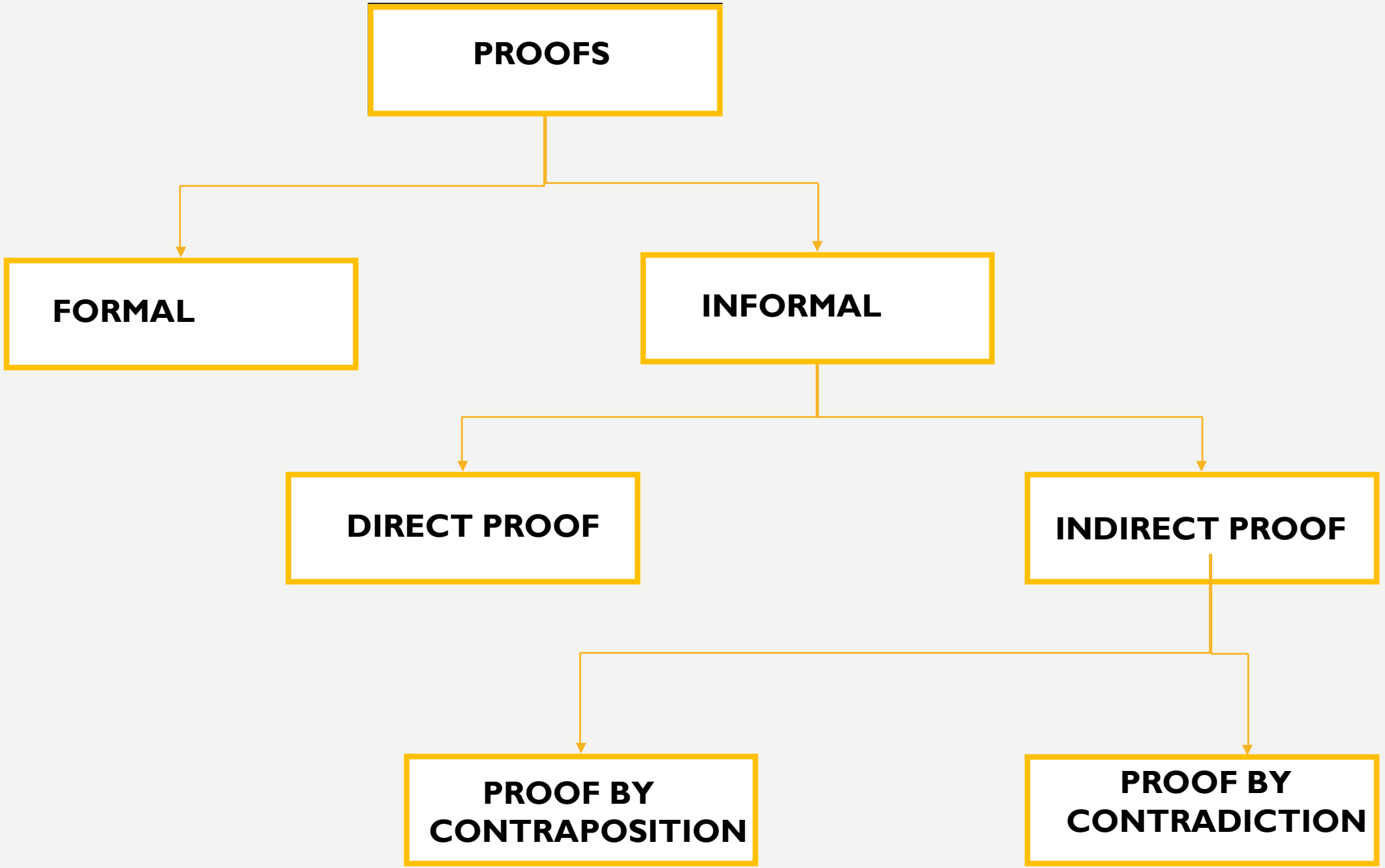
MATHEMATICAL FOUNDATION FOR COMPUTER SCIENCE

Prepared by: Er. Ankit Kharel

Nepal college of information technology


PROOFS
FORMAL
INFORMAL
DIRECT PROOF
INDIRECT PROOF
PROOF BY CONTRAPOSITION
PROOF BY CONTRADICTION

PROOF:

- An argument used to establish the truth of mathematical statement is called Proof.
- Mathematical proofs use **deductive reasoning**, where a conclusion is drawn from multiple premises.
- The premises in the proof are called statements.
- While establishing the truth, different rules and already proven facts are used.
- INDUCTIVE REASONONG : Drawing a general conclusion from what we see around us. For example, if all the sheep you have ever seen were white, you might conclude that all sheep are white.
- DEDUCTIVE REASONONG : You start from a general statement you know for sure is true and draw conclusions about a specific case. For example, if you know for a fact that all sheep like to eat grass, and you also know that the creature standing in front of you is a sheep, then you know with certainty that it likes grass.

