INTRODUCTION TO PROOFS

☆ A proof is a valid argument that establishes the truth of a mathematical statement. Such mathematical statements having proofs are called theorems.

☆ Aim: to describe methods for constructing proofs.

☆ one can use the following ingredients for proofs

1. Hypothesis of the theorem
2. Axioms assumed to be true (if any)
3. previously proven theorems

along with these ingredients one can use rules of inference to establish the truth of given statement being proved.

Lemma: A lemma is a less important theorem that is used to prove an important theorem

Corollary: A theorem that can be established from a theorem that has been proved

Conjecture: is a statement that is being proposed to be true statement, based on some partial evidence or by intuition of an expert. (but not have a proof.) usually when a proof of a conjecture is found, the conjecture becomes a theorem.

Remark: many theorems are stated like a property hold for all elements of a domain, so that a universal quantifier is used there. But in mathematics conventionally we avoid using universal quantifier explicitly.

Example:

"If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$"

really means that

"for all positive real numbers x and y, if $x > y$, then $x^2 > y^2$"

☆ Generally these kind of theorems are proved by using the law of universal instantiation without explicit mention.

The first step of the proof is usually involve selecting a general element from the domain and subsequent steps shows

this element has property in question. finally universal generalization implies that the theorem hold for all members of the domain.

Methods of proving theorems

There are many theorems which involve the conditional statements. So first we focus on some methods of proofs for theorems involving conditional statements of the form $\forall x (P(x) \rightarrow Q(x))$.

we know the conelitional statement $p \rightarrow q$ is true unless p is true, but q is false.

So to prove $p \rightarrow q$ is true, it is enough to show that q is true if p is true.

1. Direct proof

many theorems / Results have direct proofs. which are some (obvious) sequence of steps leading from the hypothesis to conclusion. That is start with premises, continue with a sequence of deductions, and end with the conclusion.

Definition: An integer n is **even**, if there exist an integer k such that $n = 2k$, and n is **odd** if there exist an integer k such that $n = 2k+1$ (note that an integer is either even or odd, no integer is both even and odd)

Example: Give a direct proof of the theorem

"If n is an odd integer, then n^2 is odd"

Proof:

Note that given theorem equivalent to $\forall n\,(P(n) \rightarrow Q(n))$ where

$P(n)$: n is odd integer.

$Q(n)$: n^2 is odd integer.

Assume hypothesis of this conditioned stmt is true that is, assume that n is odd.

$\therefore n = 2k+1$ (by def. of odd integer)

Thus, $n^2 = (2k+1)^2$

$= 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$

Now it follows by the definition of odd integer that n^2 is odd.

Example 2: Give a direct proof for

" If m and n are perfect squares, then mn is also perfect square"

(An integer a is a perfect square, if there is an integer b such that $a = b^2$.)

proof:

suppose hypothesis of this conditional stmnt is true. that is

assume that m and n are perfect squares.

∴ by definition of perfect squares there are integers s and t such that

$m = s^2$ and $n = t^2$

Thus $mn = s^2 \cdot t^2$

$= (st)^2$

(using commutativity and associativity of multiplication)

by definition of perfect square, it follows that mn is also a perfect square, because it is the square of st, which is an integer.

Hence we proved that if m and n are perfect squares, then mn is also perfect square.

2. Proof by Contraposition

For some results, involving the conditional statements of the form $\forall x (P(x) \rightarrow Q(x))$, attempts of direct proofs often reach - dead ends. (i.e. we started from hypothesis, continued deductions, but cannot reach conclusion)

proofs that do not start with the hypothesis and end with the conclusion, are called indirect proofs.

The proof by contraposition is an indirect proof, where we use the idea that the conditional statement $P \rightarrow Q$ is equivalent to the - contrapositive $\neg Q \rightarrow \neg P$.

In method of proof by contraposition we take $\neg Q$ as hypothesis, and we use axioms, definitions and previously proven theorems together with rules of inference we show that $\neg P$ must follow.

Example: prove that if n is an integer and $3n+2$ is odd then n is odd

proof.

Trying by direct method:

The given statement can be written in conditional form as follows

"If $3n+2$ is odd, then n is odd"

that is of the form $p \rightarrow q$.

Assume p is true, that is

Assume $3n+2$ is odd.

Then by definition of odd integer, there exist an integer k such that

$$3n+2 = 2k+1$$

Thus $3n+1 = 2k$,

further any deduction will not help us to conclude n is odd. #

proof by method of contrapositron:

The contrapositive of given statement is,

"If n is even, then $3n+2$ is even"

This is of the form $\neg q \rightarrow \neg p$.

now assume $\neg q$ is true,

that is, assume that n is even,

then by definition of even integer, there exist an integer k such that

$$n = 2k.$$

Next we substitute this value of 'n' in $3n+2$

Then we get, $3n+2 = 3(2k)+2$

$= 2(3k)+2$

$= 2(3k+1)$

This shows that, $3n+2$ is an even integer, as $3n+2$ is a multiple of 2.

