Lecture 1. The Language, sets, Mathematical statements & Negation, Quantifiers and Quantified Statements.

1.2 Set: Order & Repetition don't matter

$\in$ membership

$\notin$ non-membership

$\emptyset$ empty set

$\mathbb{N}$ = Natural num

$\mathbb{Z}$ = Integers

$\mathbb{Q}$ = Rational num

1.3 Mathematical Statements & Negation

Statement: A Sentence that has a define state of being either true or false.

Negation: $\neg$, $\neg A$ is opposite truth of A.

$$\neg(\neg A) \equiv A$$

1.4. Quantifiers & Quantified Statements.

A statement is a sentence that's either TRUE or FALSE.

A quantified statements contains :

1. Domain: Specifies the possible choices for the variable in each case.

2. Open Sentence: A sentence that contains a variable, where truth of the sentence is determined by the value of variable chosen from the domain of the variable.

Become statement When a variable is replaced with a "value".

3. A dummy variable. i, a, x, z All fine

4. A quantifier (Universally, existential) $\forall$, $\exists$

Universal: $\forall x \in S, P(x)$

For all x in S, P(x) is true

Existential: $\exists x \in S, P(x)$

There exist x in S such that P(x) is true.

Ex. P(x): x wear Pink Shirt.

$\forall x \in T$, $P(x) \Rightarrow$ False
$\exists x \in T$, $P(x) \Rightarrow$ True
$\forall z \in T$, $P(z) \Rightarrow$ False

E.x. Let $P(x)$ be $x^2 > 0$

$\forall x \in \mathbb{Z}$, $P(x) \Rightarrow$ False
$\exists x \in \mathbb{Z}$, $P(x) \Rightarrow$ True
$\forall x \in \mathbb{N}$, $P(x) \Rightarrow$ True
$\exists x \in \mathbb{N}$, $P(x) \Rightarrow$ True

E.x. Let $P(x)$ be "x can fly"

$\forall x \in \mathbb{Q}$, $P(x)$ (vacuously True)

$\exists x \in \mathbb{Q}$, $P(x)$ (vacuously False)

Let $P(x)$ be "$0 = 4 - 1 - 3$"

$\forall x \in \mathbb{Z}$, $P(x) \Rightarrow$ True

Perfect Square Ex.

1) $\exists x \in \mathbb{Z}$, $75 = x^2$
2) $\forall x \in \mathbb{R}$, $x^2 + 3x + 8 \neq 0$

1.5 Nested Quantifiers.

Ex. The square of an odd Integer is never an even integer.

$(\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n = 2k+1), (\exists m \in \mathbb{Z}, n^2 = 2m+1)$

$\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, x + y = 13$

$\forall x, \forall y \longleftarrow \forall x, y \in \mathbb{Z}$

Nested $\begin{cases} \forall x, \exists y \\ \exists x, \forall y \end{cases}$

$\exists^{\geq 2} x, \exists^{!} x \longleftarrow \exists x, y \in \mathbb{Z}$

$\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, P(y,x) \to T$

E.x. Let A = set of all people in this room

$B = \{17, 18, \ldots, 40\}$

Let $P(x,y)$ be "x is y years old"

$\forall x \in A, \exists y \in B, P(x,y)$ T

$\forall y \in B, \exists y \in A, p(x,y)$ F

Ex. $\forall y \in R, \exists y \in \mathbb{Z}, \forall w \in \mathbb{Z}, \underbrace{(x+wy)(z)^2 > 5}$

$A(x,y,z,w)$

$B(x,y,z)$

$C(x)$

$D(y)$

1.5.3 Negation of Nested Quantifiers.

$\exists x \in \mathbb{Q}, P(x)$ F

$\forall x \in \mathbb{Q}, \neg P(x)$ T !

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

Ex. Negate S, where S is $\forall x \in \mathbb{R}, \exists y \in \mathbb{Q}, x+y \notin \mathbb{Q}$

$$\neg S \equiv \exists x \in \mathbb{R}, \neg(\exists y \in \mathbb{Q}, x+y \notin \mathbb{Q})$$

$$\equiv \exists x \in \mathbb{R}, \forall y \in \mathbb{Q}, \neg(x+y \notin \mathbb{Q})$$

$$\equiv \exists x \in \mathbb{R}, \forall y \in \mathbb{Q}, x+y \in \mathbb{Q}$$

STEP BY STEP, LEFT TO RIGHT

2.1 Truth Tables

2.2 Conjunction and Disjunction

$A \vee B$ (Disjunction, or)

$A \wedge B$ (Conjunction, and)

A	B	$A \wedge B$	$\neg(A \wedge B)$	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$(\neg A) \vee (\neg B)$	$(\neg A) \wedge (\neg B)$
T	T	T	F	T	F	F	F	F	F
T	F	F	T	T	F	F	T	T	F
F	T	F	T	T	F	T	F	T	F
F	F	F	T	F	T	T	T	T	T

(De Morgan's Laws (DML))

For statement variables A and B, we have

1. $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$
2. $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$

For statement variables A, B and C, the following rules hold for the logical operators $\wedge$ and $\vee$:

Commutative Laws:

- $A \wedge B \equiv B \wedge A$
- $A \vee B \equiv B \vee A$

Associative Laws:

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

Distributive Laws:

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

Ex. (No TT allowed) Show that

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

$\neg(A \wedge (\neg B \wedge C)) \equiv \neg A \vee \neg(\neg B \wedge C)$ by DML

$\equiv \neg A \vee (B \vee \neg C)$ by DML

$\equiv (\neg A \vee \neg C) \vee B$ by associative law

$\equiv \neg(A \wedge C) \vee B$ by DML

2.4 Implication

The truth value for "A **implies** B", written symbolically as $A \implies B$, is defined by the truth table

A	B	$A \implies B$
T	T	T
T	F	F
F	T	T
F	F	T

We also refer to $A \implies B$ as an **implication**; component A is referred to as the **hypothesis** for this implication, and component B is referred to as the **conclusion**.

$A \Rightarrow B$

↳ A: Hypothesis

↳ B: Conclusion

Ex. $\forall x \in \mathbb{R}\ (x>2 \Rightarrow x^2>4)$ $P(x)$ (T)

$P(6)$: $6>2 \Rightarrow 36>4$ (T)

$P(0)$: $0>2 \Rightarrow 0>4$ (T)

Ex. $\forall x \in \mathbb{R}\ (x^2>4 \Rightarrow x>2)$ $Q(x)$ (F)

Q(1): $1>4 \Rightarrow 1>2$ (T)

Q(3): $9>4 \Rightarrow 3>2$ (T)

Q(-3): $9>4 \Rightarrow -3>2$ (F)

☆: $A \Rightarrow B \equiv (\neg A) \vee B$

Case 1: $\neg A$ is true, A is false, see table.

2: B is true, see table.

Exercise: show $(A \vee B) \Rightarrow C \equiv (A \Rightarrow C) \wedge (B \Rightarrow C)$

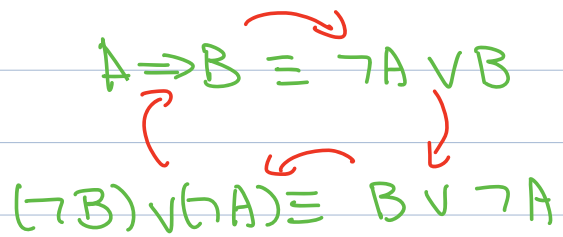
2.5 Converse & Contrapositive

Converse of $A \Rightarrow B$ is $B \Rightarrow A$

$A \Rightarrow B \not\equiv B \Rightarrow A$

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

$$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$$



2.6 If and only if

The truth value for "A **if and only if** B", written symbolically as $A \iff B$, is defined by the truth table

A	B	$A \iff B$
T	T	T
T	F	F
F	T	F
F	F	T

Sometimes we concisely write A if and only if B as "A **iff** B".

Ex. $\forall x \in \mathbb{R}[|x| = 2 \iff (x = 2 \vee x = -2)]$

Chapter 2 Formulas:

(De Morgan's Laws (DML))

For statement variables A and B, we have

1. $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$
2. $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$

For statement variables A, B and C, the following rules hold for the logical operators $\wedge$ and $\vee$:

Commutative Laws:

- $A \wedge B \equiv B \wedge A$
- $A \vee B \equiv B \vee A$

Associative Laws:

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

Distributive Laws:

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

REMARK

For statement variables A, B and C, we have

$$\big((A \vee B) \implies C\big) \equiv \big((A \implies C) \wedge (B \implies C)\big). \tag{2.2}$$

REMARK

For statement variables A and B, we have

$$\big(A \implies B\big) \equiv \big((\neg B) \implies (\neg A)\big). \tag{2.3}$$

In other words, an implication is logically equivalent to its contrapositive.

REMARK

For statement variables A and B, we have

$$\big(A \implies B\big) \equiv \big((\neg A) \vee B\big), \qquad \neg\big(A \implies B\big) \equiv \big(A \wedge (\neg B)\big). \tag{2.4}$$

REMARK

1. For statement variables A and B, we have
$$\big(A \iff B\big) \equiv \big((A \implies B) \wedge (B \implies A)\big). \tag{2.5}$$
2. We also have the logical equivalence for universally quantified statements
$$\Big(\forall\, x \in X,\ P(x) \iff Q(x)\Big) \tag{2.6}$$
$$\equiv \Big(\big(\forall\, x \in X,\ P(x) \implies Q(x)\big) \wedge \big(\forall\, x \in X,\ Q(x) \implies P(x)\big)\Big).$$

Defn:

Let $n \in \mathbb{Z}$, n is a perfect square if

$n = k^2$ for some $k \in \mathbb{Z}$.

Ex1. Proof: There exist a perfect square k,

such that $k^2 - \frac{31}{2}k = 8$

"Discovery" Solve $k^2 - \frac{31}{2}k - 8 = 0$

$k = \frac{31 \pm 33}{4}$ (16)

Proof: ① Note that 16 is a perfect square, since $16 = 4^2$ and $4 \in \mathbb{Z}$.

② Also, note that

$$16^2 - \frac{31}{2}(16) = 16\left[16 - \frac{31}{2}\right] = 16\left(\frac{1}{2}\right) = 8$$

③ This is what we needed to show.

To prove $\forall x \in T, P(x)$: fix an arbitrary number of T. Prove P holds for that member.

Ex. 2. Prove $\forall x, y \in \mathbb{R}, x^4 + x^2y + y^2 \geq 5x^2y - 3y^2$

Rough Work: $x^4 + x^2y + y^2 \geq 5x^2y - 3y^2$

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

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

Proof / Solution: Let $a, b \in \mathbb{R}$. We know that

$(a^2 - 2b)^2 \geq 0$

Expanding gives us that $a^4 - 4a^2b + 4b^2 \geq 0$

Adding $5a^2b - 3b^2$ to both sides gives us that $a^4 - a^2b + b^2 \geq 5a^2b - 3b^2$. This completes the proof.

$(\exists x \in \mathbb{Z}, x > 10) \wedge (\exists x \in \mathbb{Z}, x \leq 7)$ T

Separate

$\exists x \in \mathbb{Z}, (x > 10 \wedge x \leq 7)$ F

Together

E.x.3. Let $x \in \mathbb{R}$, Prove that $|x-3| + 2|x+2| \geq 5$

Rough Work: We should consider when $|x-3|, |x+2|$

"switch signs" $\Longrightarrow$ 3 cases: $x \leq -2$

$-2 \leq x \leq 3$

$3 \leq x$

Proof: We consider each of the following 3 cases:

$x \leq -2$, or $-2 \leq x \leq 3$, $x \geq 3$

Case 1 ($x \leq -2$), Then $|x+2| = -x-2$ and $|x-3| = 3-x$.

Then, $|x-3| + 2|x+2| = 3-x-2x-4$

$= -3x-1 \geq -3(-2)-1 = 5$

Case 2 ($-2 \leq x \leq 3$), Then $|x+2| = x+2$ and $|x-3| = 3-x$

Note $x \leq 3$ implies $-x \geq -3$

Then, $|x-3| + 2|x+2| = 3 - x + 2(x+2)$

$= 7 + x \geq 7 - 2 = 5$

Case 3 ($x \geq 3$), Then,

$|x-3| + 2|x+2| = x - 3 + 2x + 4$

$= 3x + 1 \geq 9 + 1 \geq 5$

In all 3 cases, we established the desired inequalities. Since every real number is in one case, we're done.

E.x. Prove $\forall x, y \in \mathbb{R}$, $\frac{x+y+|x-y|}{2} = \max\{x, y\}$

Proof #1: Let $x, y \in \mathbb{R}$, either $x \geq y$ or $x \leq y$.

Case 1: $(x \geq y)$ We have $|x-y| = x-y$ and

$\max\{x,y\} = x$.

Then, $\frac{x+y+|x-y|}{2} = \frac{x+y+x-y}{2} = x$

$= \max\{x,y\}$

Case 2: We omit this since it's similar to case 1.

Proof #2: Let $x, y \in \mathbb{R}$. The identity is symmetric in x & y.