SOME TERMINOLOGIES:

1. THEOREM: A mathematical statement that is proved using rigorous mathematical reasoning. The process of showing a theorem to be correct is called a proof.

2. **AXIOM:** An axiom is a statement, usually considered to be self- evident, that is assumed to be True without proof. It is used as starting point in mathematical proof.

Example: Parallel lines in same plane , do not meet one another in either direction when extended infinitely.

3. COROLLARY: A corollary is the theorem that can be proven to be a Logical consequence of another theorem.

Example: If a+ b=c then an example of corollary is c= b- a.

SOME TERMINOLOGIES:

4. CONJECTURE : A conjecture is a mathematical statement that has not yet been rigorously proved. Conjectures arises when one notices a pattern that holds True for many cases.

Example: 2, 4, 6, ,8 ,10 ,12, ?

The next number is more likely to be 14.

5. LEMMA: It is generally minor, proven proposition which is used as a stepping stone to a larger result. It is also known as a "Helping Theorem" or " Auxillary Theorem"

Example: For all real numbers r, |-r| = |r|

FORMAL & INFORMAL PROOF:

Formal proof : A formal proof of a conclusion q given hypotheses p1, p2, . . . , pn is a sequence of steps, each of which applies some inference rule to hypotheses or previously proven statements (antecedents) to yield a new true statement (the consequent).

Informal proof : where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and rule of inference used are not explicitly stated.

1. DIRECT PROOF:

- A direct proof of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true

- A direct proof shows that a conditional statement $p \rightarrow q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs.

- In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true

Example:

1. Prove that "If n is odd, then n^2 is odd."

Solution:

Let,

p: Hypothesis: " n is odd"

q: Conclusion: "n^2 is odd"

Now, we assume Hypothesis is TRUE. i.e.

n is odd(TRUE)

By the definition of odd integer, we can write,

$n= 2k+1$; for integer k

Squaring both sides,

$$n^2 = (2k+1)^2$$
$$= 4k^2 + 4k + 1$$
$$=2(2k^2 + 2k) +1$$
$$=2k_1 + 1; \text{where } k_1 = (2k^2 + 2k) \text{ is an integer}$$

Therefore, n2 is odd.

2. Prove that "If 'm' and 'n' are odd, then 'm + n' is even." [The sum of two odd numbers is even.]

Solution:

Let,

p: Hypothesis: " m and n are odd"

q: Conclusion: "m + n is even"

Now, we assume Hypothesis is TRUE. i.e.

m and n are odd(TRUE)

By the definition of odd integer, we can write,

$m = 2i+1$; for integer i

$n = 2j+1$; for integer j

Now,

$$m + n = (2i+1) + (2j+1)$$
$$= 2i+2j+2$$
$$= 2(i+j+1)$$
$$= 2k \quad ; \text{where } k = (i+j+1) \text{ is an integer}$$

Therefore, m + n is even.

3. If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof.

Suppose x is an even integer. Then $x = 2a$ for some $a \in Z$, by definition of an even integer.

So

$$x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5$$
$$= 4a^2 - 12a + 5$$
$$= 4a^2 - 12a + 4 + 1$$
$$= 2(2a^2 - 6a + 2) + 1.$$

Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in Z$.

Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number

4. If n is any even integer, then $(-1)^n = 1$.

Proof:

Suppose n is even integer. [We must show that $(-1)^n = 1$.].

Then by the definition of even numbers,

$n = 2k$ for some integer k

we have

$$(-1)^n = (-1)^{2k}$$
$$= ((-1)^2)^k$$
$$= (1)^k$$
$$= 1$$

This is what was to be shown. And this completes the proof.

5. Let a, b and c be integers, directly prove that if a divides b and a divides c then a also divides b + c.

Solution

Let **a**, **b** and **c** be integers and assume that **a** divides **b** and **a** divides **c**.
Then as **a** divides **b**, by definition, there is some integer **k** such that **b** = **ak**.
Also as **a** divides **c**, by definition, there is some integer **l** such that **c** = **al**.

