100b = 234.567 + 0.000\overline{67}.$$

Simple arithmetic then gives

$$b = \frac{232222}{99000}.$$

(c) There are two ways of computing this. We could work out the fraction for each term separately, then add them, or we can compute the recurring fraction corresponding to this sum. We follow the second method - you can check the first method leads to the same solution. So first we compute

$$c = 1.23\overline{45} + 2.4\overline{19} = 3.65\overline{37} = 3.65 + 0.00\overline{37}$$

which gives

$$100c = 365.37 + 0.00\overline{37}.$$

Now a simple computation gives

$$c = \frac{36172}{9900}.$$

Question 2. Show that if A and B are finite sets, then if $A \subset B$ we have

$$\min B \leq \min A$$

Solution 2. This is very easy. Let $b_0 = \min B$ and $a_0 = \min A$. By definition we have $b_0 \leq b$ for all $b \in B$. Since $A \subset B$ it follows that $b_0 \leq a$ for all $a \in A$ and so in particular since $a_0 \in A$ we have $b_0 \leq a_0$.

Question 3. Let X and Y be finite sets with $|X| < |Y|$. Show there does not exist a surjection $\phi\colon X \to Y$.

Solution 3. Suppose there exists a surjection $\phi\colon X \to Y$. Then there exists a right inverse $g\colon Y \to X$ of ϕ. By definition, we have $f(g(y)) = y$ for all $y \in Y$. Suppose that $g(y_1) = g(y_2)$. Then since $y_1 = f(g(y_1)) = f(g(y_2)) = y_2$, it follows that g is an injection. But this mean we have an injection $g\colon Y \to X$ whilst $|Y| > |X|$. This is a contradiction to the pigeonhole principle.

Question 4. Let $X = \{x_1, x_2, x_3, x_4\}$ and $Y = \{y_1, y_2, y_3, y_4, y_5\}$.

(a) How many maps are there $f\colon X \to Y$?
(b) How many maps are there $f\colon Y \to X$?
(c) What is $|\{f \in \mathrm{Fun}(X, Y) \mid y_4 \notin \mathrm{im} f\}|$?

Solution 4.

(a) $|\mathrm{Fun}(X, Y)| = |Y|^{|X|} = 5^4 = 625$.
(b) $|\mathrm{Fun}(Y, X)| = |X|^{|Y|} = 4^5 = 1024$.
(c) We can consider this set to be the set of functions $\mathrm{Fun}(X, \{y_1, y_2, y_3, y_5\})$, which has cardinality $4^4 = 256$.

Question 5. Suppose we pick 17 elements from the set $\mathbb{N}_{32}$. Show that we must have picked a pair of integers whose sum is 33.

Solution 5. We note there are 16 pairs in $\mathbb{N}_{32}$ whose sum adds up to 33. These are $\{1, 32\}, \{2, 31\}, \ldots, \{15, 18\}, \{16, 17\}$. Since we pick 17 elements, the pigeonhole principle ensures that one of these pairs will have both elements picked, and so there exists a pair of integers whose sum adds to 33.

Question 6. Four people visit a restaurant and each choose one meal from a choice of seven on the menu.

(a) How many possible combinations are there if we record who chose which dish?
(b) How many possible combinations are there if we do not record who chose each dish?
(c) How many possible combinations are there if we record who chose which dish and each person chose a different dish from everyone else?

Solution 6. (a) This can be thought of as the set of functions from a four element set to a seven element set. Thus the number of possible combinations is $7^4 = 2401$.

