radlin@uwaterloo.c
MC6238

MATH 135 Introduction — Sep 8/2017

Read Chapter 1 on learn. Assignment 0

Chapter 2 Notes:

Definitions:

- Statement: T/F sentence (one or the other) - capletter
- Proposition: Statement that needs to be proven
- Theorem: Strong proposition (big) (pythag)
- Lemma: Helper proposition (small) (proven during proof)
- Corollary: Prop. follows prop (theorem) {we know theorem, so ____.} (need little proof)
- Axiom: Given truth (assumed)

Ex: Rem. Theorem
↳ Factor theorem is a corollary

Symbols:

- $\neg A$: Not A (like !A in CS)
- $A \wedge B$: A and B
- $A \vee B$: A or B
- $\equiv$: Logically equivalent (Truth table Left : Right)
- De Morgan's Laws:
  - $\neg(A \vee B) \equiv \neg A \wedge \neg B$
  - $\neg(A \wedge B) \equiv \neg A \vee \neg B$
- $A \Rightarrow B$: 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 : $A: (5=2) \vee (3<6<7)$

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

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

$(5 \neq 2) \wedge [(6 \not< 3) \vee (6 \not< 7)]$

Chapter 3 Notes:

Laws:

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

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

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

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 (RS).

Proving Implications:

- Direct Proofs: start w "Assume A is true", end w "$\therefore$ B must be true".

Lecture 2

Sept 11/2017

Example:

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

1) Discovery (can do anything)

$x^4 - 4x^2y + 4y^2 \geq 0$

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

2) Prove:

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

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

expand to get original eqn. $\square \in \mathbb{R}$

MATH 135 - Chapter 5 & 6 Sep 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)

↳ ex: even # $= 2m$, $m \in \mathbb{Z}$

Divisibility:

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

↳ n is a multiple of m

Example:

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

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

$\therefore n = 3k$ and $n^2 = 9k^2$ ← need this!

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

$\therefore n^2 = 3k$ $\quad 3 \mid n^2$ $\quad$ (Q.E.D)

Bounds by Divisibility (BBD): $\ni$: such that

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

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

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

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

can't these formats.

$$\begin{aligned} |b| &= |ka| \\ &= |k||a| \\ &\geq |a| \end{aligned}$$ (Q.E.D)

- Since $a \mid b$ and $b \neq 0$, $|a| \leq |b|$
  - ↳ Then if $|a| > |b|$, $a \nmid b$ or $b = 0$
  - → $|a| \leq |b|$ 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.I)

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

Divisibility of Integer Combinations:

Sep 15, 2017

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

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 $n \in \mathbb{Z}$.

$\therefore bx + cy$

$= kax + nay$

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

$= ma$. (Q.E.I)

move *

Sets:

Collection of unique objects (elements)

- ↳ No order
- ↳ Don't need to have anything in common
- ↳ $x \in A$
- ↳ $A = \{-2, 5, \{1, 2, 3\}, 9\}$ 4 elements } trick question
  - ↳ $1, 2, 3 \notin A$!
- ↳ $\mathbb{N}: \{1 \ldots \infty\}$ Natural #s
- ↳ $\mathbb{W}: \{0 \ldots \infty\}$ whole #s $\{0\} \cup \mathbb{N}$
- ↳ $\mathbb{Z} = \{\pm x : x \in \mathbb{W}\}$
- ↳ $\mathbb{Q}$
- ↳ $\{\}$: Null set ~~$\emptyset$~~ Empty Set
- ↳ $\mathbb{Q}: \{\frac{a}{b}, b \neq 0 : a, b \in \mathbb{Z}\}$ Rationals

Cardinality:

- # of elements.
  - $S = \{1, 2, 3, 4\}$ $\quad |S| = 4$

The Universe of Discourse:

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

↳ Eggs? $\mathbb{N}$
↳ Time? $\mathbb{R}$
↳ Divisibility? $\mathbb{Z}$

} Variable type, kinda.

Set Builder Notation:

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

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

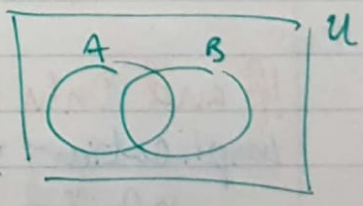
Example:

1) $\{x \in \mathbb{Z} : (3 \mid x)\} = \{x \in \mathbb{Z} : (11 \mid x) \wedge (3 \mid x)\}$
2) $\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 144\}$
   ↳ Set of all points 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:

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

Complement:

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

Cartesian Product:

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

Sep 18, 2017

Subsets:

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

↳ B is superset of A

↳ "Proper subset" when elements in B not in A

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

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

Example:

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

i) discover:

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

$n = 4a+3$

$n = 4a+2+1$

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

$= 2k+1$.

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

∴ $A \subseteq B$, 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 $A \Rightarrow B$

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

If and Only If:

Implication & Converse are true.

↳ A iff B = $A \Longleftrightarrow B$

and ↓ A if B: $B \Rightarrow A$

A only if B: $A \Rightarrow B$

if AND only if

A	B	A⇔B
T	T	T
T	F	F
F	T	F
F	F	T

Proving iffs:

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

$\frac{A}{x=y}$ $\quad$ $\frac{B}{\frac{x+y}{2} = \sqrt{xy}}$

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

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

$= \sqrt{xy}$

NEED THIS ✶

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

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

CAN square both sides → $(x+y)^2 = 4xy$

$(x-y)^2 = 0$

$x = y$.

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

Set Equality:

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

Example:

Nah.

Quantifiers:

Sep 19, 2017

"Some", "Many", "All"

↳ How many elements in domain satisfy property.

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

Universal Quantifier:

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

↳ Can talk about null set and be true.

Existential Quantifier:

$\exists$ · At least one is true → $\exists x \in S \ni P(x)$ ("such that") "there exists"

↳ Guarantees that there are elements in S

Quantifier – Variable – Domain (set) – Open sentence

Proving Quantified Statements:

Select Method:

Universal

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 $x \in \mathbb{R}$.

$$x^2+3x+5 > x^2+3x+\frac{9}{4}$$
$$= (x+\tfrac{3}{2})^2$$
$$\geq 0$$

original exp. is >, so ≥0 means >0.

$\therefore x^2+3x+5 > 0$ for all $x \in \mathbb{R}$

Construct Method:

Existential

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 $x^2+3x = \left(\frac{-3+\sqrt{29}}{2}\right)^2 + 3\left(\frac{-3+\sqrt{29}}{2}\right)$

$= 5$ Q.E.D.

Quantifiers in the Hypothesis:

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

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

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

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

Then when $x=1$, $a \mid (b+c)$. Q.E.D.

This is valid for ∀!!!!

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 $\in \mathbb{Z}$.

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. $\sqrt{\ }$"

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

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

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

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 $y^3 = x^3 - 1$.

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

$= 1$. $\quad Q \in \mathbb{R}$

Language Practice

Sep 22, 2017

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

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

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

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

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

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

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

↳ There is no largest integer.

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

↳ No prime numbers are perfect □.

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 $14 \nmid n \equiv 14 \mid n \Rightarrow 7 \mid n$

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

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 $A \wedge \neg B$ 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)

$b\sqrt{2} = a$

$2b^2 = a^2$ a^2 is even. $\therefore$ a is even.

So $a = 2k$ and $2b^2 = 4k^2$

$b^2 = 2k^2$ Absurd.

$\therefore$ b is even.

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

Assume $a, b \in \mathbb{Z}$, $a \geq 2$ (A) and (∧) $a \mid b$ and $a \mid b+1$ ($\neg B$).

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

$a(m-k) = 1$

$\therefore a \mid 1$

$\therefore a = \pm 1$ but $a \geq 2$

$\neg B$ led us here. A

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

↳ 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 $y_1, y_2 \in \mathbb{R}$, $y_1 \neq y_2$

(1) $(x+1)^2 - x^2 = 2y_1 - 1$ and $(x+1)^2 - x^2 = 2y_2 - 1$ (2)

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

$y_1 = y_2$ but $y_1 \neq y_2$, absurd.