Note that we use different letters **k** and **l** to stand for the integers because we do not know if **b** and **c** are equal or not.

So,

$b + c = (ak) + (al)$

$= a(k + l)$ since a is a common factor.

Hence a divides (b + c) since (k + l) is an integer.

1. INDIRECT PROOF:

- Direct proofs lead from the premises of a theorem to the conclusion. They begin with the premises, continue with a sequence of deductions, and end with the conclusion.

- However, we will see that attempts at direct proofs often reach dead ends. We need other methods of proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$. Proofs of theorems of this type that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called indirect proofs

  i. Proof by Contraposition
  ii. Proof by Contradiction

1.1 PROOF BY CONTRAPOSITION:

- Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$. This means that the conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, is true.

- In a proof by contraposition of $p \rightarrow q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow

Q.1 Prove that if n is an integer and 3n + 2 is odd, then n is odd.

Solution:

We first attempt a direct proof.

If 3n + 2 is odd, then n is odd.($p \rightarrow q$)

p:"3n + 2 is odd"

q:"n is odd"

To construct a direct proof, we first assume that 3n + 2 is an odd integer.

This means that 3n + 2 = 2k + 1 for some integer k.

3n + 2 = 2k +1

n = (2k-1)/3

DEAD END

$p \rightarrow q = \neg q \rightarrow \neg p$[if n is even then 3n+2 is even]

$\neg q$="n is even"

$\neg p$= "3n + 2 is even"

Now , from the definition of an even integer

n=2k, for some integer k

Substituting 2k for n , We get,

3(2k) + 2

=6k + 2

=2(3k + 1)

i.e. 3n + 2 is even because it is a multiple of 2

Therefore, 3n+2 is even.

Q.1 Prove that if xy is odd integer then x, y is odd.

Solution:

Above statement is in the Form:

$p \rightarrow q$

p: "xy is odd"

q: "x, y is odd"

Taking Contrapositive of above statement:

$p \rightarrow q = \neg q \rightarrow \neg p$

$\neg q$="x, y is even "[Hypothesis]

$\neg p$= "xy is even"

if x, y is even then xy is even

Now , from the definition of an even integer

x=2k, for some integer k

y=2l, for some integer l

Now,

xy = 2k*2l

= 4kl

=2(2kl)

i.e. xy is even because it is a multiple of 2

Therefore, xy is even.

1.2 PROOF BY CONTRADICTION:

- The basic idea is to assume that the statement we want to prove is false, and then show that this assumption leads to nonsense. We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true.

Prove there exist no integer a, b for which 5a + 15b =1.

Solution:

Step 1: Assume there exist integer a and b for which 5a + 15b =1.

Now,

$$5a + 15b = 1$$
$$5(a + 3b) = 1$$
$$a + 3b = 1/5$$

Because a and b are integers, a + 3b must also be an integer**[CONTRADICTION]**

Therefore, There exist no integer a, b for which 5a + 15b = 1.

Proposition: If a , b ∈ Z, then $a^2 - 4b \neq 2$.

Proof.

"If a and b are integers then, $a^2 - 4b \neq 2$"

Suppose this proposition is false. This conditional statement being false means:

There exist numbers a and b for which a , b ∈ Z is true but $a^2 - 4b \neq 2$ is false.

"If a and b are integers then, $a^2 - 4b = 2$"

Thus there exist integers a, b ∈ Z for which $a^2 - 4b = 2$.

From this equation we get

$a^2 = 4b + 2 = 2(2b + 1)$, so a2 is even. Since a^2 is even, it follows that a is even, so $a = 2c$ for some integer c.

Now plug $a = 2c$ back into the boxed equation $a^2 - 4b = 2$. We get

$(2c)^2 - 4b = 2$, so $4c^2 - 4b = 2$. Dividing by 2, we get $2c^2 - 2b = 1$.

Therefore $1 = 2(c^2 - b)$, and since $c^2 - b \in Z$, it follows that 1 is even. Since we know 1 is not even, something went wrong. But all the logic after the first line of the proof is correct, so it must be that the first line was incorrect. In other words, we were wrong to assume the proposition was false. Thus the proposition is true.

Prove that for all integer n, if $n^3 + 5$ is odd then n is even.