(b) This is a bit trickier, since repetitions are possible. We identify the menu with the set $Y = \{y_1, y_2, y_3, y_4, y_5, y_6, y_7\}$. Then all the possible combinations we are considering are of the form $(y_{i_1}, y_{i_2}, y_{i_3}, y_{i_4},)$ where $i_1 \leq i_2 \leq i_3 \leq i_4$. So each choice corresponds to a quadruple (i_1, i_2, i_3, i_4) with $i_1 \leq i_2 \leq i_3 \leq i_4$. We now consider the bijection ϕ from 4-tuples to $\mathcal{P}_4(\mathbb{N}_{10})$ given by

$$\phi((i_1, i_2, i_3, i_4)) = \{i_1, i_2 + 1, i_3 + 2, i_4 + 3\}.$$

Since $|\mathcal{P}_4(\mathbb{N}_{10})| = \frac{10!}{6!4!} = 210$, it follows that the total number of combinations is also 210.

(c) This can be thought of as the set of injections from a four element set to a seven element set. The cardiality of this is $7 \times 6 \times 5 \times 4 = 840$.

Question 7. Suppose $X \cap Y = \varnothing$. Show that the function

$$f \colon \bigcup_{i=0}^{k} \mathcal{P}_i(X) \times \mathcal{P}_{k-i}(Y) \to \mathcal{P}_k(X \cup Y)$$

given by $f(A, B) = A \cup B$ is a bijection. From this, deduce that

$$\binom{m+n}{k} = \sum_{i=0}^{n} \binom{m}{i}\binom{n}{k-i}.$$

Solution 7. Suppose $f(A, B) = f(C, D)$. Then since $X \cap Y = \varnothing$, we see that $A = f(A, B) \cap X = f(C, D) \cap X = C$ and a similar argument shows $B = D$. Hence f is surjective. Now suppose $Z \in \mathbb{P}_k(X \cup Y)$. Define $A = Z \cap X$ and $B = Z \cap Y$. Then $f(A, B) = Z$, so f is surjective and so f is a bijection.

Now suppose that $|X| = m$ and $|Y| = n$. Then the cardinality of $\mathcal{P}_k(X \cup Y)$ is $\binom{m+n}{k}$. On the other hand, since

$$\bigcup_{i=0}^{k} \mathcal{P}_i(X) \times \mathcal{P}_{k-i}(Y)$$

is a disjoint union, with each term having cardinality $\binom{m}{i}\binom{n}{k-i}$ by the multiplication principle, we get

$$\left|\bigcup_{i=0}^{k} \mathcal{P}_i(X) \times \mathcal{P}_{k-i}(Y)\right| = \sum_{i=0}^{n} \binom{m}{i}\binom{n}{k-i}$$

by the addition principle. The bijection from the first paragraph then shows that

$$\binom{m+n}{k} = \sum_{i=0}^{n} \binom{m}{i}\binom{n}{k-i}$$

as required.

Question 8. Which of the following sets are countably infinite?

- $\mathbb{C}$
- $\{a\sqrt{2}+b\sqrt{3}+c\sqrt{5} \mid a,b,c \in \mathbb{Q}\}$
- $\{\pi^m + e^n \mid m,n \in \mathbb{Z}\}$
- $\mathrm{Fun}(\mathbb{N}, \{0,1\})$
- The set of circles in the plane with rational centers and rational radii.

Solution 8.

- $\mathbb{C}$ is not countable, since $\mathbb{R} \subset \mathbb{C}$ and $\mathbb{R}$ is uncountable.
- This set is countable. There is the bijection from this set to $\mathbb{Q}^3$ given by $\phi(a\sqrt{2}+b\sqrt{3}+c\sqrt{5}) = (a,b,c)$. Since $\mathbb{Q}^3$ is countable, the original set is also countable.
- This time there is a bijection from the original set to $\mathbb{Z}^2$ given by $\phi(\pi^m + e^n) = (m,n)$.
- The set $\mathrm{Fun}(\mathbb{N}, \{0,1\})$ can be identified with the set of characteristic functions (see earlier homeworks) on $\mathbb{N}$, which itself can be identified with the set $\mathbb{P}(\mathbb{N})$ via the bijection which maps the set $A \subset \mathbb{N}$ to the function χ_A. Since $\mathbb{P}(\mathbb{N})$ is not countable, neither is $\mathrm{Fun}(\mathbb{N}, \{0,1\})$.
- This set can be identified with the set $\mathbb{Q}^3$. Let C be the circle with center (q_1, q_2) and radius q_3, and define $\phi(C) = (q_1, q_2, q_3)$. This is a bijection, and so the original set is countable.