$\therefore$ Unique y. Q.E.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

$a = qb + r \quad 0 \leq r < b$.

(dividend: a; divisor: b)

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

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

$a = q_1 b + r_1 \quad a = q_2 b + r_2 \quad 0 \leq r_1, r_2 < b$

$q_1 b + r_1 = q_2 b + r_2$

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

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

$\therefore r_1 - r_2 > 0$ and $r_1 - r_2 < r_1$

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

but $b > r_1$. $\quad$ QED.

Injective Functions:

$f: S \to T$ is one to one iff $\forall x_1 \in S \; x_2 \in S, (f(x_1) = f(x_2)) \Rightarrow x_1 = x_2$

↳ unique x for every $f(x)$.

Example:

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

Surjective Functions: "onto"

$f: S \to T$ iff $\forall y \in T, \exists x \in S \mid f(x) = y$.

↳ Codomain accessible through f.

Example:

1) $f: \mathbb{R} \to (-\infty, 1) \quad f(x) = 1 - e^{-x}$, 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) $\sum_{i=1}^{5} 3i^2 = 3(1)^2 + 3(2)^2 + 3(3)^2 + 3(4)^2 + 3(5)^2$

Π is same but $\times$.

↳ 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 w 0

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

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

POMI:

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 ↑. WITHOUT $\forall n \in \mathbb{N}$ (MISTAKE!) !

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

$$\sum_{i=1}^{1} i(i+1) = i(i+1) = 1 \times 2$$

$$= \frac{1 \times (1+1) \times (1+2)}{3} \quad \therefore P(1) \text{ is true.}$$

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 $P(k) \Rightarrow P(k+1)$

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

GOAL → $= \frac{(k+1)(k+2)(k+3)}{3}$

Well, $\sum_{i=1}^{k+1} i(i+1) = \sum_{i=1}^{k} i(i+1) + (k+1)[(k+1)+1]$

$= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2)$ (by ind. hyp.) * need ↑

$= \frac{(k+1)(k+2)(k+3)}{3}$ as desired. QED.

∴ by POMI, ~~~ $\forall n \in \mathbb{N}$ Q ∈ D.

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.

$4! = 24$. $\}$ $24 > 16$. ∴ $P(4)$ is true.

$2^4 = 16$.

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

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

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

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

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

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

$> (k+1)\,2^k$ (by IH)

$\geq 5 \cdot 2^k$ since $k \geq 4$

$> 2 \cdot 2^k$

$> 2^{k+1}$

Sep 29, 2017

Point Practice:

$6 \mid 2n^3 + 3n^2 + n$ $\quad 2n^3+3n^2+n = 6k \quad n \in \mathbb{N}$ ← If $n \in \mathbb{Z}$, you need to show P(k+1) and P(k-1)

Base case: Let $n = 1$

$6 = 6k \quad k = 1$

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

$\therefore \exists k \in \mathbb{Z} \mid 2x^3 + 3x^2 + x = 6k$ for some k

IC: Prove $P(x+1)$

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

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

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

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

$= 2x^3 + 6x^2 + 6x + 2 + 3x^2 + 7x + 4$

$= (2x^3 + 3x^2 + x) + 6x^2 + 5x + 7x + 6$

$= 6k + 6x^2 + 12x + 6$

$= 6(k + x^2 + 2x + 1) = 6p \quad \therefore 6 \mid P(x+1)$

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 tries for another

Let $P(n)$ be "$x_{n_1} = 2(-3)^n + 10(5)^{n-1}$" where x_m is ...

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

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

$2(-3)^1 + 10(5)^0 = 4 = x_1 \quad \therefore P(1)$ is true.

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

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

$x_k = 2(-3)^k + 10(5)^{k-1}$

and $x_{k-1} = 2(-3)^{k-1} + 10(5)^{k-2}$ $\Big\}$ $k \in \mathbb{N} \geq 3$.

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

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

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

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

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

$= 4(-3)^k + 4(5)^k - 10(-3)^k + 6(5)^k$

$= -6(-3)^k + 10(5)^k$

$= 2(-3^{k+1}) + 10(5^k)$ ·QED.

↑example where b=2.

Principle of Strong Induction:

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

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

2) $P(1), P(2) \ldots P(k) \Rightarrow P(k+1)$ 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.

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

$(x_k < 4^k) \wedge (x_{k-1} < 4^{k-1})$

$x_{k+1} = 3x_k + 2x_{k-1}$ (hopefully $< 4^{k+1}$)

$< 3(4^k) + 2(4^{k-1})$

$< 3(4^k) + 4(4^{k-1})$

$= 3(4^k) + 4^k$

$= 4^{k+1}$

Fibonacci Sequence

Oct 2, 2017

$f_1 = 1, f_2 = 1$ $\quad f_n = f_{n-1} + f_{n-2}$ for $n \geq 5$

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

Fibonacci Proofs:

1) $\sum_{r=1}^{n} f_r^2 = f_n f_{n+1} \quad \forall n \in \mathbb{N}$. 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: $\sum_{r=1}^{k+1} f_r^2 = f_{k+1} f_{k+2}$

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

$$= f_k f_{k+1} + f_{k+1}^2 \quad \text{(IH)}$$

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

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

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

Base case: $f_1 = 1 < \left(\frac{7}{4}\right)^1$ ✓ $\quad f_2 = 1 < \left(\frac{7}{4}\right)^2$ ✓

shows base case → Inductive Hypothesis: ~~$\left(f_k < \left(\frac{7}{4}\right)^k\right) \wedge \left(f_{k-1} < \left(\frac{7}{4}\right)^{k-1}\right)$~~

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

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

Now show k+1!

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

$$f_{k+1} = f_k + f_{k-1} \quad \text{(IH)}$$

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

$$= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4} + 1\right)$$

$$< \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2$$

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

Discovering Truths: Oct 3, 2017

Closed Form:

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

$= \left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{4^2}\right)$

$= \left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\left(1-\frac{1}{16}\right)$

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

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

$= \frac{(r^2-1)((r+1)^2-1)((r+2)^2-1)\cdots(n^2-1)}{(r^2)(r+1)^2(r+2)^2\cdots(n^2)}$

n	$\prod$
2	$\frac{3}{4}$
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: $n=2$ $\prod_{r=2}^{2}\left(1-\frac{1}{r^2}\right)=\frac{3}{4}=\frac{2+1}{2(2)}$ ✓

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

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

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

IH

$= \left(\frac{k+1}{2k}\right)\left(\frac{(k+1)^2-1}{(k+1)^2}\right)$ ← could cancel $(k+1)$ 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
(P(n)) ↑

Strong Induction:

BC: $n = 2$. 2 is prime ✓

IH: Assume $P(2) \wedge P(3) \wedge P(4) \wedge \ldots \wedge P(k)$ ← not this

do this! → 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, uh... yeah.

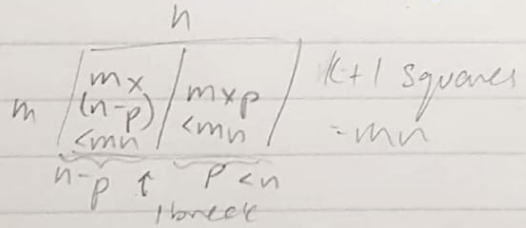
If composite, $\exists m, n \in \mathbb{N}$, $k+1 = mn$, $m, n < k+1$

→ Then $P(m)$, $P(n)$ true by IH. So $k+1$ can be written as product of primes ($Q \in \mathbb{Z}$).

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. $t \in \mathbb{N}$.



$k+1$ squares
$= mn$

each smaller rectangle falls under IH of $P(1) \ldots P(k)$.

