

MATH135 Introduction

Sep 8/2017

Read Chapter 1 or Learn, Assignment 0

Chapter 2 Notes:

Definitions:

↳ Statement: T/F sentence (one or the other) - yes/no

↳ Proposition: Statement that needs to be proven

Ex: Rem. Theorem ↳ Theorem: Strong proposition (big) (pythag)

↳ Factor theorem ↳ Lemma: Helper proposition (small) (proven during proof)

↳ Corollary: Prop. follows prop (theorem) { We know theorem, so need little proof }

↳ Axiom: Given truth (assumed)

Symbols:

↳ $\neg A$: Not A (like !A in C8)

↳ $A \wedge B$: A and B

↳ $A \vee B$: A or B

↳ \equiv : Logically equivalent (Truth table Left=Right)

↳ De Morgan's Law:

↳ $\neg(A \vee B) \equiv \neg A \wedge \neg B$

↳ $\neg(A \wedge B) \equiv \neg A \vee \neg B$

↳ $A \Rightarrow B$: A (hypothesis) implies B (conclusion) or proposition

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

only situation where false

Example:

1) Negate A w/o negation symbols : $A: (5=2) \vee (3 < 6 < 7)$

$\neg A: \neg(5=2) \wedge \neg[(3 < 6) \wedge (6 < 7)]$

$(5 \neq 2) \wedge \neg[(3 < 6) \wedge (6 < 7)]$

$(5 \neq 2) \wedge [(6 \neq 3) \vee (6 \geq 7)]$

Chapter 3 Notes:

Laws:

$$A \vee (B \vee C) \equiv (A \vee B) \vee C \text{ (same for \wedge)}$$

$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$

$$A \Rightarrow B \equiv (\neg A) \vee B \quad \} \quad \neg(A \Rightarrow B) \equiv A \wedge (\neg B)$$

Chapter 4 Notes:

* If proving $ax^2 + bx + c = 0$, DON'T start w/ eqn

→ Treat $ax^2 + bx + c$ as a standalone expression and try
to get 0 (RHS).

Proving Implications:

→ Direct Proofs: Start w/ "Assume A is true", end w/ " $\therefore B$ must be true".

Lecture 2

Sep 11/2017

Example:

$$x^4 + x^2y + y^2 \geq 5x^2y - 3y^2 \text{ for } x, y \in \mathbb{R}$$

1) Discovery (can do anything)

$$\begin{aligned} x^4 - 4x^2y + 4y^2 &\geq 0 \\ (x^2 - 2y)^2 &\geq 0 \end{aligned}$$

2) Prove:

Let $x, y \in \mathbb{R}$

$$\therefore (x^2 - 2y)^2 \geq 0$$

expand to get original eqn. QED

MATH 135 - Chapter 5 & 6

Sept 13/2017

Proving Implications:

Can prove that the counter example (negation of $A \Rightarrow B$) is true $\neg(A \Rightarrow B) \equiv A \wedge \neg B$

Definitions:

Statements that are true (no proof required)

e.g.: even # = $2m$, $m \in \mathbb{Z}$

Divisibility:

$m|n \quad n = km, k \in \mathbb{Z} \quad \exists m/0 \text{ works.}$

$\Leftrightarrow n$ is a multiple of m

Example:

1) If n is an integer and $3|n$, then $3|n^2$

Let $n \in \mathbb{Z}$ such that $3|n$

$\therefore n = 3k$ and $n^2 = 9k^2$

$n^2 = 3(3k^2)$, since $(k \in \mathbb{Z}, 3k^2 \in \mathbb{Z})$

$\therefore n^2 = 3k^2 \quad 3|n^2 \quad (\text{QED})$

✓ need
this!

Bounds by Divisibility (BBD):

\exists such that

Let $a, b \in \mathbb{Z}$ such that $a|b$ and $b \neq 0$. Prove $|a| \leq |b|$

$\therefore b = ka$ when $k \in \mathbb{Z}$

$\therefore (since) b \neq 0, k \neq 0$

But $k \in \mathbb{Z}$, so $|k| \geq 1$, so

can't have
for neg. {
 $|b| = |ka|$
 $= |k||a|$
 $\geq |a| \quad (\text{QED})$

- Since $a|b$ and $b \neq 0$, $|a| \leq |b|$

\Rightarrow Then if $|a| > |b|$, $a+b = 0$

$\Rightarrow |a| \leq |b|$ doesn't tell us anything (can't reverse implications)

Transitivity of Divisibility:

Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

Let $a, b, c \in \mathbb{Z}$ where $a|b$ and $b|c$:

\therefore there exists $k \in \mathbb{Z} \ni b = ka$ and

" " $m \in \mathbb{Z} \ni c = mb$

$$\therefore c = m(ka)$$

$$= (mk)a$$

Since $m, k \in \mathbb{Z}$, $a|c$ Q.E.D.

$$\therefore mk \in \mathbb{Z}$$

Divisibility of Integer Combinations:

Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, for any $x, y \in \mathbb{Z}$, $a|(bx+cy)$

Sep 15, 2017

Let $a, b, c, x, y \in \mathbb{Z}$ where $a|b$ and $a|c$.

$\therefore b = ka$ for some $k \in \mathbb{Z}$.

$c = na$ for $n \in \mathbb{Z}$.

$$\therefore bx + cy$$

$$= kax + nay$$

$$= a(kx + ny) \quad \text{since } k, x, n, y \in \mathbb{Z}, kx+ny = m \text{ where } m \in \mathbb{Z}$$

= ma. move *

Q.E.D.

Sets:

Collection of unique objects (elements)

→ No order

→ Don't need to have anything in common

$$\cup x \in A$$

$$\cup A = \{-2, 5, \{1, 2, 3\}, 9\} \quad \text{4 elements} \quad \text{[trick question]}$$

→ 1, 2, 3 ∉ A!

$$\cup \mathbb{N} = \{\dots, \infty\} \quad \text{Natural \#s}$$

$$\cup \mathbb{Z} = \{x : x \in \mathbb{W}\}$$

$$\cup \mathbb{W} = \{0, \dots, \infty\} \quad \text{whole \#s} \quad \cup \mathbb{Q}$$

$$\cup \{\} : \text{Null set} \neq \text{Empty set}$$

$$\cup \mathbb{D} = \{a, b \in \mathbb{N} : a, b \neq 0\} \quad \text{Natural numbers}$$

Cardinality:

- # of elements.

$$S = \{1, 2, 3, 4\} \quad |S| = 4$$

The Universe of Discourse:

\mathcal{U} : Contains all items we may need.

- ↳ Eggs? N
 - ↳ Time? R
 - Divisibility? Z
- Variable type, kinda.

Set Builder Notation:

$$\{x \in \mathcal{U} : P(x)\}$$

↳ subset of \mathcal{U} , elements x satisfy $P(x)$

Example:

- 1) $\{x \in Z : (3|x)\} = \{x \in Z : ((1|x) \wedge (3|x))\}$
- 2) $\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 144\}$
 - ↳ Set of all points \bar{w} distance 12 from $(0,0)$
 - ↳ OR: $\{(x,y) : (x \in \mathbb{R}, y \in \mathbb{R}) \wedge (x^2 + y^2 = 144)\}$

Operations:

Unions:

$$A \cup B = \{x \in \mathcal{U} : (x \in A) \vee (x \in B)\}$$

Intersections:

$$A \cap B = \{x \in \mathcal{U} : (x \in A) \wedge (x \in B)\}$$

Set Difference:

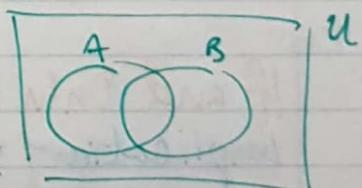
$$A - B = \{x \in \mathcal{U} : (x \in A) \wedge (x \notin B)\} \quad A \bar{w/o} B$$

Complement:

$$\overline{A} = \{x : (x \in \mathcal{U}) \wedge (x \notin A)\} \quad \text{All } \mathcal{U} \text{ w/o } A = \mathcal{U} - A$$

Cartesian Product:

$$A \times B = \{(x,y) : (x \in A) \wedge (y \in B)\} \quad |A \times B| = |A||B| \quad \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$$



Sep 18, 2017

Subsets:

A is subset of B if $x \in A \Rightarrow x \in B$

$\Leftrightarrow B$ is superset of A

\hookrightarrow "Proper subset" when elements in B not in A

$\hookrightarrow A \subseteq B$ subset $A \supseteq B$ superset.

$A \subsetneq B$ proper subset $A \not\subseteq B$ not subset

Example:

1) Prove that $\{n \in \mathbb{N} : 4|(n-3)\} \subseteq \{2k+1 : k \in \mathbb{Z}\}$

1) discover:

$4|(n-3)$ then $n-3 = 4a$. If n is odd, $= 2k+1$. \hookrightarrow need to get here.

$$n = 4a+3$$

$$n = 4a+2+1$$

$$n = 2(2a+1)+1 \quad \text{Let } k \in \mathbb{Z}$$

$$= 2k+1$$

\therefore if $x \in \{n \in \mathbb{N} : 4|(n-3)\}$ then $x \in \{2k+1 : k \in \mathbb{Z}\}$

$$\therefore A \subseteq B, Q.E.D$$

2) Prove that $\{x \in \mathbb{R} : ax^2+bx+c=0\} = \left\{ \frac{-b \pm \sqrt{b^2-4ac}}{2a} \right\}$

Converse of an Implication:

$B \Rightarrow A$ is converse of $A \Rightarrow B$

$\hookrightarrow A \Rightarrow B$ doesn't mean $B \Rightarrow A$.