Solution:

Here,

Assume the conclusion, i.e. n is odd

Because n is odd , We can write,

$N = 2k + 1$

Putting value of n in $n^3 + 5$, We get

$=(2k + 1)^3 + 5$

$=8k^3 + 12k^2 + 6k + 1 + 5$

$= 8k^3 + 12k^2 + 6k + 6$

$=2[8k^3 + 12k^2 + 6k + 6]$

=Even**[CONTRADICTION]**

Therefore, If $n^3 + 5$ is odd then n is even

Prove $\sqrt{2}$ is a irrational number using proof by contradiction.

Suppose $\sqrt{2}$ is rational. Then integers a and b exist so that $\sqrt{2} = a/b$.

Without loss of generality we can assume that a and b have no factors in common (i.e., the fraction is in simplest form).

Multiplying both sides by b and squaring,
we have $2b^2 = a^2$ so we see that a^2 is even.
This means that a is even so $a = 2m$ for some $m \in Z$.
Then $2b^2 = (2m)^2$
$= 4m^2$ which, after dividing by 2, gives $b^2 = 2m^2$ so b^2 is even. This means b is even.

We've seen that if $\sqrt{2} = a/b$ then both a and b must be even and so are both multiples of 2. This contradicts the fact that we know a and b can be chosen to have no common factors. Thus, $\sqrt{2}$ must not be rational, so $\sqrt{2}$ is irrational.

PRINCIPLE OF MATHEMATICAL INDUCTION:

- Let P(n) be a statement. Now, our concern is to show that P(n) is True using Mathematical Induction.

  a) First we show that P(n) is True for some initial value like n =0, 1 ….This is called the Basic Step.

  b) Then, we assume that P(n) is True for any arbitrary value k i.e. P(k) is True and show that P(n) is True for 'k + 1' i.e. P(k+1) is True. This step is called inductive step

Thus, Mathematical Induction can be defined as:

$[P(1) \wedge (P(k) \rightarrow P(k+1))] \rightarrow P(n)$

Q. Show that if n is positive integer then,

1 + 2 + ……. + n = [n(n + 1)]/2

Solution:

Let, P(n) be the proposition that the sum of first n positive integer , 1 + 2 + ……. + n = [n(n + 1)]/2

Basic Step: When n=1,

1= [1(1+1)]/2

1=1(TRUE) i.e. P(1) is True.

Inductive Step: Assume P(k) holds for arbitrary integer k.

i.e. 1+2+……..+k = [k(k+1)]/2

Under this assumption , it must be shown that P(k+1) is True

1 + 2 + …..+ k + (k+1)= [(k+1)(k+2)]/2

L.H.S.

1 + 2 + …..+ k + (k+1)

=[k(k+1)]/2 + (k + 1)

=[k(k+1) + 2k + 2]/2

=[k(k+1) + 2(k+1)]/2

=[(k+1)(k+2)]/2

=R.H.S

Therefore, P(n) is true.

Q. Use Mathematical induction to show that:

$$2 + 2^2 + \ldots\ldots\ldots\ldots\ldots\ldots + 2^n = 2^{n+1} - 2$$

Solution:

Let, P(n) be the proposition that, $2 + 2^2 + \ldots\ldots\ldots\ldots\ldots\ldots + 2^n = 2^{n+1} - 2$

Basic Step: When n=1,

$2 = 2^2 - 2$

2=2(TRUE) i.e. P(1) is True.

Inductive Step: Assume P(k) holds for arbitrary integer k.

i.e. $2 + 2^2 + \ldots\ldots\ldots\ldots\ldots\ldots + 2^k = 2^{k+1} - 2$

Under this assumption , it must be shown that P(k+1) is True

$$2 + 2^2 + \ldots\ldots\ldots\ldots\ldots\ldots + 2^k + 2^{k+1} = 2^{(k+1)+1} - 2$$

L.H.S.

$2 + 2^2 + \ldots\ldots\ldots\ldots\ldots\ldots + 2^k + 2^{k+1}$

$= 2^{k+1} - 2 + 2^{k+1}$

$=2.\ 2^{k+1} - 2$

$=2^{(k+1)+1} - 2$

=R.H.S

Therefore, P(n) is true.

Q. Use Mathematical induction to show that:
$8^n - 3^n$ is divisible by 5.[n≥1]

Solution:

Let, P(n) be the proposition that, $8^n - 3^n$ is divisible by 5

Basic Step: When n=1,

$8^1 - 3^1$ is divisible by 5

5 is divisible by 5(TRUE) i.e. P(1) is True.