Greatest common Divisor:

Oct 6, 2017

Let $a, b \in \mathbb{Z}$. The gcd is an integer d where

- $d \mid a$ and $d \mid b$, and
- if $c \mid a$ and $c \mid b$, then $c \leq d$.

(d is greater than any other divisor.)

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:

$$\gcd(a,b) = |a+b| = \max\{|a|, |b|\}$$

③ If $a \neq 0$, $b \neq 0$ then $1 \mid a$ and $1 \mid b$, $\therefore$ There is a divisor.

for any $c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$ then

BBD: $c \leq \min\{|a|, |b|\}$

$\therefore 1 \leq |c| \leq \min\{|a|, |b|\}$ ← c is bounded

$\therefore \gcd(a,b)$ exists

Prove 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 $n \in \mathbb{N}$.

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

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

S3VBNY

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 $d|3ab$ and $d|a$.

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

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

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

$b = (k-3m)d$

$\therefore d|b$.

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

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

Oct 12, 2017

Remainders:

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

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

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

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

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

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

Euclidean Algorithm:

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

$\therefore \gcd(1239, 735) = \gcd(735, 504)$ by GCDWR

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

Example:

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

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

By GCDWR, $\gcd(\underbrace{3a+b}_{x}, a) = \gcd(a,b)$ (from euclidean algo)

Checking GCDs:

$21 = 231 - 5(42)$ ← sub in previous lines.

$= 231 - 5[504 - 2(231)]$

$= 11(231) - 5(504)$

⋮

Just going backwards

$= 27(735) - 16(1239)$ ← linear combination ← "certificate of correctness"

Original: $1239 = 735 + 504$

$735 = 504 + 231$

$504 = 2(231) + 42$

$231 = 5(42) + 21$

$42 = 2(21) + 0$

Why does this work?

→ Suppose $c > 0$, $c \mid 735$, $c \mid 1239$

→ Then, by DIC, $c \mid 21$ → 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 $\exists\, x,y \in \mathbb{Z}$ ∋

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

$6 > 0$, $6 \mid 30$ and $6 \mid 42$. $30(3) + 42(-2) = 6$. $\therefore 6 = \gcd(30,42)$

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

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

By BBD, $|c| \leq d$. All divisors $\leq d$. $Q.E.D.$

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 $\gcd(n,n+1)=1$

$(-1)n+(1)(n+1)=1$ } GCD CT since $1|n$ and $1|(n+1)$

linear combination

3) Prove or disprove:

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

$\Rightarrow$ $kdx^2 + mdy^2 = c$

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

$d \mid c$.

$\Leftarrow$ $a=1$ $b=3$ $c=2$, so not true.

$\gcd(1,3) = 1$. $1 \mid 2$.

But, $1x^2 + 3y^2 = 2$

$x^2 + 3y^2 = 2$ never, since $x^2, y^2 \geq 0$

Tryxi's Lemma (TL): Oct 16, 2017

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

Moose's Lemma (ML):

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

Proof:

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

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

$kbe + cd = e$

$cd = (1-kb)e$

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

Extended Euclid Algorithm (EEA):

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

	x	y	r	q
1)	1	0	a	b0
2)	0	1	b	0
⋮	⋮	⋮	⋮	⋮

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 corr 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 $\gcd(ab, c) = 1$.

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

Since $bx \in \mathbb{Z}$, $\gcd(a, c) = 1$. } GCD CT $(1 \mid a) \wedge (1 \mid c) \therefore$ QED $\gcd(a, c) = 1$.

Since $ax \in \mathbb{Z}$, $\gcd(b, c) = 1$. same for (b, c)

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

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

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

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

$ab(x_1x_2) + c(ax_1y_2 + bx_2y_1 + cy_1y_2) = 1$ QED

$(1 \mid ab) \wedge (1 \mid c)$, so $\gcd(ab, c) = 1$ (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 $ax+by=1$. $1 \mid a \wedge 1 \mid b$, $\therefore$ GCD $(a,b)=1$ by GCD CT, QED.

Division by the GCD (DB GCD)

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

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

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

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

$\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$ 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:

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

↳ GCD 00, and: $acx+bcy=c$

$acx+may=c$

$a(cx+my)=c \quad \because cx+my \in \mathbb{Z}, \ a \mid c$ 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 $M=\{m_1, \ldots m_n\}$

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

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 $p \mid b$. QED.

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)

→ $p_1 \mid n$, so $p_1 \mid q_1 q_2 \cdots q_l$

→ By EL, p_1 must divide one of them, and $p_1 = q_1$

→ 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

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

is the unique PF of n into powers of distinct primes $p_1, p_2 \cdots p_k$ where $a_1, a_2 \cdots a_k \geq 1$, 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 $0 \leq d_i \leq a_i$ for $i = 1, 2, 3 \ldots k$

→ d is subset (can have 0 exponent)

Example:

12 $63 = 3^2 7^1$:

$3^0 7^0 = 1$	$3^1 7^0 = 3$	$3^2 7^0 = 9$
$3^0 7^1 = 7$	$3^1 7^1 = 21$	$3^2 7^1 = 63$

2) How many multiples of 12 are divisors of 2940? → 12

$12 : 2^2 3^1$

$2940 : 2^2 3^1 5^1 7^2$

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 $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ be PFs of a, b (exp can be 0).

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

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

Example:

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

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

Linear Diophantine Equations:

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

- → All vars deg 1? LDE.
- → Simplest is $ax = b$ ($\Rightarrow a | b$)
- → $ax + by = c$
  - → Solution exists? $LDET_1$
  - → Can we find? EEA
  - → Can find more? $LDET_2$

Example:

1) $143x + 253y = 11$
   - → $11 \nmid 143 \wedge 11 | 253$. $\therefore 11 = \gcd(253, 143)$

2) $143x + 253y = 154$
   - → $11 | 154$ ... $(x,y) \rightarrow (14x, 14y)$ 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 $d \mid a$, $d \mid b$.

$d(k_1 x_1 + k_2 y_1) = c \quad \therefore d \mid c$

$\Leftarrow$ Let $d \mid c$. $\therefore c = kd$

$ax_0 + by_0 = d$

$kax_0 + bky_0 = c$

$\therefore$ solution is (kx_0, ky_0) QED.

LDET2: Oct 23, 2017

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

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

$$\left.\begin{aligned} x &= x_0 + \frac{b}{d}n \\ y &= y_0 - \frac{a}{d}n \end{aligned}\right\} \forall n \in \mathbb{Z}$$

$\leftarrow d$ to take lowest slope form.

Example:

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

$4x + 7y = 1$

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

$$\therefore \left.\begin{aligned} x &= 2 + \frac{7}{1}n \\ y &= -1 - \frac{4}{1}n \end{aligned}\right\} \forall n \in \mathbb{Z}$$ by $LDET_2$ $\left\{\begin{array}{l}\infty \text{ correct answers.} \\ \text{Can do } -5, 3.\end{array}\right.$

↳ Can sub back in to check

LDET2 w/ Sets:

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

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

If $S \neq \emptyset$ By 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: $z \in S \Leftrightarrow z \in T$. $S = T$.

LDET2 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
Let y be # of 53¢ stamps
} need $x, y \in \mathbb{Z}$ (assume no partial stamps) $x, y \geq 0$.

$$49x + 53y = 100$$

$\gcd(53, 49) = 1$, and $1 \mid 100$, so by LDET1, 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 $n \geq \sim -24.5$ (2) means $n \leq \sim -24.4$. (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

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

$7 \equiv 2 \pmod{5}$ b/c $5 \mid (7-2)$
$n+1 \equiv 1 \pmod{n}$
$n \equiv 0 \pmod{n}$

Congruence Cont...

