MAT 200 (Logic, Language and Proof), Fall 2015

Instructor

Dr. Malik Younsi

Contact

malik.younsi@stonybrook.edu

Lecture

MW 4:00pm - 5:20pm, Hariman 116.

Office hours

Mondays 2:30pm - 4:00pm, Wednesdays 2:30pm - 4:00pm, and by appointment. Math Tower 4-118.

Special Announcements

- Please note that there will be no class on Monday, November 30 and no office hours during that week. Instead, there will be additional office hours : Monday December 7 and Tuesday December 8, all day (say 9:00-12:00 and 1:00-5:00).

Syllabus

Exams

- Solution to Midterm 1
- Solution to Midterm 2
- Solution to Final Exam

Homeworks

- Homework 1 (due in class September 2, 2015). Solution
- Homework 2 (due in class September 9, 2015). Solution
- Homework 3 (due in class September 16, 2015). Solution
- Homework 4 (due in class September 23, 2015). Solution
- Homework 5 (due in class September 30, 2015). Solution
- Homework 6 (due in class October 7, 2015). Solution
- Homework 7 (due in class October 21, 2015). Solution
- Homework 8 (due in class October 28, 2015). Solution
- Homework 9 (due in class November 4, 2015). Solution

MAT 200, Logic, Language and Proof, Fall 2015 — Syllabus

Harriman 116 — Monday, Wednesday 4:00 - 5:20

This syllabus contains the policies and expectations that the instructor has established for this course. Please read the entire syllabus carefully before continuing in this course. These policies and expectations are intended to create a productive learning atmosphere for all students. Unless you are prepared to abide by these policies and expectations, you risk losing the opportunity to participate further in the course.

Instructor: Dr. Malik Younsi (`malik.younsi@stonybrook.edu`)
Office: Math Tower 4-118
Office Hours: Mondays 2:30pm - 4:00pm, Wednesdays 2:30pm - 4:00pm, and by appointment.

Course Description

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 Euclidean geometry. There is considerable focus on writing. We will discuss logical language and operations, methods of proof, sets and functions, cardinality, and applications of these notions to number theory.

Important Dates

Exam Dates

- Midterm Exams : To be announced on the Course Website at least one week in advance.
- Final Exam : Tuesday, December 8, 8:30pm - 11:00pm.

Required Resources

- **Course Webpage:** `www.math.stonybrook.edu/∼myounsi/teaching/mat200/`
- **Lecture Notes:** Attend lectures regularly and take your own notes.
- **Textbook:** Peter J. Eccles, *An Introduction to Mathematical Reasoning*, Cambridge University Press. (Reading and homework assignments will be assigned out of this textbook. Make sure you can access a copy of the textbook.)

About Attendance

Attendance is highly encouraged. **Lectures may include material not in the textbook!** The lectures may also present material in a different order than in the textbook.

Graded Components

- **Homeworks** – 20% of course average
  There will be a homework assignment due in class on most Wednesdays. Homework assignments will be posted on the course webpage.
- **Midterm Exams** – 40% of course average
  There will be two closed book, closed notes midterm exams in class. The exams will be scheduled during the course, with the exam date posted at least one week in advance on the course webpage.
- **Final Exam** – 40% of course average
  There will be one closed book, closed notes final exam as scheduled by the university on Tuesday, December 8, 8:30pm - 11:00pm.

Your *course average* will be determined by a weighted average of the graded components above. Your *final grade* for the class will be based on your course average *and* on your participation.

Late Homework Policy

A student's homework assignment shall be considered late if it is not turned in to the instructor by the end of lecture on the due date. Late homework assignments will not be accepted.

Missed Exam Policy

No make-up exams will be given. If a student misses a midterm exam with documented evidence, then the student's final exam grade will be substituted for the missed midterm. A student must sit the final exam at the scheduled time in order to receive a passing grade in the class.

Classroom Policies

Students are expected to arrive to lecture on time and remain until the lecture is concluded. (Leaving early creates distraction and is disrespectful to the instructor and your fellow students.) Cell phones should be silenced for the duration of the lecture. Tablet and laptop computers should not be used during lecture, except for taking notes.

Disability Support Services

If you have a physical, psychological, medical, or learning disability that may impact your course work, please contact Disability Support Services (631) 632-6748 or

`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:

`www.sunysb.edu/facilities/ehs/fire/disabilities`

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 instance of academic dishonesty to the Academic Judiciary. For more comprehensive information on academic integrity, including categories of academic dishonesty, please refer to the academic judiciary website at

`www.stonybrook.edu/uaa/academicjudiciary/`

Critical Incident Management

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, and/or inhibits students' ability to learn.

Syllabus Revision

The standards and requirements set forth in this syllabus may be modified at any time by the course instructor. Notice of such changes will be by announcement in class and changes to this syllabus will be posted on the course website.

This syllabus was last revised on July 20, 2015.

MAT 200, Logic, Language and Proof, Fall 2015 Midterm Exam 1

Name :

Student ID :

Problem 1 (25 pts).

a. Use a Truth Table to show that the statements 'P or Q' and '(not P) $\Rightarrow Q$' are equivalent.

Sol. The truth table is the following :

P	Q	P or Q	(not P) $\Rightarrow Q$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

b. Prove that if x is a real number such that $x^2 \geq 5x$, then $x \leq 0$ or $x \geq 5$.

Sol. Let x be a real number with $x^2 \geq 5x$. By **a.**, it suffices to show that if $x > 0$, then $x \geq 5$. We have

$$x(x-5) = x^2 - 5x \geq 0$$

so that

$$x - 5 \geq 0$$

since $x > 0$, by the multiplicative law for inequalities. Therefore, $x \geq 5$, as required.

Problem 2 (25 pts).

Prove by induction that 3 divides $4^n + 5$ for all positive integers n.

Sol. Let us prove by induction on $n \in \mathbb{N}$ the proposition $P(n)$ that 3 divides $4^n + 5$.

Base case : If $n = 1$, then $4^n + 5 = 4^1 + 5 = 9$ and 3 divides 9, as required. Hence $P(1)$ is true.

Inductive step : Assume that 3 divides $4^k + 5$ for some positive integer k (inductive hypothesis). Then we have $4^k + 5 = 3m$ for some $m \in \mathbb{Z}$. Also,

$$4^{k+1} + 5 = 4(4^k) + 5 = 4(3m - 5) + 5 = 12m - 15 = 3(4m - 5)$$

where $4m - 5 \in \mathbb{Z}$, so that 3 divides $4^{k+1} + 5$ and $P(k+1)$ is true, as required.

Conclusion : By the inductive hypothesis, 3 divides $4^n + 5$ for all positive integers n.

Problem 3 (25 pts).

a. Let $f : X \to Y$ be a function. Define what it means for f to be injective, surjective and bijective.

Sol. Injectivity of f means that for all $x_1, x_2 \in X$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
Surjectivity of f means that for all $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$.
Bijectivity of f simply means that f is both injective and surjective.

b. Suppose that $f : X \to Y$ and $g : Y \to Z$ are two injective functions. Prove that the composition $g \circ f : X \to Z$ is injective.

Sol. Let $x_1, x_2 \in X$ such that

$$(g \circ f)(x_1) = (g \circ f)(x_2)$$

i.e

$$g(f(x_1)) = g(f(x_2)).$$

We have to show that $x_1 = x_2$. By injectivity of g, we get that $f(x_1) = f(x_2)$. Then $x_1 = x_2$ by injectivity of f, as required.

c. Suppose that $f : X \to Y$ and $g : Y \to Z$ are two surjective functions. Prove that the composition $g \circ f : X \to Z$ is surjective.

Sol. Let $z \in Z$. We have to find an element $x \in X$ such that $(g \circ f)(x) = z$. Since $g : Y \to Z$ is surjective, there is an element $y \in Y$ such that $g(y) = z$. Now, since $f : X \to Y$ is surjective, there is an element $x \in X$ such that $f(x) = y$. Therefore, we get

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

as required.

d. It follows from **b.** and **c.** that if $f : X \to Y$ and $g : Y \to Z$ are bijective functions, then $g \circ f : X \to Z$ is also bijective. Prove that in this case,

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Sol. It easily follows from the associativity of composition and Proposition 9.2.5 that

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = I_Z$$

and that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = I_X.$$

By Proposition 9.2.5 once again, this implies that $f^{-1} \circ g^{-1}$ is the inverse of $g \circ f$, as required.

Problem 4 (25 pts).

True or False? Give a short justification.

a. $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, xy = 1$.