WLOG, assume $x \geq y$

$(x \geq y)$ We have $|x-y| = x-y$ and

$\max\{x,y\} = x$.

Then, $\frac{x+y+|x+y|}{2} = \frac{x+y+x-y}{2} = x$

$= \max\{x,y\}$

we are done.

Disprove "A" $\Leftarrow$ Prove $\neg A$

E.x Prove / Disprove : $\exists x \in \mathbb{R}, \cos(2x) + \sin(7x) = \frac{11}{5}$

Soln: We prove the negation, which is

$\forall x \in \mathbb{R}, \cos(2x) + \sin(7x) \neq \frac{11}{5}$

Let $a \in \mathbb{R}$. Then $\cos(2a) \leq 1$ and $\cos(7a) \leq 1$. So

$$\cos(2a) + \cos(7a) \leq 1 + 1 = 2 < \frac{11}{5}.$$

So, $\cos(2a) + \cos(7a) \neq \frac{11}{5}$, we are done.

E.x. P/D : $\overset{P(x)}{①}$ $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^2 = 2$

$Q(x)$ ② $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x^3 - y^2 = 2$

Rough Work:

$P(5)$: $\exists y \in \mathbb{R}, 125 - y^3 = 2$ T ($y = \sqrt[3]{123}$)

$P(7)$: $\exists y \in \mathbb{R}, 343 - y^3 = 2$ T ($y = \sqrt[3]{341}$)

$P(-1): \exists y \in \mathbb{R}, -1 - y^3 = 2$ T ($y = \sqrt[3]{-3}$

$P(x): y = \sqrt[3]{x^3 - 2}$

$Q(3): \forall x \in \mathbb{R}, x^3 - 27 = 2$ (F)

$\neg Q(3): \exists x \in \mathbb{R}, x^3 - 27 \neq 2$ (T : $x = 0$)

$Q(2): \forall x \in \mathbb{R}, x^3 - 8 = 2 \Leftarrow$ (F : $x = 0$)

Soln we prove ①. Let $a \in \mathbb{R}$. We prove $\exists y \in \mathbb{R}$.

$x^3 - y^2 = 2$

Let $y = \sqrt[3]{a^3 - 2}$. Notice that:

$$a^3 - y^3 = a^3 - \left(\sqrt[3]{a^3 - 2}\right)^3$$

$$= a^3 - (a^3 - 2) = 2 \quad \# \text{QED}$$

② is false. We prove it's negation, which says

$\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, x^3 - y^3 \neq 2$.

Option 1: Let $x = \sqrt[3]{y^3 - 2 + 5}$

Then $x^3 - y^3 = y^3 - 2 + 5 - y^3 = 3 \neq 2$

Option 2: If $y \neq \sqrt[3]{-2}$, let $x = 0$. C1

If $y = \sqrt[3]{-2}$, let $x = 1$. C2

Case 1: $x^3 - y^3 = 0 - y^3 \neq 2$

Case 2: $x^3 - y^3 = 1 - (-2) = 3 \neq 2$

Week 3

3.3 Proving Implication

Defn. Let $n \in \mathbb{Z}$, n is even & $n = 2k$ for some $k \in \mathbb{Z}$. n is odd if $n = 2k+1$ for some $k \in \mathbb{Z}$.

→ Assume $\neg$ (n even) $\equiv$ n odd

E.x. Prove $\forall m \in \mathbb{Z}$, (m even $\Rightarrow 7m^2 + 4$ even)

Proof: Let $m \in \mathbb{Z}$, We've two cases; m odd or m even

Case 1: m odd. Implication is true since hypothesis is false.

Assume

Case 2: m even. We know there's an integer k such that $m = 2k$. We must show that $7m^2 + 4$ is even.

That is, we must show that $7m^2 + 4 = 2x$ for some $x \in \mathbb{Z}$.

Well, $7m^2 + 4 = 7(2k)^2 + 4$

$= 2(14k^2 + 2)$

Note that $14k^2 + 2 \in \mathbb{Z}$, since $k \in \mathbb{Z}$.

So $7m^2 + 4$ is even # QED.

SETUP EXECUTION

3.4 Divisibility of Integer

Defn: Let $a, b \in \mathbb{Z}$. We say <u>a divides b</u> or <u>b is divisible by a</u>, written $a \mid b$, if $ac = b$ for some $c \in \mathbb{Z}$.

Ex

$4 \mid 12$	$-4 \mid -28$
$4 \mid -12$	$0 \mid 7$
$20 \mid 10$	$7 \mid 0$
$1 \mid 37$	$0 \mid 0$

Ex. $\forall m \in \mathbb{Z}$, $14 \mid m \Rightarrow 7 \mid 3m + 42$

Proof: Let $a \in \mathbb{Z}$. Assume $14 \mid a$. Thus, there's an integer c such that $14c = a$. We must show that $7 \mid 3a + 42$. That is, we must show

$7d = 3a + 42$ for some $d \in \mathbb{Z}$.

(1) Well, $3a + 42 = 3(14c) + 42$

$= 7\underbrace{[(6c) + 6]}_{\in \mathbb{Z}}$.

We are done.

(2) Let $d = 6c + 6$. Note $d \in \mathbb{Z}$ and

(a) Let $a = 3c+6$. Note $c \in \mathbb{Z}$ and

$7d = 7(bc+6) = 3(14c) + 42 = 3a + 42$

$9 \mid 27 \qquad 9 \mid 45$

$9 \mid 27(5) + 45(-97)$

Proposition (DIC) Let $a, b,$ and $c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for all $x, y \in \mathbb{Z}$.

Proof: Assume $a \mid b$ and $a \mid c$. This mean we have $m, n \in \mathbb{Z}$ such that $am = b$ and $an = c$. We must prove $\forall x, y \in \mathbb{Z}$, $a \mid bx + cy$.

Let $x, y \in \mathbb{Z}$, we must show $\exists z \in \mathbb{Z}$, such that $az = bx + cy$.

Well, $bx + cy = (am)x + (an)y$

$$= a\underbrace{[mx+ny]}_{\in \mathbb{Z}}$$

E.x. Let $a \in \mathbb{Z}$, Assume $a \mid 12$ and $a \mid 35$.

Prove $a = \pm 1$.

Proof: By DIC, we know that $\forall x, y \in \mathbb{Z}$, $a \mid 12x+35y$.

Note that $12 \times 3 + 35(-1) = 1$.

So $a \mid 12(3) + 35(-1)$, ie $a \mid 1$. So $a = \pm 1$

E.x. Prove $\forall a \in \mathbb{Z}, [(\forall b \in \mathbb{Z}, a \mid 6b-29) \Rightarrow a = 1]$

Proof: Let $a \in \mathbb{Z}$, Assume that $\forall b \in \mathbb{Z}$, $a \mid 6b-29$

therefore $a \mid 6(5)-29$, ie $a \mid 1$.

$7 \mid 14$ $\quad$ $14 \mid 28$ $\quad$ $7 \mid 28$

Proposition (TD): Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

3.5 Prove by Contrapositive.

Ex. Prove $\forall x \in \mathbb{Z}, [x^2+4x-2 \text{ odd} \Rightarrow x \text{ odd}]$

Rough Work:

know $x^2+4x-2 = 2k+1$

show $x = 2m+1$

$$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$$

Proof: Let $x \in \mathbb{Z}$. We will prove the contrapositive of the original implication. Assume x is even. Let $k \in \mathbb{Z}$ satisfy that $x = 2k$. We want to show that x^2+4x-2 is even. That is, we must prove that $\exists c \in \mathbb{Z}, x^2+4x-2 = 2c$.

Well, $x^2+4x-2 = 2k^2+4(2k)-2$

$= 2[\underbrace{k^2+2k-1}_{\in \mathbb{Z} \text{ since } k \in \mathbb{Z}}]$

We're done.

Exercise: Prove $\forall x, y \in \mathbb{R}, [xy \notin \mathbb{Q} \Rightarrow (x \notin \mathbb{Q} \vee y \notin \mathbb{Q})]$

Prove $A \vee B$ 1) Assume $\neg B$, prove A.

or 2) Assume $\neg A$, prove B. $\equiv$

Ex. Prove $\forall x \in \mathbb{R}, [x^2 - 7x + 12 \geq 0 \Rightarrow (x \leq 3 \vee x \geq 4)]$

Proof 1. Let $x \in \mathbb{R}$. Assume $x^2 - 7x + 12 \geq 0$. Assume $x > 3$. Prove $x \geq 4$.

Proof 2. Let $x \in \mathbb{R}$. Assume $x > 3$ and $x < 4$. Prove $x^2 - 7x + 12 < 0$ Contrapositive

---

TD $a|b \wedge b|c \Rightarrow a|c$

DIC $a|b \wedge a|c \Rightarrow \forall x, y \in \mathbb{Z}, a|bx+cy$.

3.6 Proof by Contradiction

We want to prove A.

Assume $\neg A$. Conclude something silly.

Ex. 1 Prove no integer is both even or odd.

Proof: Proceed by contradiction. Assume there is an

integer n that is both even and odd. Let $a, b \in \mathbb{Z} \Rightarrow$

$n = 2a$ and $n = 2b+1$. Then $2a = 2b+1$. So $2[a-b] = 1$

Option 1 This says $2 \mid 1$, since $a-b \in \mathbb{Z}$. Contradiction since $2 \nmid 1$.

Option 2 This says $a-b = \frac{1}{2}$. Contradiction since $\frac{1}{2} \notin \mathbb{Z}$ but $a-b \in \mathbb{Z}$.

So no integer is both even and odd.

Ex. 2 Prove $A \Rightarrow B$

Option 1 (Contrapositive: Assume $\neg B$. Prove $\neg A$.

Option 2 Contradiction: Assume $\neg(A \Rightarrow B)$. That is assume $A \wedge \neg B$.
Typically prove $\neg A$. Contradiction.

(1, 2 "Same" for an implication)

$\exists n \in \mathbb{N} \ni \frac{19}{3} < n < \frac{50}{3}$ ← More than 1 n.

$\exists n \in \mathbb{N} \ni \frac{22}{3} < n < \frac{26}{3}$ ← Only 1 n.

Unique ← Only one.

How to say "There exist an unique member of T such that P is true."?

$$(\exists x \in T, P(x)) \wedge (\forall y, z \in T, [P(y) \wedge P(z) \Rightarrow y = z])$$

At least one solution — At most one solution.

$$(\exists x \in T, [P(x) \wedge \forall y \in T, (P(y) \Rightarrow y = x)]$$

E.x. Let $a_1, a_2, a_3, \ldots$ be a sequence. If $\lim_{n \to \infty} a_n$ exists, it is unique.

Proof: Assume $\lim_{n \to \infty} a_n = L$ and $\lim_{n \to \infty} a_n = M$. Prove $M = L$.

E.x. (coming soon) Let $n \in \mathbb{Z}$. There exist unique $q, r \in \mathbb{Z}$, such that

1) $n = 27q + r$
2) $0 \leq r \leq 27$

Example Questions.

1) Prove $\forall a, b, c \in \mathbb{Z}, [(a \nmid b \wedge a \mid b + c) \Rightarrow a \nmid c]$

Life Tip: avoid assuming $a \nmid b$.

Proof: Let $a, b, c \in \mathbb{Z}$. Assume $a \mid c$. We must prove $a \mid b \vee a \nmid b + c$. Assume $a \mid b + c$. We need to prove $a \mid b$.

By DIC, $a \mid (-1)(c) + (1)(b + c)$,

ie $a \mid b$

DIC

2) $\forall a,b,c \in \mathbb{Z}, [a|b \wedge a|c \Rightarrow \forall x,y \in \mathbb{Z}, a|bx+cy]$ ← T

$\forall a,b,c,x,y \in \mathbb{Z}, [a|b \wedge a|c \Rightarrow a|bx+cy]$ ← T

$\forall a,b,c \in \mathbb{Z}, [(\forall x,y \in \mathbb{Z}, a|bx+cy) \Rightarrow a|b \wedge a|c]$ ← T

$\forall a,b,c,x,y \in \mathbb{Z}, [a|bx+cy \Rightarrow (a|b \wedge a|c)]$ ← F

Proof 3 Let $a,b,c \in \mathbb{Z}$. Assume $\forall x,y \in \mathbb{Z}, a|bx+cy$.

Must prove that $a|b$ and $a|c$.

By (*), $a|b(1)+c(0)$, ie. $a|b$.

By (*), $a|b(0)+c(1)$, ie. $a|c$.

Disproof of #4: Let $a=13, b=4, c=2, x=5, y=3$.

Then $a|bx+cy$ (since $13|26$).

But $a \nmid b \wedge a \nmid c$.

DIC can be useful, but do remember to nested it!

