PROJECTED WRITTEN NOTES FROM THE M325K LECTURE ON TUESDAY, FEBRUARY 20, 2024, ON MORE ON PROOF: by - CONTRADICTION, Proof by Contraposition, and an Introduction to MATHEMATICAL INDUCTION

CLASS # 11

HINT FOR PROVING AN INEQUALITY

TO PROVE an inequality $A < B$,

Locate C so that

$A < C$ and $C < B$.

Then, conclude that $A < B$

by the transitivity of "Less than"

(Similarly, for proving $A \leq B$.)

HW #5A, PART II SOLUTIONS

① TO PROVE: FOR ALL INTEGERS $k \geq 3$,
if $2^0+2^1+2^2+\cdots+2^{k-1} = (2^k-1)$,

Then $2^0+2^1+2^2+\cdots+2^k = (2^{(k+1)}-1)$.

Proof: Let k be any integer such that $k \geq 3$.
Suppose $2^0+2^1+2^2+\cdots+2^{k-1} = (2^k-1)$.

Now, $2^0+2^1+2^2+\cdots+2^{k-1}+2^k$

$= (2^0+2^1+2^2+\cdots+2^{k-1}) + 2^k$

$= (2^k-1) + 2^k$, by substitution,

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

$= 2 \cdot 2^k - 1$.

$\therefore 2^0+2^1+2^2+\cdots+2^k = (2^{k+1}-1)$, by rules of algebra.

$\therefore$ For all integers $k \geq 3$,
if $2^0+2^1+\cdots+2^{k-1} = 2^k-1$,
Then $2^0+2^1+\cdots+2^k = (2^{k+1}-1)$, by Direct Proof.
QED

The "5A, Part II proof" proves:

"For all integers $k \geq 3$,
if $2^0 + 2^1 + 2^2 + \ldots + 2^{k-1} = (2^k - 1)$,
then $2^0 + 2^1 + 2^2 + \ldots + 2^k = (2^{k+1} - 1)$."

Suppose I want to prove this:

"For the integers $n = 3$, $n = 4$, $n = 5$ and $n = 6$,
$2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$"

I could proceed as follows:

proof: Let $n = 3$. $2^0 + 2^1 + 2^2 + 2^3 = 1 + 2 + 4 + 8 = 7 + 8 = 15 = 16 - 1$.

So, $2^0 + 2^1 + 2^2 + 2^3 = 2^4 - 1$. [$n = 3$ works]

Now, since $2^0 + 2^1 + 2^2 + 2^3 = 2^4 - 1$,
we have that $2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 2^5 - 1$, from applying the "5A, Part II proof" with $k = 4$. [$n = 4$ works]

Now, since $2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 2^5 - 1$,
we have that $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = 2^6 - 1$, from applying the "5A, Part II proof" with $k = 5$. [$n = 5$ works]

Now, since $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = 2^6 - 1$,
we have that $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 2^7 - 1$, from applying the "5A, Part II proof" with $k = 6$.

∴ For $n = 3, 4, 5$, and 6,
$2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$.

QED

A Theorem is a statement that has a proof.

A Corollary is a Theorem whose proof is a direct application of the previous Theorem.

A Lemma is a Theorem whose sole purpose is to be used in the proof of the following Theorem.

Recall Theorem (NIB) 1 :

For all prime numbers p, and for all integers $n > 1$,
$p \mid n$ if and only if p appears a factor in the Unique Prime Factorization of n.

Recall Theorem 4.3.4:

For any integer $n > 1$, there exists a prime number p such that $p \mid n$.

Recall Problem #16 from Section 4.3:

For all integers a and b,
if $a \mid c$ and $b \mid c$, then $a \mid (b-c)$

The Big Theorem:

Theorem 4.6.4: There are infinitely many prime numbers.

"Lemma for Theorem 4.6.4"

There does not exist a positive integer which is divisible by every prime #.

Proof: [By-Contradiction]

Suppose, BWOC, that there exists an integer $N > 0$ such that N is divisible by every prime number.

Consider the integer $N+1$. Since $N > 0$, $N+1 > 1$.

Since $N+1 > 1$, by Theorem 4.3.4, there exists a prime number p such that

$p \mid (N+1)$ [$p > 1$ since p is prime]

Since N is divisible by every prime #, N is divisible by p. So, $p \mid (N+1)$ and $p \mid N$, so,

by Problem #16 from Sec 4.3,

$p \mid ((N+1) - N)$. So, $p \mid 1$. The only positive

$= 1$

divisor of 1 is 1., So, $p = 1$.

$\therefore p = 1$ and $p > 1$, a contradiction.