That is $\neg p$ is true.

that is negation of the conclusion of the given conditional statement implies that the hypothesis is false.

Thus by method of contraposition, we proved that

"If $3n+2$ is odd, then n is odd"

Example 2: prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof.

The given conditional statement is

"If $n = ab$, where a and b are +ve integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$"

we can see that the assumption that, $n = ab$ cannot give the conclusion by any direct deductions. Thus we go with method of contraposition.

The contrapositive of given conditional stmnt is
"If $a \leq \sqrt{n}$ and $b \leq \sqrt{n}$ are false, then
$n = ab$ is false" that is
"If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $n \neq ab$"
Here $\neg q$ is $(a > \sqrt{n}) \wedge (b > \sqrt{n})$
Assume $\neg q$ is true, that is
that is $(a > \sqrt{n}) \wedge (b > \sqrt{n})$ is true
i.e. $a > \sqrt{n}$ and $b > \sqrt{n}$
never multiply these inequalities by the
fact that four +ve integers, we have if
$s < t$ and $u < v$, then $su < tv$.
we get $ab > n$
This shows that $ab \neq n$.
that is $\neg p$ is true., i.e. p is false
because the negation of conclusion of the
conditional statement implies that the hypothesis
is false, the original conditional stmnt is
true.
Thus proof followed by method of contraposition.

Vacuous and Trivial proofs.

☆ Vacuous proofs: we can quickly prove $p \to q$ is true when p is false, because $p \to q$ must be true when p is false. So, if we can show that p is false, then we have a proof, called a vacuous proof.

☆ Vacus proofs are often used to prove special cases of theorems that states a conditional stmnt is true for all +ve integers. [i.e. theorems of the form $\forall n\, P(n)$]

☆ Example: Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

Proof.

Note that $P(0)$ is "if $0 > 1$, then $0^2 > 0$"

we can show $P(0)$ by using a vacuous proof, because the hypothesis $0 > 1$ is false. This, tells us that $P(0)$ is automatically true.

Trivial proof: suppose the conclusion in the conditional statement $p \to q$, that is q is true, then $p \to q$ is always true.

If we could proove q is true, then we have a proof for $p \to q$ called trivial proof.

☆ Trivial proofs are often used to proove special cases of theorems that states a conditional stmnt is true for all +ve integers. [i.e. theorems of the form $\forall n\, P(n)$]

Example: Let P(n) be "If a and b are +ve integers with $a \geq b$, then $a^n \geq b^n$" where the domain consists of all integers. show that P(0) is true.

Proof.

P(0) is "If $a \geq b$ +ve integers with $a \geq b$, then $a^0 \geq b^0$"

Because $a^0 = 1$ and $b^0 = 1$ the conclusion of conditional Statement, $p \to q$: "If $a \geq b$, then $a^0 \geq b^0$" is $q : a^0 \geq b^0$ is true. Hence this conditional stmnt, i.e. P(0) is true.

A little proof Strategy.

So far we studied mainly two methods of proofs namely direct proof and proof by method of contraposition.

☆ when a Result or statement need to be proved, sometimes we cannot quickly identify which method to be used, due to this problem we use the following strategy -

"when you want to proove a stmnt of the form $\forall x (P(x) \rightarrow Q(x))$, first evaluate whether a direct proof looks promising. begin by expanding the definitions in the hypotheses, together with axioms and available theorems. If a direct proof does not seem to go anywhere, try the same thing with a proof by contraposition. Recall that in method of contraposition, we conclusion of conditional stmnt is false and use a direct proof to show this implies that the hypothesis must be false.

Definition: The real number r is rational if there exist integers p and q, with $q \neq 0$, such that $r = p/q$. A real number that is not rational is called irrational.

Example: proove that the sum of two rational numbers is rational.

Proof.

The given statement in logical conditional form is "for every real number r and every real number s, if r and s are rational numbers, then $r+s$ is rational number."

First we attempt a direct proof:

Suppose r and s are rational numbers.

Thus from definition of rational numbers we have, there exist p & $q \neq 0$ such that $r = p/q$ and t & $u \neq 0$ such that $s = t/u$.

now $r+s = \frac{p}{q} + \frac{t}{u}$

$= \frac{pu + qt}{qu}$

as $q \neq 0$, $u \neq 0$ we have $qu \neq 0$.

So $r+s$ is ratio of two integers $pu + qt$ and $qu \neq 0$.

This means that $r+s$ is rational.

Thus we proved sum of two rational numbers is rational.

direct proof successful in this case.

Example: prove that, if n is an integer and n^2 is odd, then n is odd.

Proof.