P(x,y)

The only real solution to '$x^2+y^2 = 2y-1$' is $x=0$ and $y=1$.

$$(\forall x,y \in \mathbb{R}.[(P(x,y) \implies x=0 \ \wedge \ y=1.)]) \wedge P(0,1)$$

$$\forall x,y \in \mathbb{R}.[P(0,1) \wedge (P(x,y) \implies x=0 \ \wedge \ y=1.)]$$

4.1 Notation for Summations, Products, and Recurrences.

Sum / Product Notation

$a_1, a_2, a_3, \ldots$ sequence

$$\sum_{k=3}^{7} a_k = a_3 + a_4 + a_5 + a_6 + a_7$$

7

$$\prod_{k=3}^{7} a_k = a_3 a_4 a_5 a_6 a_7$$

$$\sum_{i=3}^{5} i = 3+4+5 = 12$$

$$\sum_{k=10}^{10} a_k = a_{10} \qquad \prod_{k=13}^{13} a_k = a_{13}$$

$$\sum_{j=4}^{1} a_j = 0 \qquad \prod_{j=17}^{2} a_j = 1$$

$$n! = \prod_{k=1}^{n} k$$

$$1! = 1$$

$$0! = 1$$

Important Fact $a_1 + a_2 + a_3 + a_4 + a_5 = (a_1 + a_2 + a_3 + a_4) + a_5$

ie. $\sum_{k=1}^{5} a_k = \left(\sum_{k=1}^{4} a_k\right) + a_5$

$$a_1 + a_2 + a_3 + a_4 = (a_1 + a_2 + a_3) + a_4$$

$$\sum_{k=1}^{4} a_k = \left(\sum_{k=1}^{3} a_k\right) + a_4$$

Let $n \in \mathbb{Z}$, $n \geq 0$

$$\left(\sum_{k=1}^{n+1} a_k\right) = \left(\sum_{k=1}^{n} a_k\right) + a_{n+1}$$

$$\left(\prod_{k=1}^{n+1} a_k\right) = \left(\prod_{k=1}^{n} a_k\right) \cdot (a_{n+1})$$

$$\sum_{k=4}^{7} k^2 = \sum_{k=5}^{8} (k-1)^2$$

Mobius.

$$c \in \mathbb{Z} \quad \sum_{k=d}^{b} a_k = \sum_{k=d+c}^{b+c} a_{k-c}$$

4.2. Induction

Goal: Prove $\forall n \in \mathbb{N}, P(n)$ ③

Option 1. Let $k \in \mathbb{N}$. Prove $P(k)$.

Option 2. (Induction)

Prove $P(1) \Rightarrow P(2)$
$P(2) \Rightarrow P(3)$
$\vdots$

② $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

① $\boxed{P(1)}$

Knowing ① and ② lets you conclude ③.

Ex. 1 $1(2) = 2 = (\frac{1}{3})(1)(2)(3)$

$1(2) + 2(3) = 8 = (\frac{1}{3})(2)(3)(4)$

$1(2) + 2(3) + 3(4) = 20 = (\frac{1}{3})(3)(4)(5)$

Let $n \in \mathbb{N}$. Prove $\sum_{i=1}^{n} i(i+1) = \frac{1}{3} n(n+1)(n+2)$

Proof: Let $P(n)$ denote $\sum_{i=1}^{n} i(i+1) = \frac{1}{3} n(n+1)(n+2)$.
We proceed by induction.
Note $P(1)$ is true since $1(2) = 2 = \frac{1}{3}(1)(2)(3)$. Base Case
Let $k \in \mathbb{N}$. Assume $P(k)$. That is assume

$$\sum_{i=1}^{k} i(i+1) = \frac{1}{3} k(k+1)(k+2)$$ Induction Hypothesis.

We must prove $P(k+1)$, $\sum_{i=1}^{k+1} i(i+1) = \frac{1}{3}(k+1)(k+2)(k+3)$.

Well, $\sum_{i=1}^{k+1} i(i+1) = \sum_{i=1}^{k} i(i+1) + (k+1)(k+2)$

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

by our assumption.

$$= \frac{1}{3}(k+1)(k+2)[k+3]$$

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

We are done. # QED. ▨

E.x.) (Harder) Prove $\forall n \geq 1$, that $25 \mid 16^n + 10n - 1$

Proof: Proceed by induction. Let $P(n)$ be $25 \mid 16^n + 10n - 1$

Base Case: ($n=1$) note: $16 + 10(1) - 1 = 25$, so $25 \mid 16^1 + 10(1) - 1$, so $P(1)$ holds.

Inductive Hypothesis: Let $k \in \mathbb{N}$. Assume $P(k)$. That is $25 \mid 16^k + 10(k) - 1$

Induction Step: We must prove $P(k+1)$, which says $25 \mid 16^{k+1} + 10(k+1) - 1$

Well, $16^{k+1} + 10(k+1) - 1 = 16 \cdot 16^k + 10k + 10 - 1$

$= 16 \cdot 16^k + 10k + 10 - 1 + 16 \cdot 10k - 16 \cdot 10k + 16 - 16.$

$= 16[16^k + 10k - 1] - 150k + 25$

$= [16^k + 10k - 1](16) + [25](1 - 6k)$

By Induction Hypothesis and DIC, we conclude that

$25 \mid 16^{k+1} + 10k - 1$

This completes the proof by POMI.

Ex. 3 "Prove" that $n \geq n+1$ for $n \in \mathbb{N}$.

"Proof:" Let $P(n)$ be $n \geq n+1$

IH: Let $k \in \mathbb{N}$, assume $P(k)$. That is $k \geq k+1$.

IS: We must prove $P(k+1)$, which says $k+1 \geq k+2$.

From the IH, add 1 to both sides to obtain $k+1 \geq k+2$.

(Note btw, $P(1)$ is false.)

$(P(1) \wedge P(2)) \Rightarrow P(3)$

$(P(2) \wedge P(3)) \Rightarrow P(4)$

$\forall n \in \mathbb{N}, (P(n) \wedge P(n+1) \Rightarrow P(n+2))$

Ex. Define $x_1, x_2, x_3 \cdots$ by $x_1 = 4$, $x_2 = 68$, and $x_n = 2x_{n-1} + 15x_{n-2}$ for all $n \geq 3$.

Prove $\forall n \geq 1$ $x_n = 2(-3)^n + 10(5)^{n-1}$

Proof: Let $P(n)$ denote $X_n = 2(-3)^n + 10(5)^{n-1}$. Proceed by (strong) Induction.

BC. Check $P(1)$ is true.

$P(1): 2\cdot(-3)^1 + 10(5)^0 = 4 = X_1$ ✓

$P(2): 2\cdot(-3)^2 + 10(5)^1 = 68 = X_2$ ✓

I.H. Let $k \in \mathbb{N}$. Assume $P(k)$ and $P(k+1)$. That is, assume $X_k = 2(-3)^k + 10(5)^{k-1}$ and $X_{k+1} = 2(-3)^{k+1} + 10(5)^k$

I.S. We must prove $P(k+2)$, which says $X_{k+2} = 2(-3)^{k+2} + 10(5)^{k+1}$

Well, $X_{k+2} = 2\cdot X_{k+1} + 15 X_k$

$= 2\left[2(-3)^{k+1} + 10(5)^k\right] + 15\left[2(-3)^k + 10(-5)^{k-1}\right]$

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

$= (-3)^k\left[4(-3) + 30\right] + 5^{k-1}\left[20\cdot 5 + 150\right]$

$= (-3)^k\left[18\right] + (5)^{k-1}\left[250\right]$

$= (-3)^k\cdot\left[2\cdot(-3)^2\right] + (5)^{k-1}\cdot\left[10\cdot 5^2\right]$

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

By POSI #QED

$P(1) \Rightarrow P(2)$

$P(1) \wedge P(2) \Rightarrow P(3)$

$P(1) \wedge P(2) \wedge P(3) \Rightarrow P(4)$

$\vdots$

$\Big\}$ $\forall n \in \mathbb{N}, (P(1) \wedge P(2) \cdots P(n)) \Rightarrow P(n+1)$

Ex. Let $n \in \mathbb{N}$. Prove n can be written as a sum of distinct powers of 2.

Proof: Let $P(n)$ be circled above.

$100 \stackrel{?}{=}$ Sum of power of 2 ← any even n ✓

$50 \stackrel{?}{=} 2^a + 2^b + 2^c + 2^d$

$100 \stackrel{?}{=} 2^{a+1} + 2^{b+1} + 2^{c+1} + 2^{d+1}$

$99 \stackrel{?}{=}$ sum of power of 2

$98 = 2^a + 2^b + 2^c$

Proof: Let $P(n)$ be circled above. Proceed by induction.

$P(1)$: $1 = 2^0$

I.H. Let $k \in \mathbb{N}$. Assume $P(1), P(2) \ldots P(k)$.

I.S. We try to prove $P(k+1)$. $k+1$ is even or odd.

Case 1: Assume $k+1 = 2a$ for some $a \in \mathbb{Z}$.

Since $P(a)$ is true, a can be written as a sum of distinct power of 2. Thus $2a$ can be written as a sum of distinct power of 2, since multiplying by 2 increases each component by 1. That is distinctness preserved.

Case 2: Assume $k+1$ is odd. Since $P(k)$ is true, there exist $b_1, \ldots b_n \in \mathbb{Z}, \geq 0$, distinct, such that

$k = 2^{b_1} + \dots + 2^{b_n}$. Note that no b_i can be 0, since 2^0 is the only odd power of 2 and k is even. Thus $2^{b_1}, 2^{b_2}, \dots, 2^{b_n}, 2^0$ are distinct. Since $k+1 = 2^{b_1} + \dots + 2^{b_n} + 2^0$, we are done.

$P(1) \Rightarrow P(2)$ $\quad$ $2 \Rightarrow 3$

$2 \Rightarrow 4$ $\quad$ $4 \Rightarrow 5$

$3 \Rightarrow 6$ $\quad$ $6 \Rightarrow 7$

$4 \Rightarrow 8$ $\quad$ $8 \Rightarrow 9$

$\vdots$ $\quad$ $\vdots$

Ex Nuggets in boxes of 4 or 7. Prove: for all $n \geq 18$, it is possible to order n nuggets.

$P(n)$ $\exists x, y \in \mathbb{Z}, [x \geq 0 \wedge y \geq 0 \wedge 4x + 7y = n]$

Want: 101 nuggets

Can go from 97 $\rightarrow$ 101

$P(18) \Rightarrow P(22)$ $\quad$ $P(22) \Rightarrow P(26)$

$P(19) \Rightarrow P(23)$ $\quad$ $P(23) \Rightarrow P(27)$

$P(20) \Rightarrow P(24)$ $\quad$ $P(24) \Rightarrow P(25)$

$P(21) \Rightarrow P(25)$

Proof: Let $P(n)$ be as before. Proceed by induction.

Base Case $P(18)$: $4(1)+7(2)=18$

$P(19)$: $4(3)+7(1)=19$

$P(20)$: $4(5)+7(0)=20$

$P(21)$: $4(0)+7(3)=21$

Induction Hypothesis: Let $k \in \mathbb{N}$, with $k \geq 18$. Assume $P(k)$.

Let $x, y \in \mathbb{Z}$ with $x, y \geq 0$ $\ni$ $4x+7y=k$.

Induction Step: We must prove $P(k+4)$.

Well, $k+4 = 4x+7y+4 = 4(x+1)+7y$. Note $x+1, y$ are non-negative are non-negative integers since x, y are.

Induction 4 Lyfe.

5.1. Set Builder

Let $A = \{7, \pi, -\log(3), \Delta\}$ $\quad |A| = 4$ (cardinality)

? How to describe the set of all even integers?

Set-builder Notation: { object : condition it satisfies }

$$\{n : n \in \mathbb{Z} \wedge 2 \mid n\}$$

$$\{n \in \mathbb{Z} : 2 \mid n\}$$

$$\{2n : n \in \mathbb{Z}\}$$

$$\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \wedge b \neq 0\right\}$$

Ex. Let A be set set of all odd perfect squares.

$$\{A \in \mathbb{Z} : \exists B \in \mathbb{Z}, A = (2b+1)^2\}$$

$$\{n^2 : n \in \mathbb{Z} \wedge 2 \nmid n\}$$

Let A, B be sets.

$A \cap B \overset{\text{defn}}{=} \{x : x \in A \wedge x \in B\}$ or $\{x \in A : x \in B\}$

likewise $A \cup B \overset{\text{defn}}{=} \{x : x \in A \vee x \in B\}$

$\wedge$ $\vee$ — statements / open sentence

$\cap$ $\cup$ — sets

(set) difference $A - B \overset{\text{defn}}{=} \{x : x \in A \wedge x \notin B\}$

sometimes we have an uber set $\mathcal{U}$ that we are viewing all our sets as living in. In this case, the complement of A,

written $\bar{A}$. is $U - A$ $C = \{x \in U : x \notin A\}$

Ex. $U = \{m \in \mathbb{Z} : 1 \leq m \leq 12\}$

$C = \{3, 5, 7, 10\}$

$D = \{1, 3, 6, 7, 8\}$

① Find $|C \cup D|$ $\quad C \cup D = \{3, 5, 7, 10, 1, 6, 8\}$

$|C \cup D| = 7.$

② Find $|C - \bar{D}|$

$\bar{D} = \{2, 4, 5, 9, 10, 11, 12\}$

$C - \bar{D} = \{3, 7\}$

$|C - \bar{D}| = 2$

Two sets A, B are called <u>disjoint</u> if $A \cap B = \emptyset$.