If and Only If:

Implication & Converse are true.

$\hookrightarrow A \text{ iff } B = A \leftrightarrow B$

A	B	$A \leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

and \hookrightarrow If B : $B \Rightarrow A$

Only if B : $A \Rightarrow B$

if And only if

Proving -ffs:

To prove $A \Leftrightarrow B$, must prove $A \Rightarrow B$ AND $B \Rightarrow A$.

Example:

1) Suppose $x, y \geq 0$. Then $x=y$ iff $\frac{x+y}{2} = \sqrt{xy}$.

$$\begin{array}{c} A \\ \hline x=y \\ B \\ \hline \frac{x+y}{2} = \sqrt{xy} \end{array}$$

$\Rightarrow A \Rightarrow B$ Let $x, y \geq 0$ and $x=y$.

$$\therefore \frac{x+y}{2} = \frac{x+x}{2} = x = \sqrt{x^2} (\because x \geq 0)$$

NEED
THIS *

$\Leftarrow B \Rightarrow A$ Let $x, y \geq 0$ and $\frac{x+y}{2} = \sqrt{xy}$

$$x+y = 2\sqrt{xy}$$

$$\text{CAN } \sqrt{\text{both sides}} \rightarrow (x+y)^2 = 4xy$$

$$(x-y)^2 = 0$$

$$x=y \dots$$

$$\text{Q.E.D.} \therefore x=y \text{ iff } \frac{x+y}{2} = \sqrt{xy}$$

Set Equality:

$A=B$ if $(A \subseteq B) \wedge (B \subseteq A)$

Example:

Nah.

Quantifiers:

"Some", "Many", "All"

↳ How many elements in domain satisfy property.

↳ There exists some integer n such that $n^3 + 3 = 30$.

Sep 19, 2017

Universal Quantifier:

\forall = "for all" $\rightarrow \forall x \in \mathbb{R}, x^2 \geq 0$

↳ Can talk about null set and be true.

Existential Quantifier:

\exists - At least one is true $\rightarrow \exists x \in S \exists P(x)$ "there exists"
↳ Guarantees that there are elements in S

such that

Quantifier - Variable - Domain (set) - Open sentence

Proving Quantified Statements:

Select Method:

- (1) Prove that for every $x \in \mathbb{R}$, $x^2 + 3x + 5 > 0$
- ↳ Take a "representative" $x \in S$ to show $P(x)$ is true.
 - ↳ Use properties of S (in this case, \mathbb{R})
- Proof: Let $x \in \mathbb{R}$.
- $$\begin{aligned} x^2 + 3x + 5 &> x^2 + 3x + \frac{9}{4} \\ &= \left(x + \frac{3}{2}\right)^2 \\ &\geq 0 \end{aligned}$$
- original exp. is 7, so
 ≥ 0 means > 0 .
- $\therefore x^2 + 3x + 5 > 0$ for all $x \in \mathbb{R}$

Construct Method:

- (2) There exists a real number $x \in \mathbb{R}$ such that $x^2 + 3x = 5$
- ↳ Provide an explicit $x \in S$ that makes $P(x)$ true.

Proof: Consider $x = \frac{-3 + \sqrt{29}}{2}$.
Then $x^2 + 3x = \left(\frac{-3 + \sqrt{29}}{2}\right)^2 + 3\left(\frac{-3 + \sqrt{29}}{2}\right)$

$$= 5 \quad QED$$

Quantifiers in the Hypothesis:

If $\forall x \in \mathbb{N}, n|x$, then $n=1$.

Let $a, b, c \in \mathbb{Z}$. If $\forall x \in \mathbb{Z}, a|bx+c$, then $a|b+c$

↳ Substitution method: Assume hypo true, sub any value from domain

↳ Let $a, b, c \in \mathbb{Z}$, and $\forall x \in \mathbb{Z}, a|bx+c$.

Then when $x=1$, $a|b+c$. QED

This is valid
for \forall !!!!

Quantifiers in the Hypothesis:

Let $p \in \mathbb{R}, k \in \mathbb{Z}$. If there exists a non-zero $\mathbb{Z} q$ such that $\frac{p}{q} = k$, then p must be \mathbb{Z} .

If $14|n$ then $7|n$.

"There exists" integer k such that ...

Vacuousness

Sep 20, 2017

"There exists a unicorn that eats grass"

Let S be the set of all unicorns

$P(x)$ be " x eats grass"

$\exists x \in S, P(x)$ false, because $S = \emptyset$ Vacuously False

"My pug moose has won every math contest he's ever written."

Let S be set of Moose math contests

$P(x)$ be "Moose won x "

$\forall x \in S, P(x)$ true, because $S = \emptyset$ Vacuously True

Vacuously True:

$\forall x \in \emptyset, P(x)$

Vacuously False:

$\exists x \in \emptyset, P(x)$

Negating Quantifiers:

"All real numbers have a positive int. $\sqrt[n]{\cdot}$ "

↳ "There exists a real number which doesn't have +int $\sqrt[n]{\cdot}$ "

$$\neg [\forall x \in S, P(x)] \equiv [\exists x \in S, \neg P(x)]$$

$$\neg [\exists x \in S, P(x)] \equiv [\forall x \in S, \neg P(x)]$$

Proving/Disproving Quantifiers:

- 1) Single counter example disproves $\forall x \in S, P(x)$
- 2) Single example doesn't prove $\forall x \in S, P(x)$
- 3) Single example does prove $\exists x \in S, P(x)$
- 4) Proving $\exists x \in S, P(x)$ is false? Hard to do.

Nested Quantifiers:

$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$ is false.

Example:

1) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$

Proof: Let $x \in \mathbb{R}$. Let $y^3 = x^3 - 1$.

$$y^3 = x^3 - (x^3 - 1)$$

$$= 1. \quad QED$$

Language Practice

Sep 22, 2017

No multiple of 15 plus a multiple of 6 = 100.

$$\Rightarrow \forall x, y \in \mathbb{Z}, 15x + 6y \neq 100$$

Whenever 3 divides both the sum + difference of 2 integers,
it also divides each int.

$$\Rightarrow \forall a, b \in \mathbb{Z}, [(3|a+b) \wedge (3|a-b)] \Rightarrow [(3|a) \wedge (3|b)]$$

$$\forall m \in \mathbb{Z}, (\exists k \in \mathbb{Z}, m=2k) \Rightarrow (\exists t \in \mathbb{Z}, 7m^2 + 4 = 2t)$$

\Rightarrow If m is even then $7m^2 + 4$ is even (no even \mathbb{R} that's not \mathbb{Z})

$$n \in \mathbb{Z} \Rightarrow (\exists m \in \mathbb{Z}, m > n)$$

\Rightarrow There is no largest integer.

$$\forall k, m \in \mathbb{Z}, [(mk) \Rightarrow ((m^2 = 1) \vee (m^2 = k^2))] \Rightarrow [(|k| \neq 1) \Rightarrow (\sqrt{|k|} \notin \mathbb{N})]$$

\Rightarrow No prime numbers are perfect \square .

Contrapositives:

"If a student earns a grade of 50%+, then the student passed"

"If a student did not pass, they earned a grade below 50%."

$\neg B \Rightarrow \neg A$ is contrapositive of $A \Rightarrow B$

If $7 \nmid n$ then $14 \nmid n \Rightarrow \exists l \in \mathbb{Z}$

If $x^3 + 7x^2 < 9$ then $x < 1.1 \Leftrightarrow x^3 + 7x^2 \geq 9 \Leftrightarrow x \geq 1.1$

Implications Cont...

Sep 25, 2017

$$(A \wedge B) \Rightarrow C$$

$A \Rightarrow (B \wedge C)$ → prove $A \Rightarrow B$ and $A \Rightarrow C$

$(A \vee B) \Rightarrow C$ → prove $A \Rightarrow C$ and $B \Rightarrow C$

$A \Rightarrow (B \vee C)$ "elimination" → prove $(A \wedge \neg B) \Rightarrow C$

Proof by Contradiction:

Prove that the negation of a statement is absurd ($A \wedge \neg A$) if assumed to be true.

Example:

1) There is no largest integer.

Assume there is. Add 1 to it. Now the largest integer is both largest and not largest.

When to use Contradiction:

1) Negation of $A \Rightarrow B$ is $A \wedge \neg B$.

→ If B already has a negation, this is easier.

→ Or if you just like the negation better.

1) Contrapositive is similar.

→ $\neg B \Rightarrow \neg A$, but contradiction is $A \wedge \neg B$ which leads to $A \wedge \neg A$ which is like $\neg B \Rightarrow \neg A$.

Example:

1) Prove there are ∞ primes.

Let $n \in \mathbb{N}$. Can be expressed as product of primes "Prime Factorization"

Assume finite primes. Let $P = \{p_1, p_2, \dots, p_k\}$ be this set.

Let $N = p_1 p_2 p_3 \dots p_k + 1$. We see for any $p \in P$, $p \nmid N$ (breaks PF).

(so N is both $p \mid N$ and $p \nmid N$. Absurd.)

can also say this is also prime.

2) Prove $\sqrt{2}$ is irrational

Assume $\sqrt{2}$ is rational $= \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$.

A and B have no common divisors (lowest fraction)

$$b\sqrt{2} = a$$

$$2b^2 = a^2 \quad a^2 \text{ is even} \therefore a \text{ is even}$$

$$\text{so } a = 2k \text{ and } 2b^2 = 4k^2$$

$$b^2 = 2k^2$$

Absurd.

$\therefore b \text{ is even}$

3) Prove if $a, b \in \mathbb{Z}$ | $a \geq 2$, then $a|b$ or $a|b+1$.