First Let us try for direct proof:

The given conditional statement is

" If n^2 is odd, then n is odd ", where domain is all integers.

which is of the form $p \rightarrow q$.

Suppose p is true.

that is n^2 is odd.

Then by definition of odd integer, there exist an integer k such that

$$n^2 = 2k + 1$$

$$\Rightarrow n = \pm\sqrt{2k+1}$$

but from this we cannot conclude that whether n is odd or not.

So direct proof fails.

Now we try proof by contraposition:

The contrapositive of given conditional statement is as follows

$\neg q \rightarrow \neg p$: "If n is not odd, then n^2 is not odd"

Assume $\neg q$ is true.

that is assume that n is not odd integer.

thus n is even integer.

then by definition of even integer, there exist an integer k such that

$$n = 2k$$

Thus $n^2 = (2k)^2$

$$= 4k^2$$

$= 2(2k^2)$

This shows that n^2 is an even integer.

that n^2 is not an odd integer.

that is $\neg p$ is true.

thus we have proof for the given conditional stmnt by contraposition method.

---

proof by contradiction

suppose we want to prove a stmnt P is true.

suppose we find a contradiction q,

($q = r \wedge \neg r$ for some proposition r,

note that $r \wedge \neg r$ is contradiction/always F)

so that $\neg p \rightarrow q$ is true, then we have a proof for p called proof by contradiction.

because, as q contradiction, always false

if $\neg p \rightarrow q$ true.

Then $\neg p$ must be false

implies p is true.

Remark: note that this is not a direct method of proof, so it is an indirect proof method.

Example : Show that atleast four of any 22 days must fall on the same day of the week.

Ans.

Let p be the proposition

P: "Atleast four of 22 chosen days falls on same day of the week"

Here the $\neg p$ is the proposition,

$\neg P$: "atmost three of 22 chosen days falls on same day of the week"

Since there are 7 days of a week namely

Sun Mon Tues Wed Thus Fri Sat

by assigning atmost 3 days to each day of week we get a maximum of 21 days. which contradicts the hypothesis that we have 22 days under consideration.

i.e. If γ : 22 days are chosen.

Then we have shown that $\neg p \rightarrow (\gamma \wedge \neg\gamma)$

i.e. $\neg p \rightarrow (\gamma \wedge \neg\gamma)$ true.

$\Rightarrow$ $\neg p$ is false.

$\Rightarrow$ p is true.

Example : prove that

If a^2 is even, then a is even

proof : Here we use method of contraposition,

given, $p \rightarrow q$

Then to prove $\neg q \rightarrow \neg p$

Suppose a is odd

$\Rightarrow a = 2k+1$ then

$$a^2 = 4k^2 + 4k + 1$$

$$= 2(2k^2 + 2k) + 1$$

i.e. a^2 is odd $\Rightarrow \neg p$ true.

Thus proof of original stmnt follow by method of contraposition

Example : prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

proof.

Let p : $\sqrt{2}$ is irrational. then

$\neg p$: $\sqrt{2}$ is rational.

Assume $\neg p$ is true.

that is $\sqrt{2}$ is rational,

then by definition of rational numbers,

There exist a and b such that a and b have no common factors and

$$\sqrt{2} = a/b . \quad \text{---} (1)$$

Ques: (4)

Thus $2 = a^2/b^2$, (by squaring both side of (1))

that is $a^2 = 2b^2$. —— (2)

this implies a^2 is even integer, by definition of even integer.

now we use the fact that if a^2 is even then a is even.

then there exist an integer k such that $a = 2k$. — (3)

Thus, use this a in equation (2), we get $(2k)^2 = 2b^2$

$\Rightarrow 4k^2 = 2b^2$

$\Rightarrow b^2 = 2k^2$.

That is b^2 is even.

now again use the fact that if square of an integer is even then the integer itself is even.

that is b is even,

thus there exist some integer m, such that $b = 2m$ — (4)

Now (3) and (4) is a contradiction to our assumption that a and b have no common factors. because (3) and (4) says a and b have 2 as common factor.

thus if 2 divides a & b.

then we have $\neg p \to \neg r$ (by assumption on $a \leq b$)

and we also saw by some deductions that $\neg p \to r$.

that is $\neg p \to (r \wedge \neg r)$ is true.

$\Rightarrow$ $\neg p$ is false

$\Rightarrow$ p is true.

that is $\sqrt{2}$ is irrational.

Remark: proof by contradiction can be used to prove conditional statements.

Here the idea is:

suppose we want to prove $p \to q$

we assume p and $\neg q$ both are true.

then we get a contradiction F.

i.e. $p \wedge \neg q \to F$

(the reason that this proof is valid rest on the logical equivalence of $p \wedge \neg q \to F$ and $p \to q$)

so to prove $p \to q$, it is enough to find a contradiction under the assumptions that p and $\neg q$ are true.