Ex. Let $A = \{2n : n \in \mathbb{Z}\}$

$B = \{x : x \in \mathbb{Z}, 2 \nmid x\}$

Let A, B be sets. We say A is a <u>subset</u> of B, written $A \subseteq B$, if $\forall x \in A, x \in B$.

Say A is a proper subset of B if $A \subsetneq B$ and $\exists x \in B, x \notin A$. ($B$ is (proper) superset of A).

Ex. Let $A = \{n \in \mathbb{N} : 4 \mid n - 3|\}$

$B = \{2k + 3 : k \in \mathbb{Z}\}$

Prove $A \subsetneq B$

Proof: We must prove $\forall x \in A, x \in B$, and $\exists x \in B, x \notin A$.

① Let $c \in A$. Then $c \in \mathbb{N}$ and $4 \mid c-3$. Let $d \in \mathbb{Z}$ such that $4d = c-3$. We must show that $c \in B$. We must show that $c = 2(\text{some int}) + 3$.

Well, $c = 4d+3 = 2(2d)+3$,
Therefore, $c \in B$, so $A \in B$.

② Note $5 \in B$ since $5 = 2(1)+3$ and $5 \notin A$ since $4 \nmid 5-3$.

Let A, B be sets:

$$A = B \iff A \subseteq B \text{ and } B \subseteq A.$$

Let $A = \{n \in \mathbb{N} : 4 \mid n-3\}$

"Prove $A=B$" ← Prove $A \subseteq B$ and $B \subseteq A$.

Ex. Let S, T be sets:

Prove $S = T \iff S \cup T \subseteq S \cap T$

Proof: We must prove:

① $S = T \Rightarrow S \cup T \subseteq S \cap T$

② $S \cup T \subseteq S \cap T \Rightarrow S = T$

② Assume $S \cup T \subseteq S \cap T$. We need to prove that $S \subseteq T$

and $T \subseteq S$. We only prove $S \subseteq T$ as both are similar.

Let $x \in S$. Then $x \in S \vee x \in T$. So $x \in S \cup T$.
Since $S \cup T \subseteq S \cap T$ and $x \in S \cup T$, we obtained that $x \in S \cap T$. So $x \in S \wedge x \in T$. So $x \in T$, so $x \subseteq T$.

① Assume $S = T$. So $S \subseteq T$ and $T \subseteq S$. We must prove that $S \cup T \subseteq S \cap T$.
Let $x \in S \cup T$. So $x \in S \vee x \in T$.
We assume $x \in S$ & the case $x \in T$ is similar.
Since $x \in S$ and $S \subseteq T$, then $x \in T$.
So $x \in S \wedge x \in T$, so $x \in S \cap T$.

---

6 Greates Common Divisor

Prop 6.1 $\forall x \in \mathbb{R}, x \leq |x|$

Prop 6.2 (Bound by Divisibility / BBD)

$$\forall a, b \in \mathbb{Z}, [(b \mid a \wedge a \neq 0) \Rightarrow b \leq |a|]$$

Proof: Let $a, b \in \mathbb{Z}$. Assume $b \mid a$ and $a \neq 0$. Let $c \in \mathbb{Z}$ such that $bc = a$.

Note $c \neq 0$ since $a \neq 0$. Thus $|c| \geq 1$. since $c \in \mathbb{Z}$
Then, $|a| = |bc| = |b||c| \geq |b|(1) = |b| \geq b$
↳ by 6.1.

Prop (Division Algorithm / DA) Let $a, b \in \mathbb{Z}$ with $b > 0$
There exist unique $q, r \in \mathbb{Z}$ such that

① $a = qb + r$
② $0 \leq r < b$

$\lfloor x \rfloor$: floor function
$\forall x \in \mathbb{R}$, $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$
Proof: Let $q = \lfloor \frac{a}{b} \rfloor$, let $r = a - qb$.

① $qb + r = qb + (a - qb) = a$
② We know $q \leq \frac{a}{b} < q + 1$
so $(\times b)$ $qb \leq a < qb + b$
so $0 \leq a - qb < b$
so $0 \leq r < b$

Let $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ $\ni$ $a = q_1 b + r_1$, $a = q_2 b + r_2$ and $0 \leq r_1 < b$ and $0 \leq r_2 < b$
Then, $q_1 b + r_1 = q_2 b + r_2$. Then $b(q_1 - q_2) = r_2 - r_1$. So $b \mid r_2 - r_1$.

Assume $r_2 - r_1 \neq 0$, BBD, $b \leq |r_2 - r_1|$

However, by $*$, $r_2 - r_1 \leq (b-1) - 0 < b$

Also, $r_2 - r_1 > -b$. So $|r_2 - r_1| < b$. Contradicted.

So $r_2 - r_1 = 0$, so $r_2 = r_1$. It follows that $q_1 = q_2$.

E.x. $105 = 12(8) + 9$

$\frac{105}{12} : (q, r) = (8, 9)$

$\frac{105}{8} : (q, r) = (13, 1)$

quo, rem when -21 is divided by 4?

$-21 = 4(-6) + 3$

E.x. Let $n \in \mathbb{Z}$. Apply DA with $n, 2$: there exist q, r such that $n = 2q + r$ and $\underbrace{0 \leq r < 2}_{r=0 \vee r=1}$

6. Greatest Common Divisor

Defn: Let $a,b \in \mathbb{Z}$, with $d \neq 0$.

d is a common divisor of a,b if $d|a$ and $d|b$.

d is the greatest common divisor of a,b, written $d = \gcd(a,b)$,

if: (1) d is a common divisor of a,b

(2) $\forall c \in \mathbb{Z}, [c|a \wedge c|b \Rightarrow c \leq d]$

- Define $\gcd(0,0) = 0$.

E.x. Let $a \in \mathbb{Z}$. $\gcd(a,a) = |a|$

$\gcd(a,0) = |a|$

E.x. Prove $\gcd(8,20) = 4$

Proof: ① Have $4|8 \wedge 4|20$

② Let $c \in \mathbb{Z}$, assume $c|8 \wedge c|20$.

By DIC, $c|8(-2) + 20(1)$, ie $c|4$.

By BBD, $c \leq 4$.

E.x. Let $a,b \in \mathbb{Z}$. Prove $\gcd(a,b) = \gcd(a, b+3a)$.

Proof: Let E be $\gcd(a,b)$, let $F = \gcd(a, b+3a)$.

Note $a=b=0 \iff a=b+3a=0$, and equality holds in this case. Assume a,b are not both 0. We know:

① $E \mid a \wedge E \mid b$

② $\forall c \in \mathbb{Z}, [c \mid a \wedge c \mid b \Rightarrow c \leq E]$

③ $F \mid a \wedge F \mid b+3a$

④ $\forall c \in \mathbb{Z}, [c \mid a \wedge c \mid b+3a \Rightarrow c \leq F]$

know $F \mid a \wedge F \mid b+3a$.

By DIC, $F \mid a(-3) + (b+3a)(1)$. ie. $F \mid b$.

So F is a common divisor of a, b.

So by ②, $F \leq E$.

Proving $E \leq F$ is similar, So $E = F$.

6.2 GCD

Prop (CCD WR) Let $a, b, q \in \mathbb{Z}$ with $a = bq + r$.

Then, $\gcd(a,b) = \gcd(b,r)$.

Ex. $407 = 33(12) + 11$

$\gcd(407, 33) = \gcd(33, 11)$ Euclidean Algorithm!

EE: Find $\gcd(126, 48)$.

$126 = 48(2) + 30$

$48 = 30(1) + 18$

$30 = 18(1) + 12$

$\gcd(126,48) = \gcd(48,30)$

$= \gcd(30,18)$

$= \gcd(18,12)$

$= \gcd(12,6)$

$= \gcd(6,0)$

$18 = 12(1) + 6$ $\quad\quad = 6$

$12 = 6(2) + 0$

E.x. Find $\gcd(66, 42) = 6$

$66 = 42(1) + 24$

$42 = 24(1) + 18$

$24 = 18(1) + 6$

$18 = 6(3) + 0$

$6 = 24 - 18(1)$

$= 24 - (42 - 24)(1)$

$= 24(2) + 42(-1)$

$= (66 - 42)(2) + (42)(-1)$

$= 66(2) + 42(-3)$

Bezout's Lemma: Let $a, b \in \mathbb{Z}$. Let $d = \gcd(a, b)$
The equation $ax + by = d$ has an integer soln.

E.x. $2x + 6y = 17$. No soln.

$2x + 6y = 10$. Has int soln.

note that 10 isn't $\gcd(2, 6)$.

6.3 GCD CT.

GCD Characterization Theorem (GCD CT)

Let $a, b \in \mathbb{Z}$.
If $d \geq 0$, $d \mid a$, $d \mid b$, and if $ax+by=d$ has a int solution, then $d = \gcd(a,b)$.

Proof: If $d=0$, then $a=b=0$, so result is true.
Assume $d \neq 0$. Let $r, s \in \mathbb{Z}$ such that $ar+bs=d$.
We must prove: $\forall c \in \mathbb{Z}, [c \mid a \wedge c \mid b \Rightarrow c \leq d]$
Let $c \in \mathbb{Z}$, assume $c \mid a \wedge c \mid b$. Then, by DIC, $c \mid a(r)+b(s)$ so $c \mid d$. By BBD, $c \leq |d| = d$ since $d \geq 0$.

E.x. $30(3)+42(-2)=6$
$6 \geq 0$, $6 \mid 30$, $6 \mid 42$
$30(x)+42y=6$ has an int solution.
$\therefore \gcd(30,42)=6$ by GCD CT.

E.x. Let $b \in \mathbb{Z}$. Prove $\gcd(b, b^2+1) = 1$.
Note $1 \geq 0$, $1 \mid b$, $1 \mid b^2+1$.
Also, $b(-b)+(b^2+1)(1)=1$
So, $bx+(b^2+1)y=1$ has a solution.
By GCDCT, $\gcd(b, b^2+1)=1$.

6.4. The extended Euclidean Algorithm

EEA (Extended Euclidean Algorithm)

↳ Does EE + BS at same time.

Ex. Do EEA for gcd(631, 251).
a, b

	x	y	r	q
row1	1	0	631	
row2	0	1	251	
row3				2
	c	d	e	= gcd(a,b)
			0	ax+by=e

For $n \geq 3$

1) q_n = quotient when r_{n-2} / r_{n-1}

2) $z_n = z_{n-2} - z_{n-1} q_n$

$z \in \{x, y, r\}$

while $(r_n \neq 0)$ {

1) q_n = quotient when r_{n-2} is divided by r_{n-1}

2) $z_n = z_{n-2} - q_n z_{n-1}$ where z all of x, y, r.

}

Ex. Let $d = \gcd(49, 119)$. Find d, and final a soln to $49x - 119y = d$

	x	y	r	q
row1	1	0	119	
row2	0	1	49	
row3	1	-2	21	2
z_n	-2	5	7	2

$119(-2) + 49(5) = 7$

calculation		0	3
			c

Ex.1 Let $x \in \mathbb{R}$, $x > 0$. Prove $(1+x)^n > 1 + nx$ $\forall\, n \geq 2$.

Rough Work: Assume $(1+x)^k > 1 + kx$

Show $(1+x)^{k+1} > 1 + (k+1)x$

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

Ex.2 Pf: Let $P(n)$ be $(1+x)^n > 1 + nx$. Proceed by Induction.

Base Case: must prove $(1+x)^2 > 1 + 2x$.

Well, $(1+x)^2 = 1 + 2x + x^2 > 1 + 2x$

↑ since $x > 0$

IH: Let $k \in \mathbb{N}$, assume $(1+x)^k > 1 + kx$

IS: We must prove $(1+x)^{k+1} > 1 + (k+1)x$

Well,

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

QED.

Ex.3 Prove $\forall a,b \in \mathbb{Z}, [a^2 \nmid b^2 \Rightarrow a \nmid b+2a^2]$

$$a^2 k_1 = b^3 \quad , \quad a k_2 = b + 2a^2$$

$$a^2 = \frac{b^3}{k_1} \qquad a k_2 = b + 2a^2$$

$$a = \frac{\sqrt{b^3}}{\sqrt{k_1}} \qquad \sqrt{\frac{b^3}{k_1}} \cdot k_2 = b + 2 \cdot \frac{b^3}{k_1}$$

$$a \mid b+2a^2 \Rightarrow a^2 \mid b^2$$

$$ak = b+2a^2 \Rightarrow a^2 k = b^2$$

Proof: Let $a,b \in \mathbb{R}$. Assume $a \mid b+2a^2$. We must prove $a^2 \mid b^3$

Soln ① We know that $a \mid a$. By DIC, $a \mid a(-2a) + (b+2a^2)(1)$. ie. $a \mid b$
Therefore, $a^2 \mid b^2$. Since $b^2 \mid b^3$, then by TD get $a^2 \mid b^3$.

$$ka = b \Rightarrow k^3 a^3 = b^3 \Rightarrow a^2 [ak^3] \mid b^3$$

Soln (2) Let $c \in \mathbb{Z} \Rightarrow ac = b + 2a^2$.

