PROJECTED WRITTEN NOTES FROM THE M325K LECTURE ON TUESDAY, FEBRUARY 13, 2024, ON THE UNIQUE (PRIME) FACTORIZATION THEOREM, THEOREMS (NIB) 2 and 3, PROOFS USING DIVISION INTO CASES and PROOF-BY-CONTRADICTION

CLASS #9

Ex: The prime factorization of 12 is

$$12 = 3 \times 4 = 3 \times 2 \times 2 = 2 \times 3 \times 2 = 2 \times 2 \times 3$$

$$12 = 2^2 \cdot 3^1$$

The "prime Factorization" of 7 is $7 = 7^1$.

The Unique Prime Factorization Theorem

Theorem 4.3.5, The Unique Prime Factorization Theorem (UFT)
(Also called The Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist:

1) **a positive integer k (= the # of prime factors n has.) and k distinct prime numbers, $p_1, p_2, p_3, \ldots, p_k$ and**

2) **positive integers $e_1, e_2, \ldots, e_k$ (exponents), that is $e_i \geq 1, \forall\, i$,**

such that $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$

and any other factorization of n into a product of prime factors is the same as this one except that the prime factors may be rearranged in a different order.

Theorem (NIB) 1: For all integers $n > 1$ and for all prime numbers p, p is a divisor of n if, and only if, p appears as a prime factor in the Unique Prime Factorization of n (from the Unique Factorization Theorem, Theorem 4.3.5).

Theorem (NIB) 2:
For all integers a and b, and for all prime numbers p,
if p divides ab, then p divides a or p divides b.

Theorem (NIB) 3: For any integer n, and for any prime number p,
if $p \mid n^2$, then $p \mid n$.

Applying Theorem (N18)2 in a Proof

Problem: Suppose n and k are positive integers greater than 1 such that $18k = 33n$.

Prove that $11 \mid k$ and $3 \mid n$.

Proof: It is given that $18k = 33n$.

$33 = 11 \times 3$, so $11 \mid 33$ and $33 \mid 33n$.

So, by Theorem 4.3.3 (Divisibility is Transitive),

$11 \mid 33n$.

$\therefore$ By Substitution $11 \mid 18k$.

By Theorem (N18)2, [with $a = 18$ and $b = k$],

since 11 is a prime number, $11 \mid 18$ or $11 \mid k$

Since $\frac{18}{11} = 1 + \frac{7}{11}$, $1 < \frac{18}{11} < 2$. $\therefore$ $\frac{18}{11}$ is not an integer.

$11 \nmid 18$. $\therefore 11 \mid k$, by Elimination. $[11 \mid k]$

Now, $3 \times 6k = 18k = 33n = 3 \times 11n$.

By Dividing by 3, we conclude that $6k = 11n$.

Since $6 = 3 \times 2$, $3 \mid 6$ and $6 \mid 6k$.

$\therefore 3 \mid 6k$, by Theorem 4.3.3.

$\therefore 3 \mid 11n$, and, since 3 is prime, $3 \mid 11$ or $3 \mid n$, by Theorem (N18)2.

Since $\frac{11}{3} = 3 + \frac{2}{3}$, $3 < \frac{11}{3} < 4$. $\therefore$ $\frac{11}{3}$ is not an integer.

$\therefore 3 \nmid 11$. Therefore, by Elimination, $3 \mid n$. $[3 \mid n]$

$\therefore 11 \mid k$ and $3 \mid n$, by Conjunction. QED

THE PROOF STRUCTURE: DIVISION INTO CASES

IN LOGIC,

The Standard Valid Argument

"DIVISION INTO CASES"

$a \vee b$ ← "Listing of all the CASES TO CONSIDER.

$a \to c$ ←
$b \to c$ ← } CASE ARGUMENTS

$\therefore c$ ← $\therefore c$ is true, In GENERAL.

The Design for Proofs using Division into Cases:
(For three (3) cases here)

To Prove: Statement p .

Proof: . . . (statements defining variables and establishing initial results) . . .

$\therefore$ q OR r OR s by . . . . **[Required List of all possible cases]**

CASE 1: (statement q) **[Required Case Heading]**
Suppose q .
. . .
. . .
$\therefore$ p in the case that q . [or "$\therefore$ p in Case 1."] **[Case 1 Conditional Conclusion]**

CASE 2: (statement r) **[Required Case Heading]**
Suppose r .
. . .
. . .
$\therefore$ p in the case that r . [or "$\therefore$ p in Case 2."] **[Case 2 Conditional Conclusion]**

CASE 3: (statement s) **[Required Case Heading]**
Suppose s .
. . .
. . .
$\therefore$ p in the case that s . [or "$\therefore$ p in Case 3."] **[Case 3 Conditional Conclusion]**

[Since p has been proved true in all possible cases, we can conclude p is true.]

