The contrapositive proof method

The following two statements are equivalent:

1) "$P \Rightarrow Q$"

2) "Not $Q \Rightarrow$ Not P"

P	Q	$P \Rightarrow Q$	Not Q	Not P	Not $Q \Rightarrow$ 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

<u>Example:</u> Let R, S, and T be sets.

Prove that

1) $\underbrace{R \cap S = \emptyset}_{P} \Rightarrow \underbrace{(R \cup T) \cap (S \cup T) \subset T}_{Q}$.

The statement is equivalent to

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

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 $R \cap S \neq \emptyset$. $\square$

Proof by Contradiction

We assume that a statement we wish to prove is false, and derive from the asscumption 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. $\underbrace{P_1, P_2, \ldots, P_N}_{\text{all the primes}}$.

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 $\boxed{p \mid n}$. The prime p is equal to p_i, for some $1 \le i \le N$, by assumption.

So $\boxed{p \mid n-1}$. So $p \mid \underbrace{(n-(n-1))}_{1}$.

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

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

<u>Example:</u> Let a, b be integers.

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

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.

b //

$\square$

Proof by Counter example:

Consider a statement of the form

$$\forall x, \; \underline{P}(x)$$

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

"Not $(\forall x, \; P(x))$"

$\Longleftrightarrow$

"$\exists x, \;$ Not $P(x)$".

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

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

Then $\underset{\le 1}{a^2} + \underset{\le 1}{b^2} + \underset{\le 4}{c^2} \le 6 \neq 7.$

so 7 can not be written as a sum of 3 squares. $\square$

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 $\underbrace{12}_{b} = \underbrace{3}_{a} \cdot \underbrace{4}_{q}$

$-3 \mid 12$ " $12 = (-3)\underbrace{(-4)}_{q}$

$2 \nmid 5$.

$0 \nmid 2$ because

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

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

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

(ii) If $a | b$ and $a | c$, then for every integers x, y,

$$a \mid (xb + yc).$$

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

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

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

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

Proof: (i) Assume that $a | b$ and $b | c$. Then ~~there~~ exist integers q_1, q_2 such that $b = aq_1$, $c = b q_2$.

$c = bq_2 = (aq_1)q_2 = a\underbrace{(q_1 q_2)}_{q}$. So $a \mid c$.

(ii) Assume that $a \mid b$ and $a \mid c$. Then there exist integers q_1, q_2 such that $b = aq_1$, $c = aq_2$. Then for every integers x, y, we have

$$xb + yc = x(aq_1) + y(aq_2) =$$

$$= a(\underbrace{xq_1 + yq_2}_{q}).$$

Hence, the exist an integer q such that $xb + yc = aq$. Thus

$$a \mid xb + yc.$$

(iii) Assume that $a \mid b$ and $b \mid a$.

Then there exist integers q_1, q_2 such that $b = aq_1$ and $a = bq_2$.

So $b = aq_1 = (bq_2)q_1 = b(q_2 q_1)$.

If $b=0$, then $a=bq_2=0q_2=0$.
So $a=b$.

If $b\neq 0$, then $b=b(q_2q_1)$ means that $q_2q_1=\underline{1}$. So either $q_1=q_2=1$ or $q_1=q_2=\underline{-1}$.

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 q such that $b=aq$.
So $|b|=|a||q|$ and $|q|\neq 0$ (because otherwise $b=0$). So $|q|\geq 1$.
So $|b|\geq |a|\cdot 1=|a|$. ◻