So $a[c-2a] = b$

$a^3[c-2a]^3 = b^3$

So $a^2[a(c-2a)^3] = b^3$

So $a^2 \mid b^3$

Review Question MIDTERM.

1) Prove $\forall a,b,c \in \mathbb{Z}\ [(a \nmid 3b \wedge a \mid b+12c) \Rightarrow a \nmid 9c]$

Proof: Prove by contrapositive.

$\forall a,b,c \in \mathbb{Z}, [\, a \mid 9c \Rightarrow (a \mid 3b \vee a \nmid b+12c)]$

Let $a,b,c \in \mathbb{Z}$, assume $a \mid 9c$. We must prove $a \mid 3b \vee a \nmid b+12c$.

Assume $a \mid b+12c$, we must prove $a \mid 3b$.

By DIC, $a \mid (b+12c)(3) + 9c(-4)$. ie $a \mid 3b$.

2) Proceed by contradiction.

Prove there do not exist integers p, q such that $p^2 + 8q = 35$.

Assume $p, q \in \mathbb{Z}$ which satisfy $p^2 + 8q = 35$.

Since $8q$ is even, 35 is odd, p must be odd.

Let p be $(2k+1)$ for some $k \in \mathbb{Z}$, then

$$(2k+1)^2 + 8q = 35$$

$$4k^2 + 4k + 1 + 8q = 35$$

$$4k^2 + 4k + 8q = 34$$

① Since $4 \mid 4k^2+4k+8q$, and $4 \nmid 34$, contradiction.

② $2k^2 + 2k + 8q = 17$

Since $(2k^2+2k+8q)$ is even, 17 is odd, contradiction.

3. P/D. $\forall x \in \mathbb{Z}, \underbrace{\exists y \in \mathbb{Z}, \forall z \in \mathbb{Z}, (y+x+2)(x-z) \geq 0}_{P(x)}$,

$P(7)$: $\exists y \in \mathbb{Z}, \underbrace{\forall z \in \mathbb{Z}, (y+9)(7-z) \geq 0}_{Q(y)}$, ✓

$Q(5)$: $\forall z \in \mathbb{Z}\ (14)(7-z) \geq 0$ ✗

$Q(11)$: $\forall z \in \mathbb{Z}\ (20)(7-z) \geq 0$ ✗

$Q(-9)$: $\forall z \in \mathbb{Z}\ (9-9)(7-z) \geq 0$ ✓

$P(1)$: $\exists y \in \mathbb{Z}, \forall z \in \mathbb{Z}\ (3+y)(1-z) \geq 0$

True: $y = -3$.

x	y
7	-9
1	-3
x	-(x+2)

It is true, we prove this: let $x \in \mathbb{Z}$. Let $y = -(x+2)$.
Let $z \in \mathbb{Z}$, we must prove that $(x+y+2)(x-z) \geq 0$
Well, $(x+y+2)(x-z) = (x+2-(x+2))(x-z)$
$= 0(x-z) = 0 \geq 0$

QED.

Define $b_1, b_2, b_3, \ldots$ as follows:

$b_1 = 2$
$b_2 = 7$
$b_n = 3b_{n-1} + 5b_{n-2}$ for $n \geq 3$.

Prove $b_n < 5^n$ For all $n \geq 1$.

Proof: Proceed by induction. Let $P(n)$ be $b_n < 5^n$
Base Case $P(1): b_1 = 2 < 4^1$
$P(2): b_2 = 7 < 4^2$

I.H Let $k \in \mathbb{N}$, assume $P(k) \wedge P(k+1)$. That is $b_k < 4^k$ and $b_{k+1} < 5^{k+1}$

I.S We must prove that $b_{k+2} < 5^{k+2}$
Well, $b_{k+2} = 3 \cdot b_{k+1} + 5b_k < 3 \cdot (5^{k+1}) + 5 \cdot 5^k$
$= 5^{k+1}(3+1)$
$< 5^{k+1} \cdot 5 = 5^{k+2}$

4. P/D

a) $\forall a,b \in \mathbb{N}\ (a \le b \Rightarrow a = 1)$ F

b) $\forall a \in \mathbb{N}\ ((\forall b \in \mathbb{N}, a \le b) \Rightarrow a = 1)$ T

c) $\forall a \in \mathbb{Z}\ ((\forall b \in \mathbb{N}, a \le b) \Rightarrow a = 1)$ F

d) $\forall a \in \mathbb{Z}\ ((\forall b \in \mathbb{Z}, a \le b) \Rightarrow a = 1)$ T

6.5 Further Properties of the GCD.

Proposition 7.C (Common Divisor Divides GCD (CDGCD)).
For all integers $a, b,$ and c, if $c \mid a \wedge c \mid b \Rightarrow c \mid \gcd(a,b)$

Proof: Choose $r, s \in \mathbb{Z} \ni ar + bs = d$. Since $c \mid a$, $c \mid b$, by DIC, $c \mid ar + bs$. ie $c \mid d$.

E.x.1. Let $Q(a,b,c)$ denotes "$ax^2 + by^2 = c$ has a solution"
Let $a, b, c \in \mathbb{Z}$, let $d = \gcd(a,b)$.

T/F: 1) $Q(a,b,c) \Rightarrow d \mid c$

2) $d \mid c \Rightarrow Q(a,b,c)$

1) Let r, s satisfies $ar^2 + bs^2 = c$. Since $d \mid a \wedge d \mid b$, then $d \mid c$ by DIC.

2)(F) Let $a=b=1$, $c=-1$. Then $d=1$.
$d \mid c$ (T), $Q(a,b,c)$ (F): $x^2+y^2=-1$ has no solution.

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

Prop 8 (Coprimeness Characterization Theorem (CCT)).
For all integers a and b, $\gcd(a,b)=1 \iff \exists\, s,t \in \mathbb{Z}$ $\ni as+bt=1$ has a solution.

Proof: $\Rightarrow$ True by Bezout's Lemma.
$\Leftarrow$ Since $1>0$, $1 \mid a$, $1 \mid b$, so $\gcd(a,b)=1$ by GCDCT.

E.x. $\Rightarrow$ True
$\Leftarrow$ False $3x+5y=2$ has a solution, but $\gcd(3,5) \neq 2$.

E.x. Let $a,b \in \mathbb{Z}$. Prove
$\gcd(a,bc)=1 \iff \gcd(a,b)=\gcd(a,c)=1$.

Proof: $\Rightarrow$
Let $r,s \in \mathbb{Z} \ni ar+(bc)s=1$.
Then $a(r)+b(cs)=1$
Thus $ax+by=1$ has a solution.
Thus $\gcd(a,b)=1$. Similar proof for $\gcd(a,c)=1$.

$\Leftarrow$ Let $m,n,r,s \in \mathbb{Z} \ni am+bn=1 \wedge ar+cs=1$.

Multiply them: $1 = 1 \cdot 1$

$= (am+bn)(ar+cs)$

$= a^2mr + acms + abrn + bcns$.

$= a(amr+cms+brn) + b(cns)$

So $ax+by=1$ has a soln. So $\gcd(a,bc)=1$.

Prop 9. Division by the GCD (DBG CD).
Let $a,b \in \mathbb{Z}$, not both zero. Let $d = \gcd(a,b)$.
$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Proof: Note $d \neq 0$ since a, b are not both zero. Also note $\frac{a}{d} \wedge \frac{b}{d} \in \mathbb{Z}$.

Choose $r,s \in \mathbb{Z} \ni ar+bs=d$.
Then $\left(\frac{a}{d}\right)r + \left(\frac{b}{d}\right)s = 1$.
So $\left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1$ has a solution, so $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Prop 10 (Coprimeness and Divisibility (CAD)).
Let $a b \in \mathbb{Z}$, $c \mid ab \wedge \gcd(a,c)=1 \Rightarrow c \mid b$.

Proof: Let $r,s \in \mathbb{Z} \ni ar+cs=1$.
Then $bar + bcs = b$
Since $c \mid ab$ and $c \mid c$,

by DIC then $c \mid b$.

Defn: Let $n \in \mathbb{N}$, $n \geq 2$. n is prime if $\forall c \in \mathbb{N}$, $[c \mid n \Rightarrow (c = 1 \text{ or } c = n)]$

$P(n)$

Prop (PF) Let $n \in \mathbb{N}$, $n \geq 2$, n may be written as a product of primes.

Proof: $P(2)$ is true. Let $k \in \mathbb{N}$, $k \geq 2$, assume $P(2), P(3) \ldots P(k) \ldots$

If $(k+1)$ is prime, we're done. Assume $k+1$ is composite.

Let $a, b \in \mathbb{Z} \ni k+1 = ab$ and $1 \leq a, b \leq k$.

By induction hypothesis, a, b are both a product of primes.

Therefore so is ab.

Theorem: (Euclid's Theorem) There are infinitely many primes.

Proof: Let $p_1, \cdots, p_n$ be a finite list of primes. We will prove there is a prime not on this list.

Let $N = (p_1 \cdot p_2 \cdot \ldots \cdot p_n) + 1$. Let q be a prime divisor of N.

When N is divided by q, the remainder is 0.

When N is divided by p_i, the remainder is 1.

So q is distinct for all from all the p_i's.

Prop: (Euclid's Lemma) Let $a, b, p \in \mathbb{Z}$ with p primes.

If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: Assume $p \mid ab$ and $p \nmid a$. Then $\gcd(a, p) = 1$

[since p is prime, get $\gcd(a, p) \in \{1, p\}$. It isn't

p since $p \nmid a$].

So by CAD, $p \mid b$.

Generalized Euclid Lemma: $p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_i$ for some i.

Unique Factorization Theorem (UFT) Let $n \in \mathbb{N}$, $n \geq 2$
Up to the order of the primes, n may be uniquely written as a product of primes.

$60 = 2 \cdot 2 \cdot 5 \cdot 3$ uniquely

UFT Let $n \in \mathbb{N}$, $n \geq 2$. $\exists\ k \in \mathbb{N}$, distinct primes $p_1, p_2, \ldots, p_k$, positive integers $a_1, a_2, \ldots, a_k$

such that $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$. This is unique up to the order of the p_i's, (and a_i's)

Theorem $\sqrt{3} \notin \mathbb{Q}$

Proof: Assume $\sqrt{3} = \frac{a}{b}$ for some $a, b \in \mathbb{N}$

Then $3b^2 = a^2$

Write $a = 3^{\alpha} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ where, $3, p_1, p_n$ are distinct primes.

$b = 3^{\beta} \cdot p_1^{b_1} \cdot \ldots \cdot p_m^{b_m}$

$a^2 = 3^{2\alpha} \cdot p_1^{2a_1} \cdot p_2^{2a_2} \cdots p_n^{2a_n}$ a^2 has even # of 3's

$3b^2 = 3^{2\beta+1} \cdot p_1^{2b_1} \cdot \ldots \cdot p_m^{2b_m}$ $3b^2$ has odd # of 3's

Contradiction UFT.

Prop (DFPF) Let $n \in \mathbb{N}$. Write $n = p_1^{a_1} \cdots p_k^{a_k}$ where the p_i's are distinct primes and a_i's non-negative integers. The positive divisors of n are precisely the numbers $p_1^{b_1} \cdots p_k^{b_k}$ where $0 \le b_i \le a_i$ for all i.

ex. $63 = 3^2 \cdot 7^1$ $\quad k=2$ $p_1 = 3$ $a_1 = 2$, $p_2 = 7$ $a_2 = 7$

$3^0 7^0, 3^1 7^0, 3^2 7^0, 3^0 7^1, 3^1 7^1, 3^2 7^1.$

$1 \quad 3 \quad 9 \quad 7 \quad 21 \quad 63$

E.x. How many multiples of 12 are divisors of 5880?

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

$5880 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^2$

Want $n \mid 5880 \wedge 12 \mid n$

$n \mid 5880 \Rightarrow n = 2^a \cdot 3^b \cdot 5^c \cdot 7^d$

$n > 0$

$0 \le a \le 3$	$12 \mid n \Rightarrow a \ge 2$
$0 \le b \le 1$	$b \ge 1$
$0 \le c \le 1$	$c \ge 0$
$0 \le d \le 2$	$d \ge 0$

Combine: $2 \le a \le 3$ (2) $\Rightarrow 2 \cdot 1 \cdot 2 \cdot 3 = 12$ such n.

$1 \le b \le 1$ (1)

$0 \le c \le 1$ (2)

$0 \le d \le 2$ (3)

GCD PF Let $a, b \in \mathbb{N}$ with $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$

with p_i's distinct primes.