Remark: proof by contraposition of a conditional stmt can be written as proof by contradiction as follows.

To prove $p \to q$, by contraposition we assume $\neg q$ true, then by deductions we prove $\neg p$.

the same proof in contradiction way;
assume p and $\neg q$ true.
get $\neg p$ true by contraposition method,
then we have the contradiction $p \wedge \neg p$
completing the proof.

Example: Give a proof by contradiction of the theorem "If $3n+2$ is odd, then n is odd"

Ans: given stmt is of the form $p \to q$.
p: $3n+2$ is odd
q: n is odd.
For proof by contradiction,
assume p and $\neg q$ are true.
i.e. $3n+2$ is odd and n is even.
n even $\Rightarrow$ $n = 2k$

Thus $3n+2 = 3(2k)+2$

$= 2(3k)+2$

$= 2(3k+1)$

That is $3n+2$ is even.

That is $\neg p$ is true.

$p \wedge \neg p$ true is a contradiction.

This completes proof by contradiction.

i.e. If $3n+2$ odd then n is odd.

Remark: The method of direct proof of a conditional stmnt can be written as proof by contradiction as follows.

To prove $p \to q$, by direct method we assume p true, then by deductions we prove q.

the same proof in contradiction way;
assume p and $\neg q$ true.
get q is true by direct proof method,
then we have the contradiction $q \wedge \neg q$.
completing the proof.

Proofs of Equivalence

To prove theorems having a biconditional stmnt $p \leftrightarrow q$, it is enough to show - that $p \to q$ and $q \to p$ are both true.
[validity of this is approach is based on

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p) \quad]$$

Example : If n is positive integer, then n is odd if and only if n^2 is odd.

Ans. (proof.)

The given stmnt is of the form $p \leftrightarrow q$ where p : n is odd and q : n^2 is odd.

we proved $p \to q$ by direct method, and $q \to p$ by proof by contraposition.

Hence $p \leftrightarrow q$ follows.

Note : If a theorem having $p \leftrightarrow q$, then we say that p is equivalent to q. or p and q are equivalent.

Sometimes, a theorem states that several propositions are equivalent, that is of the form the propositions $p_1, p_2, p_3 \cdots p_n$ are equivalent. This can be written as

$$p_1 \leftrightarrow p_2 \leftrightarrow p_3 \leftrightarrow \cdots \leftrightarrow p_n.$$

note that this says that all n propositions have same truth value, and thus for any $0 \leq i, j \leq n$, p_i and p_j are equivalent.

one can show that

$$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n \equiv (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_n \rightarrow p_1)$$

similarly

$$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n \equiv (p_n \rightarrow p_{n-1}) \wedge (p_{n-1} \rightarrow p_{n-2}) \wedge \cdots \wedge (p_2 \rightarrow p_1) \wedge (p_1 \rightarrow p_n).$$

Example: show that following statements about integer n are equivalent.

p_1 : n is even

p_2 : n-1 is odd

p_3 : n^2 is even.

Proof.

$p_1 \rightarrow p_2$: direct proof can use.

suppose p_1 true.

i.e. n is even.

then there exist k such that

$n = 2k$ (by def of even)

then $n-1 = 2k-1$

$= 2k-1+(1-1)$

$= 2k-2+1$

$= 2(k-1)+1$

This shows n-1 is odd.

$p_2 \to p_3$: direct proof can use.

suppose p_2 true.

i.e. $n-1$ is odd

then there exist k such that

$n-1 = 2k+1$ (by def of odd)

then $n = 2k+2$

so $n^2 = 4k^2+8k+4$

$= 2(2k^2+4k+2)$

This shows n^2 is even.

$p_3 \to p_1$: proof by contraposition.

suppose $\neg p_1$ is true.

i.e. n is odd.

then there exist k such that,

$n = 2k+1$ (by def. of odd)

$n^2 = 4k^2+4k+1$

$= 2(2k^2+2k)+1$

This shows n^2 is odd

that is $\neg q$ is true.

thus proof follows by — contraposition.

Counterexample : we know that the — quantified proposition $\forall x\, p(x)$ is false if there exist an x_0 in domain for which $p(x_0)$ is false, such an element x_0 is called counterexample.

Suppose by the attempts of all proof methods fails for a statement of the form $\forall x P(x)$, and we feel that $\forall x P(x)$ is false, then we look for a counter example.

Example : Show that the stmnt " Every positive integer is the sum of the squares of two integers" is false.

Ans : The given stmnt says that if n is a positive integer then there exist integers s and t such that $n = s^2 + t^2$.

To show given stmnt false - we look for counterexample.

Let try with 1,

we have $1 = 1^2 + 0^2$

when $n = 2$, $2 = 1^2 + 1^2$.

but for $n = 3$, there is no integers s and t so that $3 = s^2 + t^2$.

thus 3 is a counterexample for the given stmnt. Hence given stmnt is false.