$\therefore$ p <u>in general</u>. **[The Conclusion Without Conditions]**

QED

On the following pages is an example of a proof which uses Division into Cases.

The commentary provided is important to read.

A Theorem and The Parity Corollary

Theorem: Every integer n can be written as $n = 2k$ or as $n = 2k+1$, for some integer k.

[$\forall n \in \mathbb{Z}$, $\exists k \in \mathbb{Z}$ such that $n = 2k$ or $n = 2k+1$.]

Proof: Let n be any integer. Let $d = 2$.
[We apply the Q-R Theorem to n and d.]

By the Quotient-Remainder Theorem, there exist unique integers q and r such that $n = 2q + r$ and $0 \leq r < 2$.

$\therefore r = 0$ or $r = 1$. [These are the cases to consider.]

CASE 1: ($r = 0$)

Suppose $r = 0$. Then, $n = 2q + 0 = 2q$.

$\therefore n = 2q$. $\therefore n = 2q$ or $n = 2q+1$, by generalization.

$\therefore$ There exists an integer k [here, $k = q$] such that
$n = 2k$ or $n = 2k+1$, in CASE 1. [END of CASE 1]

CASE 2: ($r = 1$)

Suppose $r = 1$. Then, $n = 2q + 1$.

$\therefore n = 2q$ or $n = 2q + 1$, by generalization.

$\therefore$ There exists an integer k [here, $k = q$] such that
$n = 2k$ or $n = 2k+1$, in CASE 2. [END of CASE 2].

$\therefore$ In General, there exists an integer k such that $n = 2k$ or $n = 2k+1$.

QED, by Direct Proof.

The Parity Corollary:

For every integer n, n is even or n is odd.

Proof: Exercise, using the theorem above.

OUTLINE OF A PROOF USING "DIVISION INTO CASES"

To Prove: For every integer n, $n(n+1)$ is even.

Proof OUTLINE:

Let n be any integer.
By the Parity Corollary, n is even OR n is odd.

Case 1 (n is even):

Suppose n is even.

⋮

$\therefore n(n+1)$ is even in Case 1. [END of Case 1]
[OR "in the case that n is even."]

Case 2 (n is odd):

Suppose n is odd.

⋮

$\therefore n(n+1)$ is even in Case 2. [END of Case 2]
[OR "in the case that n is odd."]

$\therefore n(n+1)$ is even in general.

$\therefore$ For every integer n, $n(n+1)$ is even, by Direct Proof.

QED

To Prove: For every integer n, $n^2 + 5n + 7$ is odd.

Proof: Let n be any integer. [NTS: $n^2 + 5n + 7$ is odd .]

By the Parity Corollary, n is even or n is odd.

Case 1: (n is even.)

Suppose that n is even.

By definition of "even", there exits an integer k such that $n = 2k$.

$\therefore n^2 + 5n + 7 = (2k)^2 + 5(2k) + 7$ by substitution,

$= 4k^2 + 10k + (6+1)$

$= (4k^2 + 10k + 6) + 1$ by Rules of Algebra.

$\therefore n^2 + 5n + 7 = 2(2k^2 + 5k + 3) + 1$ by Rules of Algebra.

Let $t = 2k^2 + 5k + 3$, which is an integer since sums and products of integers are integers.

$\therefore n^2 + 5n + 7 = 2t + 1$, by substitution, and t is an integer.

$\therefore n^2 + 5n + 7$ is odd, by definition of "odd" in the case that n is even . [End of Case 1]

Case 2: (n is odd.)

Suppose that n is odd.

By definition of "odd", $n = 2k + 1$ for some integer k .

$\therefore n^2 + 5n + 7 = (2k + 1)^2 + 5(2k + 1) + 7$ by substitution,

$= (4k^2 + 4k + 1) + (10k + 5) + 7$

$= (4k^2 + 14k + 12) + 1$

$= 2(2k^2 + 7k + 6) + 1$ by Rules of Algebra

$\therefore n^2 + 5n + 7 = 2t + 1$, where $t = (2k^2 + 7k + 6)$, and t is an integer.

$\therefore n^2 + 5n + 7$ is odd, by definition of "odd" in the case that n is odd . [End of Case 2]

$\therefore n^2 + 5n + 7$ is odd in general .

$\therefore$ For every integer n, $n^2 + 5n + 7$ is odd, by Direct Proof.

QED

Proof-by-Contradiction

A Contradiction is a statement that is false in all cases.

Ex: $p \wedge \sim p$

p	$p \wedge \sim p$
T	F
F	F

The STD VALID ARGUMENT FORM "PROOF-BY-CONTRADICTION"

$\sim p \rightarrow (r \wedge \sim r)$

$\therefore p$

A Well-KNOWN fact:

Every rational number $\frac{a}{b}$ can be reduced to "Lowest Terms", $\frac{a}{b} = \frac{m}{n}$ such that m and n have no common prime factor.