Then $\gcd(a,b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot p_2^{\min\{\alpha_2 \beta_2\}} \cdot \ldots \cdot p_n^{\min\{\alpha_n, \beta_n\}}$

E.x. Find $\gcd(11(42000), 10!)$

$11(42000) = 2^4 \cdot 3^1 \cdot 5^3 \cdot 7^1 \cdot 11^1$

$10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^1 \cdot 11^0$

$\gcd(11(42000), 10!) = 2^4 \cdot 3^1 \cdot 5^2 \cdot 7^1 \cdot 11^0$

$= 8400$

Linear Diophantine Equations

DE: eqn when you only care about integer solutions.

$x^2 + y^2 = 50$

$x^2 + y^2 = z^2$

$x^n + y^n = z^n$

$4x + 7y = 15$ ← Linear DE in 2 Variables

Let $a, b, c \in \mathbb{Z}$. Consider eqn $ax+by=c$.

① Does the equation has a solution?

② If "yes" to ①, how to understand structure of all solns.

Ex i) $a=b=0$ ① soln $\iff c=0$

$0x+0y=c$ ② $c=0 \Rightarrow x, y$ any integers.

ii) $b=0$ $ax+0y=c$ ① soln $\iff a \mid c$

$a \neq 0$ ② $a \mid c \Rightarrow x = \frac{c}{a}$, y any $\mathbb{Z}$.

Theorem (LDET 1) Let $a, b, c \in \mathbb{Z}$. Let $d = \gcd(a, b)$

$ax + by = c \iff d \mid c$.

has solution

Proof $\Rightarrow$ Let $r, s \in \mathbb{Z} \ni ar+bs=c$.

Since $d \mid a \wedge d \mid b$, by DIC $d \mid ar+bs$, ie. $d \mid c$.

$\Leftarrow$ Let $k \in \mathbb{Z} \ni dk = c$.

Let $r, s \in \mathbb{Z} \ni ar+bs=d$.

Then $a(kr) + b(ks) = k[ar+bs] = kd = c$.

So $x=kr \wedge y=ks$ is a soln to $ax+by=c$.

E.x. $352x - 418y = 110$

x	y	r	q
1	0	418	0
0	1	352	0
1	-1	66	1
-5	6	22	5
		0	

So $\gcd(418, 352) = 22$

and $418(-5) + 352(6) = 22$

Since $22 \mid 110$, the eqn $352x - 418y = 110$ has a soln by LDET.

$\because 358(30) - 418(25) = 110$

$\therefore (x, y) = (30, 25)$ is a soln.

E.x $14x + 20y = 8$. Note $(2, -1)$ is soln.

claim: Another soln is $(2+20, -1-14) = (22, -15)$

Pf: $14(2+20) + 20(-1-14)$

$= 14(2) + 20(-1) + 14(20) + 20(-14)$

$= 8$

claim: Another soln is $(2+20(-3), -1-14(-3)) = (-58, 51)$

Pf: $14(2+20(-3)) + 20(-1-14(-3)) = 14(2) + 20(-1)$

$+14(20(-3))+20(-14(-3)) = 8$

claim: For all $n \in \mathbb{Z}$, $(2+20n, -1-14n)$ is a soln

Fact 1): $\forall n \in \mathbb{Z}$, $(2+10n, -1-7n)$ is a soln.

2): No other solns.

Theorem (LDET 2) Let $a, b \in \mathbb{Z}$, assume $a \neq 0 \wedge b \neq 0$. Let $g = \gcd(a,b)$.
Let (x_0, y_0) be an integer soln to $ax+by=c$. *
The set of all solns to * is

$\{x_0 + (\frac{b}{d})n, y_0 - (\frac{a}{d})n) : n \in \mathbb{Z}\}$ Set A

$14x + 20y = 8$

$a = 14, \ b = 20, \ d = 2$

$\frac{a}{d} = 7, \ \frac{b}{d} = 10 \quad (x_0, y_0) = (2, -1)$

Proof: Let $B = \{(r,s) : r \in \mathbb{Z} \wedge s \in \mathbb{Z} \wedge ar+bs = c\}$
We prove $A = B$.

We know $ax_0 + by_0 = c$
$B \subseteq A$: Let $(r,s) \in B$. So $r, s \in \mathbb{Z}$ and $ar+bs = c$.
Then $ar+bs = ax_0+by_0$
So $a(r-x_0) = -b(s-y_0)$. So $(\frac{a}{d})(r-x_0) = -(\frac{b}{d})(s-y_0)$

So $\frac{b}{d} \mid (\frac{a}{d})(r - x_0)$. By DBGCD, $\gcd(\frac{b}{d}, \frac{a}{d}) = 1$.

By CAD, $\frac{b}{d} \mid r - x_0$. Let $k \in \mathbb{Z} \ni (\frac{b}{d})k = r - x_0$.

So $r = x_0 + (\frac{b}{d})k$.

Also, $s = \frac{c - ar}{b} = \frac{c}{b} - \frac{a}{b}(x_0 + \frac{b}{d}k) = \frac{c}{b} - \frac{a}{b}x_0 - \frac{a}{d}k$

$= y_0 - \frac{a}{d}k$.

$r = x_0 + (\frac{b}{d})k$

$s = y_0 + (\frac{a}{d})k$. } shows $(r, s) \in A$.

Ex. $35x - 84y = 168$

Brandon:

x	y	r	q
1	0	84	
0	1	35	
1	-2	7	2
-2	5	7	2

$\gcd(35, 84) = 7$,

$35(5) - 84(2) = 7$

$35(120) - 84(48) = 7$

$$x = 120 - \left(\frac{-84}{7}\right)n = 120 + 12n$$
$$y = 48 + \left(\frac{35}{7}\right)n = 48 + 5n$$

Inspection: $(0,-2)$ is a soln and $\gcd(35,84) = 7$.

So general soln is: $x = 0 + \left(\frac{-84}{7}\right)n = -12n$ $\quad n \in \mathbb{Z}$

$y = 2 - \left(\frac{35}{7}\right)n = -2 - 5n$

E.x. Have bunch of 7¢ and 23¢. 550¢?

soln: $7x + 23y = 550$ $\quad (*)$

Turns out $\gcd(7,23) = 1$ and $7(10) + 23(-3) = 1$. So

$7(5500) + 23(-1650) = 550$.

General Solution to $(*)$ is $x = 5500 + 23n$ $\quad n \in \mathbb{Z}$

$y = -1650 - 7n$

Want $x \geq 0 \wedge y \geq 0$ $\quad n \in \mathbb{Z}$

$x \geq 0 \iff 5500 + 23n \geq 0 \iff 23n \geq -5500 \iff$

$n \geq -239.13\ldots \iff n \geq -239$

$y \geq 0 \iff -1650 - 7n \geq 0 \iff -1650 \geq 7n \iff n \leq -235.7$

$\iff n \leq -236$

$-239 \leq n \leq -236$

n	$x = 5500 + 23n$	$y = -1650 - 7n$
-236	72	2
-237	49	9
-238	26	16
-239	3	23

Chapter 8 Congruence & Modular Arithmetic.

Sometimes when dividing a by b, only care about remainder.

$$365 = 7(\ ) + 1$$

Turns out we can find remainders super fast.

Defn: Let $m \in \mathbb{N}$, let $a, b \in \mathbb{Z}$

Say a is congruent to b mod m, written

$$a \equiv b \bmod m$$

if $m \mid a-b$

E.x. $14 \equiv 6 \bmod 4$ $\quad$ $12 \not\equiv 19 \bmod 4$

$6 \equiv 14 \bmod 4$

E.x. $a \equiv b \bmod 4 \iff a-b$ is a multiple of 4.

$\iff a = b + (\text{multiple of } 4)$

E.x. Why $m \in \mathbb{N}$?

$a \equiv b \bmod -5 \iff a \equiv b \bmod 5$

$a \equiv b \bmod 0 \iff 0 \mid a-b \iff a-b = 0$

$\iff a = b$

E.x. Let $a, b \in \mathbb{Z}$. Prove $a \mid b \iff a^2 \mid b^2$

$\Leftarrow$ Assume $a^2 \mid b^2$. If $a = 0$, $0 \mid b$ is true.

If $b = 0$: $a^2 \mid 0 \Rightarrow a^2 = 0 \Rightarrow a = 0 \Rightarrow a \mid b$

Assume a and b are both non-zero. WLOG, assume $a \cdot b > 0$.

Write $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, p_i's are distinct primes

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, α_i's, β_i's are non-negative integers.

Since $a^2 \mid b^2$, we know $2\alpha_i \leq 2\beta_i \ \forall i$ by DFPF
Then $\alpha_i \leq \beta_i$ for all i. By DFPF, $a \mid b$

$(8 \bmod 3) \rightarrow$ Num in programming

$8 \equiv 2 \bmod 3 \rightarrow$ Statement

Prop ($\subset ER$) Let $a, b, c \in R$.

① $a \equiv a \bmod m$ (Reflexive)

② $a \equiv b \bmod m \rightarrow b \equiv a \bmod m$

③ $a \equiv b \bmod m \ \wedge \ b \equiv c \bmod m \Rightarrow$
$a \equiv c \bmod m$

- Divisibility is R, T, not S
-> is T, not R, not S

Moral $\equiv \bmod m$ is a lot like $=$.

Proof ③ Assume $a \equiv b \bmod m$ and $b \equiv c \bmod m$. So $m \mid a-b$ and $m \mid b-c$

by DIC, $m \mid a-b+b-c$, ie. $m \mid a-c$. So $a \equiv c \bmod m$.

Prop Let $a, b, c, d \in \mathbb{Z}$. Assume $a \equiv b \bmod m$ and $c \equiv d \bmod m$

Then ① $a+c \equiv b+d \bmod m$

② $a-c \equiv b-d \bmod m$

③ $ac \equiv bd \bmod m$

Proof ③ know $m \mid a-b$ and $m \mid c-d$. Show $m \mid ab-cd$.

Well, DIC, $m \mid (a-b)c + (c-d)b$, ie. $m \mid ac-bd$

E.X. This tells us that if $a \equiv b \bmod m$ then $3a \equiv 3b \bmod m$

$$\left.\begin{array}{l} a \equiv b \bmod m \\ 3 \equiv 3 \bmod m \end{array}\right\} 3a \equiv 3b \bmod m$$

Corollary For all $a_1, \dots a_n, b_1, \dots b_n, b_n \in \mathbb{Z}$, if $(a_i \equiv b_i \bmod m$ for all i)

then ① $a_1 + \dots + a_n \equiv b_1 + \dots + b_n \bmod m$

② $a_1 \times \dots \times a_n \equiv b_1 \times \dots \times b_n \bmod m$

↳ Convergence of Addition & Multiplication

Ex $15 \equiv 1 \mod 7$
$15 \equiv 1 \mod 7$
$15 \equiv 1 \mod 7$
$15 \equiv 1 \mod 7$
$\Rightarrow 15^4 \equiv 1^4 \mod 7$
$\therefore 15^4 \equiv 1 \mod 7$

Corollary (CP) If $a \equiv b \mod m$ then, $\forall n \in \mathbb{N}$, $a^n \equiv b^n \mod m$

Ex. Determine Whether $7 \mid 5^9 + 62^{2000}$

Soln $62 \equiv -1 \mod 7$
$\Rightarrow 62^{2000} \equiv -1^{2000} \mod 7$
$\equiv 1 \mod 7$

$5 \equiv -2 \mod 7$
$5^9 \equiv -2^9 \mod 7 \equiv [(-2)^3]^3 \mod 7$
$\equiv (-8)^3 \mod 7 \quad (-8 \equiv -1 \mod 7)$
$\equiv (-1)^3 \mod 7$
$\equiv -1 \mod 7$

$\boxed{62^{2000} + 5^9} \equiv 1 + -1 \mod 7 \equiv \boxed{0} \mod \boxed{7}$
$\Rightarrow 7 \mid 62^{2000} + 5^9 - 0$
$\Rightarrow 7 \mid 62^{2000} + 5^9$

☆ $a \equiv b \mod m \Rightarrow m \mid a - b$

False: $a \equiv b \mod m \Rightarrow c^a \equiv c^b \mod m$
$5 \equiv 1 \mod 4 \not\Rightarrow 2^5 \equiv 2^1 \mod 4$

$19 \equiv 3 \mod 8 \Rightarrow 19^7 \equiv 3^7 \mod 8$

$\forall a,b,c \in R, [ab = ac \wedge a \neq 0 \Rightarrow b = c]$

$9(3) \equiv 1(3) \mod 6 \not\Rightarrow 9 \not\equiv 1 \mod 6$ because $\gcd(3,6) \not\equiv 1$

Prop (CD) Let $a,b,c \in \mathbb{Z}$
If $ab \equiv ac \mod m$ and $\gcd(a,m) = 1$, then $b \equiv c \mod m$.

Proof Assume $ab \equiv ac \mod m$
So $m \mid ab - ac$
so $m \mid a(b-c)$
(AD) $\Rightarrow m \mid b-c$
$\Rightarrow b \equiv c \mod m$

Prop (CISR) Let $a,b \in \mathbb{Z}$
$a \equiv b \mod m \iff a,b$ have the same remainder when divided by m.

