

The contrapositive proof method

The following two statements are equivalent;

1) " $P \Rightarrow Q$ "

2) " $\text{Not } Q \Rightarrow \text{Not } P$ "

P	Q	$P \Rightarrow Q$	$\text{Not } Q$	$\text{Not } P$	$\text{Not } Q \Rightarrow \text{Not } P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Example! Let R, S, and T be sets.

Prove that

1) $R \cap S = \emptyset \Rightarrow (R \cup T) \cap (S \cup T) \subset T$.

The statement $\overset{P}{R \cap S = \emptyset}$ is equivalent to $\overset{Q}{(R \cup T) \cap (S \cup T) \subset T}$

$$2) (R \cup T) \cap (S \cup T) \not\subseteq T \Rightarrow R \cap S \neq \emptyset.$$

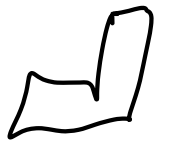
Assume that there exists an element $x \in (R \cup T) \cap (S \cup T)$ such that $x \notin T$.
We need to show that $R \cap S \neq \emptyset$.

Now $(x \in R \cup T)$ AND $(x \in S \cup T)$

AND $(x \notin T)$. So $x \in R$ and

$x \in S$. So $x \in R \cap S$. So

$R \cap S \neq \emptyset$.



Proof by Contradiction

We assume that a statement we wish to prove is false, and derive from the assumption a contradiction,

Recall: An integer $p \neq 1$ is PRIME, if the only positive integers dividing it are 1 and p .

Fact: Every integer $n > 1$ is divisible by some prime > 1 .

Proposition: (Euclid) There are infinitely many positive primes.

Proof by contradiction:

Assume that there are only finitely many positive primes. $p_1, p_2, \dots, p_N$.
all the primes

Let $n = (p_1 \cdot p_2 \cdots p_N) + 1$.

product of all^N primes

Then $n > 1$. So there exists a positive prime $p > 1$, such that $p \mid n$. The prime p is equal to p_i , for some $1 \leq i \leq N$, by assumption. So $p \mid n - 1$. So $p \mid (n - \underbrace{(n-1)}_1)$.

This is a contradiction, since $p > 1$. Hence, there are infinitely many primes. $\square$

Next proof method:

Proving " $P \Rightarrow (Q \text{ OR } R)$ ".

If Q is true, then the statement is true. If Q is false, then the statement is equivalent to " $P \Rightarrow R$ ". So the above statement is equivalent to

" $P \text{ AND } (\text{NOT } Q) \Rightarrow R$ "

Example: Let a, b be integers.

"If $\underbrace{a^3 + b}_{\text{I}}$ is odd, then $\underbrace{a \text{ is odd OR } b \text{ is odd}}_{\text{R}}$."

Assume that $a^3 + b$ is odd and a is even. Then a^3 is even.

So $\underbrace{(a^3 + b)}_{\text{odd}} - \underbrace{a^3}_{\text{even}}$ is odd. So b is odd. 

Proof by Counter Example:

Consider a statement of the form

$$\forall x, P(x)$$

Suppose that we want to show that it is NOT true.

$$\text{"Not } (\forall x, P(x))\text{"}$$



$$\text{"} \exists x, \text{Not } P(x) \text{"}$$

It suffices to find ONE x for which $P(x)$ is false."

Example: Disprove the following:

"Every positive integer can be written as a sum of three squares (of integers)."

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$4 = 2^2 + 0^2 + 0^2$$

$$5 = 2^2 + 1^2 + 0^2$$

$$6 = 2^2 + 1^2 + 1^2$$

$$7 =$$

Proof that 7 is a counter

Example: Suppose that a, b, c are integers (we may assume non negative as we square them) such that $a^2 + b^2 + c^2 < 8$.

Then $a, b, c \in \{0, 1, 2\}$.

Furthermore, at most one of them is equal to 2. So we may assume that

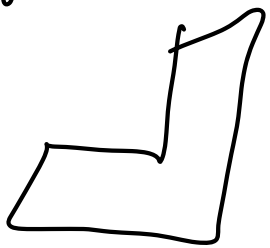
$a, b \in \{0, 1\}$ and $c \in \{0, 1, 2\}$.

Then $a^2 + b^2 + c^2 \leq 6 \neq 7$.

$\wedge$
1

$\wedge$
1

$\wedge$
4

So 7 can not be written as
a sum of 3 squares. 

Ch. 2 Integers and Diophantine Equations.

Sec 2.1: The Division Algorithm

Def: Let a, b be integers.

Then " a divides b ", denoted by
" $a \mid b$ "

if there exists an integer q ,
such that $b = aq$.

Ex: $3 \mid 12$ because $\underset{b}{12} = \underset{a}{3} \cdot \underset{q}{4}$

$-3 \mid 12$ " $12 = (-3) \cdot \underset{q}{(-4)}$
 $2 \nmid 5$.

$0 \nmid 2$ because

$$0 \cdot q = 0 \neq 2.$$

Prop 2.11: Let a, b, c be integers.

(i) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(ii) If $a \mid b$ and $a \mid c$, then

for every integers x, y ,
 $a \mid (xb + yc)$.

In particular, $a \mid b+c$ and

(iii) If $a \mid b$ and $b \mid a$, then
 $a=b$ or $a=-b$.

(iv) If $a \mid b$ and $b \neq 0$, then

$$|a| \leq |b|.$$

Proof: (i) Assume that $a \mid b$ and $b \mid c$. Then there exist integers g_1, g_2 such that $b = ag_1$, $c = bg_2$.

$$c = b g_2 = (a g_1) g_2 = a (\underbrace{g_1 g_2}_g). \text{ So } a | c.$$

(ii) Assume that $a | b$ and $a | c$. Then there exist integers g_1, g_2 such that $b = a g_1$, $c = a g_2$. Then for every integers x, y , we have

$$x b + y c = x(a g_1) + y(a g_2) =$$

$$= a (\underbrace{x g_1 + y g_2}_g).$$

Hence, there exist an integer g such that $x b + y c = a g$. Thus

$$a | x b + y c.$$

(iii) Assume that $a | b$ and $b | a$.

Then there exist integers g_1, g_2 such that $b = a g_1$ and $a = b g_2$.

$$\text{So } b = a g_1 = (b g_2) g_1 = b (g_2 g_1).$$

If $b = 0$, then $a = b g_2 = 0 g_2 = 0$.

So $a = b$.

If $b \neq 0$, then $b = b(g_2 g_1)$ means

that $g_2 g_1 = 1$. So

either $g_1 = g_2 = 1$ or $g_1 = g_2 = -1$.

So either $b = a \cdot 1 = a$ or

$$b = a \cdot (-1) = -a.$$

(iv) Assume $a|b$ and $b \neq 0$.

Then there exists an integer g_1 such that $b = a g_1$.

So $|b| = |a| |g_1|$ and $|g_1| \neq 0$ (because otherwise $b = 0$). So $|g_1| \geq 1$.

So $|b| \geq |a| \cdot 1 = |a|$.