Mistakes in proof

There are many common errors made in constructing mathematical proofs.

most common errors are mistakes in arithmetic and basic formulae

each steps of mathematical proof needs to to be correct and the conclusion needs to follow logically from the steps that precede it.

Example: what is wrong with the proof that $1 = 2$?

proof.

Let a and b be two equal +ve integers.

1. $a = b$ given
2. $a^2 = ab$ multiplying both side of (1) with a.
3. $a^2 - b^2 = ab - b^2$ substract b^2 on both side of (2)
4. $(a-b)(a+b) = b(a-b)$ factor both side of (3)
5. $(a+b) = b$, divide both side of (4) by $(a-b)$
6. $2b = b$, substitute $a=b$ on (5)
7. $2 = 1$, divide both side of (6) by b.

Here every step is valid except for step 5, where we divided both side by $a-b$. The error is that $a-b=0$; division of both side of an equation by the same quantity is valid as long as this quantity is not zero.

Example: what is wrong with the given proof of "if n^2 is positive, then n is positive"

Proof: Suppose n^2 is +ve. — (1)

we know that

"If n is +ve, then n^2 is +ve" — (2)

From (1) and (2) we conclude that n is +ve.

But, Let $P(n)$: n is +ve &

$Q(n)$: n^2 is +ve

Then the statement (2) is equivalent to

$\forall n\,(P(n) \rightarrow Q(n))$ and

(1) is equivalent to $Q(n)$.

Thus we used that

$$\frac{\forall n\,(P(n) \rightarrow Q(n)) \quad Q(n)}{\therefore P(n)}$$

This is not a valid rules of inference.

Hence the given proof is not true.

as a counterexample for above statement we can give $(-1)^2 = 1$ is +ve but -1 is $-ve$.

Example: what is wrong with the proof of the statement

"If n is not +ve, then n^2 is not +ve"

given proof:

Suppose n is not +ve. — ①

We know that,

"If n is +ve, then n^2 is +ve" — ②

From ① and ② we conclude that

n^2 is not +ve.

Here, Let $P(n)$: n is +ve

$Q(n)$: n^2 is +ve.

Then ② is $\forall n (P(n) \rightarrow Q(n))$ and

① is $\neg P(n)$

So we used that

$$\frac{\forall n (P(n) \rightarrow Q(n)) \quad \neg P(n)}{\therefore \neg Q(n)}$$

because here also we are not using a valid rules of inference.

Hence the given proof is not true.

As a counter example, -1 is not +ve, but $(-1)^2 = 1$ is +ve.

Remark: When one or more steps of a proof are based on the truth of the statement being proved, then

the proof is not correct; such reasoning are called circular reasoning.

Example: what is wrong with given proof of the stmt

" n is even integer, whenever n^2 is an even integer"

proof. suppose that n^2 is even.

Then $n^2 = 2k$ for some integer k.

Let $n = 2l$ for some integer l.

this shows that n is even.

This proof is incorrect because the stmt "let $n = 2l$ for some integer l" used in proof, but no argument has been given to show that n can be written as $2l$ for some integer l. This is a circular reasoning, because this stmt is equivalent to the stmt being proved.

Proof by cases.

Suppose we want to prove a conditional statement of the form

$(P_1 \vee P_2 \vee \cdots \vee P_n) \longrightarrow Q$

Then it is enough to prove that

$(P_1 \to Q) \wedge (P_2 \to Q) \wedge \cdots \wedge (P_n \to Q)$.

This is because of the logical equivalence

$(P_1 \vee P_2 \vee \cdots \vee P_n) \to Q \equiv (P_1 \to Q) \wedge (P_2 \to Q) \wedge \cdots \wedge (P_n \to Q)$

Such a proof is called proof by cases.

Remark: Some time to prove the conditional Stmnt $p \to q$ is tough, it is convenient to prove $(P_1 \vee P_2 \vee \cdots \vee P_n) \longrightarrow q$ where

$p \equiv (P_1 \vee P_2 \vee \cdots \vee P_n)$

Exhaustive proof: Some theorems can be proved by examining relatively small number of examples. Such proofs are called exhaustive proofs.

For example, when a result stated for few elements of a domain, we can prove the statement for each element separately.

Remark: Note that exhaustive proofs are some special type of proof by cases.