Assume $a, b \in \mathbb{Z}$, $a \geq 2$ and $a \nmid b$ and $a \nmid b+1$.

$$\therefore \exists k, m \in \mathbb{Z} \mid b = ka \quad b+1 = ma$$

$$a(m-k) = 1$$

$$\therefore a \mid 1$$

$$\therefore a = \pm 1 \quad \text{but } a \geq 2$$

$\neg B$ led us here.

A

Uniqueness:

For each $x \in \mathbb{R}$, \exists a unique $y \in \mathbb{R}$ | $(x+1)^2 - x^2 = 2y - 1$.

↳ Only 1 solution exists.

↳ Prove y exists and no other y exists.

1) Isolate y to prove existence.

2) Uniqueness: Assume y is not unique. Let $y_1, y_2 \in \mathbb{R}$, $y_1 \neq y_2$

$$\textcircled{1} \quad (x+1)^2 - x^2 = 2y_1 - 1 \quad \text{and} \quad (x+1)^2 - x^2 = 2y_2 - 1 \quad \textcircled{2}$$

$$\therefore 2y_1 - 1 = 2y_2 - 1$$

$$y_1 = y_2 \quad \text{but} \quad y_1 \neq y_2, \text{ absurd.}$$

\therefore Unique y . $\square \in \mathbb{D}$.

$P(x) \wedge P(y) \Rightarrow x = y$ states uniqueness.

Division Algorithm:

If $a, b \in \mathbb{Z}$, $b > 0 \Rightarrow \exists$ unique q and r where

$$\text{dividend } a = qb + r \quad 0 \leq r < b.$$

Assume $a, b \in \mathbb{Z} > 0$ and q, r not unique.

$$\therefore \exists q_1, q_2, r, r_2 \in \mathbb{Z} \mid q_1 \neq q_2, r_1 \neq r_2$$

$$a = q_1 b + r, \quad a = q_2 b + r_2 \quad 0 \leq r, r_2 < b$$

$$q_1 b + r = q_2 b + r_2$$

$$b(q_2 - q_1) = r_2 - r_1 \quad b \mid (r_1 - r_2)$$

w/o loss of generality, assume $r_1 > r_2$. b/c one must be greater.

$$\therefore r_1 - r_2 > 0 \quad \text{and} \quad r_1 - r_2 < r,$$

Since $b \mid (r_1 - r_2)$, BBD: $b \leq r_1 - r_2 < r$,
but $b > r$. QED.

Injective Functions:

$f: S \rightarrow T$ is one to one iff $\forall x_1, x_2 \in S, (f(x_1) = f(x_2)) \Rightarrow x_1 = x_2$
↳ unique x for every $f(x)$.

Example:

1) $f: [1, \infty) \rightarrow (0, 0.5] \quad f(x) = \frac{x}{1+x^2}$ is 1-1.

Surjective Functions: "onto"

$f: S \rightarrow T$ iff $\forall y \in T, \exists x \in S \mid f(x) = y$.
↳ Codomain accessible through f .

Example:

1) $f: \mathbb{R} \rightarrow (-\infty, 1) \quad f(x) = 1 - e^{-x}$ is onto.

Sigma Notation

Sep 27, 2017

$\sum_{i=m}^n x_i$; i is the index variable. {Always +1}.
 m is initial. n is ending.

Pi Notation:

$\prod_{i=m}^n x_i$; Exact same as Σ , but with multi.

Example:

1) $\sum_{i=1}^5 3i^2 = 3(1)^2 + 3(2)^2 + \underbrace{3(3)^2 + 3(4)^2 + 3(5)^2}$

Π is same but x .

\rightarrow To increment by 2: $\sum_{i=1}^5 3(2i)^2$

Special Cases:

1) $\sum_{i=m}^m x_m = x_m$

2) $\sum_{j=5}^2 x_j = 0$ All sums begin to 0

3) $\prod_{i=m}^m x_m = x_m$

4) $\prod_{j=5}^2 x_j = 1$. All multi begin to 1.

Mathematical Induction:

Let $P(n)$ be a proposition depending on $n \in \mathbb{N}$.

→ If $P(1)$ is true, and First domino falls

→ $P(k) \Rightarrow P(k+1)$ Every domino makes next fall

→ Then $P(n)$ is true for all $n \in \mathbb{N}$. All fall!

POI:

1) Base Case:

→ Prove $P(1)$ (doesn't have to be 1).

2) Inductive Hypothesis:

→ Assume $P(k)$ for some $k \in \mathbb{N}$ (should write out $P(k)$)

3) Inductive Conclusion:

→ Prove $P(k) \Rightarrow P(k+1)$ (should write out $P(k+1)$)

Example:

$$1) \sum_{i=1}^n i(i+1) = \frac{n(n+1)(n+2)}{3}, \forall n \in \mathbb{N}$$

Let $P(n)$ be that $\sum_{i=1}^n i(i+1)$ WITHOUT $\forall n \in \mathbb{N}$ (MISTAKE!)

Base Case: Show $P(1)$ is true.

$$\begin{aligned} \sum_{i=1}^1 i(i+1) &= 1(1+1) = 1 \times 2 \\ &= \frac{1 \times (1+1) \times (1+2)}{3} \quad \therefore P(1) \text{ is true.} \end{aligned}$$

Inductive Hypothesis: Assume $P(k)$ is true.

$$\sum_{i=1}^k i(i+1) = \frac{k(k+1)(k+2)}{3} \text{ for some } k \in \mathbb{N}$$

Inductive Conclusion: Show $P(k) \Rightarrow P(k+1)$

$$\text{RTP: } \sum_{i=1}^{k+1} i(i+1) = \frac{(k+1)((k+1)+1)((k+1)+2)}{3}$$

$$\text{GOAL} \rightarrow = \frac{(k+1)(k+2)(k+3)}{3}$$

Well,

$$\begin{aligned}
 \sum_{i=1}^{k+1} i(i+1) &= \sum_{i=1}^k i(i+1) + (k+1)[(k+1)+1] \\
 &= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \quad (\text{by ind. hypo.}) \\
 &\quad * \text{ needs } \\
 &= \frac{(k+1)(k+2)(k+3)}{3} \quad \text{as desired. QED.}
 \end{aligned}$$

\therefore by POMI, $\forall n \in \mathbb{N} \ \& \exists \delta$.

2) $n! > 2^n, \forall n \in \mathbb{Z}, n \geq 4$

Let $P(n)$ be the statement $n! > 2^n$.

Base Case: Show $P(4)$ is true.

$$\begin{aligned}
 4! &= 24. \\
 2^4 &= 16.
 \end{aligned}
 \quad \left\{ \begin{array}{l} 24 > 16 \\ \therefore P(4) \text{ is true.} \end{array} \right.$$

Inductive Hypothesis: Show $P(k)$ is true. Assume $k! > 2^k$

Assume $k! > 2^k$ for some $k \geq 4$.

Inductive Conclusion: Prove $P(k+1) \Leftarrow P(k)$

Prove $(k+1)! > 2^{k+1}$

$$\begin{aligned}
 (k+1)! &> 2^{k+1} \\
 = k!(k+1) &> 2^{k+1} \\
 &> (k+1) 2^k \quad (\text{by IH}) \\
 &\geq 5 \cdot 2^k \quad \text{since } k \geq 4 \\
 &> 2 \cdot 2^k \\
 &> 2^{k+1}
 \end{aligned}$$

Sep 29, 2017

Point Practice:

$6 | 2n^3 + 3n^2 + n$ $2n^3 + 3n^2 + n \equiv 6k \pmod{6} \iff n \in \mathbb{Z}$ if $n \in \mathbb{Z}$, you
 Base case: Let $n = 1$. need to show $P(k+1)$ and $P(k-1)$

$$6 | 6k \quad k = 2, 3, \dots$$

IH: Assume $P(x)$ is true.

$$\therefore \exists k \in \mathbb{Z} \mid 2x^3 + 3x^2 + x \equiv 6k \pmod{6}$$

IC: Prove $P(x+1)$:

$$2(x+1)^3 + 3(x+1)^2 + x+1$$

$$= 2(4x^3 + 6x^2 + 4x + 1) + 3(x^2 + 2x + 1) + x + 1$$

$$= 2[x^3 + 2x^2 + x + x^2 + 2x + 1] + 3x^2 + 6x + 3 + x + 1$$

$$= 2(x^3 + 3x^2 + 3x + 1) + 3x^2 + 7x + 4$$

$$= 2x^3 + 6x^2 + 6x + 2 + 3x^2 + 7x + 4 \equiv 6x^3 + 9x^2 + 13x + 6 \pmod{6}$$

$$= (2x^3 + 3x^2 + x) + 6x^2 + 5x + 3x + 6 \pmod{6}$$

$$= 6k + 6x^2 + 12x + 6 \pmod{6}$$

$$= 6(k+x^2 + 2x + 1) \Rightarrow 6 \mid P(x+1)$$

The sequence $\{x_n\}$, $x_1 = 4$, $x_2 = 68$, $x_m = 2x_{m-1} + 15x_{m-2}$ for $m \geq 3$, $x_n = 2(-3)^n + 10(5)^{n-1}$ for $n \geq 1$ need two base cases 2 times for another

Let $P(n)$ be " $x_n = 2(-3)^n + 10(5)^{n-1}$ " where x_m is ...

needed $\rightarrow x_1 = 4$, $x_2 = 68$, $x_m = 2x_{m-1} + 15x_{m-2}$ for $m \geq 3$.