Question 9.

(a) Let $a < b$ and $c < d$. Show that the map $f\colon [a,b] \to [c,d]$ given by
$$f(x) = \frac{(b-x)c}{b-a} + \frac{(x-a)d}{b-a}$$
is a bijection. Deduce that any two closed intervals have the same cardinality.

(b) Show that all intervals containing more than one point has the same cardinality. (Hint: it is not necessary to find an explicit bijection to do this).

(c) Show that all intervals containing more than one point has the same cardinality as $\mathbb{R}$.

Solution 9.

(a) There are a number of ways to show that f is a bijection. First we can write down the inverse
$$f^{-1}(y) = \frac{(d-y)a}{d-c} + \frac{(y-c)b}{d-c}.$$
Alternatively, we can use calculus to show that f is a continuous increasing function, and therefore is both injective and surjective. Finally, we could just check injectivity and surjectivity from the formula. Note that f is just a linear function whose graph is the line between (a,c) and (b,d). Since f is a bijection, it follows that all closed intervals have the same cardinality.

(b) Let $\langle x, y \rangle$ be any interval, with $\langle \in \{\,(\,,\,[\,\}$ and $\rangle \in \{\,)\,,\,]\,\}$. Then $[a,b] \subset \langle x,y \rangle \subset [c,d]$ for some $a,b,c,d \in \mathbb{R}$. The inclusion $\iota\colon \langle x,y \rangle \to [c,d]$ is an injection. Moreover, since $|[a,b]| = |[c,d]|$ from part (a), there is a bijection $\phi\colon [c,d] \to [a,b]$. Then if $i\colon [a,b] \to \langle x,y \rangle$ is the inclusion, the composition $i \circ \phi$ is an injection from $[c,d]$ to $\langle x,y \rangle$. Thus, by the Cantor-Schröder-Bernstein Theorem, we have $|\langle x,y \rangle| = |[c,d]|$.

(c) It remains to show that there is a bijection from some interval $\langle a,b \rangle \subset \mathbb{R}$ to $\mathbb{R}$. The map
$$\tan^{-1}\colon \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R}$$

is a good example.

Question 10. By considering the map $f\colon [0,1)\times[0,1)\to[0,1)$, defined by

$$f((0.a_1a_2,\ldots a_n\ldots,0.b_1b_2\ldots b_n\ldots)) = 0.a_1b_1a_2b_2\ldots a_nb_n\ldots$$

(and using the expansion ending in recurring 0s if there is a choice) deduce that $|\mathbb{R}\times\mathbb{R}| = |\mathbb{R}|$.

Solution 10. Since neither $0.a_1a_2,\ldots a_n\ldots$ nor $0.b_1b_2\ldots b_n\ldots$ end in recurring 9s, it follows that $0.a_1b_1a_2b_2\ldots a_nb_n\ldots$ also does not end in recurring 9s. Suppose

$$f((0.a_1a_2,\ldots a_n\ldots,0.b_1b_2\ldots b_n\ldots)) = f((0.a_1'a_2',\ldots a_n'\ldots,0.b_1'b_2'\ldots b_n'\ldots)).$$

Since the image does not end in recurring 9s, then by checking each decimal place, we see that $a_i = a_i'$ and $b_j = b_j'$ for each i and j. This means that f is an injection from $\mathbb{R}\times\mathbb{R}$ to $\mathbb{R}$. On the other hand, the projection onto the first coordinate from $\mathbb{R}$ to $\mathbb{R}\times\mathbb{R}$ is also an injection. Thus, by the Cantor-Schröder-Bernstein theorem, we have $|\mathbb{R}\times\mathbb{R}| = |\mathbb{R}|$.