Oct 24, 2017

$a \equiv b \pmod m$

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

Congruence is an Equivalence Relation (CER):

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

1) $x \diamond x$ (reflexivity)
2) $x \diamond y \Rightarrow y \diamond x$ (symmetry)
3) $[(x \diamond y) \wedge (y \diamond z)] \Rightarrow (x \diamond z)$ (transitivity)

Proof:

1) $a \equiv a \pmod m$ $\quad m \mid 0$
2) $a \equiv b \pmod m \implies b \equiv a \pmod m$
3) $a \equiv b \pmod m \wedge b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

$167 \equiv 2015 \pmod 4$?

$167 \equiv 3 \pmod 4$ 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) $a + b \equiv a' + b' \pmod m$ (and -)
2) $ab \equiv a'b' \pmod m$ (not ÷)

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?

$ab \equiv a'b'$, 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 b4 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 $\gcd(c,m) = 1$, $m \mid (a-b)$ (CAD) Qed.

Congruence iff Same Remainder (CISR):

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

*Try: proof

Example:

1) $77^{100}(999) - 6^{83} \bmod 4 = ?$

$77 \equiv 1 \pmod 4$ $\quad 999 \equiv -1 \pmod 4$

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

$6 \equiv 2 \pmod 4$ $\quad 77^{100}(999) - 6^{83} \equiv -1 - 2^{83} \pmod 4$

$6^{83} \equiv 2^{83} \pmod 4$ $\quad \equiv -1 \equiv 3$

$4(2^{81}) \equiv 0 \pmod 4$ $\quad \therefore$ remainder -1 (or 3)

2) Last Digit of $5^{32}3^{10} + 9^{22}$? $\bmod 10$

$5^{32}3^{10} + 9^{22} \equiv 5^{22}15^{10} + (-1)^{22} \pmod{10}$

$\equiv 5^{32} + 1 \pmod{10}$ Last dig: 5+1

So, 6.

Proof of CISR: Oct 27, 2017

Lecture 27 slide 5.

Linear Congruences:

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

Example:

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

$\therefore \exists \alpha \Rightarrow 8\alpha = 4x - 5$ ← let $y = -\alpha$.

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

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

$5x + 7y = 3$ $1 \mid 3$, so soln exists.

By LDET2: $x = x_0 + 7n, n \in \mathbb{Z}$. $(x_0, y_0) = (2, -1)$

$x = 2 + 7n \rightarrow$ | $\therefore x \equiv 2 \pmod{7}$ | Need this form

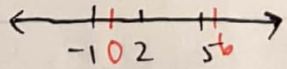
3) $2x \equiv 4 \pmod{6}$

$2x + 6y = 4$

$x + 3y = 2$

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

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



$x \equiv 2 \pmod{3}$ so:

$x \equiv 2, 5 \pmod{6}$

Linear Congruence Theorem 1 (LCT1):

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

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

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

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

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

Oct 30, 2017

Congruence Class Mod m:

$a \in \mathbb{Z}$. 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) $[2] = \{\ldots -5, 2, 9, 16 \ldots\}$
3) $[12] = [5] = [-2] \pmod 7$ b/c $12 \equiv 5 \bmod 7$
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:

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

Treat as #s and perform modular arithmetic.

Definitions:

1) $[a] + [b] = [a+b]$ and −
2) $[a][b] = [ab]$

Example: $\mathbb{Z}_4$:

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

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

0 acts like $\mathbb{Z}$ — 0 and 1 acts like $\mathbb{Z}$.

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 $\mathbb{Z}_{14}$

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

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

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

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

LDE: $10x + 14y = 1$ No soln since gcd $\nmid$ 1 (LOET2)

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

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

LDE: $10x + 14y = 2$

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

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

$x \equiv 3 \pmod 7$ so $[x] = [3]$ 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:

Oct 31, 2017

$[a] = [b]$ in $\mathbb{Z}_m$ ↗

$a \equiv b \pmod m$ ↘

LCT2:

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

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

$\hookrightarrow$ Exact same as LCT1.

Example:

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

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

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

$ab \equiv 1 \pmod m$

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

$ab-km=1$ $\therefore \gcd(a,m)=1$ by GCD00.

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

BL: $ax-my=1$

$ax \equiv 1 \bmod m$

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

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

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

$[a][b]=1$ and $[a][c]=[1]$

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

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

Fermat's Little Theorem (FLT):

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

$[a^{p-1}]=[1]$ 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 $\forall [x]$ in $\mathbb{Z}_p$, if $[ax]=[b]$ where $0\le b<p$, then $[b]$ is distinct in $\mathbb{Z}_p$.

Let $T=\{[0],[a],\ldots,[(p-1)a]\}$ Then $T=\mathbb{Z}_p$ (just multi by a)! (order may diff)

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

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

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

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

Examples:

1) $6^6 \equiv 1 \bmod 7$
2) $4^6 \equiv 1 \bmod 7$.
3) $39^6 \equiv 1 \bmod 7$.
4) Remainder when $7^{92}/11$? $7^{92} \equiv ? \bmod 11$

$7^{10} \equiv 1 \bmod 11$. (FLT)

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

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

$\equiv 5 \bmod 11$

FLT Corollaries: Nov 1, 2017.

1) If p is prime, $a \in \mathbb{Z}$, $a^p \equiv a \pmod p$
   - Proof: If $p \mid a$, then $0 \equiv 0 \pmod p$.
     else $p \nmid a$, 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 $[a] \in \mathbb{Z}_p$, $a < p$, so $p \nmid a$.
     - FLT: $[a][a^{p-2}] = [1]$.

Example:

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

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

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

$a^{r-s} = (a^{p-1})^k$

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

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

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.

Add: $[-7] = [4]$.

Multi: Since 11 is prime, inverse is a^{p-2}, so $[7]^9 = [8]$

Linear Systems of Equations:

Find all n where:

$n \equiv 2 \bmod 3 \quad n \equiv 17 \bmod 29$.

1) $n = 2 + 3x$, so

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

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

$x \equiv 5 \pmod{29}$

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

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

$= 17 + 87y$.

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

Chinese Remainder Theorem (CRT):

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

If $\gcd(m_1, m_2) = 1$, then exists a 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's are coprime.

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

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

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,

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

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

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

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

$\equiv 10 \pmod{11}$

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

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

2) CRT with a twist:

$3x \equiv 2 \pmod 5$
$2x \equiv 6 \pmod 7$ } x is not isolated

→ 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:

$x \equiv 4 \pmod 6$
$x \equiv 2 \pmod 8$ } 6 and 8 are not coprime, can't use CRT

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

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

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

$99 = 11 \times 9$ (co-primes)

$x^2 \equiv 34 \pmod{11}$
$x^2 \equiv 34 \pmod 9$ } Now use CRT. Lecture 31, slide 11.

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

Splitting the Modulus (SM):

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

$x \equiv a \pmod{m_1}$
$x \equiv a \pmod{m_2}$ } $\Leftrightarrow$ $x \equiv a \pmod{m_1 m_2}$

Example:

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

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

$\equiv 0 \pmod 2 \equiv 0 \pmod 3$

RSA Cryptography:

Nov 8, 2017

1) 2 distinct primes — 2, 11 — larger = more secure
2) $n = pq$ — 22
3) $\phi(n) = (p-1)(q-1)$ — 10
4) $1 < e \leq \phi(n)$ and $\gcd(e, \phi(n)) = 1$ — $e = 3$
5) Find d: $ed \equiv 1 \pmod{\phi(n)}$, $0 < d \leq \phi(n)$ — $d = 7$
6) Publish public key (e, n) — $(3, 22)$
7) Secure private key (d, n) — $(7, 22)$

Example:

1) $p = 5$ $q = 19$ $e = 13$. $n, \phi(n), d$?

$n = pq = 95$

$\phi(n) = (4)(18) = 72$

$ed \equiv 1 \mod 72$

$13d \equiv 1 \mod 72$

$13d + 72y = 1$

$d \equiv 61 \mod 72$

Public $(13, 95)$

Private $(61, 95)$

Encrypting Messages:

1) Message M $0 \leq M < n$ — $M = 8$
2) $M^e \equiv C \pmod{n}$ $0 \leq C < n$ — $8^3 \equiv 6 \mod 22$
3) Send C as message

Example:

1) Encrypt $M = 5$, $e = 13$ $n = 95$.