Example: prove that $(n+1)^2 \geq 3^{n-1}$ if n is a positive integer with $n \leq 3$.

proof. we use proof by exhaustion.

we only need to verify the inequality $(n+1)^2 \geq 3^{n-1}$ when $n = 1, 2,$ and 3

when $n = 1$: $(n+1)^2 = (1+1)^2 = 2^2 = 4$ and

$3^{n-1} = 3^{1-1} = 3^0 = 1$

Thus $4 = (n+1)^2 \geq 3^{n-1} = 1$ holds.

when $n = 2$: $(n+1)^2 = (2+1)^2 = 3^2 = 9$ and

$3^{n-1} = 3^{2-1} = 3^1 = 3$

Thus $9 = (n+1)^2 \geq 3^{n-1} = 3$ true.

when $n = 3$: $(n+1)^2 = (3+1)^2 = 4^2 = 16$ and

$3^{n-1} = 3^{3-1} = 3^2 = 9$

in each of these 3 cases - we have $(n+1)^2 \geq 3^{n-1}$

Thus we proved the given result.

Example: prove that the only consecutive +ve integers not exceeding 100 that are perfect powers are 8 and 9.

(An integer is a perfect power if it is equals n^a, where a is an integer > 1)

proof.

The perfect powers which are less than (or =) 100 are

power 2 : 1, 4, 9, 16, 25, 36, 49, 64, 81, 100

power 3 : 1, 8, 27, 64

power 4 : 1, 16, 81

power 5 : 1, 32

power 6 and above we have only 1.

by looking into these perfect powers we can see that only 8 and 9 are consecutive.

Thus by method of exhaustion we proved the given result.

Some examples for proof by cases.

Example : prove that, if n is an integer, then $n^2 \geq n$.

proof.

we prove $n^2 \geq n$ for all integers n by considering the following 3 cases.

case 1 : when $n = 0$.

as $0^2 = 0$ we have

$0 = n^2 \geq n = 0$ is true.

Thus $n^2 \geq n$ when $n = 0$.

case 2 : when $n \geq 1$.

we multiply both sides of inequality $n \geq 1$ by +ve integer n, we get $n^2 \geq n$.

This implies that $n^2 \geq n$ when $n \geq 1$.

case 3 : when $n \leq -1$

as $n^2 \geq 0$ and $n \leq -1$

it follows that $n^2 \geq 0 \geq n$

that is $n^2 \geq n$.

this implies that $n^2 \geq n$ when $n \leq -1$.

These 3 cases include all integers. Thus - $n^2 \geq n$ for all integers.

Example: use a proof by cases to show that $|xy| = |x||y|$, where $x, y \in \mathbb{R}$.

Proof.

we have $|a| = \begin{cases} a & a \geq 0 \\ -a & a \leq 0 \end{cases}$

To prove $|xy| = |x||y|$ we prove - the following 4 cases.

case 1: $x \geq 0$ & $y \geq 0$.

in this case we have

$|xy| = xy = |x| \cdot |y|$

case 2: $x \geq 0$ & $y < 0$

in this case we have

$|xy| = -xy = x(-y) = |x||y|$

case 3: $x < 0$ & $y \geq 0$.

in this case we have

$$|xy| = -xy = (-x)y = |x||y|$$

case 4: $x < 0$ & $y < 0$

in this case we have

$$|xy| = xy = (-x)(-y) = |x||y|$$

when can we use a proof by cases is that, when there is no obvious way to begin a proof, but when extra information in each case helps move the proof forward.

Example: Formulate a conjecture about the decimal digits that occur as the final digit of the squares of an integer and prove your result.

Ans: Let us observe squares of some of the smallest integers. that are

integer:	±1	±2	±3	±4	±5	±6	±7	±8	±9	±10
square:	1	4	9	16	25	36	49	64	81	100

±11	±12	±13	±14	±15
121	144	169	196	225

and so on.

we observe that final digits of these squares are 0, 1, 4, 5, 6, 9.
with 2, 3, 7 and 8 never come as final digit
Thus we make the following conjecture:
" The final decimal digit of a perfect square is 0, 1, 4, 5, 6 or 9 "
To prove this result:
we can observe that, any integer n can be written as $n = 10a + b$.
(because when we divide n by 10 we get quotient a and reminder b and in that case $n = 10a + b$)
where b can be 0, 1, 2, 3, 4, 5, 6, 7, 8 or 9.
now, $n^2 = (10a + b)^2$
$= 100a^2 + 20ab + b^2$
$= 10(10a^2 + 2ab) + b^2$.
This shows that final digit of n^2 is same as the final digit of b^2.
moreover we can see that final digit of b^2 is same as that of $(10-b)^2$,
as $(10-b)^2 = 100 - 20b + b^2$
$= 10(10 - 2b) + b^2$
(i.e. b^2 and $(10-b)^2$ have same final digits.)
Now let us consider the following cases.

Case 1: when final decimal digit of n are 1 or 9

Then final decimal digit of n^2 is $1^2 = 1$, which is same as final decimal digit of $9^2 = (10-1)^2 = 81$,

Case 2: when final digits of n are 2 or 8

Then final digits of n^2 will be final digit of $2^2 = 4$ or final digit of $8^2 = (10-2)^2 = 64$

Case 3: final digits of n are 3 or 7.