Base Case: Prove $P(1)$ and $P(2)$

$$2(-3)^1 + 10(5)^0 = 4 = x \therefore P(1) \text{ is true.}$$

$$2(-3)^2 + 10(5)^1 = 68 = x_2 \therefore P(2) \text{ is true.}$$

IH: Assume $P(k)$ and $P(k-1)$ are true.

$$\begin{aligned} x_k &= 2(-3)^k + 10(5)^{k-1} \\ \text{and } x_{k-1} &= 2(-3)^{k-1} + 10(5)^{k-2} \end{aligned} \quad \left\{ \begin{array}{l} k \in \mathbb{N} \geq 3 \\ \end{array} \right.$$

IC: Prove ($P(k) \wedge P(k-1) \Rightarrow P(k+1)$) Want: $x_{k+1} = 2(-3)^{k+1} + 10(5)^k$

$$x_{k+1} = 2x_k + 15x_{k-1}$$

$$= 2[2(-3)^k + 10(5)^{k-1}] + 15[2(-3)^{k-1} + 10(5)^{k-2}] \text{ by IH}$$

$$= 4(-3)^k + 20(5)^{k-1} + 30(-3)^{k-1} + 150(5)^{k-2}$$

$$= 4(-3)^k + 4(5)^k - 10(-3)^k + (6)(25)(5^{k-2})$$

$$\begin{aligned}
 &= 4(-3)^k + 4(5)^k - 10(-3)^k + 6(5)^k \\
 &= -6(-3)^k + 10(5)^k \\
 &= 2(-3^{k+1}) + 10(5^k) \quad \text{QED.}
 \end{aligned}$$

↑ example where $b=2$.

Principle of Strong Induction:

Let $P(n)$ be a statement $n \in \mathbb{N}$.

1) $P(1), P(2), \dots, P(b)$ true for some $b \in \mathbb{Z}^{>0}$

2) $P(1), P(2), \dots, P(k) \Rightarrow P(k+1)$ for all $k \in \mathbb{N}$

Then $P(n)$ is true $\forall n \in \mathbb{N}$. b is "suitably long"

Example:

1) Suppose $x_1 = 3, x_2 = 5, x_n = 3x_{n-1} + 2x_{n-2}$ for $n \geq 3$. Then $x_n < 4^n \forall n \in \mathbb{N}$.

Base Case: $P(1)$ and $P(2)$ are true.

$$3 = x_1 < 4^1 \quad 5 = x_2 < 4^2$$

$$\begin{aligned}
 &(x_k < 4^k) \wedge (x_{k-1} < 4^{k-1}) \\
 &x_{k+1} = 3x_k + 2x_{k-1} \quad (\text{hopefully } < 4^{k+1}) \\
 &< 3(4^k) + 2(4^{k-1}) \\
 &< 3(4^k) + 4(4^{k-1}) \\
 &= 3(4^k) + 4^k \\
 &= 4^{k+1}
 \end{aligned}$$

Fibonacci Sequence

$$\begin{aligned}
 f_1 &= 1, f_2 = 1 \quad f_n = f_{n-1} + f_{n-2} \quad \text{for } n \geq 3 \\
 \sum_{r=1}^n f_r^2 &= f_n f_{n+1} \quad \text{for all } n \in \mathbb{N}
 \end{aligned}$$

Oct 2, 2017

Fibonacci Proofs:

1) $\sum_{r=1}^n f_r^2 = f_n f_{n+1}$ for $n \in \mathbb{N}$. Weak

Base Case: $\sum_{r=1}^1 f_r^2 = 1^2 = 1 \times 1 = f_1 \times f_2$

Inductive Hypothesis: $\sum_{r=1}^k f_r^2 = f_k f_{k+1}$

Inductive Conclusion:

$$\sum_{r=1}^{k+1} f_r^2 = f_{k+1} f_{k+2}$$

$$= \left(\sum_{r=1}^k f_r^2 \right) + f_{k+1}^2$$

$$= \underbrace{f_k f_{k+1}}_{\text{IH}} + f_{k+1}^2$$

$$= f_{k+1} (f_k + f_{k+1})$$

$$= f_{k+1} f_{k+2}$$

2) $f_n < \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{N}$. Strong

shows base case $f_1 = 1 < \left(\frac{7}{4}\right)^1$ $f_2 = 1 < \left(\frac{7}{4}\right)^2$

Inductive Hypothesis: $f_k < \left(\frac{7}{4}\right)^k$ $f_{k-1} < \left(\frac{7}{4}\right)^{k-1}$

$f_1 < \left(\frac{7}{4}\right), f_2 < \left(\frac{7}{4}\right)^2 \dots f_k < \left(\frac{7}{4}\right)^k$ * need this way!

→ Assume you can go from 1 ... k. Now show how you can get the next one.

Inductive Conclusion:

$$f_{k+1} < \left(\frac{7}{4}\right)^{k+1}$$

$$\begin{aligned} \text{IH } f_{k+1} &= f_k + f_{k-1} \\ &< \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} \\ &= \left(\frac{7}{4}\right)^{k-1} \left(\frac{7}{4} + 1 \right) \\ &\leq \left(\frac{7}{4}\right)^{k-1} \left(\frac{7}{4}\right)^2 \\ &= \left(\frac{7}{4}\right)^{k+1} \end{aligned}$$

Discovering Truths:

Oct 3, 2017

Closed Form:

Determine a closed form for $\prod_{r=2}^n \left(1 - \frac{1}{r^2}\right)$

$$\begin{aligned}
 &= \left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{3^2}\right) \left(1 - \frac{1}{4^2}\right) \\
 &= \left(1 - \frac{1}{4}\right) \left(1 - \frac{1}{9}\right) \left(1 - \frac{1}{16}\right) \\
 &= \left(\frac{n^2 - 1}{n^2}\right) \left(\frac{(n+1)^2 - 1}{(n+1)^2}\right) \\
 &= \left(\frac{n^2 - 1}{n^2}\right) \left(\frac{n^2 + 2n}{n^2 + 2n + 1}\right) \\
 &= \frac{(n^2 - 1)}{(n^2)} \cdot \frac{(n+1)^2 - 1}{(n+1)^2} \cdot \frac{(n+2)^2 - 1}{(n+2)^2} \cdots \frac{(n^2 - 1)}{(n^2)}
 \end{aligned}$$

n	$\prod_{r=2}^n \left(1 - \frac{1}{r^2}\right)$
2	$\frac{1}{4}$
3	$\frac{3}{4} \times \frac{8}{9} = \frac{2}{3} = \frac{4}{6}$
4	$\frac{2}{3} \times \frac{15}{16} = \frac{5}{8}$
5	$\frac{5}{8} \times \frac{24}{25} = \frac{3}{5} = \frac{6}{10}$

$$\frac{n+1}{2n} ?$$

Now, proof by induction:
BC: $n=2 \quad \prod_{r=2}^2 \left(1 - \frac{1}{r^2}\right) = \frac{3}{4} = \frac{2+1}{2(2)}$ ✓

IH: $k: \prod_{r=2}^k \left(1 - \frac{1}{r^2}\right) = \frac{k+1}{2k}$

IC: $\prod_{r=2}^{k+1} \left(1 - \frac{1}{r^2}\right) \rightarrow \text{want to equal } \frac{(k+1+1)}{2(k+1)}$

$$\Rightarrow \left(\prod_{r=2}^k \left(1 - \frac{1}{r^2}\right) \right) \times \left(1 - \frac{1}{(k+1)^2}\right)$$

IH: $\left(\frac{k+1}{2k} \right) \left(\frac{(k+1)^2 - 1}{(k+1)^2} \right) \leftarrow \text{add cancel } (k+1) \text{ but need to state } k \neq -1.$

$$= \left(\frac{k+1}{2k} \right) \left(\frac{k^2 + 2k}{k^2 + 2k + 1} \right)$$

= Finish w $\frac{k+2}{2(k+1)}$ ✓

Examples:

1) Prove every integer $n > 1$ can be written as a product of primes

Strong Induction:

$\cap (P(n)) \uparrow$

BC: $n=2$. 2 is prime ✓

IH: Assume $P(2) \wedge P(3) \wedge P(4) \wedge \dots \wedge P(k)$ \leftarrow not this

do this! \rightarrow or, $P(n)$ true for $2 \leq n \leq k$ for some $k \geq 2$. *more formal

IC: $k+1$ is prime or composite.

If prime, wh... yeah.

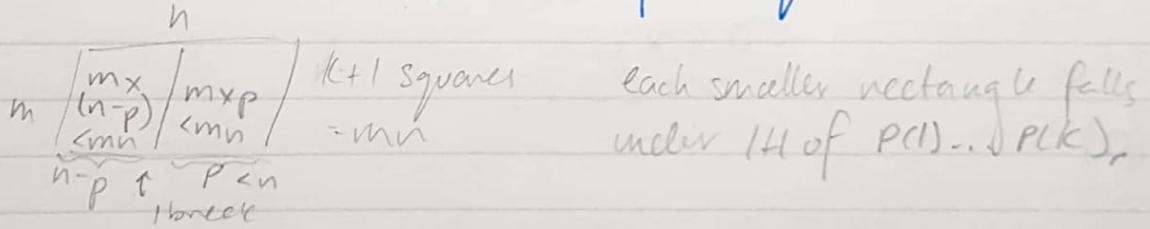
If composite, $\exists m, n \in \mathbb{N}$, $k+1 = mn$, $m, n < k+1$

\rightarrow Then $P(m), P(n)$ true by IH. So $k+1$ can
be written as product of primes (QED).

Didn't need 2 base cases, but had to assume string of truth.

2) Exactly $mn-1$ breaks are needed to break an $m \times n$ chocolate bar into unit squares.