$5^{13} \equiv C \mod 95$

$(5^3)^4 5 \equiv C \mod 95$

$(30)^4 5 \equiv C \mod 95$

$(900)^2 5 \equiv C \mod 95$

$(-50)^2 5 \equiv C \equiv 45^2 \cdot 5 \equiv 55 \mod 95$

Decryption:

1) Recieve C
2) $C^d \equiv R \pmod{n}$ $0 \leq R < n$
3) Read R

$C = 6$

$6^7 \equiv 8 \pmod{22}$

Example:

1) $d = 61$ $n = 22$ $C = 55$

$55^{61} \equiv R \pmod{55}$

$R = 5.$

RSA Theorem:

* Let:

p, q prime, $p \neq q$

$n = pq$

$e, d \in \mathbb{Z}$ where $ed \equiv 1 \pmod{(p-1)(q-1)}$ $\phi(n) = (p-1)(q-1)$

** If:

$0 \leq M < n$ and $0 \leq R < n$ where:

$M^e \equiv C \pmod{n}$ and $C^d \equiv R \pmod{n}$

Then $R = M$.

Proof:

Let * above. Assume ** above.

$R \equiv (M^e)^d \bmod n$

$ed = 1 + K\phi(n)$, so $R \equiv M^{1+k\phi(n)} \bmod n$

Complex Numbers: Nov 10, 2017

$3x^2 - 7 = 41$

$x^2 = 16$

$(x^2 = 16) \wedge (x \in \mathbb{R}) \iff (x = \sqrt{16}) \vee (x = -\sqrt{16})$

$x^2 = -1 \rightarrow$ No real solutions. Imagine uni. of discourse where exists.

$i^2 = -1$, so ~~$i = \sqrt{-1}$~~

↳ because $\sqrt{-1}$ doesn't work on $\mathbb{R}$.

i:

- $i^2 = -1$, but $i \neq \sqrt{-1}$
- $|i| = 1$ and $|3i| = 3$
- The Imaginary Number set:
  $\mathbb{I} = \{ai : a \in \mathbb{R}, i^2 = -1\}$ * $\mathbb{I} \cap \mathbb{R} = \{0\}$ (one # in both sets)
- $ai + bi = (a+b)i$ and $ai + (-a)i = 0$.
  ↳ $(3i)(2i) = 6i^2 = -6$.

Example:

1) $x^2 - 6x + 10 = 0$

$(x-3)^2 = -1$

$x - 3 = i$ or $x - 3 = -i$. *can't add both sides, because not defined in $\mathbb{I}$..

Complex Numbers: Nov 13, 2017

- $\mathbb{C} = \{a + bi, a, b \in \mathbb{R}, i^2 = -1\}$
  → $z = x + yi$ in std form if $x, y \in \mathbb{R}$ (real + im. parts x, yi)
  → $\mathbb{C} \supsetneq \mathbb{R}$ and $\mathbb{I}$ and $\mathbb{C} \neq \mathbb{R} \cup \mathbb{I}$

Properties of Complex Numbers:

$|z| = \sqrt{a^2+b^2}$

$(a+bi)+(c+di) = (a+c)+(b+d)i$

→ $0 = 0+0i$ → additive identity

$(a+bi)(c+di) = (ac-bd)+(ad+bc)i$

→ $1 = 1+0i$ → multi identity

Complex Conjugates + Inverses:

Conj of z is $\bar{z} = a-bi$. (PCJ)

- $\overline{z+w} = \bar{z} + \bar{w}$
- $\overline{zw} = \bar{z}\bar{w}$
- $\bar{\bar{z}} = z$
- $z+\bar{z} = 2(\mathrm{Re}(z))$
- $z-\bar{z} = 2i(\mathrm{Im}(z))$
- $(z)(\bar{z}) = |z|^2$
  - → if $z \neq 0$, $|z|^2 \neq 0$
  - → So, $z\bar{z}/|z|^2 = 1$ (multiplicitave inverse)
  - → Inverse of z (multi) is $\bar{z}/|z|^2$
  - → To do $x, y \in \mathbb{C}$, $x \div y$, you need xy^{-1}

Exponents:

$z^0 = 1$

$z^{k+1} = z^k z$, $k \in \mathbb{N}$

Example:

1) Real soln to $6z^3+(1+3\sqrt{2}i)z^2-(11-2\sqrt{2}i)z-6 = 0$

If $z \in \mathbb{R}$, $z = x+0i$. $6x^3+(1+3\sqrt{2}i)x^2-(11-2\sqrt{2}i)x-6 = 0+0i$

$(6x^3+x^2-11x-6)+(3\sqrt{2}x^2+2\sqrt{2}x)i = 0+0i$

$6x^3+x^2-11x-6 = 0$ and $3\sqrt{2}x^2+2\sqrt{2}x = 0$

$x = -\frac{2}{3}$

Powers of i:

0	1
1	i
2	-1
3	$-i$
4	1
⋮	⋮

Repeats

If power $\equiv 0 \mod 4$ $i^{\text{power}} = 1$
$\equiv 1 \mod 4$ $i^{\text{power}} = i$
$\equiv 2 \mod 4$ $i^{\text{power}} = -1$
$\equiv 3 \mod 4$ $i^{\text{power}} = -i$

(Goes backwards too)

Negative Integer Exponents

Nov 14, 2017

Multiplicative inverse of i is $-i$.

$\rightarrow i^4 = 1$, and $i^3 = -i = i^{-1}$

Converting:

$$i^{-x} \ (x > 0, x \in \mathbb{Z}) = (i^{-1})^x$$
$$= (-i)^x$$
$$= (-1)^x (i)^x$$

Rational Exponents

$z_1 = a_1 + b_1 i \quad z_2 = a_2 + b_2 i \quad * z_1 = z_2 \Leftrightarrow a_1 = a_2 \wedge b_1 = b_2$

Let $i^{\frac{1}{2}} = a + bi$.

$$(i^{\frac{1}{2}})^2 = (a+bi)^2$$
$$0 + 1i = a^2 - b^2 + 2abi$$

$* a^2 - b^2 = 0$ and $2ab = 1$.

$$i^{\frac{1}{2}} = \pm\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i\right)$$

If $z = a + bi$, $z^{\frac{1}{2}} =$

$$z^{\frac{1}{2}} = \pm\left(\sqrt{\frac{|z|+a}{2}} + i\frac{b}{|b|}\sqrt{\frac{|z|-a}{2}}\right)$$

Example:

1) $z^2 = i\bar{z}$ let $z = x+yi$ and $\bar{z} = x-yi$

$(x+yi)^2 = i(x-yi)$

$x^2 - y^2 + 2xyi = xi + y$

$x^2 - y^2 - y + (2xy - x)i = 0 + 0i$ 2 eqn 2 unknowns

$z = \{0, -i, \frac{\sqrt{3}}{2} + \frac{1}{2}i, -\frac{\sqrt{3}}{2} + \frac{1}{2}i\}$

Properties of Modulus (PM):

1) $|z| = 0 \iff z = 0$
2) $|\bar{z}| = |z|$
3) $z\bar{z} = |z|^2$
4) $|zw| = |z||w|$
5) $|z+w| \leq |z| + |w|$ (Δ ineq.)

Example:

1) $\frac{z}{1+z^2} \in \mathbb{R} \iff z \in \mathbb{R}$ or $|z| = 1$ and $z \neq \pm i$

$\Rightarrow$ Assume $\frac{z}{1+z^2} \in \mathbb{R}$. let $z = x+yi$, $x, y \in \mathbb{R}$.