Ex: $\frac{18}{12} = \frac{2 \times 3 \times 3}{2 \times 3 \times 2} = \frac{3}{2}$ in "Lowest Terms".

Proof-by-Contradiction and Proof-by-Contraposition

Proof-by-Contradiction

To Prove: Statement p.

	Task:
Proof: (by Contradiction)	
Suppose ~p .	[Suppose ~p]
. . .	
∴ q	[∴ q]
. . .	
∴ ~q	[∴ ~q]
∴ q ∧ ~q ("This is a contradiction.")	[∴ q ∧ ~q]
∴ p , by proof-by-contradiction. QED	[∴ p]

Comments about Proof-by-Contradiction:

1.) An explicit statement that a contradiction has been reached is required:

Example: Assume that, earlier in the proof, it was pointed out that ½ is not an integer.

Assume that now it has just been established that ½ is an integer.

You can state: "Therefore, ½ is not an integer and ½ is an integer, which is a contradiction."

Or, you can state: "Therefore, ½ is an integer, which contradicts the fact that ½ is not an integer."

Notice that this second wording combines the [∴ ~q] task and the [∴ q ∧ ~q] task into one sentence.

Thus, a proof-by-contradiction requires the use of one of the terms "contradicts" or "contradiction".

2.) After arriving at a contradiction, you must immediately conclude the negation of the supposition.

3.) You are not allowed to start a proof-by-contradiction with the phrase "Suppose not." Instead, you must "Suppose" the explicit wording of the negation of the statement to be proved.

4.) Use "Proof-by-Contradiction" to prove that something does not exist or that an object does not have a particular property.

Example:	Task
To Prove: There does not exist an integer which is both even and odd.	
Proof: (Proof-by-Contradiction)	
Suppose there exists an integer n which is both even and odd.	[Suppose ~p]
Note, ½ is not an integer.	[∴ q]
By definitions of "even" and "odd", there exist integers k and ℓ such that $n = 2k$ and $n = 2\ell + 1$.	
∴ $2k = 2\ell + 1$, by substitution. ∴ $2(k - \ell) = 1$. ∴ $(k - \ell) = ½$.	
∴ ½ is an integer since $(k - \ell)$ is an integer.	[∴ ~q]
∴ ½ is an integer and ½ is not an integer, a contradiction	[∴ q ∧ ~q]
∴ There does not exist an integer which is both even and odd, by proof-by-contradiction. **QED**	[∴ p]

Irrational Square Roots:

$\sqrt{2}$ and $\sqrt{n}$ when n is a Positive Integer and Not a Perfect Square

[It is recommended that you review Theorem (NIB) 3 in the handout "Theorems (NIB) 1,2, and 3."]

Theorem 4.6.1: $\sqrt{2}$ is irrational.

Proof: [Proof by Contradiction]

Suppose, by way of contradiction, that $\sqrt{2}$ is rational.

Since $\sqrt{2}$ is rational and positive, there exist positive integers m and n, with $n \neq 0$, such that $\sqrt{2} = \frac{m}{n}$, and we can assume that $\frac{m}{n}$ is written in lowest terms, so that m and n have no common prime factor.

[The author mistakenly says that m and n "have no common factor", but 1 is always a common factor.]

Since $\sqrt{2} = \frac{m}{n}$, $2 = \left(\sqrt{2}\right)^2 = \left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2}$ by substitution.

Since $2 = \frac{m^2}{n^2}$, $2n^2 = m^2$.

[The contradiction that we will establish is that $2 \mid m$ and $2 \mid n$,

which contradicts the fact that m and n have no common prime factor.]

Since $m^2 = 2n^2$ and n^2 is an integer, $2 \mid m^2$, by definition of "divides".

$\therefore$ Since $2 \mid m^2$ and 2 is prime, $2 \mid m$, by Theorem (NIB) 3.

$\therefore$ There exists an integer k such that $m = 2k$, by definition of "divides". Recall that $2n^2 = m^2$.

$\therefore$ $2n^2 = (2k)^2 = 2(2k^2)$, by substitution and the rules of algebra.

Dividing by 2, we conclude that $n^2 = 2k^2$, and k^2 is an integer.

$\therefore$ $2 \mid n^2$, by definition of "divides".

$\therefore$ Since $2 \mid n^2$ and 2 is prime, $2 \mid n$, by Theorem (NIB) 3.

$\therefore$ $2 \mid m$ and $2 \mid n$, which contradicts the fact that m and n have no common prime factors.

Therefore, $\sqrt{2}$ is irrational, by proof-by-contradiction

QED

[You might consider how this proof can be adapted to prove that $\sqrt{5}$ and $\sqrt{7}$ are irrational.]