

CSCI 150 Discrete Mathematics
Homework 1
Due 09/11/09

Saad Mneimneh
Visiting Professor
Hunter College of CUNY

Problem 1: Surprising implication

The OR operator \vee has the following truth table:

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

Show that for every two propositions P and Q , regardless of their truth value, the following is true:

$$(P \Rightarrow Q) \vee (Q \Rightarrow P)$$

This means that either P implies Q or Q implies P , a rather surprising result because P and Q can be completely unrelated.

Show this in two ways:

- (a) using a truth table
- (b) replacing implication by an equivalent expression, e.g. $(p \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

Problem 2: Finally a proof

Consider Fermat's theorem:

$$\forall \text{ integers } n > 2, a > 0, b > 0, c > 0, \quad a^n + b^n \neq c^n$$

(a) Identify the different parts of this proposition:

- the quantifier, and what it means
- the variables, and the possible values they can take
- the predicate

(b) This proposition was stated by Fermat in 1637, and was proved by Andrew Wiles in 1995. A student in CSCI 150, who has just learned about the logic of implications, suggested the following proof:

pigs can fly \Rightarrow Fermat's theorem

The student argues that since $P \Rightarrow Q$ is true whenever P is false, that implication must be true and, therefore, is a proof of Fermat's theorem. What is wrong about the student's proof?

Problem 3: Proof by exhaustion

The absolute value of a real number x is defined as:

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Prove by exhaustions that for any two real numbers a and b , we have:

$$|a + b| \leq |a| + |b|$$

Note that there are infinite cases to consider for a and b (which would make proof by exhaustion impossible), but it is enough to consider only four cases:

- $a \geq 0, b \geq 0$
- $a \geq 0, b < 0$
- $a < 0, b \geq 0$
- $a < 0, b < 0$

Prove that the statement is true for each of the four case. Make sure you understand why these four cases are exhaustive.

Problem 4: Proof by contradiction

Prove by contradiction that there is no rational solution for $x^3 + x + 1 = 0$. This means assume that a rational solution r exists and, therefore,

$$\begin{aligned} r^3 + r + 1 &= 0 \\ r &= a/b \end{aligned}$$

where a/b is in reduced form, and both a and b are integers ($b \neq 0$). Arrive at a contradiction (argue about a and b being odd or even the same way we did in class for proving that $\sqrt{2}$ is irrational).

Problem 5: Prime generating polynomial

Consider the following proposition:

$$\forall x \in \mathbb{N}, x^2 + x + 41 \text{ is prime}$$

We argued in class that this proposition is false because the predicate

$$x^2 + x + 41 \text{ is prime}$$

is false for $x = 40$ (try it).

The polynomial $x^2 + x + 41$ is the best known polynomial for generating prime numbers because it gives distinct primes for the 40 consecutive non-negative

integers 0 to 39. This polynomial was discovered by Euler in 1772. In general, a polynomial of $p(x)$ of degree d can be written as

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

where $a_d \neq 0$. It is not hard to show that no polynomial of degree $d \geq 1$ generates only prime numbers. In this problem you are asked to prove this **by contradiction**. Use the following true propositions:

- any polynomial $p(x)$ of degree $d \geq 1$ can be written as $p(x) = xq(x) + c$ where $q(x)$ is a polynomial of degree $d - 1$.
- if $p(x)$ generates only primes, then c must be prime.
- if x is a multiple of c , then $p(x)$ is also a multiple of c , e.g. if $x = kc$, then $p(kc) = kc \cdot q(kc) + c = c[k \cdot q(kc) + 1]$.
- a multiple of c is prime only if it is equal to c .
- if $q(x)$ has degree $d - 1$, then there can be at most $d - 1$ values for x for which $q(x) = 0$.