Let $t = mn$, which is # of unit squares in choc. bar. $t \in \mathbb{N}$.



Greatest Common Divisor:

Oct 6, 2017

Let $a, b \in \mathbb{Z}$. The gcd is an integer d where
d is greater than any other divisor \downarrow if $c|a$ and $c|b$, then $c \leq d$.

Notation:

$\gcd(a, b)$.

- ↳ $\gcd(0, 0) = 0$ *exception*
- ↳ $\gcd(a, a) = |a|$

Proof of $\gcd(a, b)$ existence:

Let $a, b \in \mathbb{Z}$.

- ① If $a = b = 0$, $\gcd(a, b) = 0$ by def.
- ② If one of $a, b = 0$ but not both:
 $\gcd(a, b) = |ab| = \max\{|a|, |b|\}$
- ③ If $a \neq 0, b \neq 0$ then $|a|$ and $|b|$, \therefore There is a divisor.
for any $c \in \mathbb{Z}$, if $c|a$ and $c|b$ then
BBD: $c \leq \min\{|a|, |b|\}$
 $\therefore 1 \leq c \leq \min\{|a|, |b|\} \leftarrow c \text{ is bounded}$
 $\therefore \gcd(a, b)$ exists

Drove they're unique? Assume they're not unique. \therefore One must be bigger

Finding the GCD:

Let $a, b \in \mathbb{N}$. If $n = ab$, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Assume $a > \sqrt{n}$, $b > \sqrt{n}$ where $n \in \mathbb{N}$.

$$ab > \sqrt{n} \sqrt{n}$$

$$ab > n \quad \therefore n \neq ab \text{ QED.}$$

Example:

1) Prove $\gcd(3a+b, a) = \gcd(a, b)$.

Let $a, b \in \mathbb{Z}$, $c = \gcd(a, b)$, $d = \gcd(3a+b, a)$.

$\therefore |c|a$, $|c|b$ and $|d|3a+b$ and $|d|a$.

\therefore By DIC, $|c|3a+b$

$$\therefore \exists k \in \mathbb{Z} \ni 3a+b = kd, \exists m \in \mathbb{Z} \ni a = md.$$

$$\Rightarrow 3(md) + b = kd$$

$$b = (k-3m)d$$

$$\therefore d|b.$$

$\therefore c \leq d$ and $d \leq c$. $c=d$ QED.

Since c is divisor of things d is gcd of, and vice versa.

Remainders:

Oct 12, 2017

If $a, b, q, r \in \mathbb{Z} \ni a = qb+r$, then

$$\gcd(a, b) = \gcd(b, r) \quad \text{"GCD WR"}$$

Proof:

Let $a, b, q, r \in \mathbb{Z}$ where $a = qb+r$. Let $d = \gcd(a, b)$.

$r = a - qb$, and since $d = \gcd(a, b)$, $d|q(a-qb)$ by DIC.

$\therefore d|r$, and we already know $d|b$.

Let $e = \gcd(b, r)$. $\therefore e|d$.

$a = qb+r$, then by DIC, $e|a$. Also, $e|b$.

But $d = \gcd(a, b)$. $\therefore d \geq e$. Thus, $e = d$.

Euclidean Algorithm:

$$\gcd(1239, 735) : 1239 = (1)(735) + 504$$

$$\therefore \gcd(1239, 735) = \gcd(735, 504) \text{ by GCD WR}$$

Keep going until $r=0$. last non-zero r is answer.

55 VBNY
1919 2221425

1919 , 2, 22, 4/25
4 M 5 4 M

Example:

1) Prove $\gcd(3a+b, a) = \gcd(a, b)$, again.

Let $a, b \in \mathbb{Z}$, $x = 3a+b$.

By GCD WR, $\gcd(\underline{3a+b}, a) = \gcd(\cancel{a}, \cancel{b})$
 \times (from euclidean algo)

Checking GCDs:

$$\begin{aligned} 21 &= 231 - 5(42) \quad \text{sub in previous lines} \\ &= 231 - 5[504 - 2(231)] \\ &= 11(231) - 5(504) \end{aligned}$$

Just going
backward

$$= 27(235) - 16(1239) \quad \text{"certificate of correctness"}$$

$$\begin{aligned} \text{Original: } 1239 &= 735 + 504 \\ 735 &= 504 + 231 \\ 504 &= 2(231) + 42 \\ 231 &= 5(42) + 21 \\ 42 &= 2(21) \end{aligned}$$

Why does this work?

→ Suppose $c > 0$, $c | 735$, $c | 1239$

→ Then, by DIC, $c | 21 \rightarrow c | b$ b/c it's a linear comb.
→ BBD says $|c| \leq 21$.

GCD Characterization Theorem (GCD CT):

If $d > 0$ is common divisor of $a, b \in \mathbb{Z}$, then $\exists x, y \in \mathbb{Z} \ni$

$$ax+by = d \Rightarrow d = \gcd(a, b)$$

$$6 > 0, 6 | 30 \text{ and } 6 | 42. 30(3) + 42(-2) = 6. \therefore 6 = \gcd(30, 42)$$

Proof of GCD CT:

Let $a, b, d \in \mathbb{Z} \ni d > 0$ and $d|a$ and $d|b$.

Suppose $\exists x, y \in \mathbb{Z} \ni ax + by = d$.

Let $c \in \mathbb{Z} \mid cla$ and $c|b$.

$\therefore d = ax + by$, $c|d$ by DIC.

By BBD, $|c| \leq d$. All divisors $\leq d$. $\square \in \emptyset$.

Bézout's Lemma (BL):

If $a, b \in \mathbb{Z}$ where $d = \gcd(a, b)$, then $\exists x, y$ such that $ax + by = d$ (d, x, y can be computed).

Can always certify correctness

Example:

1) If $a, b, x, y \in \mathbb{Z} \ni \gcd(a, b) \neq 0$ and $ax + by = \gcd(a, b)$ then $\gcd(x, y) = 1$.

Let $a, b, x, y \in \mathbb{Z}$. Let $d = \gcd(a, b) \neq 0$

$d = ax + by$. $d|a$, $d|b$, so $\exists k, m \in \mathbb{Z}$ where $a = kd$, $b = md$.

so $kdx + mdy = d$ $d \neq 0$, so

$$kx + my = 1$$

2) If $n \in \mathbb{Z}$ then $\gcd(n, n+1) = 1$

$$(-1)n + (1)(n+1) = 1. \quad \left\{ \begin{array}{l} \text{GCD CT since} \\ 1|n \text{ and } 1|(n+1) \end{array} \right.$$

linear combination

3) Prove or disprove:

$$\text{Let } a, b, c \in \mathbb{Z}. \text{ If } \exists x, y \in \mathbb{Z} \text{ where } ax^2 + by^2 = c, \text{ then } \gcd(a, b) \mid c. \quad d = \gcd(a, b).$$

$$\Rightarrow kd^2x^2 + md^2y^2 = c$$

$$d(kx^2 + my^2) = c$$

$$d \mid c.$$

$$\Leftarrow a=1, b=3, c=2, \text{ so not true!}$$

$$\gcd(1, 3) = 1. \quad 1 | 2.$$

$$\text{But, } 1x^2 + 3y^2 = 2$$

$$x^2 + 3y^2 = 2 \text{ never, since } x^2, y^2 \geq 0.$$

Tryxi's Lemma (TL):

$$a, b, c \in \mathbb{Z}. \quad (\gcd(a, b) = 1) \wedge (a \mid bc) \Rightarrow a \mid c.$$

Oct 16, 2017

Moose's Lemma (ML):

$$a, b, c, d, e \in \mathbb{Z}. \quad (e = ab + cd) \wedge (e \mid a) \wedge (\gcd(e, c) = 1) \Rightarrow e \mid d$$

Proof:

$$\text{Let } a, b, c, d, e \in \mathbb{Z} \Rightarrow \gcd(e, c) = 1, e \mid a, e = (ab + cd)$$

$$\therefore \exists k \in \mathbb{Z} \Rightarrow a = ke.$$

$$kbe + cd = e$$

$$cd = (1 - kb)e$$

$$\therefore e \mid cd. \text{ But, } \gcd(e, c) = 1, \text{ so by TL, } e \mid d.$$

Extended Euclid Algorithm (EEA):

Find $\gcd(a, b)$, $a > b$.

	x	y	r	q
1)	1	0	a	0
2)	0	1	b	0
:	:	:	:	:

$$\text{Row}_i : 1) q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$$

$$2) \text{Row}_i = \text{Row}_{i-2} - q_i \text{Row}_{i-1}$$

Stop when $r_i = 0$. 2nd last row will have $\gcd(a, b)$ in r column, x, y cert values too.

Example:

$$\gcd(399, -4145) = \gcd(4145, 399)$$

1)	x	y	r	q
	1	0	4145	0
	0	1	399	0
	1	-10	155	10
	-2	21	89	2
	3	-31	66	1
	-5	52	23	1
	13	-135	20	2
	-18	187	3	1
	121	-1257	2	6
	-139	1444	1	1
	399	-4145	0	2

$$\therefore \gcd(399, -4145) = 1$$

2) Prove $\gcd(ab, c) = 1 \Rightarrow \gcd(a, c) = \gcd(b, c) = 1$. Oct 17, 2017

$\Rightarrow abc \in \mathbb{Z}$. Let $\gcd(ab, c) = 1$.