Proof $\Leftarrow$ Write $a = q_1 m + r$, $b = q_2 m + r$ for some $q_1, q_2, r \in \mathbb{Z}$, $0 \leq r < m$.

So $a-b = q_1 m + r - (q_2 m + r) = m(q_1 - q_2)$

So $m \mid a-b$, so $a \equiv b \bmod m$.

$\Rightarrow$ Assume $a \equiv b \bmod m$

Write $a = q_1 m + r_1$, for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with
$b = q_2 m + r_2$ $\quad 0 \leq r_1, r_2 < m$.

$$\begin{aligned} \text{So } r_1 - r_2 &= (a - q_1 m) - (b - q_2 m) \\ &= (a - b - q_1 m + q_2 m) \\ &= \underbrace{(a-b)}_{m \mid (a-b)} + \underbrace{m(q_2 - q_1)}_{m \mid m(q_2 - q_1)} \end{aligned}$$

By DIC, $m \mid r_1 - r_2$
Note, $-m < r_1 - r_2 < m$
$\Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2$

Corollary (CRT) Let $a, b \in \mathbb{Z}$ with $0 \leq b < m$

$a \equiv b \bmod m \iff a$ has remainder b when dividing by m.

Proof: Note $b = 0(m) + b \wedge 0 \leq b < m$
So b has remainder b when divided by m.

By CISR, $a \equiv b \bmod m \iff a, b$ have some remainder.
$\iff a$ have remainder b.

PL: 22 mod 8,
number, 6

M135: $22 \equiv 6 \bmod 8 \wedge 0 \leq 6 < 8$
22 has a remainder 6 when divides by 8.

$3 \mid 1462 \iff 3 \mid 1+4+6+2+1$
$\iff 3 \mid 14$ False

Prop $3 \mid abcd \iff 3 \mid a+b+c+d$
$10 \equiv 1 \bmod 3$

Proof: $3 \mid abcd \iff abcd \equiv 0 \bmod 3$
$\iff 10^3 a + 10^2 b + 10^1 c + 10^0 d \equiv 0 \bmod 3$
$\iff 1^3 \cdot a + 1^2 b + 1^1 c + d \equiv 0 \bmod 3$
$\iff 3 \mid a+b+c+d$

$9 \mid abcd \iff 9 \mid a+b+c+d$ $(10 \equiv 1 \bmod 9)$

Prop $11 \mid ABCDE \iff 11 \mid E-D+C-B+A$
$\iff 10^4 A + 10^3 B + 10^2 C + 10D + E \equiv 0 \bmod 11$
$\iff (-1)^4 A + (-1)^3 B + (-1)^2 C + (-1)D + E \equiv 0 \bmod 11$
$\iff E - D + C - B + A \equiv 0 \bmod 11$

$\iff 11 \mid A - B + C - D + E$

$7 \mid 128 - 092 + 46 \iff 7 \mid 82$

key fact: $7 \cdot 11 \cdot 13 = 1001 = 10^3 - 1$

$\Rightarrow 7 \mid 10^3 + 1 \Rightarrow 10^3 \equiv -1 \bmod 7$

$7 \mid 1456$ True $\iff 7 \mid 145 - 2 \times 6$

$\iff 7 \mid 133$

$\iff 7 \mid 13 - 2 \times 3$

$\iff 7 \mid 7$ True

Prop $7 \mid ABCD \iff 7 \mid ABC - 2 \times D$

Proof $7 \mid ABCD \iff 10^3 A + 10^2 B + 10^1 C + D \equiv 0 \bmod 7$

$\iff 10^3 A + 10^2 B + 10^1 C + D - 21D \equiv 0 \bmod 7$

$\iff 10(10^2 A + 10B + (C - 2D)) \equiv 0 \bmod 7$

$\gcd(10, 7) = 1 \iff 10^2 A + 10B + C - 2D \equiv 0 \bmod 7$

$\iff 7 \mid ABC - 2D$

Solve $4x \equiv 6 \bmod 10$ } Linear Congruence Theorem

$4x \equiv 6 \bmod 10 \iff 10 \mid 4x - 6$ has a soln

$\iff 10y = 4x - 6$ has a soln

$\Leftrightarrow 4x' - 10y = 6$ has a soln.

A soln to $4x - 10y = 6$ is $x_0 = 4$, $y_0 = 1$

$\therefore$ General soln: $x = 4 - (-\frac{10}{2})n = 4 + 5n$

$y = 1 + (\frac{4}{2})n = 1 + 2n$

Soln to $4x \equiv 6 \bmod 10$ is $x = 4 + 5n$, $n \in \mathbb{Z}$

Equivalently, Soln to $4x \equiv 6 \bmod 10$ is

$x \equiv 4 \bmod 5$

Make our answer mod 10?

$\therefore$ $x \equiv 4 \bmod 10$

$x \equiv 9 \bmod 10$

Theorem: (Linear Congruence Theorem) (LCT = LDET1 + LDET2)

Let $m \in \mathbb{N}$, let $a, c \in \mathbb{Z}$, $a \neq 0$. Consider, $ax \equiv c \bmod m$.

① ** has soln $\Leftrightarrow \gcd(a, m) \mid c$

② Suppose x_0 is a soln to **. Let $d = \gcd(a, m)$.

Here are two ways to describe full soln of **.

(i) (1 soln mod $\frac{m}{d}$) $\quad x \equiv x_0 \bmod \frac{m}{d}$

(ii) (d soln mod m) $\quad x \equiv x_0 \bmod m$

$x \equiv x_0 + \frac{m}{d} \bmod m$

$x \equiv x_0 + 2(\frac{m}{d}) \bmod m$

$$x \equiv x_0 + (d-1)\left(\frac{m}{d}\right) \bmod m$$

E.x. $15x \equiv 20 \bmod 35$

Let $d = \gcd(15, 35) = 5$, $5 \mid 20$, has soln.

One solution is $x_0 = 6$.

Two ways to write complete sdns.

(i) $x \equiv 6 \bmod 7$ (1 soln mod 7)

(ii) $x \equiv 6 \bmod 35$

$x \equiv 6+7 \bmod 35$

$x \equiv 6+2(7) \bmod 35$

$x \equiv 27 \bmod 35$

$x \equiv 34 \bmod 35$

Let z be a soln to (**)

So $z = 6 + 7k$ for some $k \in \mathbb{Z}$.

Write $k = 5q + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r \le 5$.

So $r \in \{0, 1, 2, 3, 4\}$

r	z
0	$z = 6 + 7(5q) = 6 + 35q$

1	$z = 6 + 7(5q+1) = 13 + 35q$
2	$z = 20 + 35q$
3	$z = 27 + 35q$
4	$z = 34 + 35q$

E.X. Solve: $x \equiv 13 \mod 8$

Already solved!

E.X. Solve $7x \equiv 2 \mod 10$

Let $d = \gcd(7, 10) = 1$. So has a soln.

$$7x \equiv 2 \mod 10$$

$$\Updownarrow$$

$$7x \equiv 42 \mod 10 \iff x \equiv 6 \mod 10$$

(i) 1 soln mod $\frac{m}{d}$

(ii) d soln mod m

$\Big\rangle$ same!

Find soln to $ax \equiv c \mod m$

① Find soln to $ax - my = \gcd(a, m)$

② Scale up to $ax - my = c$

① $9x \equiv 3 \bmod 15$ has soln $\iff 3 \mid 15$ ✓

② $X_0 = 2$

i) $x \equiv 2 \bmod \frac{15}{3} \rightarrow x \equiv 2 \bmod 5$

ii) $x \equiv 2 \bmod 15$

$x \equiv 7 \bmod 15$

$x \equiv 12 \bmod 15$

Non-Linear Congruence

Ex. Solve $x^2 \equiv 6 \bmod 10$

TLDR Trial / Error

Let $y \in \mathbb{R}$. Write $y = 10q + r$ with $0 \leq r \leq 9$

Suppose r is a soln to $x^2 \equiv 6 \bmod 10$. Then so is y:

$y \equiv r \bmod 10$

$y^2 \equiv r^2 \bmod 10$

$r^2 \equiv 6 \bmod 10$

Transitive $\Rightarrow y^2 \equiv 6 \bmod 10$

$\Rightarrow y$ soln also

$x \bmod 10$	0	1	2	3	4	5	6	7	8	9		
$x^2 \bmod 10$	0	1	4	9	6	5	6	9	4	1		

Solns are $x \equiv 4 \bmod 10$

$x \equiv 6 \bmod 10$

Test 2 Line

Congruence Classes

Defn: Let $m \in \mathbb{N}$, let $a \in \mathbb{Z}$. The congruence class of a mod m, write $[a]$ or $[a]_m$, is the set

$$\{x \in \mathbb{Z},\ x \equiv a \bmod m\}$$

Ex $m=4$ $[18] = \{x \in \mathbb{Z},\ x \equiv 18 \bmod 4\}$

$= \{\ldots, 10, 14, 18, 22, 26\}$

$= \{18+4k : k \in \mathbb{Z}\}$

$[3] = \{x \in \mathbb{Z},\ x \equiv 3 \bmod 4\}$

$= \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

$= \{3+4k,\ k \in \mathbb{Z}\}$

$[2] = \{x \in \mathbb{Z},\ x \equiv 2 \bmod 4\}$

$= \{x \in \mathbb{Z},\ x \equiv 18 \bmod 4\}$

$= [18]$

- each b gives a mod 4 congruence class, but there are only 4 mod 4 congruence classes.

More generally, $[a] = [b] \iff a \equiv b \bmod m$
$([a]_m = [b]_m)$

CC pros / cons

pro: get to use $=$ again
cons: objects that are equals are sets, not numbers.

Defn: Let $m \in \mathbb{N}$. The integers mod m, written $\mathbb{Z}_m$, is the set of all mod m congruence classes.

Ex. $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

$[12] \in \mathbb{Z}_5$: $[12] = [2]$
$[-39] \in \mathbb{Z}_5$: $[-39] = [1]$

yet $|\mathbb{Z}_5| = 5$

$[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$

$[1] \cap [2] = \emptyset$

$[3]_5 \supsetneq [3]_{10}$

Proof: Let $x \in [3]_{10}$. So $x \equiv 3 \bmod 10$

So $10 \mid x-3$. By TD, since $5 \mid 10$, $5 \mid x-3$.

So $x \in 3 \bmod 5$, so $x \in [3]_5$

Proper since $8 \in [3]_5$ and $8 \notin [3]_{10}$

Ex $[4]_7$ $[4]_9$

$11 \in [4]_7$, $11 \notin [4]_9$

$13 \in [4]_9$, $13 \notin [4]_7$

$4 \in [4]_7$, $4 \in [4]_9$ → not disjoint

Ex. $[2]_5 = [2]_{15} \cup [7]_{15} \cup [12]_{15}$

Ex. Solve ① $6x+2y+22z \equiv 7 \bmod 23$

② $x+21y+z \equiv 6 \bmod 23$

③ $4x+6y+z \equiv 9 \bmod 23$

- add ①②: $\Rightarrow 7y \equiv 13 \bmod 23$

$\Rightarrow y \equiv 15 \bmod 23$

② $15+21y+z \equiv 6 \bmod 23$

③ $60+6y+z \equiv 9 \bmod 23$

② $21y+z \equiv 14 \bmod 23$

③ $6y+z \equiv 18 \bmod 23$

② - ③ : $15y \equiv 19 \bmod 23$

$\Rightarrow y \equiv 12 \bmod 23$

③ : $z \equiv 9 - 4x - 6y \bmod 23$

$\equiv 9 - 4(15) - 6(12) \bmod 23$

$\equiv 15 \bmod 23$

$23(-3) + 7(10) = 1$

$23(-39) + 7(130) = 13$

$23 \mid 7(130) - 13$

$7(130) \equiv 13 \bmod 23$

$x \equiv 130 \bmod 23$

$x \equiv 15 \bmod 23$

$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$

$[4] = \{x \in \mathbb{Z} : x = 4 \bmod 6\}$

$[a] = [b] \Leftrightarrow a \equiv b \bmod 6$

Defn: Let $[a], [b] \in \mathbb{Z}_m$

$[a] + [b] \overset{\text{defn}}{=} [a+b]$

$[a] \cdot [b] \overset{\text{defn}}{=} [a \cdot b]$

E.x. In $\mathbb{Z}_7$, calculate $[4][5]$

B $[4][5] = [4(5)] = [20]$ $(= [6])$

S $[4] = [18]$

Same

$[5] = [-2]$ $[4][5] = [18][-2] = [36] (= [6])$

Given: $4 \equiv 18 \bmod 7$

$5 \equiv -2 \bmod 7$

$20 \equiv -36 \bmod 7$

E.x. Additional table for $\mathbb{Z}_4$

	$[0]$	$[1]$	$[2]$	$[3]$	
$[0]$	$[0]$				
$[1]$				$[0]$	
$[2]$		$[3]$	$[0]$		
$[3]$				$[2]$	

$ax \equiv c \bmod m$

$\hookrightarrow [a][x] = [c]$ in $\mathbb{Z}_m$

$[ax]$

MAT (cc version of LCT) Let $m \in \mathbb{N}$, let $a, c \in \mathbb{Z}$, let $d = \gcd(a, m)$. Consider the eqn $[a][x] = [c]$ in $\mathbb{Z}_m$.