Sol. False. Indeed, given $y \in \mathbb{R}$, if we put $x = 0$, then $x \in \mathbb{R}$ but $xy = 0 \neq 1$.

b. $f : \mathbb{R}_{\geq} \to \mathbb{R}$ defined by $f(x) = 1 + x^2$ is injective.

Sol. True. If $x_1, x_2 \in \mathbb{R}_{\geq}$ and $f(x_1) = f(x_2)$, then $x_1^2 = x_2^2$ so that $x_1 = x_2$, since x_1 and x_2 are non-negative.

c. If $X = \{1, 2\}$, then $X \times X = \{(1, 1), (2, 2)\}$.

Sol. False. we have $X \times X = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

d. If X and Y are two sets, then

$$|X \cup Y| = |X| + |Y|.$$

Sol. False, X and Y must be disjoint. Indeed, if $X = \{1, 2\}$ and $Y = \{2, 3\}$, then $X \cup Y = \{1, 2, 3\}$ so that $|X \cup Y| = 3$ but $|X| + |Y| = 2 + 2 = 4$.

MAT 200, Logic, Language and Proof, Fall 2015 Midterm Exam 2
Solution

Name :

Student ID :

Problem 1 (25 pts).

Let X, Y be non-empty finite sets and let $f : X \to Y$ be a function.

a. If $|X| > |Y|$, what does the Pigeonhole Principle tells us about f?

b. If $|X| < |Y|$, what can we say about f? No justification is required here.

c. Use the above to show that $|X| = |Y|$ if and only if there is a bijection $X \to Y$.

Sol.

a. If $|X| > |Y|$, then f cannot be injective, by the Pigeonhole principle.

b. If $|X| < |Y|$, then f cannot be surjective.

c. If $|X| = |Y| = n$, then there exist bijections $f : \mathbb{N}_n \to X$ and $g : \mathbb{N}_n \to Y$, and $g \circ f^{-1} : X \to Y$ is a bijection.
Conversely, assume that there is a bijection $f : X \to Y$. Then in particular $f : X \to Y$ is injective, so that $|X| \leq |Y|$, by part **a.** On the other hand, $f : X \to Y$ is surjective, so that $|X| \geq |Y|$ by **b**. It follows that $|X| = |Y|$.

Problem 2 (25 pts).

a. Let $X = \{x_1, x_2, x_3\}$ and $Y = \{y_1, y_2, y_3, y_4, y_5, y_6\}$. What is the cardinality of the set $\{f \in \mathrm{Inj}(X, Y) : y_6 \notin \mathrm{Im}\, f\}$?

b. Three people visit a restaurant and each select a different dish from a menu of six items. The menu includes one vegetarian dish. How many choices are possible if we record who chose which dish and if no one wants to order the vegetarian dish?

Sol.

a. Note that $\{f \in \mathrm{Inj}(X, Y) : y_6 \notin \mathrm{Im}\, f\} = \mathrm{Inj}(X, Y')$, where $Y' = \{y_1, y_2, y_3, y_4, y_5\}$. The cardinality of the latter is $5 \times 4 \times 3 = 60$.

b. It is easy to see that the number of choices is actually the same as the number in part **a.**, which is 60.

Problem 3 (25 pts).

a. State the division theorem and prove its uniqueness part.

b. Use the Euclidean algorithm to find the greatest common divisor of 136 and 232.

c. Find integers m, n such that

$$16 = 136m + 232n.$$

Sol.

a. The division theorem says that if a, b are integers with $b > 0$, then there are unique integers q, r such that

$$a = bq + r$$

and $0 \leq r < b$.

The proof of the uniqueness part can be found on p.195 of the book.

b. We find that $(136, 232) = 8$.

c. Going backwards in the Euclidean algorithm, we find

$$8 = 136(12) + 232(-7)$$

and thus

$$16 = 136(24) + 232(-14).$$

Hence $m = 24$ and $n = -14$ work.

Problem 4 (25 pts).

True or False? Give a short justification.

a. If X and Y are infinite sets, then $|X| = |Y|$.

b. $\sqrt{2}$ is an algebraic number because it is rational.

c. For a, b, c positive integers, if a divides bc then a divides b.

d. Let Y be a set and let X be a proper subset of Y. Then $|X| < |Y|$.

Sol.

a. False. We saw in class that $|\mathbb{N}| < |\mathbb{R}|$, for example.

b. False. The number $\sqrt{2}$ is indeed algebraic (it is a solution to $x^2 - 2 = 0$), but it is not rational, as we proved in class.

c. False. A counterexample is $a = 6, b = 2, c = 3$.

d. False. For example, $\mathbb{N}$ is a proper subset of $\mathbb{Z}$ but $|\mathbb{N}| = |\mathbb{Z}|$, since they are both denumerable.

MAT 200, Logic, Language and Proof, Fall 2015 — Final Exam

Name :

Student ID :

Problem 1 (20 pts).

a. Let A and B be two sets. Give the *mathematical* definitions of $A \cup B$, $A \cap B$ and $A \setminus B$, and illustrate each of these three sets by a Venn diagram.

Sol. We have $A \cup B = \{x : x \in A \text{ or } x \in B\}$, $A \cap B = \{x : x \in A \text{ and } x \in B\}$ and $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$. The Venn diagrams can be found in the book, p.69.

b. Let X be a set. Give the definition of $\mathcal{P}(X)$, the power set of X.

Sol. $\mathcal{P}(X)$ is the set of all subsets of X :

$$\mathcal{P}(X) = \{A : A \subseteq X\}.$$

c. If $X = \{1, 2, 3\}$, what is $\mathcal{P}(X)$?

Sol. We have

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

d. If A and B are two subsets of some universal set U, write $(A \cup B)^c$ and $(A \cap B)^c$ in terms of A^c and B^c. In other words, state the De Morgan laws. No justification is needed here.

Sol. We have $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$.

Problem 2 (20 pts).

a. Give the definition of the binomial coefficient $\binom{n}{r}$, where r and n are two non-negative integers.

Sol. The binomial coefficient $\binom{n}{r}$ is the cardinality of $\mathcal{P}_r(X)$ when $|X| = n$, i.e. it is the number of subsets of a set of cardinality n which have cardinality r.

b. What is the relationship between the two binomial coefficients $\binom{132}{37}$ and $\binom{132}{95}$? Give a short justification.

Sol. They are equal, since

$$\binom{n}{r} = \binom{n}{n-r}$$

for any integers n, r with $0 \leq r \leq n$.

c. State the Binomial Theorem.

Sol. The theorem states that for all real numbers a and b and non-negative integers n, we have

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j.$$

Problem 3 (20 pts).

a. Let a and b be positive integers, and suppose that there exist integers m and n such that

$$ma + nb = 1.$$

Prove that $(a, b) = 1$.

Sol. If $d = (a, b)$, then d divides both a and b, so that it must divide $ma + nb = 1$. It follows that $d = 1$.

b. Let a and b be positive integers, and let m and n be integers such that

$$ma + nb = d,$$

where $d = (a, b)$. Prove that $(m, n) = 1$.

Sol. From $ma + nb = d$ we get

$$m\frac{a}{d} + n\frac{b}{d} = 1.$$

Since a/d and b/d are integers (d is a common divisor of a and b), it follows from part **a.** that $(m, n) = 1$.

c. Find all solutions m, n to the diophantine equation

$$133m + 56n = 35.$$

Sol. With the euclidean algorithm, we find that $(133, 56) = 7$. Since 7 divides 35, the equation has solutions. Proceeding backwards in the euclidean algorithm, we find that

$$3 \times 133 - 7 \times 56 = 7,$$

so that $m_0 = 15$ and $n_0 = -35$ is a solution to

$$133m_0 + 56n_0 = 35.$$

It follows from a theorem proved in class that all solutions m and n are given by

$$m = m_0 + \frac{b}{(a,b)}q = 15 + 8q$$

and

$$n = n_0 - \frac{a}{(a,b)}q = -35 - 19q$$

for some $q \in \mathbb{Z}$.

Problem 4 (20 pts).

a. Prove that 7 divides $3 \cdot 2^{101} + 9$.

Sol. Since $2^3 \equiv 1 \mod 7$, we have that

$$3 \cdot 2^{101} + 9 = 3 \cdot (2^3)^{33} \cdot 2^2 + 9 \equiv 3 \cdot 2^2 + 9 \mod 7 \equiv 21 \mod 7 \equiv 0 \mod 7,$$

which proves the result.

b. Prove that a positive integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.
(*Hint* : Write $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0$, where $a_0, a_1, \ldots, a_{k-1}, a_k$ are the digits of n.)