$\therefore \exists x, y \in \mathbb{Z}, \exists abx + cy = 1$. (BL)

Since $bx \in \mathbb{Z}$, $\gcd(a, c) = 1$. $\left\{ \begin{array}{l} \text{GCD CT } (1/a) \wedge (1/c) \\ \text{QED } \gcd(a, c) = 1. \end{array} \right.$
since $ax \in \mathbb{Z}$, $\gcd(b, c) = 1$. $\left\{ \begin{array}{l} \text{QED } \gcd(b, c) = 1. \\ \text{same for } (b, c) \end{array} \right.$

$\Leftarrow abc \in \mathbb{Z}$. Let $\gcd(a, c) = \gcd(b, c) = 1$.

$\therefore \exists x_1, y_1, x_2, y_2 \in \mathbb{Z} \ni ax_1 + cy_1 = 1$ and $bx_2 + cy_2 = 1$ (by BL)

$$(ax_1 + cy_1)(bx_2 + cy_2) = 1$$

$$abx_1x_2 + acx_1y_2 + bcx_2y_1 + c^2y_1y_2 = 1$$

$$ab(x_1x_2) + c(acx_1y_2 + bcx_2y_1 + c^2y_1y_2) = 1 \quad \text{QED}$$

$$(1|ab) \wedge (1|c), \text{ so } \gcd(ab, c) = 1 \quad (\text{by GCD CT})$$

GCD of one (GCD 00)

- 3) $\gcd(a, b) = 1 \iff \exists x, y \in \mathbb{Z} \ni ax + by = 1$.
 \Rightarrow Let $\gcd(a, b) = 1$. BL, QED.
 \Leftarrow Let $ax + by = 1$. $1 \mid a \wedge 1 \mid b \Rightarrow \gcd(a, b) = 1$ by GCD CT, QED.

Division by the GCD (DB GCD)

4) $\gcd(a, b) = d \neq 0 \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Let $\gcd(a, b) = d \neq 0$.

$\therefore ax + by = d \neq 0$ by BL

$$\frac{a}{d}x + \frac{b}{d}y = 1 \quad (d \neq 0)$$

$\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$ since $\gcd(a, b) = d$

Coprimes and Divisibility (CAD)

$a, b \in \mathbb{Z}$ are coprime if $\gcd(a, b) = 1$.

Let $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $a \mid bc \Rightarrow a \mid c$ (CAD)

Proof:

$$ax + by = 1 \quad bc = ma$$

\hookrightarrow GCD 00, and: $acx + bcy = c$

$$acx + may = c$$

$$a(cx + my) = c \quad : \text{since } cx + my \in \mathbb{Z}, a \mid c \text{ QED.}$$

Euclid's Lemma (EL):

Oct 18, 2017

Let $a, b, p \in \mathbb{Z}$. If p is prime and $p \mid ab \Rightarrow p \mid a \vee p \mid b$

Generalized EL:

Let $p \in \mathbb{Z}$ and $M \subseteq \mathbb{Z}$ with $|M| = n$. Let $M = \{m_1, \dots, m_n\}$

If p is prime and $p \mid \prod_{i=1}^n m_i \Rightarrow \exists x \in M \ni p \mid x$

$\nearrow p$ must divide all elements

Proof of EL:

Let $a, b, p \in \mathbb{Z}$. Let p be prime where $p \mid ab$.

Either $p \mid a$, or $\gcd(p, a) = 1$, where CAD says $p \nmid b$.

Unique Factorization Theorem (UFT):

$n \in \mathbb{Z}, n > 1$. n can be written as product of prime factors uniquely

↳ "Fundamental Theorem of arithmetic"

↳ Proof on Lecture 22 slide 6

↳ Basically, $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$

paper proof
w/ induction
(problematic)

↳ $p_i \mid n$, so $p_i \mid q_1 q_2 \cdots q_l$

↳ By EL, p_i must divide one of them, and $p_i = q_i$

↳ keep going until $p_k = q_l$, $k=l$.

Divisors From Prime Factorization (DFPF):

Let $n > 1 \in \mathbb{Z}$, $d \in \mathbb{N}$. If

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

is the unique PF of n into powers of distinct primes $p_1, p_2 \dots p_k$ where $\alpha_1, \alpha_2, \dots, \alpha_k \geq 1$, then d is a positive divisor of n iff

$$d = p_1^{d_1} p_2^{d_2} p_3^{d_3} \cdots p_k^{d_k}$$

where $0 \leq d_i \leq \alpha_i$ for $i = 1, 2, 3, \dots, k$

↳ d is subset (can have 0 exponent)

Example:

$$12 \cdot 63 = 3^2 \cdot 7^1 \cdot 2^2 \cdot 3^1$$

$$3^0 \cdot 7^0 = 1$$

$$3^1 \cdot 7^0 = 3$$

$$3^2 \cdot 7^0 = 9$$

$$3^0 \cdot 7^1 = 7$$

$$3^1 \cdot 7^1 = 21$$

$$3^2 \cdot 7^1 = 63$$

2) How many multiples of 12 are divisors of 2940? $\rightarrow 12$

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

$$2940 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^2$$

need this 6 possible remaining. Negatives would be $6 \cdot 2 = 12$.

1) Proof: If $a^2 | b^2 \Leftrightarrow a | b$.

→ Lecture 22 slide 11

GCD from PF: (GCD PF)

Oct 20, 2017

Let $a = p_1^{d_1} \cdots p_k^{d_k}$, $b = p_1^{B_1} \cdots p_k^{B_k}$ be PFs of a, b (exp can be 0).

$$\therefore \gcd(a, b) = p_1^{\min\{d_1, B_1\}} \cdots p_k^{\min\{d_k, B_k\}}$$

$d_i = \min\{d_i, B_i\}$ (think common factoring)

Example:

1) Prove $\gcd(ab) * \text{lcm}(a, b) = ab$.

$$\text{lcm}(a, b) = p_1^{l_1} \cdots p_k^{l_k} \text{ where } l_i = \max\{d_i, B_i\} \text{ QED.}$$

Linear Diophantine Equations:

DE's: Eqns w/ int coeffs, int solutions are sought.

→ All vars deg 1? LDE.

→ Simplest is $ax = b$ ($\Rightarrow a | b$)

→ $ax + by = c$

→ Solution exists? LDET,

→ Can we find? EEA

→ Can find more? LDET₂

Example:

1) $143x + 253y = 11$

$$\rightarrow 11 | 143 \wedge 11 | 253 \therefore 11 = \gcd(253, 143)$$

2) $143x + 253y = 154$

$$\rightarrow 11 | 154 \dots (x, y) \rightarrow (14x, 253y) \text{ solution}$$

LDE Theorem Pt 1:

Let $\gcd(a, b) = d$. The LDE $ax + by = c$ has solution $\Leftrightarrow d | c$.

Proof:

Let $d = \gcd(a, b)$. $\therefore \exists x_0, y_0 \in \mathbb{Z} \mid ax_0 + by_0 = d$ (BL)

\Rightarrow Let $ax + by = c$ have a solution.

$$\therefore \exists x_1, y_1 \in \mathbb{Z} \ni ax_1 + by_1 = c$$

And we know $d \mid a, d \mid b$.

$$d(x_1 x_0 + k_1 y_0) = c \quad \therefore d \mid c$$

\Leftarrow let $d \mid c \therefore c = kd$

$$ax_0 + by_0 = d$$

$$kax_0 + bk y_0 = c$$

\therefore solution is (kx_0, ky_0)

QED.

LDET2:

Oct 23, 2017

Let $\gcd(a, b) = d \neq 0, b \neq 0$.

If x_0, y_0 is a solution to $ax + by = c$, then:

$$x = x_0 + \frac{b}{d}n \quad \left\{ \begin{array}{l} n \in \mathbb{Z} \\ \text{and } d \mid b \end{array} \right.$$

$$y = y_0 - \frac{a}{d}n \quad \left\{ \begin{array}{l} n \in \mathbb{Z} \\ \text{and } d \mid a \end{array} \right. \quad \text{to take lowest slope form.}$$

Example:

1) Solve the LDE $20x + 35y = 5$

$$4x + 7y = 1$$

$\gcd(4, 7) = 1$, and $1/1$. one soln: $x_0 = 2, y_0 = -1$

$$\therefore x = 2 + \frac{7}{1}n \quad \left\{ \begin{array}{l} n \in \mathbb{Z} \\ \text{and } d \mid 7 \end{array} \right. \quad \text{by LDET2} \quad \left\{ \begin{array}{l} \text{correct answers.} \\ \text{and } -5, 3 \end{array} \right.$$

\hookrightarrow Can sub back in to check

LDET2 \equiv Sets:

$ax + by = c, a, b, c \in \mathbb{Z} \neq 0$. Set solutions:

$$S = \{(x, y) : x, y \in \mathbb{Z}, ax + by = c\} \quad \text{Non empty iff } \gcd(a, b) \mid c$$

$\emptyset \neq S \Leftrightarrow$ LDET2: $T = \{(x, y) : x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n, n \in \mathbb{Z}\}$

To prove LDET2: $S \subseteq T \Leftrightarrow T \subseteq S$.

LDEI2 Proof:

Lecture 24, slide 9.

Example:

- 1) How many ways can you spend \$1.00 buying 49¢, 53¢ stamps.
Let x be # of 49¢ stamps {need $x, y \in \mathbb{Z}$ (assume no partial stamps)}
Let y be # of 53¢ stamps $x, y \geq 0$.

$$49x + 53y = 100$$

$\gcd(53, 49) = 1$, and $1 \mid 100$, so by LDEI1, solution exists.
EEA says $(13, -12)$ is one solution.