$\frac{x+yi}{1+(x+yi)^2} = a + 0i$, $a \in \mathbb{R}$.

possible $\bar{w}$ complex num's →

if $1 + z^2 \neq 0$, $x+yi = a(1+(x+yi)^2)$

if $1 + z^2 = 0$ $\frac{z}{1+z^2} \notin \mathbb{R}$

$x+yi = a + ax^2 - ay^2 + 2axyi$

1) $x = a + ax^2 - ay^2$
2) $y = 2axy$

let $x_1 = \frac{x}{a}$, $y_1 = \frac{y}{a}$ ~~(if $a=0$, $x=y=0$ $\therefore z = 0 \in \mathbb{R}$)~~ Doesn't help...

Assume $y \neq 0$.

Complex Numbers and Geometry:

Nov 15, 2017

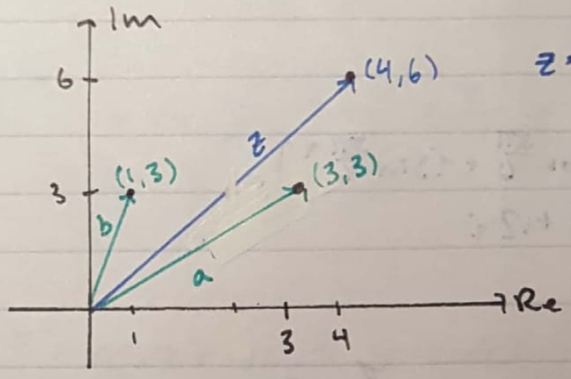
$z = x + yi$

→ can say $z = (x, y)$

→ Horizontal: $\mathbb{R}$ Vertical: $\mathbb{I}$

→ $\bar{z}$ is refl of z in $\mathbb{R}$ axis.

→ $|z|$ is distance from origin.



$z = 4 + 6i$

Polar Coordinates:

Can be represented as θ and radius.

→ θ wouldn't be unique. "an argument" for z.

→ (r, θ) is unique z. $r = |z|$

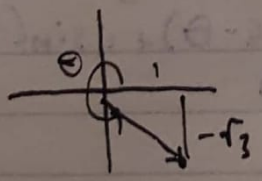
→ $x = r\cos\theta$, $y = r\sin\theta$.

Polar Form:

$z = r(\cos\theta + i\sin\theta)$

Examples:

1) $z_1 = 1 - \sqrt{3}i$ $\tan^{-1}\left(\frac{\sqrt{3}}{1}\right) = \frac{\pi}{3}$.



$\theta = \frac{5\pi}{3}$. $r = 2$. $\Big\} z_1 = 2\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right)$

Notes about Polar Forms:

→ θ not unique. (Chose $[0, 2\pi)$)

Polar Multiplication:

$z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ and $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$

$$z_1 z_2 = r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$$

Example:

1) $(\sqrt{6}+\sqrt{2}\,i)(-3\sqrt{2}+3\sqrt{6}\,i)$

$= \left[2\sqrt{2}\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)\right]\left[6\sqrt{2}\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)\right]$

$= 24\left(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}\right) = -12\sqrt{3} + 12i$

Multiplying by i:

Since $i = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$, zi rotates by $\frac{\pi}{2}$ cclockwise

De Moivre's Theorem (DMT):

$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$ $(\theta \in \mathbb{R},\ n \in \mathbb{Z})$

Proof:

Nov 17, 2017.

Inductive Hypo: Assume k.

IC: $(\cos\theta + i\sin\theta)^{k+1} = (\cos\theta + i\sin\theta)^k(\cos\theta + i\sin\theta)$

$\Rightarrow$ $(IH) = (\cos k\theta + i\sin k\theta)(\cos\theta + i\sin\theta)$

$= \cos(k+1)\theta + i\sin(k+1)\theta$ (PMCN)

$\Leftarrow (\cos\theta + i\sin\theta)^{k-1} = (\cos\theta + i\sin\theta)^k(\cos\theta + i\sin\theta)^{-1}$

$= (\cos k\theta + i\sin k\theta)\left(\frac{\cos\theta - i\sin\theta}{\cos^2\theta + \sin^2\theta}\right)$

$= (\cos(k\theta) + i\sin(k\theta))(\cos(-\theta) + i\sin(-\theta))$

$= \cos(k-1)\theta + i\sin(k-1)\theta$

Taylor Series Expansions: (Not needed)

$$\sin x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!} = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots$$

$\frac{d}{dx}$ ↓

$$\cos x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \dots$$

(same $\frac{d}{dx}$) $$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots$$

$$e^{ix} = 1 + ix \frac{-x^2}{2!} - \frac{ix^3}{3!} + \frac{x^4}{4!} + \frac{ix^5}{5!} - \frac{x^6}{6!} + \dots$$

$$= \cos x + i \sin x$$

Complex exponentials:

$e^{ix} = \cos x + i \sin x$ *needed

→ $z = re^{i\theta}$ where $r \neq 1$

→ $\overline{e^{i\theta}} = e^{-i\theta}$ $\qquad e^{\pi i} = -1$

Example:

1) $\overline{(2e^{i13\pi/6})^6}$ one of the 6 roots

$= 64(\cos 13\pi + i \sin 13\pi)$

$= -64$

Properties:

→ $e^{ia} e^{ib} = e^{i(a+b)}$

→ $(e^{i\theta})^n \cdot e^{in\theta}$ (DMT)

→ Derivatives work (i const)

Example:

1) $z^{12} + 63z^6 - 64 = 0$

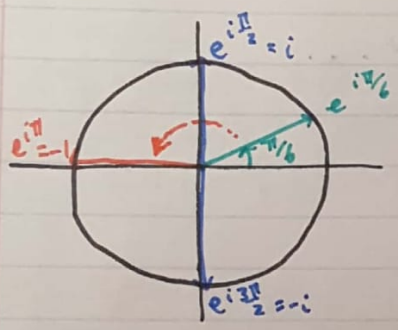
$(z^6 + 64)(z^6 - 1) = 0$

$z^6 = -64$ $\quad$ $z^6 = 1$

↳ Since $2^6 = 64$, $r = 2$ in any $z = re^{i\theta}$

↳ Now want $e^{6i\theta} = -1 = i^2 = i^6 = (-i)^6$

↳ $e^{i\pi/2} = i$ and $e^{i\frac{3\pi}{2}} = -i$



Goal:

Find θ where $6\theta = \pi, 3\pi, 5\pi, \ldots$

$6\theta = \pi + 2k\pi$ for $k \in \mathbb{Z}$.

$\theta = \frac{\pi}{6} + \frac{\pi}{3}k$

↳ $\frac{\pi}{6} + \frac{\pi}{3}k_1$ and $\frac{\pi}{6} + \frac{\pi}{3}k_2$ give same 6^{th} root iff $k_1 \equiv k_2 \pmod 6$

↳ (Just sub in $0 \le k < 6$)

$\therefore \theta \in \left\{\frac{\pi}{6}, \frac{3\pi}{6}, \frac{5\pi}{6}, \frac{7\pi}{6}, \frac{9\pi}{6}, \frac{11\pi}{6}\right\}$

↳ converting, $z^6 = -64 \Rightarrow z \in \{\sqrt{3}+i, 2i, -\sqrt{3}+i, -\sqrt{3}-i, -2i, \sqrt{3}-i\}$

Complex n^{th} Roots Theorem (CNRT):

Nov 20, 2017

Any non zero $\mathbb{C}$ has n distinct n^{th} roots

↳ Roots lie on circle spaced by $\frac{2\pi}{n}$

↳ Refer above

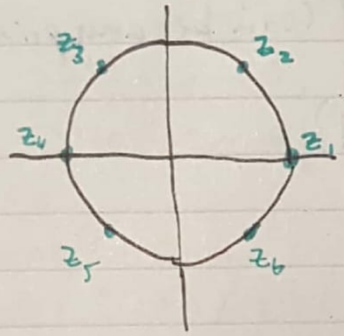
n^{th} Root of Unity:

A number z where $z^n = 1$.

Example:

1) Find all 6^{th} roots of unity.