Sol. Since $10 \equiv 1 \mod 9$, we have

$$n \equiv 1^k a_k + 1^{k-1} a_{k-1} + \cdots + 1a_1 + a_0 \mod 9 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \mod 9,$$

so that n is divisible by 9 if and only if $a_k + a_{k-1} + \cdots + a_1 + a_0$ is divisible by 9, as required.

Problem 5 (20 pts).

a. Define what is a prime number, and state the Fundamental Theorem of Arithmetic.

Sol. A positive integer n is prime if $n > 1$ and the only positive divisors of n are 1 and n. The Fundamental Theorem of Arithmetic states that every positive integer greater than 1 can be written uniquely as a product of prime numbers, with the prime factors in the product written in non-decreasing order.

b. Prove by contradiction that there are infinitely many prime numbers. (*Hint* : Suppose that $p_1, p_2, \ldots, p_n$ are the only prime numbers, and consider the number $m = p_1 p_2 \cdots p_n + 1$.)

Sol. See Theorem 23.5.1, p.285

MAT 200, Logic, Language and Proof, Fall 2015 **Homework 1**

Due in Class : September 2, 2015.

Reading : Read p.3–29.

Turn in the following exercices.

Problem 1. Explain why the sentence '*This sentence is false*' is not a proposition.

Problem 2. By using truth tables, prove that, for all statements P and Q, the statement '$P \Rightarrow Q$' and its *contrapositive* '$(\text{not}\, Q) \Rightarrow (\text{not}\, P)$' are equivalent.

Problem 3. By using truth tables, prove that, for all statements P and Q, the following statements are equivalent :

(1) '$P \Rightarrow Q$',
(2) '$(P\,\text{or}\, Q) \Leftrightarrow Q$',
(3) '$(P\,\text{and}\, Q) \Leftrightarrow P$'.

Problem 4. Use the properties of addition and multiplication of real numbers given in Properties 2.3.1 to deduce that, for all real numbers a and b,

(1) $a \times 0 = 0 = 0 \times a$,
(2) $(-a)b = -(ab) = a(-b)$,
(3) $(-a)(-b) = ab$.

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

Problem 1. Explain why the sentence '*This sentence is false*' is not a proposition.

Sol. Assume that it is a proposition, so that it is either true or false, but not both. If the sentence is true, then it is true that '*This sentence is false*' and thus the sentence is false. Similarly, if the sentence is false, then it is true. This is a contradiction.

Problem 2. By using truth tables, prove that, for all statements P and Q, the statement '$P \Rightarrow Q$' and its *contrapositive* '$(\text{not}\, Q) \Rightarrow (\text{not}\, P)$' are equivalent.

Sol. The truth tables are

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$(\text{not}\, Q) \Rightarrow (\text{not}\, P)$
T	T	T
T	F	F
F	T	T
F	F	T

Problem 3. By using truth tables, prove that, for all statements P and Q, the following statements are equivalent :

(1) '$P \Rightarrow Q$',
(2) '$(P \,\text{or}\, Q) \Leftrightarrow Q$',
(3) '$(P \,\text{and}\, Q) \Leftrightarrow P$'.

Sol. The truth tables are

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$(P \,\text{or}\, Q) \Leftrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$(P \,\text{and}\, Q) \Leftrightarrow P$
T	T	T
T	F	F
F	T	T
F	F	T

Problem 4. Use the properties of addition and multiplication of real numbers given in Properties 2.3.1 to deduce that, for all real numbers a and b,

(1) $a \times 0 = 0 = 0 \times a$,
(2) $(-a)b = -(ab) = a(-b)$,
(3) $(-a)(-b) = ab$.

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

Sol. To prove (1), note that $0 = 0 + 0$ by the Zero law, so that $a \times 0 = a \times (0 + 0) = a \times 0 + a \times 0$, by the Distributivity law. Adding $-(a \times 0)$ on both sides, we get

$$a \times 0 + (-(a \times 0)) = (a \times 0 + a \times 0) + (-(a \times 0)).$$

By the Subtraction law and the Associativity law, this yields

$$0 = a \times 0 + (a \times 0 + (-(a \times 0))) = a \times 0 + 0,$$

and thus $0 = a \times 0$ by the Zero law. Similarly, $0 \times a = 0$.

To prove (2), note that $a + (-a) = 0$, so that, by multiplying both sides by b, we get

$$(a + (-a))b = 0 \times b = 0,$$

by (1). Using the Distributivity law, it follows that

$$ab + (-a)b = 0,$$

and thus $(-a)b = -(ab)$ by the Substraction law. Similarly, $a(-b) = -(ab)$.

To prove (3), note that $a + (-a) = 0$, so that, by multiplying both sides by $-b$ and using the Distributivity law, we get

$$a(-b) + (-a)(-b) = 0 \times (-b).$$

By (2) and the Zero law, this gives

$$-(ab) + (-a)(-b) = 0.$$

Finally, adding (ab) on both sides and using Associativity and Zero, we obtain

$$(-a)(-b) = ab + 0 = ab,$$

which is what we had to prove.

Due in Class : September 9, 2015.

Reading : Read p.30–51.

Turn in the following exercices.

Problem 1.
Prove the following statements for x a real number.

(1) $x^2 - x - 2 = 0 \Leftrightarrow x = -1$ or $x = 2$.
(2) $x^2 - x - 2 > 0 \Leftrightarrow x < -1$ or $x > 2$.

Problem 2.
Prove by contradiction that there does not exist a largest integer.

Problem 3.
Prove by contradiction that there does not exist a smallest positive real number.

Problem 4.
Use induction to prove Bernouilli's inequality :

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

for all non-negative integers n and real numbers $x > -1$.

Problem 5.
Let us prove by induction on $n \geq 1$ the statement 'In any group of n people, all people have the same sex', which we denote by $P(n)$.

Base case: Clearly, in any group of one people, all people have the same sex. Thus $P(1)$ is true.

Inductive step : Suppose that $P(k)$ is true for some integer k, that is, in any group of k people, all people have the same sex (inductive hypothesis). We have to prove that $P(k + 1)$ is true. To do this, consider a group of $k + 1$ people.

First, exclude the last person and consider only the first k people. Then all these people have the same sex, by the induction hypothesis. Likewise, exclude the first person and consider only the last k people. Then these too must have the same sex. Therefore, the first person in the group is of the same sex as the people in the middle, who in turn are of the same sex as the last person. Hence everyone in the group is of the same sex.

This shows that $P(k+1)$ is true.

Conclusion Therefore, by the induction principle, $P(n)$ is true for all integers $n \geq 1$. In other words, in any group of n people, all people have the same sex.

But this is clearly false! Explain what is wrong in the above proof.

Problem 1.
Prove the following statements for x a real number.

(1) $x^2 - x - 2 = 0 \Leftrightarrow x = -1$ or $x = 2$.
(2) $x^2 - x - 2 > 0 \Leftrightarrow x < -1$ or $x > 2$.

Sol. To prove (1), first note that $x^2 - x - 2 = (x+1)(x-2)$. To prove the first implication ($\Rightarrow$), assume that $(x+1)(x-2) = 0$. We want to prove that $x = -1$ or $x = 2$. If $x \neq -1$, then $x + 1 \neq 0$ and we can divide through by $x + 1$ to obtain $x - 2 = 0$, i.e. $x = 2$. This shows that $x = -1$ or $x = 2$. The converse easily follows from the fact that $0 \times a = 0 = a \times 0$ for all real numbers a.

Let us now prove (2). For the first implication ($\Rightarrow$), assume that $(x+1)(x-2) > 0$. We want to prove that $x < -1$ or $x > 2$. Suppose that $x \geq -1$. If $x = -1$, then $x + 1 = 0$ and $(x+1)(x-2) = 0$, which is a contradiction. Hence $x > -1$, i.e. $x+1 > 0$. This, together with $(x+1)(x-2) > 0$, implies that $x - 2 > 0$, by the multiplicative law for inequalities. Thus $x < -1$ or $x > 2$.
For the converse ($\Leftarrow$), we proceed by cases. If $x < -1$ (i.e. $x + 1 < 0$), then $x < 2$ (i.e. $x - 2 < 0$) and, by the multiplicative law for inequalities, we get $x^2 - x - 2 = (x+1)(x-2) > 0$. Likewise, if $x > 2$ (i.e. $x - 2 > 0$), then $x > -1$ (i.e. $x + 1 > 0$) and we also get $x^2 - x - 2 = (x+1)(x-2) > 0$. Therefore, $x < -1$ or $x > 2$ implies $x^2 - x - 2 > 0$, which is what we wanted to prove.