So, one solution is $(x, y) = (1300, -1200)$ (no negatives)

$$T = \{1300 + 53n, -1200 - 49n, n \in \mathbb{Z}\}$$

$$1300 + 53n \geq 0 \quad (1)$$

$$-1200 - 49n \geq 0. \quad (2)$$

(1) means $n \geq n - 24.5$ (2) means $n \leq -24.4$. (no integer soln).
 \therefore , no solutions.

Congruence:

Let m be a fixed \mathbb{Z}^+ . If $a, b \in \mathbb{Z}$, a is congruent to b modulo m iff $m \mid (a-b)$.

$$a \equiv b \pmod{m}$$

If $m \nmid (a-b)$, then

$$a \not\equiv b \pmod{m}$$

$$7 \equiv 2 \pmod{5} \quad b/c \quad 5 \mid (7-2)$$

$$n+1 \equiv 1 \pmod{n}$$

$$n \equiv 0 \pmod{n}$$

Congruence Cont...

Oct 24, 2017

$$a \equiv b \pmod{m}$$

$$\Leftrightarrow \exists k \in \mathbb{Z}, a - b = km.$$

Congruence is an Equivalence Relation (ER):

A relation \diamond is an ER on a set S iff $\forall x, y, z \in S$:

$$1) x \diamond x \quad (\text{reflexivity})$$

$$2) x \diamond y \Rightarrow y \diamond x \quad (\text{symmetry})$$

$$3) [(x \diamond y) \wedge (y \diamond z)] \Rightarrow (x \diamond z) \quad (\text{transitivity})$$

Proof:

$$1) a \equiv a \pmod{m} \quad m \mid 0$$

$$2) a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$$

$$3) a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

$$167 \equiv 2015 \pmod{4}?$$

$$167 \equiv 3 \pmod{4} \text{ and } 2015 \equiv 3 \pmod{4}.$$

Find closest multiple of 4 below #

Properties of Congruence (PC):

Let $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m}$

$$1) a+b \equiv a'+b' \pmod{m} \quad (\text{and } -)$$

$$2) ab \equiv a'b' \pmod{m} \quad (\text{not } \div)$$

Proof 1)

$$a = a' + xm, b = b' + ym. \quad a+b = (a'+b') + (x+y)m$$

Is $5^9 + 62^{2000} - 14$ divisible by 7?

$$ab \equiv a'b' \text{ so } a^n \equiv (a')^n$$

$$5^9 + 62^{2000} - 14 \equiv (-2)^9 + (-1)^{2000} - 0 \pmod{7}$$

$$\equiv (-2)^3(-2)^6 + 1 \equiv -2^3(64) + 1 \equiv -8 + 1 \equiv -7 \pmod{7}$$

Yes

Congruence Division (CD):

Oct 25, 2017

Let $a, b, c \in \mathbb{Z}$. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1 \Rightarrow a \equiv b \pmod{m}$. Must check by dividing.

Proof:

$abc \in \mathbb{Z} \Rightarrow ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$.

$$ac - bc = km \quad (m \mid ac - bc)$$

$$c(a-b) = km \quad (m \mid c(a-b))$$

Since $\gcd(c, m) = 1$, $m \mid (a-b)$ (CAO) QED.

Congruence Iff Same Remainder (CISR):

Let $a, b \in \mathbb{Z}$. $a \equiv b \pmod{m} \iff a, b$ have same remainder \pmod{m} .

* Try: proof

Example:

1) $77^{100}(999) - 683^4 \pmod{4} = ?$

$$77 \equiv 1 \pmod{4}$$

$$999 \equiv -1 \pmod{4}$$

$$77^{100} \equiv 1 \pmod{4}$$

$$6 \equiv 2 \pmod{4}$$

$$77^{100}(999) - 683^4 \equiv 1 - 2^4 \pmod{4}$$

$$683 \equiv 2^3 \pmod{4}$$

$$\equiv -1 \equiv 3$$

$$4(2^4) \equiv 0 \pmod{4}$$

$$\therefore \text{remainder } -1 \text{ or } 3$$

2) Last digit of $5^{32} 3^{10} + 9^{22} \pmod{10}$

$$5^{32} 3^{10} + 9^{22} \equiv 5^{22} 5^{10} + (-1)^{22} \pmod{10}$$

$$\equiv 5^{32} + 1 \pmod{10} \quad \text{Last dig} = 5+1$$

$$80, 6 \dots$$

Proof of CISR:
Lecture 27 slide 5.

Oct 27, 2017

Linear Congruences:

$\alpha x \equiv c \pmod{m}$ - linear congruence in x .

Example:

1) $4x \equiv 5 \pmod{8}$

$\therefore 3\alpha \Rightarrow 8\alpha = 4x - 5 \leftarrow \text{let } y = -\alpha.$

$4x + 8y = 5$ | No soln by LDET2 (gcd + 5)

2) $5x \equiv 3 \pmod{7}$

$5x + 7y = 3 \quad 1|3, \text{ so soln exists.}$

By LDET2: $x = x_0 + 7n, n \in \mathbb{Z} \quad (x_0, y_0) = (2, -1) \leftarrow$
 $x = 2 + 7n \rightarrow \boxed{\therefore x \equiv 2 \pmod{7}}$ Need this form

3) $2x \equiv 4 \pmod{6}$

$2x + 6y = 4$

$x + 3y = 2$

By LDET2: $x = 2 + 3n, n \in \mathbb{Z} \quad \therefore x \equiv 2 \pmod{3}$

Want mod 6? $x \in \{-4, -1, 2, 5, 8, \dots\}$

$\xleftarrow{-1 \ 0 \ 2 \ 5 \ 8} \quad x \equiv 2 \pmod{3} \text{ so:}$
 $x \equiv 2, 5 \pmod{6}$

Linear Congruence Theorem 1 (LCT1):

$a, c, d, m \in \mathbb{Z}$ where $m > 0, \text{gcd}(a, m) = d$.

Solution to $\alpha x \equiv c \pmod{m}$ (if any):

$x \equiv x_0 \pmod{\frac{m}{d}}$

$1 \frac{m}{d}$ soln, d in soln.

Try: $9x \equiv 6 \pmod{15} \quad x \equiv 4 \pmod{5}$

Congruence Class Mod m:

Oct 30, 2017

$a \in \mathbb{Z}$. CCM m is: (set)

$$[a] = \{x \in \mathbb{Z}, x \equiv a \pmod{m}\}$$

Example:

$$1) [4] = \{x \in \mathbb{Z}, x \equiv 4 \pmod{7}\}$$

$$2) [2] = \{-5, 2, 9, 16, \dots\}$$

$$3) [12] = [5] + [-2] \pmod{7} \text{ because } 12 \equiv 5 \pmod{7}$$

$$4) [a] = [a + 7k], k \in \mathbb{Z}$$

↳ "Representative member" → between 0 and modulus $[0, m)$

↳ For #3, it would be 5

\mathbb{Z}_m :

Set of congruence classes:

$$\mathbb{Z}_m = \{[0], [1], [2], \dots, [m-1]\}$$

Treat as #'s and perform modular arithmetic.

Definitions:

$$1) [a] + [b] = [a+b] \text{ and -}$$

$$2) [a][b] = [ab]$$

Example: \mathbb{Z}_4 :

+	[0]	[1]	[2]	[3]	x	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[0]	[1]	[0]	[1]	[2]	[3]
[2]	[2]	[3]	[0]	[1]	[2]	[0]	[2]	[0]	[2]
[3]	[3]	[0]	[1]	[2]	[3]	[0]	[3]	[2]	[1]

0 acts like \mathbb{Z}

0 and 1 acts like \mathbb{Z} .

$$\text{Identities: } [0] + [a] = [a] + [0] = [a]$$

$$[1][a] = [a][1] = [a]$$

Inverses:

For any operation \diamond w/ identity e (ex, 0 or 1), then

a, b inverse if $a \diamond b = b \diamond a = e$

$[a]$ is additive inv of $[a]$

If $[a][b] = [b][a] = [1]$, then multi. inv is $[b] = [a]^{-1}$.

Examples:

1) $[75] - [x] = [50]$ in \mathbb{Z}_{14}

$$[75] - [50] - [x] = [0]$$

$$[25] = [x] \therefore [x] \cdot [11]$$

2) $[10][x] = [1]$ in \mathbb{Z}_{14}

$$10x \equiv 1 \pmod{14}$$

LDE: $10x + 14y = 1$ No soln since $\gcd \nmid 1$ (LDET1)

3) $[10][x] = [2]$ in \mathbb{Z}_{14}

$$10x \equiv 2 \pmod{14}$$

LDE: $10x + 14y = 2$

$$5x + 7y = 1 \text{ Soln exists. } (3, -2) = (x_0, y_0)$$

$$\therefore x = 3 + 7n, n \in \mathbb{Z}$$

$$x \equiv 3 \pmod{7} \text{ so } [x] = [3] \text{ in } \mathbb{Z}_7$$

$x \equiv 3 + 7n \pmod{14}, n \in \mathbb{Z}$. Sub values for n.

$\hookrightarrow x \equiv 3 \pmod{14}, 10 \pmod{14}$, repeat.

Equivalent Statements:

$$[a] = [b] \text{ in } \mathbb{Z}_m$$

$$a \equiv b \pmod{m}$$

Oct 31, 2017

LCT2:

$[a][x] = [c]$ in \mathbb{Z}_m has solution $\iff \gcd(a, m) | c$

If $[x] = [x_0]$ is one soln, $\{[x_0], [x_0 + \frac{2m}{d}], \dots, [x_0 + (d-1)\frac{m}{d}]\}$ in \mathbb{Z}_m

\hookrightarrow Exact same as LCT1.