$z^6 = 1$, $z \in \mathbb{C}$



$z_1 = 1$ works ($\theta = 0$)

↳ keep adding $\theta = \frac{2\pi}{n} = \frac{\pi}{3}$

$z_1 = e^0$

$z_2 = e^{i\frac{\pi}{3}} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$

$z_3 = e^{i\frac{2\pi}{3}} = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$

$z_4 = e^{i\pi} = -1$

$z_5 = e^{i\frac{4\pi}{3}} = \frac{-1}{2} - \frac{\sqrt{3}}{2}i$

$z_6 = e^{i\frac{5\pi}{3}} = \frac{1}{2} - \frac{\sqrt{3}}{2}i$

2) $z^5 = -16\bar{z}$ $\quad z = 0$, or...

$z^6 = -16|z|^2$

$|z|^6 = 16|z|^2$

$|z| = 2$, so...

$z^6 = -64$, and solve. $\quad$ **7 roots: 0 + 6 others**

Fields: Nov 21, 2017

A set where $+ - \times \div$ defined and behave same as $\mathbb{R}$.

→ $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (p prime)

→ if $a, b \in \mathbb{F}$, $ab = 0 \Leftrightarrow (a = 0) \vee (b = 0)$

↳ $[5][2] = 0$, so $\mathbb{Z}_{10}$ not a field.

Polynomials over $\mathbb{F}$:

$n \in \mathbb{N}$, $A = \{a_0, a_1 \dots a_n\}$ subset of some $\mathbb{F}$.

$$\sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

"Polynomial in x over $\mathbb{F}$", belongs to $\mathbb{F}[x]$

Examples:

1) $p_1(x) = (2+i)x^6 - (1-\sqrt{2})x^5 + \frac{2}{3} \in \mathbb{C}[x]$. "complex polynomial"
2) $p_2(x) = 2x^4 - \sqrt{2}x^3 + \frac{2}{3} \in \mathbb{R}[x]$ (and, technically $\mathbb{C}[x]$)
3) $p_3(x) = [3][x]^4 - [5][x]^2 + [1] \in \mathbb{Z}_{13}[x]$ (can be any prime)
   - ↳ Also written w/o. sq []
4) $x^3 + 2x + \frac{1}{x}$ is not polynomial ($-1 \notin \mathbb{N}$)
   - ↳ $\sqrt{x}$ too ($\frac{1}{2} \notin \mathbb{N}$)

Terminology:

Zero polynomial: $p(x) = 0$ has no degree

Equality: $f(x) = g(x) \in \mathbb{F}[x]$ iff
$a_k = b_k$ for all k (same terms)

↳ In $\mathbb{Z}_2[x]$, $3x^5 - 6x^2 + 1 = x + 1$

↳ ✱ NOT the same as solving for POI! Equivalence statement.

↳ == instead of =

Example:

1) $(x^5 + x^2 + 1)(x+1) + (x^3 + x + 1)$ in $\mathbb{Z}_2[x]$.
   $= x + 1 \quad + 1$
   $= \bar{x}$

Division Algorithm (DAP):

In $\mathbb{R}[x]$, no $a, b \in \mathbb{R}$ where $(x-1)(ax+b) = x^2 + 1$ ✱ == not = !

$f(x) = (x-1)(ax+b)$, $g(x) = x^2 + 1$

$f(x) = ax^2 + (b-a)x - b$

$f(x) = x^3$: $\begin{cases} b - a = 0 & a = 1, \text{ and } b = -1, \text{ contradiction} \\ b = a & \text{Q.E.D.} \end{cases}$

DAP Theorem:

If $f(x), g(x)$ in $F(x)$, $g(x) \neq 0$, then $\exists$ unique $q(x), r(x) \in F[x]$ where

$$f(x) = q(x)\,g(x) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$ } $\deg q(x) = \deg(f(x)) - \deg g(x)$

→ If $r(x) = 0$, $g(x) \mid f(x)$

→ last example proved in $\mathbb{R}[x]$, $(x-1) \nmid (x^2+1)$

Long Division:

1) $z + (i+1) \,/\, iz^3 + (i+3)z^2 + (5i+3)z + (2i-2)$:

$$\begin{array}{r} iz^2 + 4z + (i-1) \\ \hline z+(i+1) \;\big|\; iz^3 + (i+3)z^2 + (5i+3)z + (2i-2) \\ -\,(iz^3 + (i-1)z^2) \\ \hline 4z^2 + (5i+3)z \\ -\,(4z^2 + (4i+4)z) \\ \hline (i-1)z + (2i-2) \\ -\,((i-1)z - 2) \\ \hline 2i \end{array}$$

2)

$$\begin{array}{r} 3x^2 + 4x + 4 \\ \hline 2x^2+3x+4 \;\big|\; x^4 + 2x^3 + 2x^2 + 2x + 1 \\ -\,(x^4 + 4x^3 + 2x^2) \\ \hline -2x^3 + 0 + 2x \end{array}$$

$\mathbb{Z}_r$

Nov 22, 2017

Proof:

1) Let $f(x), g(x) \in \mathbb{F}[x]$. If $f(x) | g(x)$ and $g(x) | f(x) \Rightarrow f(x) = cg(x)$.

$g(x) = q_1(x) f(x)$

$f(x) = q_2(x) g(x)$

$f(x) = q_1(x) q_2(x) f(x)$ if $f(x) = 0, g(x) = 0$ or $(0|0)$

$\therefore q_1(x) q_2(x) = 1$, so $q_2(x) \in \mathbb{F} = c$.

Remainder Theorem (RT):

If $f(x) \in \mathbb{F}[x]$, $c \in \mathbb{F}$, then $r(x)$ when $f(x) \div (x-c) = f(c)$

Proof:

By DPA, $\exists$ unique $q(x), r(x)$:

$f(x) = q(x)(x-c) + r(x)$ $\deg r(x) < \deg (x-c)$

↳ so $r(x) =$ constant $= r$.

$f(c) = 0 \, q(c) + r = r = r(x)$.

* State b/c IF is field, this is true.

Example:

1) Remainder when $4x^3 + 2x + 5 \div (x+6)$ in $\mathbb{Z}_7$

$[6] \equiv [1]$, so $f(1) = 4 + 2 + 5 = 4$.

Factor Theorem (FT):

Factor iff $f(c) = 0$.

Example:

1) Prove no real lin factors of $x^8 + x^3 + 1$

↳ Next page.

Show $\exists$ no $x \in \mathbb{R}$ where $x^8 + x^3 + 1 = 0$.

Case 1: $x \in [0, \infty]$

$x^8 \geq 0$, $x^3 \geq 0$, $1 \geq 0$, so $x^8 + x^7 + 1 \geq 1$ (never 0)

case 2: $x \in (-\infty, -1]$

$x^8 \geq 0$, and, $x^8 \geq |x^3|$ $(x^3 < 0)$.

↳ then $x^8 + x^3 \geq 0$.

Case 3: $x \in (-1, 0)$

$x^8 < |x^3| < 1$, $(x^3 < 0)$

so $x^3 + x^8 > -1$

$x^3 + x^8 + 1 > 0$.

$\therefore$ No roots, QED.

Reducible Polynomials:

Nov 25, 2017

Let $f(x) \in F(x)$ have degree $n > 0$.

$f(x)$ reducible when $f(x) = g_1(x) g_2(x)$ where } Depends on $\mathbb{F}$

$0 < \deg(g_1(x)) \leq \deg(g_2(x)) < n$.

→ A linear poly $\Rightarrow$ irreducible (one way $\Rightarrow$).

→ when $\mathbb{F} = \mathbb{C}$, roots are related to reducibility.

FTA:

$f(z) \in \mathbb{C}[x]$, $\deg(f(z)) \geq 1$.

↳ Then $\exists z_0 \in \mathbb{C} \ni f(z_0) = 0$.

↳ Every complex poly of + degree has 1+ $\mathbb{C}$ root.