Problem 2.
Prove by contradiction that there does not exist a largest integer.

Sol. Suppose, for a contradiction, that there exists a largest integer, say n. But then $n + 1$ is an integer which is larger than n (since $n + 1 > n$ by the addition law for inequalities), a contradiction. Hence there does not exist a largest integer.

Problem 3.
Prove by contradiction that there does not exist a smallest positive real number.

Sol. Suppose, for a contradiction, that there exists a smallest positive real number, say $x > 0$. But then $x/2$ is a positive real number which is smaller than x (since $x/2 < x$ by the multiplicative law for inequalities), a contradiction. Therefore, there does not exist a smallest positive real number.

Problem 4.
Use induction to prove Bernouilli's inequality :

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

for all non-negative integers n and real numbers $x > -1$.

Sol. Fix some real number $x > -1$. We use induction on $n \geq 0$ to prove the statement $(1+x)^n \geq 1+nx$, which we denote by $P(n)$.

Base case: If $n = 0$, then $(1+x)^n = (1+x)^0 = 1$ and $1+nx = 1+0 = 0$. Since $1 \geq 0$, we get that $P(1)$ is true.

Inductive step: Suppose that $P(k)$ is true for some integer k, that is $(1+x)^k \geq 1+kx$ (inductive hypothesis). We have to show that $P(k+1)$ is true, i.e. $(1+x)^{k+1} \geq 1+(k+1)x$. We have

$$\begin{aligned}(1+x)^{k+1} = (1+x)^k(1+x) &\geq (1+kx)(1+x) \\ &= 1+(k+1)x+kx^2 \\ &\geq 1+(k+1)x,\end{aligned}$$

where we used the inductive hypothesis and the multiplicative law for inequalities, which is valid since $1+x > 0$. Thus $P(k+1)$ is true.

Concolusion: Therefore, by the induction principle, $P(n)$ is true for all $n \geq 0$, that is $(1+x)^n \geq 1+nx$ for all $n \geq 0$.

Problem 5.
Let us prove by induction on $n \geq 1$ the statement 'In any group of n people, all people have the same sex', which we denote by $P(n)$.

Base case: Clearly, in any group of one people, all people have the same sex. Thus $P(1)$ is true.

Inductive step : Suppose that $P(k)$ is true for some integer k, that is, in any group of k people, all people have the same sex (inductive hypothesis). We have to prove that $P(k+1)$ is true. To do this, consider a group of $k+1$ people.

First, exclude the last person and consider only the first k people. Then all these people have the same sex, by the induction hypothesis. Likewise, exclude the first person and consider only the last k people. Then these too must have the same sex. Therefore, the first person in the group is of the same sex as the people in the middle, who in turn are of the same sex as the last person. Hence everyone in the group is of the same sex.

This shows that $P(k+1)$ is true.

Conclusion Therefore, by the induction principle, $P(n)$ is true for all integers $n \geq 1$. In other words, in any group of n people, all people have the same sex.

But this is clearly false! Explain what is wrong in the above proof.

Sol. The problem is that the inductive step breaks down in the case $k = 1$. In other words, the implication $P(1) \Rightarrow P(2)$ is false. Indeed, in this case, the argument doesn't work since the middle group is empty.

MAT 200, Logic, Language and Proof, Fall 2015 — Homework 3

Due in Class : September 16, 2015.

Reading : Read p.61–99.

Turn in the following exercices.

Problem 1.

Prove by induction on n that $n! > 2^n$ for all integers $n \geq 4$.

Problem 2.

Prove by induction on n that

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

for all positive integers n.

Problem 3.

For a positive integer n, the number a_n is defined inductively by

$$a_1 = 1$$

and

$$a_{k+1} = \frac{6a_k + 5}{a_k + 2}$$

for k a positive integer. Prove by induction on n that $0 < a_n < 5$.

Problem 4.

Prove by induction on n that

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

for integers $n \geq 2$. See Problem 18 p.55 for the inductive definition of the product.

Problem 1.

Prove by induction on n that $n! > 2^n$ for all integers $n \geq 4$.

Sol. Let us prove by induction on $n \geq 4$ the statement $n! > 2^n$, which we denote by $P(n)$.

Base case: If $n = 4$, then $n! = 4! = 24$ and $2^n = 2^4 = 16$. Since $24 > 16$, $P(4)$ is true.

Inductive step: Suppose that $k! > 2^k$ for some integer $k \geq 4$ (inductive hypothesis). We have

$$(k+1)! = (k+1)k! > (k+1)2^k > (2)2^k = 2^{k+1},$$

by the induction hypothesis and by the fact that $k+1 > 2$. This shows that $P(k+1)$ is true, as required.

Conclusion: Therefore, by the induction principle, $n! > 2^n$ for all $n \geq 4$.

Problem 2.

Prove by induction on n that

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

for all positive integers n.

Sol. We prove by induction on $n \geq 1$ the equality, which we denote by $P(n)$.

Base case: For $n = 1$, the sum on the left-hand side is equal to the first term, which is $1/2$. The right-hand side is also equal to $1/2$, which shows that $P(1)$ is true.

Inductive step: Assume that

$$\sum_{j=1}^{k} \frac{1}{j(j+1)} = \frac{k}{k+1}$$

for some integer $k \geq 1$ (inductive hypothesis). We have

$$\sum_{j=1}^{k+1} \frac{1}{j(j+1)} = \sum_{j=1}^{k} \frac{1}{j(j+1)} + \frac{1}{(k+1)(k+2)} = \frac{k}{k+1} + \frac{1}{(k+1)(k+2)},$$

by the induction hypothesis. This last expression is equal to

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

Hence $P(k+1)$ is true.

Conclusion: Therefore, by the induction principle, the equality

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

holds for all positive integers n.

Problem 3.

For a positive integer n, the number a_n is defined inductively by

$$a_1 = 1$$

and

$$a_{k+1} = \frac{6a_k+5}{a_k+2}$$

for k a positive integer. Prove by induction on $n \geq 1$ that $0 < a_n < 5$.

Sol. Let us prove by induction on $n \geq 1$ the statement $0 < a_n < 5$, which we denote by $P(n)$.

Base case : For $n = 1$, $a_1 = 1$ and so clearly $0 < a_1 < 5$. This shows that $P(1)$ is true.

Inductive step : Suppose that $0 < a_k < 5$ for some positive integer k (inductive hypothesis). First, since $a_k > 0$, we have $6a_k + 5 > 0$ and $a_k + 2 > 0$, from which it follows that

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

Secondly, we have

$$5 > a_{k+1} = \frac{6a_k+5}{a_k+2}$$

if and only if

$$5a_k + 10 > 6a_k + 5$$

if and only if $5 > a_k$, which is true. This shows that $0 < a_{k+1} < 5$ and thus $P(k+1)$ is true.

Conclusion : Therefore, by the induction principle, $0 < a_n < 5$ for all positive integers n.

Problem 4.

Prove by induction on n that

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

for integers $n \geq 2$. See Problem 18 p.55 for the inductive definition of the product.

Sol. Let us prove by induction on $n \geq 2$ the equality, which we denote by $P(n)$.

Base case : For $n = 2$, the product is equal to the first factor, which is $1 - 1/4 = 3/4$. The right-hand side of the equality is also equal to $3/4$, so that $P(2)$ is true.

Inductive step : Suppose that

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

for some integer $k \geq 2$ (inductive hypothesis). We have

$$\begin{aligned}\prod_{j=2}^{k+1}\left(1-\frac{1}{j^2}\right)=\prod_{j=2}^{k}\left(1-\frac{1}{j^2}\right)\left(1-\frac{1}{(k+1)^2}\right) &= \frac{k+1}{2k}\left(1-\frac{1}{(k+1)^2}\right)\\ &= \frac{k+1}{2k}\frac{(k+1)^2-1}{(k+1)^2}\\ &= \frac{k^2+2k}{2k(k+1)}=\frac{k+2}{2(k+1)},\end{aligned}$$

which proves $P(k+1)$.

Conclusion : Therefore, by the induction principle,

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

for integers $n \geq 2$.

MAT 200, Logic, Language and Proof, Fall 2015 | Homework 4

Due in Class : September 23, 2015.

Turn in the following exercices.

Problem 1.
By using a truth table, prove that, for sets A, B and C,

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

Illustrate the proof with a Venn diagram.

Problem 2.
Prove that for sets A, B and C, $A \cap B = A \cap C$ and $A \cup B = A \cup C$ if and only if $B = C$.