Inductive Step: Assume P(k) holds for arbitrary integer k.

i.e. $8^k - 3^k$ is divisible by 5

Under this assumption , it must be shown that P(k+1) is True

i.e. $8^{k+1} - 3^{k+1}$ is divisible by 5

Now,

$8^{k+1} - 3^{k+1}$

$=8^k.8 - 3^k.3$

$=8^k(5+3) - 3^k.3$

$= 8^k.5 + 8^k.3 - 3^k.3$

$= 8^k.5 + 3(8^k - 3^k)$

Here, $8^k.5$ is multiple of 5 and $(8^k - 3^k)$is divisible by 5.

Therefore, P(n) is true.

Q. Use Mathematical induction to show that:

$2n+1<2^n$ $[n\geq 3]$

Solution:

Let, P(n) be the proposition that, $2n+1<2^n$

Basic Step: When n=3,

$2*3+1<2^3$

$7<8$ i.e. P(3) is True.

Inductive Step: Assume P(k) holds for arbitrary integer k $[k\geq 3]$

i.e. $2k+1<2^k$

Under this assumption , it must be shown that P(k+1) is True

i.e. $2(k+1)+1<2^{k+1} = 2k+2+1<2^{k+1}$

Now,

$2k+1<2^k$

$= 2k+1+2<2^k + 2$

$= 2k+1+2<2\cdot 2^k$

$= 2k+2+1<2^{k+1}$

$= 2(k+1)+1<2^{k+1}$

Therefore, P(n) is true.

Q. Use Mathematical induction to show that:

$3^n > 2n+5$ **[n>2]**

Solution:

Let, P(n) be the proposition that, $3^n > 2n+5$ **[n>2]**

Basic Step: When n=3,

$27 > 11$

i.e. P(3) is True.

Inductive Step: Assume P(k) holds for arbitrary integer k [k>2]

i.e. $3^k > 2k+5$

Under this assumption , it must be shown that P(k+1) is True

i.e. $3^{k+1} > 2(k+1)+5 = 3^k > 2k+2+5$

Now,

$3^k > 2k+5$

$3^k + 2 > 2k+2+5$

$3^k .3 > 2k+2+5$

$3^{k+1} > 2k+2+5$

$3^{k+1} > 2(k+1)+5$

Therefore, P(n) is true.

Q. Use Mathematical induction to show that:

$3^n \geq 1+2n \ [n \geq 0]$

Solution:

Let, P(n) be the proposition that, $3^n > 2n+5 \ [n>2]$

Basic Step: When n=0,

$1 \geq 1$

i.e. P(0) is True.

Inductive Step: Assume P(k) holds for arbitrary integer k [$k \geq 0$]

i.e. $3^k \geq 1+2k$

Under this assumption , it must be shown that P(k+1) is True

i.e. $3^{k+1} \geq 1+2(k+1) = 3^{k+1} \geq 2k+3$

Now,

$3^k \geq 1+2k$

$3^k .3 \geq 3(1+2k)$

$3^k .3 \geq 6k+3$

$3^{k+1} \geq 6k+3$

$3^{k+1} \geq 2k+3$

Therefore, P(n) is true.

Q. Prove that 21 divides $4^{n+1} + 5^{2n-1}$ whenever n is a positive integer.

Solution.

BASIS STEP: For the basis step (n = 1), we simply observe that $4^{1+1} + 5^{2(1)-1} = 16 + 5 = 21$ which is divisible by 21.

2. INDUCTIVE STEP: Then we assume the inductive hypothesis, that $4^{k+1} + 5^{2k-1}$ is divisible by 21,

Now, We have to proof for n=k+1,

i.e. $4^{k+2} + 5^{2(k+1)-1}$ is divisible by 21

$= 4^{k+2} + 5^{2k+1}$

$= 4 \cdot 4^{k+1} + 5^2 \cdot 5^{2k-1}$

$= 4 .4^{k+1} + 25.5^{2k-1}$

$= 4 .4^{k+1} + (4 + 21) \cdot 5^{2k-1}$

$= 4 .4^{k+1} + 4. 5^{2k-1} + 21. 5^{2k-1}$

$= 4 [4^{k+1} + 5^{2k-1}] + 21. 5^{2k-1}$

Looking at the last line, we see that the expression in parentheses is divisible by 21 by the inductive hypothesis, and obviously the second term is divisible by 21 , so the entire quantity is divisible by 2

Therefore, P(n) is true.