Then final decimal digits of n^2 will be, final digit of $3^2 = 9$ or final digit of $7^2 = (10-3)^2 = 49$

case 4: final digits of n are 4 or 6

Then final digit of n^2 will be final digit of $4^2 = 16$ (i.e. 6) or final digit of $6^2 = (10-4)^2 = 36$

Case 5: final decimal digit of n is 5.

Then final decimal digit of n^2 will be final digit of $5^2 = 25$.

Case 6: final decimal digit of n is 0

Then final decimal digit of n^2 will be final digit of $0^2 = 0$

These 6 cases cover all possible case of an

integer n, and in these 6 cases we observed that final digit of n^2 can be 0, 1, 2, 4, 5, 6 or 9.

This proves our result -

Remark: Some times we can eliminate all but few examples in a proof by cases. Following example shows this fact

Example: Show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$

Solution: We can quickly observe that

$x^2 > 8$ when $|x| \geq 3$ and

$3y^2 > 8$ when $|y| \geq 2$.

This implies that x can only take values

$x : -2, -1, 0, 1, 2$ and

possible values for y are

$y : -1, 0, 1$

Consequently

$x^2 : 0, 1, 4$ and

$y^2 : 0, 1$

Thus the maximum value of $x^2 + 3y^2$ is $4 + 3 \cdot 1 = 7$

Thus, it is impossible for $x^2 + 3y^2 = 8$ to hold when x and y are integers.

without loss of generality:

In many mathematical proofs by cases several cases use same arguments, to simplify the proof, by saying that all cases follow with same argument, it is enough to focus on a particular case. To say all such cases use same argument we use the sentance "without loss of generality".

For example: we have seen that in the proof of $|xy| = |x| \cdot |y|$ the cases $x \geq 0$ & $y < 0$ and

$$x < 0 \ \& \ y \geq 0$$

uses same argument. Thus we can use "without loss of generality" and proove one of the cases, so that one case get reduced and thus proof is bit simpler than the originally proved one.

Example: Show that $(x+y)^r \leq x^r + y^r$, whenever x and y are +ve real numbers and r is a real number with $0 < r < 1$.

Proof.

without loss of generality assume that

$x + y = 1$

[because, we can see that if the result is proved in this case, then it is proved in all other cases, as follows:

suppose $x+y=t$ then

$$(x/t)+(y/t)=1 \quad \text{---}①$$

as we prove result for $x+y=1$ case, we can say result hold for ①

i.e. $((x/t)+(y/t))^r \leq (x/t)^r + (y/t)^r$.

now multiply it by t^r, we get

$(x+y)^r \leq x^r+y^r$, the general case.]

as $0<x<1$ & $0<y<1$ with

$0<r<1$

we get

$$x^{1-r} < 1 \quad \text{and}$$

$$y^{1-r} < 1$$

That is $x < x^r$ and

$$y < y^r$$

That is $x^r+y^r > x+y = 1$.

Thus $(x+y)^r = 1^r < x^r+y^r$

Thus result follows in this case.

Thus without loss of generality assumption will give proof in general case also.

Hence we proved given results.

Remark: One of the common mistake in proof by cases is that when we do not consider all possible cases.

Existence proofs:

Many theorems says the existence of elements having some special properties. A theorem of this type is a proposition of the form $\exists x P(x)$. A proof of such theorems are called existence proof.

There are mainly two methods of proving an existence proof.

1. Constructive proof: The proof of $\exists x P(x)$ can be given by finding an element a for which $P(a)$ is true. Such an existence proof is called constructive.

2. Non-constructive: If we prove $\exists x P(x)$ by not finding an a for which $P(a)$ is true is called non-constructive proof. One of main non-constructive proof is by method of contradiction.

Example: A constructive existence proof show that there is a +ve integer that can be written as the sum of cubes of positive integers in two different ways.

proof.

After a considerable computation one can find that (such as a computer search)

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

Hence the proof.

Example

(A non-constructive existence proof.)

show that there exist irrational number x and y such that x^y is rational.

proof

we know that $\sqrt{2}$ is irrational

Let us consider the number $\sqrt{2}^{\sqrt{2}}$

if $\sqrt{2}^{\sqrt{2}}$ is rational, then we have 2 irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ such that $x^y = \sqrt{2}^{\sqrt{2}}$ is rational.

If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

so that $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$ is rational.

That is we have shown that either the

pair $x = \sqrt{2}$, $y = \sqrt{2}$ or the pair $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ have the desired property. this shows existence of irrational numbers x & y such that x^y is rational

---

uniqueness proof.

Some theorems says existence of a unique element with a particular property.

OR

theorems which may say that there is exactly one element with particular property.

The result of this form we need to show that an element exist with the property and that no other element have this property.