Problem 3.
Prove or disprove each of the following statements.

(1) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy \geq 0$;
(2) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, (x + y > 0 \text{ or } x + y = 0)$;
(3) $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0)$ and $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0)$.

Problem 4.
Suppose that $A \subseteq \mathbb{Z}$. Write the following statement and its negative entirely in symbols using the quantifiers $\forall$ and $\exists$:

There is a greatest number in the set A.

Give an example of a set A for which the statement is true, and another example for which it is false.

Problem 5.
Prove that, for sets A, B, C and D,

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
(2) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Problem 1.

By using a truth table, prove that, for sets A, B and C,

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

Illustrate the proof with a Venn diagram.

Sol. The truth table is

$x \in A$	$x \in B$	$x \in C$	$x \in A \cup (B \cap C)$	$x \in (A \cup B) \cap (A \cup C)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

The Venn diagram is easy to draw.

Problem 2.

Prove that for sets A, B and C, $A \cap B = A \cap C$ and $A \cup B = A \cup C$ if and only if $B = C$.

Sol. ($\Leftarrow$) Clearly, if $B = C$, then $A \cap B = A \cap C$ and $A \cup B = A \cup C$.

($\Rightarrow$) Conversely, assume that $A \cap B = A \cap C$ and $A \cup B = A \cup C$ but that $B \neq C$. Then either there is an element in B not in C or there is an element in C not in B. Suppose that the first case holds and let $x \in B$, $x \notin C$. Then $x \in A \cup B = A \cup C$, so that $x \in A$ since $x \notin C$. Thus $x \in A \cap B = A \cap C$ and so $x \in C$, a contradiction. We obtain a similar contradiction if the second case holds, i.e. if there is an element in C not in B. Therefore, ($A \cap B = A \cap C$ and $A \cup B = A \cup C$) implies $B = C$.

Problem 3.

Prove or disprove each of the following statements.

(1) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy \geq 0$;
(2) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, (x + y > 0$ or $x + y = 0)$;
(3) $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0)$ and $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0)$.

Sol. The first statement is true. Indeed, given $x \in \mathbb{R}$, if we put $y = 0$, then $y \in \mathbb{R}$ and $xy = 0$, so that in particular $xy \geq 0$.

The second statement is true. Indeed, if $x \in \mathbb{R}$, if we put $y = -x$, then $y \in \mathbb{R}$ and $x + y = 0$. In particular, $(x + y > 0$ or $x + y = 0)$.

The third statement is true. Indeed, given $x \in \mathbb{R}$, if we put $y = -x + 1$, then $y \in \mathbb{R}$ and $x + y = 1 > 0$. This proves $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0)$. On the other hand, given $x \in \mathbb{R}$, if we put $y = -x$, then $x + y = 0$. This proves $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0)$. Hence both statements are true, so that $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0)$ and $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0)$ is true.

Problem 4.

Suppose that $A \subseteq \mathbb{Z}$. Write the following statement and its negative entirely in symbols using the quantifiers $\forall$ and $\exists$:

There is a greatest number in the set A.

Give an example of a set A for which the statement is true, and another example for which it is false.

Sol. The statement is

$$\exists n \in A, \forall m \in A, m \leq n$$

and its negative is

$$\forall n \in A, \exists m \in A, m > n.$$

The statement is true for instance if A is any finite set and it is false if $A = \mathbb{N}$.

Problem 5.

Prove that, for sets A, B, C and D,

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
(2) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Sol. To prove (1), assume that $(x, y) \in A \times (B \cup C)$. By definition of the cartesian product, we have $x \in A$ and $y \in B \cup C$. If $y \in B$, then $(x, y) \in A \times B$. If $y \in C$, then $(x, y) \in A \times C$. In both cases, $(x, y) \in (A \times B) \cup (A \times C)$. This proves $(\subseteq)$.
To prove the reverse inclusion, suppose that $(x, y) \in (A \times B) \cup (A \times C)$, so that either $(x, y) \in A \times B$ or $(x, y) \in A \times C$. In the first case, we have $x \in A$ and $y \in B$. Since $B \subseteq B \cup C$, we get that $y \in B \cup C$. Hence $(x, y) \in A \times (B \cup C)$. The second case is treated similarly and we obtain $(x, y) \in A \times (B \cup C)$.

To prove (2), assume that $(x, y) \in (A \times B) \cap (C \times D)$. Then $x \in A$, $y \in B$ and $x \in C$, $y \in D$. Thus $x \in A \cap C$ and $y \in B \cap D$, so that $(x, y) \in (A \cap C) \times (B \cap D)$. This proves $(\subseteq)$.
To prove the reverse inclusion, suppose that $(x, y) \in (A \cap C) \times (B \cap D)$. Then $x \in A$, $x \in C$, $y \in B$, $y \in D$. Thus $(x, y) \in A \times B$ and $(x, y) \in C \times D$, from which it follows that $(x, y) \in (A \times B) \cap (C \times D)$.

MAT 200, Logic, Language and Proof, Fall 2015 **Homework 5**

Due in Class : September 30, 2015.

Reading : Read Chap.9

Turn in the following exercises.

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

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

for $x \in X$.
Suppose now that A and B are two subsets of X.

(1) Prove that $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x)$ for all $x \in X$.
(2) Prove that $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x)$ for all $x \in X$.

Problem 2.
Define functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} x+2 & \text{if } x < -1 \\ -x & \text{if } -1 \leq x \leq 1 \\ x-2 & \text{if } x > 1 \end{cases}$$

$$g(x) = \begin{cases} x-2 & \text{if } x < -1 \\ -x & \text{if } -1 \leq x \leq 1 \\ x+2 & \text{if } x > 1 \end{cases}$$

(1) Find the functions $f \circ g$ and $g \circ f$.
(2) Is g the inverse of the function f? Explain.
(3) Is f injective or surjective? Explain.
(4) Is g injective or surjective? Explain.

Problem 3.
Let X be a set with three elements, say $X = \{a, b, c\}$. Find all bijective functions from X to X.

Problem 4.
Let X, Y, Z be sets and suppose that $f : X \to Y$ and $g : Y \to Z$ are surjective functions. Prove that the composition $g \circ f : X \to Z$ is surjective.

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

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

for $x \in X$.
Suppose now that A and B are two subsets of X.

(1) Prove that $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x)$ for all $x \in X$.
(2) Prove that $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x)$ for all $x \in X$.

Sol. To prove (1), suppose that x is any element of X.

If $x \in A$ and $x \in B$, then $x \in A\cap B$ and $\chi_{A\cap B}(x) = 1$, $\chi_A(x) = 1$, $\chi_B(x) = 1$ so that $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x)$.

If $x \in A$ and $x \notin B$, then $x \notin A\cap B$ and $\chi_{A\cap B}(x) = 0$, $\chi_A(x) = 1$, $\chi_B(x) = 0$, thus the relation $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x)$ also holds.
Similarly if $x \notin A$, $x \in B$.

Lastly, if $x \notin A$ and $x \notin B$, then $x \notin A \cap B$ and $\chi_{A\cap B}(x) = 0$, $\chi_A(x) = 0$, $\chi_B(x) = 0$, so that once again we have $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x)$.

We have considered all cases and therefore the equation $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x)$ holds for all $x \in X$.

The equation in (2) is proved in the same way.

Problem 2.
Define functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} x+2 & \text{if } x < -1 \\ -x & \text{if } -1 \leq x \leq 1 \\ x-2 & \text{if } x > 1 \end{cases}$$

$$g(x) = \begin{cases} x-2 & \text{if } x < -1 \\ -x & \text{if } -1 \leq x \leq 1 \\ x+2 & \text{if } x > 1 \end{cases}$$

(1) Find the functions $f \circ g$ and $g \circ f$.
(2) Is g the inverse of the function f? Explain.
(3) Is f injective or surjective? Explain.

(4) Is g injective or surjective? Explain.

sol.

(1): To find $f \circ g$, let $x \in \mathbb{R}$. If $x < -1$, then $g(x) = x - 2 < -1$ so that $(f \circ g)(x) = f(g(x)) = f(x-2) = (x-2)+2 = x$. If $-1 \le x \le 1$, then $-1 \le g(x) = -x \le 1$ and $(f \circ g)(x) = f(-x) = -(-x) = x$. Lastly, if $x > 1$, then $g(x) = x+2 > 1$ and $(f \circ g)(x) = f(x+2) = (x+2)-2 = x$. We have considered all cases and found that $f \circ g(x) = x$ for all $x \in \mathbb{R}$.