$\therefore$ There does not exist an integer that is divisible by every prime #, by proof-by-contradiction

QED.

The Big Theorem

Theorem 4.6.4: The set $\mathbb{P}$ of all prime numbers is an infinite set.

Proof: Let $\mathbb{P}$ be the set of all prime numbers.

Suppose, ROOC, that $\mathbb{P}$ is a finite set.

Then, for some positive integer k, there are exactly k prime numbers,

say, $p_1, p_2, p_3, \dots, p_k$

$\mathbb{P} = \{p_1, p_2, \dots, p_k\}$

Let $N = p_1 p_2 p_3 \cdots p_k$ and this factorization of N is the Unique Prime factorization of N. (Note: $N > 0$)

By Thm W1RJ 1, $p_1 | N$, $p_2 | N$, $p_3 | N$, $\dots$, $p_k | N$

$\therefore N$ is a positive integer, divisible by every prime, which contradicts "Lemma for Thm 4.6.4."

$\therefore \mathbb{P}$, the set of all primes is an infinite set, by proof-by-contradiction.

QED.

The Principle of Mathematical Induction

Let a be the first value of n to be considered and let P(n) be a predicate with n as the predicate variable.

IF

(1) P(a) is true (i.e, P(n) when n is set to its first value, a) and

(2) For every integer $k \geq a$,

If P(k) is true, Then P(k+1) is true,

THEN

P(n) is true for every integer $n \geq a$.

In a proof by Mathematical Induction, the whole proof involves proving that the "IF" conditions of the Principle of Mathematical Induction shown above are true.

The BASIS STEP is the part of the proof which proves condition (1).

The INDUCTIVE STEP is the part of the proof which proves condition (2).

After (1) and (2) have been proved, we can invoke the Principle of Mathematical Induction to conclude: "$\therefore$ *P(n) for every integer $n \geq a$ by the Principle of Mathematical Induction.*"

Mathematical Induction (in Diagram Form with $a = 1$):

Given an infinite list of statements:

$P_1, P_2, P_3, P_4, \ldots$

IF we prove :

If we prove: (1) P_1, and

If we prove: (2) For all integers $k \geq 1$, if P_k, then P_{k+1},

Then, we can conclude:
For all integers $n \geq 1$, P_n,
by the Principle of Mathematical Induction.

that this is true, and that, for all integers $k \geq 1$,

If this is true, then this is true,

THEN . . .

$P_1, P_2, P_3, P_4, \ldots, P_k, \quad P_{k+1}, \ldots$

We can logically conclude that ALL of these statements are true.

$P_1, P_2, P_3, P_4, \ldots, P_k, P_{k+1}, \ldots$

M 325K

The Basis Step Worksheet

A proof by Mathematical Induction is used for proving a universal statement of the form

For all integers n $\geq$ an initial integer value, predicate P(n) is true.

For example, one such universal statement of this form is as follows:

$$\text{For all integers } n \geq 3, \quad 1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2 .$$

The first step in writing a proof by Mathematical Induction is to write the Basis Step. In the Basis Step, it is proved that the predicate P(n) is a true statement when the value of the variable n is set to be equal to the initial integer value of n.

In this class, there are certain rules that the writing of the Basis Step of a proof by Mathematical Induction must follow. It is the purpose of this worksheet to teach you what the rules of the writing of the Basis Step are and how to write a Basis Step that follows these rules.

The Rules for Writing a Basis Step of a Proof by Mathematical Induction

In the Basis step of a proof by Mathematical Induction:

1) Using a "Let" statement, the first statement of the Basis Step must set the variable equal to its specified initial value.

2) Referring to the predicate P(n) of the universal statement-to-be-proved, every expression in the predicate that has the variable must be evaluated individually, and each evaluation must proceed as follows:
First, the expression using the variable must be written as it appears in the predicate using the variable, and second, that expression is equated (by substitution) to the same expression with the initial integer value formally substituted for the variable, and third, the resulting calculation is simplified to an appropriate simple form.

3) After each expression containing the variable has been evaluated in this manner, the **assertion** of the predicate P(n) must be verified using the calculated values of the expressions found in part (2).

4) The final conclusion of the Basis Step is as follows:

"$\therefore$ For <variable> = <initial integer value>,
<predicate P(n) exactly as it appears in the statement-to-be-proved>, by substitution."

Note: You are not allowed to use the terminology "Property P(n)" as the Author Epp does in her proofs!

On the next pages are examples of Basis Step writing that follow the Rules for

Writing a Basis Step of a Proof by Mathematical Induction.

There is one example for each of three types of assertions of the predicate P(n):

(1) Assertion of Equality, (2) Assertion of Divisibility, (3) Assertion of Inequality