So, there are two parts for a uniqueness proof.

1. Existence part : we show that an element x with desired property exists.
2. uniqueness part : we show that if $y \neq x$, then y does not have the desired property.

Remark : note that, there is a unique element such that $P(x)$ is equivalent to $\exists x\,(P(x) \wedge \forall y\,(y \neq x \rightarrow \neg P(y)))$.

Example: Show that, if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Proof.

Existence part: Let $a \neq 0$, $b \in \mathbb{R}$.
take $r = -b/a$ then
$ar + b = 0$.
This proves existence of such a real number r.

Uniqueness part: Suppose s is a real number with $as + b = 0$.
Then, $ar + b = 0 = as + b$
that is $ar + b = as + b$ — ①
that is $ar = as$ — ②
(by subtracting b from both side of above eqtn ①)
now ② $\div a$ we get
$r = s$.
This means if $s \neq r$ then
$as + b \neq 0$.
This proves uniqueness part.

Hence we proved given result.

Forward and Backward Reasoning.

Forward Reasoning for a conditional stmnt $p \rightarrow q$ is the method of direct proof for $p \rightarrow q$.

Backward Reasoning for a conditional stmnt $p \rightarrow q$ is a method of proving $p \rightarrow q$ as follows:

we assume that q is true.

then by a sequence of deductions we get p.

now we trace back to q from this obtained p by following the deduction paths/ideas we used to reach from q to p in reverse direction to get p to q.

Example: Given two positive real numbers x & y, their arithmetic mean (AM) is $(x+y)/2$ and their

geometric mean (GM) is $\sqrt{xy}$, when we compare the AM & GM, for distinct pair of +ve numbers, we find that AM > GM.

Soln: To proove AM > GM for distinct numbers we need to P.T

If $x \neq y$, then $\frac{x+y}{2} > \sqrt{xy}$.

by using backward reasoning,

Start with $\frac{x+y}{2} > \sqrt{xy}$

$\Rightarrow \frac{(x+y)^2}{4} > xy$

$\Rightarrow (x+y)^2 > 4xy$

$\Rightarrow x^2 + 2xy + y^2 > 4xy$

$\Rightarrow x^2 - 2xy + y^2 > 0$

$\Rightarrow (x-y)^2 > 0$

$\Rightarrow x \neq y$.

Now we construct proof by backtracing.

Suppose $x \neq y$

$\Rightarrow (x-y)^2 > 0$

$\Rightarrow x^2 - 2xy + y^2 > 0$

$\Rightarrow x^2 + 2xy + y^2 > 4xy$ ⊕ $4xy$ on both side.

$\Rightarrow (x+y)^2 > 4xy.$

$\Rightarrow (x+y)^2/4 > xy$

$\Rightarrow (x+y)/2 > \sqrt{xy}$ taking sqr root on both side.

So we conclude that, if $x \& y$ are distinct, then AM > G.M.

Example: Suppose that two people play a game taking turns removing 1, 2, or 3 stones at a time from a pile that begins with 15 stones. The person who remove the last stone wins the game. Show that the first player can win the game no matter what the second player does.

Ans: The given stmnt can be written as

If P_1 & P_2 play game G, then P_1 wins.

where P_1 & P_2 are persons and

G be the given game.

we use backward reasoning.

To win P_1 the Game Gn,

- P_1 has to remove 1, 2, or 3 stones in his last move.
- To get this choice, in his 2nd last move P_1 has to leave 4 stones balence for P_2 when there are 5, 6, 7 stones left
- To get this choice, in his 3rd last move P_1 has to leave 8 stones balence for P_2 when there are 9, 10, 11 stones left
- To get this choice, in his first move P_1 has to leave 12 stones balence for P_2 when there are 15 stones left

P_1 move from	P_1 keep balence for P_2
4. 1, 2, 3	4
3. 5, 6, 7	8
2. 9, 10, 11	12
1. (13, 14) 15	

now by back tracking

P_1 : remove 3 stones from 15

keep 12 for P_2.

or or

P_1 : remove 1, 2, 3 from 11, 10, 9

and keep 8 for P_2.

P_1 : remove 1 or 2 or 3 from 5, 6, 7

and keep 4 for P_2.

now P_1 can remove remaining 1 or 2 or 3 to win the game.

adapting existing proofs:

An excellent way to look for possible approaches that can be used to prove a statement is to take advantage of existing proofs. Often an existing proof can be adapted to prove a new result. Even when this is not the case, some of the ideas used in existing proofs may be helpful. because existing proofs

provide clues for new proofs.

Ex! : Try to prove $\sqrt{3}$ is irrational.

Theorem: FERMAT'S LAST THEOREM

The equation

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

has no solution in integers $x, y,$ and z with $xyz \neq 0$, whenever n is an integer with $n > 2$.

Ex: Read the story about the theorem.