To find $g \circ f(x)$ for $x \in \mathbb{R}$, it is best to first consider the case $x < -3$. Then $f(x) = x+2 < -1$, so that $g(f(x)) = g(x+2) = x+2-2 = x$. Next, if $-3 \le x < -1$, we have $-1 \le f(x) = x+2 < 1$, so that $g(f(x)) = -(x+2) = -x-2$. If $-1 \le x \le 1$, then $g(f(x)) = g(-x) = x$ since $-1 \le -x \le 1$. If $1 < x \le 3$, then $-1 < x-2 \le 1$ so that $g(f(x)) = g(x-2) = -x+2$. Finally, if $x > 3$, then $f(x) = x-2 > 1$ and $g(f(x)) = g(x-2) = (x-2)+2 = x$. To summarize, we found

$$g(f(x)) = \begin{cases} x & \text{if } x < -3 \\ -x-2 & \text{if } -3 \le x < -1 \\ x & \text{if } -1 \le x < 1 \\ -x+2 & \text{if } 1 < x \le 3 \\ x & \text{if } x > 3 \end{cases}$$

(2): No by Proposition 9.2.5, since $g \circ f$ is not the identity on $\mathbb{R}$.

(3): Note that to check whether the function f is injective or surjective, it is useful to consider its graph. We find that f is not injective, since $f(0) = 0 = f(2)$ but $0 \ne 2$. On the other hand, f is surjective. This is easy to see from the graph, but a rigorous argument is the following. On $(-\infty, -1)$, $f(x) = x+2$ so that f takes all values in $(-\infty, 1)$. On $[-1, 1]$, $f(x) = -x$ and f takes all values in $[-1, 1]$. Lastly, on $(1, \infty)$, $f(x) = x-2$ so that f takes all values in $(-1, \infty)$. Since the intervals $(-\infty, 1)$, $[-1, 1]$ and $(1, \infty)$ cover the whole of $\mathbb{R}$, the image of f is the set of all real numbers, i.e. f is surjective.

(4): Again, consideration of the graph of g shows that g is injective but not surjective. More rigorously, on $(-\infty, -1)$, $g(x) = x-2$ takes all values in $(-\infty, -3)$. On $[-1, 1]$, $g(x) = -x$ takes all values in $[-1, 1]$. Lastly, on $(1, \infty)$, $g(x) = x+2$ takes all values in $(3, \infty)$. Since the intervals $(-\infty, -3)$, $[-1, 1]$ and $(3, \infty)$ do not overlap, we get that g is injective. On the other hand, these intervals do not cover $\mathbb{R}$, so g is not surjective.

Problem 3.

Let X be a set with three elements, say $X = \{a, b, c\}$. Find all bijective functions from X to X.

Sol. To find all bijective functions $X \to X$, we only need to assign the value of a and the (different) value of b, since the value of c then has to be the remaining element. Proceeding in this way, we find

$$f_1(a) = a, f_1(b) = b, f_1(c) = c;$$
$$f_2(a) = a, f_2(b) = c, f_2(c) = b;$$
$$f_3(a) = b, f_3(b) = a, f_3(c) = c;$$
$$f_4(a) = b, f_4(b) = c, f_4(c) = a;$$
$$f_5(a) = c, f_5(b) = a, f_5(c) = b;$$
$$f_6(a) = c, f_6(b) = b, f_6(c) = a.$$

These are just the six permutations of $\{a, b, c\}$.

Problem 4.
Let X, Y, Z be sets and suppose that $f : X \to Y$ and $g : Y \to Z$ are surjective functions. Prove that the composition $g \circ f : X \to Z$ is surjective.

Sol. Let $z \in Z$. We have to show that there is an element $x \in X$ such that $(g \circ f)(x) = z$. First, since $g : Y \to Z$ is surjective, there is an element $y \in Y$ with $g(y) = z$. Now, since $f : X \to Y$ is surjective, there is an element $x \in X$ such that $f(x) = y$. We get

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

as required.

MAT 200, Logic, Language and Proof, Fall 2015 Homework 6

Due in Class : October 7, 2015.

Reading : Read Chap.10

Turn in the following exercises.

Problem 1.
Let $f : X \to Y$ be a function. Prove that there exists a function $g : Y \to X$ such that $f \circ g = I_Y$ if and only if f is surjective. Here I_Y denotes the identity function on Y.

Problem 2.
Let $f : X \to Y$ be a function, let A_1, A_2 be subsets of X and B_1, B_2 be subsets of Y.

(1) Prove that $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$, but that the converse is false in general. Is the converse true if f is injective? Explain.
(2) Prove that $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$, but that the converse is false in general. Is the converse true if f is surjective? Explain.
(3) Prove that $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. Give an example for which equality does not hold.
(4) Prove that $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

Problem 3.
Suppose that there are 153 students enrolled in at least one of the three first year core Mathematics courses (Logic, Algebra and Calculus). If 100 of these students like Logic, 100 like Algebra, 100 like Calculus, 56 like Logic and Algebra, 60 like Logic and Calculus, 57 like Algebra and Calculus, and 25 like all three courses, how many of the students like none of the courses?

Problem 4.
At a Mathematics Conference of 100 participants, 75 speak English, 60 speak Spanish and 45 speak Italian, and everyone present speaks at least one of these languages.

(1) What is the maximum number of participants who can speak only one language?
(2) What is the maximum number of participants who speak only english?

(3) Prove that the greater the number of participants who speak all three languages, the greater the number of participants who speak only one language.

Problem 1.
Let $f : X \to Y$ be a function. Prove that there exists a function $g : Y \to X$ such that $f \circ g = I_Y$ if and only if f is surjective. Here I_Y denotes the identity function on Y.

Sol.
($\Rightarrow$) Suppose that such a function $g : Y \to X$ exists. Let us prove then that f is surjective. Suppose that $y \in Y$. If we put $x = g(y)$, then $x \in X$ and $f(x) = f(g(y)) = I_Y(y) = y$. This shows that f is surjective.

($\Leftarrow$) Suppose that f is surjective. This means for any $y \in Y$, there exists an element $x \in X$ such that $f(x) = y$. We can therefore define a function $g : Y \to X$ by the rule that, for each $y \in Y$, $g(y)$ is some element in X with $f(g(y)) = y$. Then by construction, $f \circ g = I_Y$.

Problem 2.
Let $f : X \to Y$ be a function, let A_1, A_2 be subsets of X and B_1, B_2 be subsets of Y.

(1) Prove that $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$, but that the converse is false in general. Is the converse true if f is injective? Explain.
(2) Prove that $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$, but that the converse is false in general. Is the converse true if f is surjective? Explain.
(3) Prove that $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. Give an example for which equality does not hold.
(4) Prove that $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

Sol.
(1): Suppose that $A_1 \subseteq A_2$. If $f(x) \in f(A_1)$ where $x \in A_1$, then $x \in A_2$, so that $f(x) \in f(A_2)$, as required. To see that the converse is false in general, define a function f on $\{0, 1\}$ by $f(0) = f(1) = 0$, and put $A_1 = \{0\}$ and $A_2 = \{1\}$. Then $f(A_1) = f(\{0\}) = \{0\}$ and $f(A_2) = f(\{1\}) = \{0\} = f(A_1)$, so that in particular $f(A_1) \subseteq f(A_2)$, but $A_1 \nsubseteq A_2$.

The converse is true though if f is injective. Indeed, suppose that $f(A_1) \subseteq f(A_2)$ and let $x_0 \in A_1$. Then $f(x_0) \in f(A_1) \subseteq f(A_2)$ and thus there exists an element $x_1 \in A_2$ with $f(x_1) = f(x_0)$. By injectivity, we get $x_0 = x_1 \in A_2$. This shows that $A_1 \subseteq A_2$.

(2): Suppose that $B_1 \subseteq B_2$, and let $x_0 \in f^{-1}(B_1)$. Then $f(x_0) \in B_1 \subseteq B_2$, so that $x_0 \in f^{-1}(B_2)$ by definition. This shows that $f^{-1}(B_1) \subseteq f^{-1}(B_2)$.

To see that the converse is false in general, define a function $f : \{0\} \to \{0, 1\}$ by $f(0) = 0$, and take $B_1 = \{1\}$, $B_2 = \{0\}$. Then $f^{-1}(B_1) = \emptyset \subseteq \{0\} = f^{-1}(B_2)$ but clearly $B_1 \nsubseteq B_2$.