Example:

1) Prove $[a]^{-1}$ exists in $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

\Rightarrow Assume $[a]^{-1}$ exists in \mathbb{Z}_m . Let $[b] = [a]^{-1}$

$$[a][b] = [1]$$

$$ab \equiv 1 \pmod{m}$$

$$ab - 1 = km, k \in \mathbb{Z}$$

$$ab - km = 1 \therefore \gcd(a, m) = 1 \text{ by GCD defn.}$$

\Leftarrow Assume $\gcd(a, m) = 1$.

$$\text{BL: } ax - my = 1$$

$$ax \equiv 1 \pmod{m}$$

$$x = [a]^{-1}. \therefore [a]^{-1} \text{ exists.}$$

2) Prove $[a]^{-1}$ is unique in \mathbb{Z}_m .

Let $[b] = [a]^{-1}$ and $[c] = [a]^{-1}$.

$$[a][b] = 1 \text{ and } [a][c] = [1]$$

$$[a][b] = [a][c] \text{ Since } [a]^{-1} \text{ exists,}$$

$$[a]^{-1}[a][b] = [a]^{-1}[a][c]. \therefore [b] = [c], \text{ QED.}$$

Fermat's Little Theorem (FLT):

Let $a, p \in \mathbb{Z}$ where p is prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$

$$[a^{p-1}] = [1] \text{ in } \mathbb{Z}_p$$

Proof:

Let $a, p \in \mathbb{Z}$ where p is prime and $p \nmid a$. $\therefore \gcd(a, p) = 1$.

If $ax \equiv b \pmod{p}$ then $ay \equiv b \pmod{p}$, then $ax \equiv ay$.

Since $\gcd = 1$, we can do: $x \equiv y \pmod{p}$.

Then $\forall [x] \text{ in } \mathbb{Z}_p$, if $[ax] = [b]$ where $0 \leq b < p$, then $[b]$ is distinct in \mathbb{Z}_p .

Let $T = \{[0], [a], \dots, [(p-1)a]\}$ Then $T = \mathbb{Z}_p$ (just multi' by a)! (order may diff)

$$\prod_{i=1}^{p-1} [ia] = \prod_{i=1}^{p-1} [a] * \text{excluded zero (product of two sets).}$$

$$[(p-1)! \cdot a^{p-1}] = [(p-1)!] (p-1)! \text{ has no } p, \text{ so } \gcd = 1.$$

$$\therefore a^{p-1} \equiv 1 \pmod{p} \text{ QED.}$$

Note: if $[a][b] = [1]$, then $[b] = [a^{p-2}]$ in \mathbb{Z}_p .

Example:

$$1) 6^6 \equiv 1 \pmod{7}$$

$$2) 4^6 \equiv 1 \pmod{7}$$

$$3) 39^6 \equiv 1 \pmod{7}$$

$$4) \text{Remainder when } 7^{92} / 11? \quad 7^{92} \equiv ? \pmod{11}$$

$$7^{10} \equiv 1 \pmod{11}. \quad (\text{FET})$$

$$7^{90} \equiv 1 \pmod{11}$$

$$7^{92} \equiv 49 \pmod{11}$$

$$\equiv 5 \pmod{11}$$

FET Corollaries:

Nov 1, 2017.

1) If p is prime, $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$

→ Proof: If $p \nmid a$, then $0 \equiv 0 \pmod{p}$.

else, $p \mid a$, then multi both sides by a .

2) If p is prime and $[a] \neq [0]$ in \mathbb{Z}_p , then $\exists [b] \in \mathbb{Z}_p \ni [a][b] = [1]$

→ Proof: Since $[a] \in \mathbb{Z}_{p-1}$ and $a < p$, so $p \nmid a$.

→ FET: $[a][a^{p-2}] = [1]$.

Example:

1) Let $a \in \mathbb{Z}$. p prime, $p \nmid a$ and $r \equiv s \pmod{p-1} \Rightarrow a^r \equiv a^s \pmod{p}$

$$r \equiv s \pmod{p-1}$$

$$r-s = k(p-1) \text{ and } a^{p-1} \equiv 1 \pmod{p} \text{ so } (a^{p-1})^k \equiv 1 \pmod{p}.$$

$$a^{r-s} \equiv 1 \pmod{p}$$

$$a^r \equiv a^s \pmod{p}$$

2) $a, r, s, k \in \mathbb{Z}$. p is prime, $r = s + kp$, then $a^r \equiv a^{s+k} \pmod{p}$

$$r = s + kp$$

$$= s + k + kp - k$$

$$= s + k + k(p-1)$$

$r \equiv s + k \pmod{p-1}$ Now, use ① to finish. *written for p a case.

3) Find add and multi inverses of [7] in \mathbb{Z}_{11} . 11 is prime.

$$\text{Add: } [-1] = [4]$$

Multi: Since 11 is prime, inverse is a^{p-2} , so $[7]^{10} = [8]$

Linear Systems of Equations:

Find all n where:

$$n \equiv 2 \pmod{3} \quad n \equiv 17 \pmod{29}$$

$$1) n = 2 + 3x, \text{ so}$$

$$2 + 3x \equiv 17 \pmod{29}$$

$$3x \equiv 15 \pmod{29} \quad \gcd(29, 3) = 1$$

$$\therefore x \equiv 5 \pmod{29}$$

$\therefore \exists y \in \mathbb{Z} \ni x = 5 + 29y$. substituting ...

$$n = 2 + 3(5 + 29y)$$

$$= 17 + 87y$$

$$\therefore n \equiv 17 \pmod{87}$$

Chinese Remainder Theorem (RT)

Let $a_1, a_2 \in \mathbb{Z}, m_1, m_2 \in \mathbb{N}$.

If $\gcd(m_1, m_2) = 1$, then \exists solution to:

$$n \equiv a_1 \pmod{m_1}$$

$$n \equiv a_2 \pmod{m_2}$$

If $n = n_0$ is one soln, then complete soln is:

$$n \equiv n_0 \pmod{m_1 m_2}$$

Generalized GCRT:

Nov 3, 2017

$$n \equiv 2 \pmod{3} \quad \equiv 3 \pmod{5} \quad \equiv 2 \pmod{7}$$

$M \subseteq \mathbb{N}$. $M = \{m_1, m_2, \dots, m_k\}$. All m_i 's are coprime.

→ For any $a_1, a_2, \dots, a_k \in \mathbb{Z}$, when:

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned} \quad \left. \begin{array}{l} \text{exists a solution} \\ \text{ } \end{array} \right.$$

If $n = n_0$ is one solution, then complete soln:

$$n \equiv n_0 \pmod{m_1 m_2 \dots m_k}$$

Example:

1) Find all x where:

$$x \equiv 5 \pmod{6}$$

$$x \equiv 2 \pmod{7}$$

$$x \equiv 3 \pmod{11}$$

CRT means 1 and 2 have soln ($\gcd(6, 7) = 1$) $x = 23$

→ Can combine to get $x \equiv 23 \pmod{42}$

$x = 23 + 42y$ for some $y \in \mathbb{Z}$. So,

$$23 + 42y \equiv 3 \pmod{11}$$

$$42y \equiv -20 \equiv 2 \pmod{11}$$

$$(-2)y \equiv 2 \pmod{11} \quad \text{CD since } \gcd(-2, 11) = 1$$

$$y \equiv -1 \pmod{11}$$

$$\equiv 10 \pmod{11}$$

$$\therefore x = 23 + 42(10 + 11z) \text{ for some } z \in \mathbb{Z}.$$

$$= 443 + 462z \quad x \equiv 443 \pmod{462}$$

2) CRT with a twist:

$$\begin{aligned} 3x &\equiv 2 \pmod{5} \\ 2x &\equiv 6 \pmod{7} \end{aligned} \quad \left. \begin{array}{l} x \text{ is not isolated} \\ \hline \end{array} \right.$$

→ Can solve each LC individually then use CRT.

→ In ①, instead of finding $[3]^{-1}$ in \mathbb{Z}_5 , keep adding 5 to 2 until you get a multiple of 3.

→ Then divide by 3. Becomes $x \equiv 4 \pmod{5}$ and $x \equiv 3 \pmod{7}$: CRT: $x \equiv 24 \pmod{35}$

3) Twist 2:

$$\begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 2 \pmod{8} \end{aligned} \quad \left. \begin{array}{l} 6 \text{ and } 8 \text{ are not coprime, can't use CRT} \\ \hline \end{array} \right.$$

$$x \equiv 4 \pmod{6} \Rightarrow x \equiv 1 \pmod{3} \text{ now, solve. } x \equiv 10 \pmod{24}$$

* Mod is $\text{lcm}(m_1, m_2)$

4) $x^2 \equiv 34 \pmod{99}$

$$99 = 11 \times 9 \text{ (prime)}$$

$$\begin{aligned} x^2 &\equiv 34 \pmod{11} \\ x^2 &\equiv 34 \pmod{9} \end{aligned} \quad \left. \begin{array}{l} \text{Now use CRT} \\ \text{lecture 31, slide 11.} \end{array} \right.$$

Soln: $x \equiv 67, 23, 76, 32 \pmod{99}$

Splitting the Modulus (SM):

If m_1, m_2 coprime, then for any $x, a \in \mathbb{Z}$:

$$\begin{aligned} x &\equiv a \pmod{m_1} \\ x &\equiv a \pmod{m_2} \end{aligned} \quad \Leftrightarrow \quad x \equiv a \pmod{m_1 m_2}$$

Example:

1) For what x is $x^5 + x^3 + 2x^2 + 1$ divisible by 6?

$$x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod{6}$$

$$\equiv 0 \pmod{2} \equiv 0 \pmod{3}$$