Example:

1) Factor (solve) $f(x) = ix^3 + (3-i)x^2 + (-3-2i)x - 6$ (-1 is root)

$$x+1 \overline{)\, ix^3 + (3-i)x^2 + (-3-2i)x - 6}$$

$$ix^2 + (3-2i)x - 6$$

$$-(ix^3 + ix^2)$$

$$3 - 2ix^2 + (-3-2i)x$$

$$-(3 - 2ix^2 + (3-2i)x)$$

$$-6x - 6$$

$\therefore f(x) = (x+1)(ix^2+(3-2i)x-6)$ ← $q(x)$

$q(x) = ix^2+(3-2i)x-6$

$= i(x^2+(-2-3i)x+6i)$ what if this wasn't nice?

$= i(x-2)(x-3i)$

$\therefore f(x) = i(x+1)(x-2)(x-3i)$

lecture 43, slide 9, QF

$c\frac{\theta}{2} = \sqrt{\frac{1+\cos\theta}{2}}$ $s\frac{\theta}{2} = \sqrt{\frac{1-\cos\theta}{2}}$

Complex Poly. of Degree N: (CPN)

If $f(z) \in \mathbb{C}[x]$ with $\deg(f(z)) \geq 1$, then

$\exists$ $\mathbb{C}$ $c_1, c_2, \ldots, c_n$ and a $c \neq 0$ where:

$f(z) = c(z-c_1)(z-c_2)\ldots(z-c_n)$

→ Roots ←

Proof: "A poly. of deg. k can be written as $c(z-c_1)..(z-c_n)$.

BC: $f(z) = az+b = a[z-(-\frac{b}{a})]$

IH: Assume P(k) true for some $k \in \mathbb{Z}$.

IC: P(k+1): $f(z) = cz^{k+1} + dz^k + \ldots$

→ By FTA, every fcn over $\mathbb{C}$ has at least one root (1. factor)

→ so factor out $(z-z_1)$, and you have deg k.

Multiplicity:

Largest $k \in \mathbb{Z}$ where $(x-c)^k$ is factor of $p(x)$.

Rational Roots Theorem:

Nov 27, 2017

If $f(x) \in \mathbb{Z}[x]$, $r = \frac{a}{b}$ rational root of $f(x)$, then:

a | constant and b | leading coefficient.

↳ Coef. must be $\mathbb{Z}$ (but can clear rational coefs)

Proof of RRT:

Let $f(x) = \sum_{i=0}^{n} a_i x^i$, where $a_n \neq 0$, $a_i \in \mathbb{Z}$. $r = \frac{a}{b}$ root.

$$\sum_{i=0}^{n} a_i \left(\frac{a}{b}\right)^i = 0 \Rightarrow \sum_{i=1}^{n} a_i \left(\frac{a}{b}\right)^i = -a_0$$

$$\frac{a}{b}\left(\sum_{i=1}^{n} a_i \left(\frac{a}{b}\right)^{i-1}\right) = -a_0 \quad \text{(Doesn't help...)}$$

$$a\left(\sum_{i=1}^{n} a_i \left(\frac{a}{b^i}\right)\right) = -a_0$$

$$a \sum_{i=1}^{n} a_i a^{i-1} b^{n-i} = -b^n a_0$$

$a \mid b^n a_0$, $\gcd(a,b) = 1$, so $a \mid a_0$.

For part 2, isolate a_n after multiplying by b^n.

Example:

1) Prove $\sqrt{7}$ irrational.

$x^2 = 7$
$x^2 - 7 = 0$

RRT: R. Roots must be $\pm 1, \pm 7$.
Thus, $\sqrt{7}$ is irrational root.

2) Prove $\sqrt{5} + \sqrt{3}$ irrational.

$x - \sqrt{5} = \sqrt{3}$

$x^2 - 2\sqrt{5}x + 5 = 3$

$2\sqrt{5}x = x^2 - 2$

$(2\sqrt{5}x)^2 = (x^2-2)^2$

$20x^2 = x^4 - 4x^2 + 4$.

$x^4 - 24x^2 + 4 = 0$. Only possible r. roots: ± 4. Q.E.D.

Conjugate Roots Theorem (CJRT): Nov 28, 2017

If $c \in \mathbb{C}$ root of $f(x) \in \mathbb{R}[x]$, then $\bar{c}$ is also a root.

Example:

1) Factor $x^5-x^4-x^3+x^2-2x+2$ over $\mathbb{Z}$, given i is a root.

→ i is a root by CJRT

→ $\therefore x^2+1$ is a factor

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

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

*Exam

2) $x^4-5x^3+16x^2-9x-13$ if given $2-3i$ is a root.

→ $2+3i$ root by CJRT

$\therefore (x-(2-3i))(x-(2+3i))$

$=(x-2(+3i))((x-2)-3i)$

$=x^2-4x+4+9$. a factor.

Dividing:

$=(x-(2-3i))(x-(2+3i))\left(x-\frac{1+\sqrt{5}}{2}\right)\left(x-\frac{1-\sqrt{5}}{2}\right)$

Real Quadratic Factors (RQF):

$f(x) \in \mathbb{R}[x]$. If $c \in \mathbb{C}$ and $\text{Im}(c) \neq 0$ where c is root, then $\exists$ quadratic $g(x) \in \mathbb{R}[x]$ and polynomial $q(x) \in \mathbb{R}[x]$ where $f(x) = g(x)\,q(x)$

→ FTA means complex root } Almost always

→ CJRT means conjugate too } make quadratic

Real Factors of Real Polynomials (RFRP):

Every non-const polynomial w real coefficients can be written as a product of real linear and/or quadratic factors.

→ Real roots ⇒ linear factors

→ Complex w $\text{Im} \neq 0$ + conjugate ⇒ quadratic

Nov 29, 2017

Composition:

$f \circ g$ exists $\Leftrightarrow$ codomain of g = domain of f.

Example:

1) $f: T \mapsto V$ $g: S \mapsto T$ be onto fcns. Prove $f \circ g$ is onto.

$\because g$ onto, $\forall t \in T, \exists s_0 \in S \ni g(s_0) = t$.

Let $v \in V$. $\because f$ is onto, $\exists t_2 \in T \ni f(t_2) = v$.

$\because \exists s_0 \ni f(g(s_0)) = f(t_2) = V$

} same as one-to-one fcns.

One to One?

Let $f(g(s_1)) = f(g(s_2))$

Since f is one to one, $g(s_1) = g(s_2)$.

Since g is one to one, $s_1 = s_2$.

Bijections:

Injective and Surjective functions.

Example:

1) If $p \neq 3$ prime, then $f(x) = [3]x$ is bijective. $\mathbb{Z}_p \to \mathbb{Z}_p$

Since $p \neq 3$, $[3] \neq [0]$.

Since p prime, $[3]^{-1}$ exists.

1↔1: $f(x_1) = f(x_2)$

$[3]x_1 = [3]x_2$. $[3]^{-1}$ exists, so $x_1 = x_2$

Onto: Let $y \in \mathbb{Z}_p$.

$y = [3]x$

$y[3^{-1}] = x$ $\therefore$ Onto.

Counting:

Is a bijection. $f: \mathbb{N}_{52} \to C$ where C is set of cards.
→ where $\mathbb{N}$ is nat. numbers up to 52 ($|C|$).

Counting Set:

$N_0 = \{0\}$, $N_1 = \{1\}$. $\forall n \geq 2$, $\mathbb{N}_n = \mathbb{N}_{n-1} \cup \{n\}$

Cardinality (finite):

If $\exists$ bijection $f: \mathbb{N}_{52} \to S$, then $|S| = n$. (order doesn't matter)
↳ S is finite if $\exists$ bijection, else infinite.

Cardinality (finite + infinite):

If $\exists$ bijection $f: S \to T$, then $|S| = |T|$

Example:

1) Show $|\mathbb{Q}| = |\mathbb{N}|$