The converse is true though if f is surjective. Indeed, suppose that $f^{-1}(B_1) \subseteq f^{-1}(B_2)$ and let $y_0 \in B_1$. By surjectivity, there exists an element $x_0 \in X$ with $f(x_0) = y_0$. Then $x_0 \in f^{-1}(B_1) \subseteq f^{-1}(B_2)$, so that $y_0 = f(x_0) \in B_2$. This shows that $B_1 \subseteq B_2$.

(3): Let $f(x) \in f(A_1 \cap A_2)$ where $x \in A_1 \cap A_2$. Then $x \in A_1$ and $x \in A_2$, so that $f(x) \in f(A_1)$ and $f(x) \in f(A_2)$, i.e. $f(x) \in f(A_1) \cap f(A_2)$, as required. To see that equality does not hold in general, define a function f on $\{0, 1\}$ by $f(0) = f(1) = 0$, and put $A_1 = \{0\}$ and $A_2 = \{1\}$. Then $f(A_1) = \{0\} = f(A_2)$ so that $f(A_1) \cap f(A_2) = \{0\}$, but $A_1 \cap A_2 = \emptyset$ so that $f(A_1 \cap A_2) = \emptyset$.

(4): Let $f(x) \in f(A_1 \cup A_2)$ where $x \in A_1 \cup A_2$. Then $x \in A_1$ or $x \in A_2$. In the first case, we get $f(x) \in f(A_1)$ and in the second case, we get $f(x) \in f(A_2)$. In both cases, $f(x) \in f(A_1) \cup f(A_2)$ and therefore $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$.
For the reverse inclusion, assume that $y \in f(A_1) \cup f(A_2)$, so that $y \in f(A_1)$ or $y \in f(A_2)$. In both cases, there exists an element $x \in A_1 \cup A_2$ with $y = f(x)$, so that $y \in f(A_1 \cup A_2)$, as required.

Problem 3.
Suppose that there are 153 students enrolled in at least one of the three first year core Mathematics courses (Logic, Algebra and Calculus). If 100 of these students like Logic, 100 like Algebra, 100 like Calculus, 56 like Logic and Algebra, 60 like Logic and Calculus, 57 like Algebra and Calculus, and 25 like all three courses, how many of the students like none of the courses?

Sol. Let X be the set of all students who like Logic, Y the set of all students who like Algebra and Z the set of all students who like Calculus. Then the number we are looking for is $153 - |X \cup Y \cup Z|$. By the inclusion-exclusion principle, we have

$$\begin{aligned} |X \cup Y \cup Z| &= |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z| \\ &= 100 + 100 + 100 - 56 - 60 - 57 + 25 = 152. \end{aligned}$$

Thus the answer is $153 - 152 = 1$.

Problem 4.
At a Mathematics Conference of 100 participants, 75 speak English, 60 speak Spanish and 45 speak Italian, and everyone present speaks at least one of these languages.

(1) What is the maximum number of participants who can speak only one language?
(2) What is the maximum number of participants who speak only english?
(3) Prove that the greater the number of participants who speak all three languages, the greater the number of participants who speak only one language.

Sol. Let X be the set of all participants who speak English, Y the set of all participants who speak Spanish and Z the set of all participants who speak Italian. Then $|X \cup Y \cup Z| = 100, |X| = 75, |Y| = 60$ and $|Z| = 45$.

(1): To maximize the number of participants who can speak only one language, we need to minimize the number of people who speak more than one language. A Venn diagram shows that this quantity is

$$|X \cap Y| + |X \cap Z| + |Y \cap Z| - 2|X \cap Y \cap Z|.$$

By the inclusion-exclusion principle, we have

$$100 = 180 - (|X \cap Y| + |X \cap Z| + |Y \cap Z|) + |X \cap Y \cap Z|,$$

since $|X| + |Y| + |Z| = 180$, so that

$$(|X \cap Y| + |X \cap Z| + |Y \cap Z|) - |X \cap Y \cap Z| = 80$$

and thus we want to minimize

$$80 - |X \cap Y \cap Z|,$$

which is equivalent to maximizing $|X \cap Y \cap Z|$, which proves (3).
To maximize $|X \cap Y \cap Z|$, note that we have

$$|X \cap Y| + |X \cap Z| + |Y \cap Z| \geq 3|X \cap Y \cap Z|,$$

since the set on the right-hand side is a subset of each of the sets on the left-hand side. We get

$$80 = (|X \cap Y| + |X \cap Z| + |Y \cap Z|) - |X \cap Y \cap Z| \geq 2|X \cap Y \cap Z|,$$

so that the maximal value of $|X \cap Y \cap Z|$ is 40, which is attained when each of the double intersection is equal to $X \cap Y \cap Z$. By the first equation, the answer is $100 - (40 + 40 + 40 - 2(40)) = 100 - 40 = 60$.

(2): To maximize the number of participants who speak only English, we need to minimize the number of people who speak Spanish or Italian. This number is at least 60, since 60 people speak Spanish. Therefore the number of participants who speak only English is at most $100 - 60 = 40$.

MAT 200, Logic, Language and Proof, Fall 2015 **Homework 7**

Due in Class : October 21, 2015.

Reading : Read Chap.11 and Chap.12

Turn in the following exercises.

Problem 1.

Suppose that X and Y are non-empty finite sets with $|X| = |Y|$, and let $f : X \to Y$ be a function. Show that f is injective if and only if it is surjective.

Problem 2.

Let X be a set and suppose that $f : \mathbb{N} \to X$ is injective. Prove that X is an infinite set.

Problem 3.

Prove that if seven distinct numbers are chosen from the set $\{1, 2, \ldots, 11\}$, then there are two of these numbers which sum to 12.

Problem 4.

Let A be a set containing 51 positive integers, each less than or equal to 100. Prove that there are two elements of A which are consecutive numbers.

Problem 5.

Prove that if five points are chosen inside a square of side length 2, then there are two of them which are at distance no greater than $\sqrt{2}$ from each other.

Problem 6.

Let A be a set containing ten positive integers, each less than or equal to 100. Prove that there exist two disjoint non-empty subsets of A which have the same sum of elements.

Problem 1.

Suppose that X and Y are non-empty finite sets with $|X| = |Y|$, and let $f : X \to Y$ be a function. Show that f is injective if and only if it is surjective.

Sol. Assume that f is injective. Then f can be viewed as an injection $X \to \operatorname{Im} f$, so that $|Y| = |X| \leq |\operatorname{Im} f|$, by Corollary 11.1.1. On the other hand, $\operatorname{Im} f$ is a subset of the finite set Y, so that $|\operatorname{Im} f| \leq |Y|$ by Corollary 11.1.5. Therefore, we get that the subset $\operatorname{Im} f$ of Y has the same cardinality as Y, which clearly implies that $\operatorname{Im} f = Y$, so that f is surjective, as required.

Conversely, assume that $f : X \to Y$ is surjective. By Homework 6, Problem 1, f has a right-inverse $g : Y \to X$, meaning that $f \circ g = I_Y$. It easily follows from this that g is injective. By the first part of the proof, g is also surjective, i.e. g is a bijection. This implies that f is injective. Indeed, let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$. Since $g : Y \to X$ is surjective, there exist $y_1, y_2 \in Y$ with $x_1 = g(y_1)$ and $x_2 = g(y_2)$. Then the equality $f(x_1) = f(x_2)$ becomes $f(g(y_1)) = f(g(y_2))$, i.e. $y_1 = y_2$ since $f \circ g = I_Y$. Therefore, $x_1 = g(y_1) = g(y_2) = x_2$, as required.

Problem 2.

Let X be a set and suppose that $f : \mathbb{N} \to X$ is injective. Prove that X is an infinite set.

Sol. Assume for a contradiction that X is finite, say $|X| = n$ for some $n \in \mathbb{N}$. Since $f : \mathbb{N} \to X$ is injective, the restriction $f|_{\mathbb{N}_{n+1}} : \mathbb{N}_{n+1} \to X$ also is, so that $n + 1 = |\mathbb{N}_{n+1}| \leq |X| = n$ by Corollary 11.1.1, a contradiction. Hence X is infinite.

Problem 3.

Prove that if seven distinct numbers are chosen from the set $\{1, 2, \ldots, 11\}$, then there are two of these numbers which sum to 12.

Sol. Consider the following six sets : $\{1, 11\}, \{2, 10\}, \{3, 9\}, \{4, 8\}, \{5, 7\}, \{6\}$. By the Pigeonhole Principle, one of these sets must contain two of our chosen numbers. These two numbers must add to 12.

Problem 4.

Let A be a set containing 51 positive integers, each less than or equal to 100. Prove that there are two elements of A which are consecutive numbers.

Sol. Consider the following 50 sets : $\{1,2\},\{3,4\},\{5,6\},\ldots,\{99,100\}$. By the Pigeonhole principle, one of these sets must contain two elements of A. These two elements of A are then consecutive numbers.

Problem 5.

Prove that if five points are chosen inside a square of side length 2, then there are two of them which are at distance no greater than $\sqrt{2}$ from each other.

Sol. Divide the square into four squares of side length 1 by joining the middle points of opposite sides. By the Piegeonhole principle, one of these square must contain two of the points. These two points are contained in a square of side length 1, hence the distance between them is less than or equal to the length of the diagonal of the square, which is $\sqrt{2}$.

Problem 6.

Let A be a set containing ten positive integers, each less than or equal to 100. Prove that there exist two disjoint non-empty subsets of A which have the same sum of elements.

Sol. Consider the function f on $\mathcal{P}(A)\setminus\{\emptyset\}$ which maps a subset B of A to the sum of its elements. Each sum is certainly less than

$$91+92+93+94+95+96+97+98+99+100=955,$$

so that the image of f is contained in $\mathbb{N}_{955}$. Now, by Proposition 12.2.1, there are $2^{10}-1=1023$ non-empty subsets of A. By the Pigeonhole Principle, the function f is not injective, which is equivalent to saying that two non-empty subsets of A have the same sum of elements. If these two sets are disjoint, we are done. If not, note that any of the two sets is not a subset of the other, since otherwise the sum of their elements would be different. By removing from each of the sets their common element, we obtain two disjoint non-empty sets which still have the same sum of elements.

MAT 200, Logic, Language and Proof, Fall 2015 **Homework 8**

Due in Class : October 28, 2015.

Reading : Read Chap.12 and Chap.14

Turn in the following exercises.

Problem 1.

Suppose that X and Y are disjoint sets. One can prove that the function

$$\bigcup_{j=0}^{k} \mathcal{P}_j(X) \times \mathcal{P}_{k-j}(Y) \to \mathcal{P}_k(X \cup Y)$$

defined by

$$(A, B) \mapsto A \cup B$$

is a bijection. Taking this for granted, deduce that

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j} \binom{n}{k-j}. \tag{1}$$

Problem 2.

Prove that for $n \in \mathbb{N}$,

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} = 0.$$

Problem 3.

What is the sum of the coefficients of the polynomial $(1 + x)^{53}$?

Problem 1.

Suppose that X and Y are disjoint sets. One can prove that the function

$$\bigcup_{j=0}^{k} \mathcal{P}_j(X) \times \mathcal{P}_{k-j}(Y) \to \mathcal{P}_k(X \cup Y)$$

defined by

$$(A, B) \mapsto A \cup B$$

is a bijection. Taking this for granted, deduce that

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}. \tag{1}$$

Sol. Let $m, n \in \mathbb{N}$ and let X and Y be disjoint finite sets with $|X| = m, |Y| = n$. Then we have

$$\left|\bigcup_{j=0}^{k} \mathcal{P}_j(X) \times \mathcal{P}_{k-j}(Y)\right| = |\mathcal{P}_k(X \cup Y)| \tag{2}$$

since there is a bijection between these two finite sets. By a theorem proved in class, the cardinality in the right-hand side is equal to $\binom{m+n}{k}$, since

$$|X \cup Y| = |X| + |Y| = m + n$$

(recall that X and Y are disjoint). On the other hand, the sets in the union in the left-hand side are clearly pairwise disjoint so that we have, by the addition and multiplication principles,

$$\begin{aligned}\left|\bigcup_{j=0}^{k} \mathcal{P}_j(X) \times \mathcal{P}_{k-j}(Y)\right| &= \sum_{j=0}^{k} |\mathcal{P}_j(X) \times \mathcal{P}_{k-j}(Y)| \\ &= \sum_{j=0}^{k} |\mathcal{P}_j(X)||\mathcal{P}_{k-j}(Y)| = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}.\end{aligned}$$

Combining this with equation (2) gives the result.

Problem 2.

Prove that for $n \in \mathbb{N}$,

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} = 0.$$

Sol. We have, by the binomial theorem with $a = 1$ and $b = -1$,

$$0 = (1 + (-1))^n = \sum_{j=0}^{n} \binom{n}{j} 1^{n-j} (-1)^j = \sum_{j=0}^{n} (-1)^j \binom{n}{j}.$$

Problem 3.

What is the sum of the coefficients of the polynomial $(1 + x)^{53}$?

Sol. By the binomial theorem, we have

$$(1 + x)^{53} = \sum_{j=0}^{53} \binom{53}{j} 1^{53-j} x^j = \sum_{j=0}^{53} \binom{53}{j} x^j$$

hence the sum of the coefficients is

$$\sum_{j=0}^{53} \binom{53}{j} = 2^{53}.$$

MAT 200, Logic, Language and Proof, Fall 2015 — Homework 9

Due in Class : November 4, 2015.

Reading : Read Chap.15 and Chap.16

Turn in the following exercises.

Problem 1.

Prove that there does not exist a rational number whose square is 10.

Problem 2.

Prove that the set of polynomials with integer coefficients is denumerable. Deduce that the set of algebraic numbers is denumerable.

Hint : You can take for granted the fact that a polynomial equation

$$a_0 + a_1 x + \ldots a_n x^n = 0$$

has at most n real solutions.

Problem 3.

Prove that if an integer n is the sum of two perfect squares ($n = a^2 + b^2$ for $a, b \in \mathbb{Z}$), then n is of the form $4q + r$ for some $q \in \mathbb{Z}$, where $r = 0$, $r = 1$ or $r = 2$. Deduce that 1234567 cannot be written as the sum of two squares.

Problem 1.

Prove that there does not exist a rational number whose square is 10.

Sol. Assume for a contradiction that $\sqrt{10} = a/b$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. We can assume that the fraction a/b is in lowest terms. Then we have

$$10b^2 = a^2$$

which implies that a^2, and therefore a, is even. Write $a = 2a_0$ for some $a_0 \in \mathbb{Z}$. Then we have

$$10b^2 = 4a_0^2$$

i.e.

$$5b^2 = 2a_0^2$$

and so $5b^2$ is even. It is easy to see that this implies that b is even, a contradiction since we assumed that a and b had no common factor.

Problem 2.

Prove that the set of polynomials with integer coefficients is denumerable. Deduce that the set of algebraic numbers is denumerable.

Hint : You can take for granted the fact that a polynomial equation

$$a_0 + a_1x + \dots a_nx^n = 0$$

has at most n real solutions.

Sol. For $n \in \mathbb{Z}_{\geq}$, let P_n be the set of all polynomials of degree n with integer coefficients. Define a function $f : P_n \to \mathbb{Z}^{n+1}$ by

$$a_0 + a_1x + \cdots + a_nx^n \mapsto (a_0, a_1, \dots, a_n).$$

Clearly, f is bijective, so that P_n is denumerable, since $\mathbb{Z}^{n+1}$ is denumerable. Now, note that the set of polynomials with integer coefficients is the union over all $n \in \mathbb{Z}_{\geq}$ of the denumerable sets P_n. It is easy to see that this implies that the set is denumerable (we can display the elements of the union in a double infinite array as in the proof of Proposition 14.2.3).

To deduce that the set of algebraic numbers is denumerable, write the set of all polynomials with integer coefficients as an infinite list $\{p_1, p_2, \dots\}$ and for $j \in \mathbb{N}$, let R_j be the set whose elements are the roots of the polynomial p_j. Then each R_j is finite and the set of algebraic numbers is precisely the union over all $j \in \mathbb{N}$ of the sets R_j, which is denumerable.

Problem 3.

Prove that if an integer n is the sum of two perfect squares ($n = a^2 + b^2$ for $a, b \in \mathbb{Z}$), then n is of the form $4q + r$ for some $q \in \mathbb{Z}$, where $r = 0$, $r = 1$ or $r = 2$. Deduce that 1234567 cannot be written as the sum of two squares.

Sol. Suppose that $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. By the division theorem, we have

$$a = 2q_1 + r_1$$

and

$$b = 2q_2 + r_2$$

for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, with $r_j \in \{0, 1\}$, $j = 1, 2$. Using this, it is easy to find the remainder of $n = a^2 + b^2$ after division by 4. The remainders are displayed in the following table.

r_1	r_2	$r(n)$
0	0	0
0	1	1
1	0	1
1	1	2

We see that the only possible remainders for n are $0, 1, 2$, as required. Finally, since $1234567 = 4 \times 308641 + 3$, it follows from the above that 1234567 is not the sum of two perfect squares.