① has soln $\Leftrightarrow$ $d \mid c$

② If $[x_0]$ is one soln, the complete soln is

$[x_0], [x_0 + \frac{m}{d}], \ldots, [x_0 + (d-1)\frac{m}{d}]$ (in $\mathbb{Z}_m$)

Ex. In $\mathbb{Z}_{99}$, solve $[24][x] = [39]$

Soln Solve $24x \equiv 39 \bmod 99$.

Here, $m = 99$, $d = 3$, so $\frac{m}{d} = 33$.

EEA $\Rightarrow$ a soln is $x_0 = -52$.

So complete soln is:

$[-52], [-52+33], [-52+2(33)]$.

(or $[14], [47], [80]$)

$[0]$ is the additive identity of $\mathbb{Z}_m$

$[-a]$ is the additive inverse of $[a]$ (MI)

$[1]$ is the multiplicative identity of $\mathbb{Z}_m$

If $[a][b] = [1]$, say $[a], [b]$ are multiplicative inverses.

Ex. In $\mathbb{Z}_{10}$: $[3], [7]$ are MI's, since $[3] \cdot [7] = [21] = [1]$

$[4]$ has no MI's.

Does $[a]$ have a MI in $\mathbb{Z}_m$?

(corollary (Inv $\mathbb{Z}_m$) $[a]$ has a MI in $\mathbb{Z}_m \iff \gcd(a, m) = 1$

Proof: $[a]$ has a MI in $\mathbb{Z}_m \iff [a][x] = [1]$ has a soln in $\mathbb{Z}_m$

$\iff \gcd(a, m) \mid 1$

$\iff \gcd(a, m) = 1$

Cor (Inv $\mathbb{Z}_p$) (p primes). If $[a] \neq [0]$ then $[a]$ has a MI in $\mathbb{Z}_p$.

Proof: $[a] \neq [0] \Rightarrow a \not\equiv 0 \bmod p \Rightarrow p \nmid a \Rightarrow \gcd(a,p) = 1$.

E.x.

$[a] \in \mathbb{Z}_{14}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
MI?	X	[1]	X	[5]	X	[3]	X	X	X	[11]	X	[9]	X	[13]

$[a] \in \mathbb{Z}_{11}$	0	1	2	3	4	5	6	7	8	9	10
MI?	X	[1]	[6]	[4]	[3]	[9]	[2]	[8]	[7]	[5]	[10]

E.x. $7x \equiv 2 \bmod 10$

we know $7(3) \equiv 1 \bmod 10$

$\rightarrow 21x \equiv 6 \bmod 10 \Rightarrow x \equiv 6 \bmod 10$

Fermat Little Theorem (FLT)

$20^6 \equiv 1 \mod 7$

$19^{16} \equiv 1 \mod 17$

$58^{22} \equiv 1 \mod 23$

Let p be a prime. Let $a \in \mathbb{Z}$ $\ni$ $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$.

Proof: Consider following 2 lists.

L_1: $a, 2a, 3a, \ldots (p-1)a$.

L_2: $1, 2, 3, \ldots, p-1$

Proof has 2 steps:

① Every member of list 1 is $\equiv$ mod p to exacty 1 member of list 2, and vice versa.

② Profit! (using step ①)

Proof ① Let $1 \leq k \leq p-1$, we'll show $ka \not\equiv 0 \mod p$.

Assume $ka \equiv 0 \mod p$, then $p \mid ka$. By EA, $p \mid k$ or $p \mid a$.

Know $p \nmid a$. Since $1 \leq k \leq p-1$, also know $p \nmid k$. So $ka \not\equiv 0 \mod p$.

Let $1 \leq m, n \leq p-1$, assume $am \equiv an \mod p$.

Then, $p \mid a(m-n)$. By EL, $p \mid (m-n)$ or $p \mid a$, since $p \nmid a$, then $p \mid m-n$. Since $-p < m-n < p$, get $m-n = 0$, so $m = n$.

This shows that different members of L_1 go to different members of L_2. But L_1 and L_2 have the same length. So every member of L_2 is "hit" from a member of L_1.

② By ①, the product of all members of $L1$ is congruent mod p to the product of all members of $L2$.

So, $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \bmod p$.

$$(p-1)! \cdot a^{(p-1)} \equiv (p-1)! \bmod p$$

Since p is a prime, $\gcd(p, (p-1)!) = 1$

By Congruence Division, $a^{p-1} \equiv 1 \bmod p$

Cor Let p be prime, let $a \in \mathbb{Z}$. Then $a^p \equiv a \bmod p$

Proof: Either $p \mid a$ or $p \nmid a$.

If $p \mid a$, then $a \equiv 0 \bmod p$, then $a^p \equiv 0^p \bmod p$

$\equiv 0 \bmod p$.

So $a^p \equiv a \bmod p$

If $p \nmid a$, then by FLT, $a^{p-1} \equiv 1 \bmod p$. Multiply by a gives $a^p \equiv a \bmod p$.

E.x. Find the remainder when 9^{101} is divided by 13.

By FLT, $9^{12} \equiv 1 \bmod 13$

Write $101 = 12(8) + 5$

$$9^{101} = 9^{12(8)+5} = (9^{12})^8 + 9^5 \equiv 1^8 + 9^5 \bmod 13$$
$$\equiv 9^5 \bmod 13$$

$9^2 = 81 \equiv 3 \bmod 13$

So $9^5 = 9^4 9^1 = (9^2)^2 9^1 \equiv 3^2 9^1 \bmod 13 \equiv 9^2 \bmod 13$
$\equiv 3 \bmod 13$

E.x 2. Pattern for $3^1, 3^2, 3^3, \ldots, \bmod 5$

Know $3^4 \equiv 1 \bmod 5$

Let $x \in \mathbb{N}$, $x \equiv 0 \bmod 4 \vee x \equiv 1 \bmod 4$
$x \equiv 2 \bmod 4 \vee x \equiv 3 \bmod 4$

↳ $x = 3 + 4k$

$$3^x = 3^{(3+4k)} = 3^3 (3^4)^k \equiv 3^3 \cdot 1^k \bmod 5$$
$$\equiv 3^3 \bmod 5$$

Let $p = 14689237123$ Is a prime?

① (Brute force) Test if $n \mid p$ for all $2 \le n \le \sqrt{p}$

② (Probability) Is $5^{p-1} \equiv 1 \bmod p$. No $\Rightarrow$ p composite.

Is $12^{p-1} \equiv 1 \bmod p$. No $\Rightarrow$ p composite.

E.x. ① $x \equiv 3 \bmod 4$
② $x \equiv 2 \bmod 7$
} Solve simultaneous congruence.

① $x = 3 + 4a$ sub to ②

$3 + 4a \equiv 2 \bmod 7$

$4a \equiv 6 \bmod 7$

5 is a solution.

By LCT $a \equiv 5 \bmod 7$ (complete soln)

$a = 5 + 7b$

$x = 3 + 4(5 + 7b) = (23 + 28b)$

$x \equiv 23 \bmod 28$

Theorem: Chinese Remainder Theorem (CRT) Sunzi

Let $m_1, m_2 \in \mathbb{N}$ with $\gcd(m_1, m_2) = 1$. Let $a_1, a_2 \in \mathbb{Z}$.

Consider system $x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

① There is a soln

② The soln is unique mod $m_1 \cdot m_2$: that is, if x_0 is one soln, the full soln is $x \equiv x_0 \mod m_1 m_2$.

E.x. $x \equiv \quad \mod 12$

$x \equiv \quad \mod 7$

$x \equiv 4 \mod 12$	$x \stackrel{?}{\equiv} 5 \mod 7$
4	x
16	x
28	x
40	✓

40 is a soln.

CRT: Full soln: $x \equiv 40 \mod 12 \cdot 7$

$x \equiv 40 \mod 84$

E.x. Robert has N chocolate's (c's)

When given equally to 3 students, 2 remain. $N \equiv 2 \bmod 3$

When given equally to 5 students, 3 remain. $N \equiv 3 \bmod 5$

When given equally to 8 students, 6 remain. $N \equiv 6 \bmod 8$

Smallest possible N? Pro: Start with biggest mod.

③ $N = 6 + 8a \rightarrow$ ②:

$6 + 8a \equiv 3 \bmod 5$

$3a \equiv 2 \bmod 5$

LCT $\Rightarrow a \equiv 4 \bmod 5$

$\Rightarrow a = 4 + 5b$

So $N = 6 + 8(4 + 5b) = 38 + 40b \rightarrow$ ①

$38 + 40b \equiv 2 \bmod 3$

$b \equiv 0 \bmod 3$

$b = 3c$

So $N = 38 + 40(3c)$

$N \equiv 38 \bmod 120$

G CRT: Let $m_1, m_2, \ldots, m_k \in \mathbb{N}$ with $\gcd(m_i, m_j) = 1$ for all $i \neq j$. Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Consider the system

$x \equiv a_1 \bmod m_1$

$x \equiv a_2 \bmod m_2$

$\vdots$

$x \equiv a_k \mod m_k$

① System has a soln
② If x_0 is a soln, full soln is
$x \equiv x_0 \mod (m_1 m_2 \cdots m_k)$

E.x (Chocolate trial/error)

$N \equiv 6 \mod 8$	$N \equiv 3 \mod 5$	$N \equiv 2 \mod 3$
6	X	
14	X	
22	X	
30	X	
38	✓	✓

38 is a soln. GCRT ⇒ full soln.
$x \equiv 38 \mod 120$.

E.x. $3x \equiv 2 \mod 7$ $\xrightarrow{\times 3}$ $x \equiv 3 \mod 7$ ①

$2 + 5x \equiv 6 \mod 9$

$5x \equiv 4 \mod 9$ $\xrightarrow{\times 2}$ $x \equiv 8 \mod 9$ ②

17 is a soln to ① ∧ ②, so

$x \equiv 17 \bmod 63$: full soln.

E.x. $x \equiv 4 \bmod 6 \rightarrow x = 4+6a$

$x \equiv 5 \bmod 8$

$\rightarrow 4+6a \equiv 5 \bmod 8$

$6a \equiv 1 \bmod 8$ $\gcd(6,8) \nmid 1$

No soln by LCT.

E.x. • $x \equiv 4 \bmod 6 \rightarrow x = 4+6a$

• $x \equiv 6 \bmod 8$

• $4+6a \equiv 6 \bmod 8$

• $6a \equiv 2 \bmod 8$

one soln : $a = -1$

full soln : $a \equiv -1 \bmod 4$

$\Rightarrow a = -1+4b$

So • $x = 4+6a = 4+6(-1+4b) = -2+24b$

so $x \equiv -2 \bmod 24 \rightarrow \frac{8 \cdot 6}{\gcd(8,6)}$

$x \equiv 22 \bmod 24$ 4通

E.x. $45x - 120y = 30$

x	y	r	q
1	0	120	☹

0	1	45	120
1	-2	30	2
-1	3	15	1
			2

$\gcd(120, 45) = 15$ and

$120(-1) + 45(3) = 15$

$120(-2) + 45(6) = 30$

$45(6) - 120(2) = 30$

$x_0 = 6$, $y_0 = 2$

$x = 6 + -8n$

$y = 2 - 3n$

$\gcd(m_1, m_2) = 1$

CRT: The system $x \equiv a_1 \bmod m_1$, $x \equiv a_2 \bmod m_2$ has a soln.

If x_0 is a soln, full soln is $x \equiv x_0 \bmod m_1 m_2$

E.x. $x \equiv 4 \bmod 16$

$x \equiv 4 \bmod 13$

4 is a soln!

CRT $\Rightarrow$ full soln is $x \equiv 4 \bmod 78$

Corollary (Splitting Modulus Theorem) (SMT)

Let $m_1, m_2 \in \mathbb{N}$ with $\gcd(m_1, m_2) = 1$. Let $a, b \in \mathbb{Z}$.

① (Book) System $x \equiv b \bmod m_1$, $x \equiv b \bmod m_2$ and $x \equiv b \bmod m_1 m_2$ has the same solution.

② (R.G) $a \equiv b \bmod m_1 \wedge a \equiv b \bmod m_2 \iff a \equiv b \bmod m_1 m_2$

Proof ②: $\Leftarrow$ Duh

$\Rightarrow$ Assume $a \equiv b \bmod m_1 \wedge a \equiv b \bmod m_2$. Consider system $x \equiv b \bmod m_1$, $x \equiv b \bmod m_2$

$a \wedge b$ are both solns. By CRT, $a \equiv b \bmod m_1 m_2$

E.x. Solve $x^2 \equiv 16 \bmod 77$

Soln 1 Check 0 - 76 (Horrible)

Soln 2 Note $77 = 7 \times 11$ and $\gcd(7,11) = 1$

Let's solve $\underbrace{x^2 \equiv 16 \bmod 7}_{①}$, and $\underbrace{x^2 \equiv 16 \bmod 11}_{②}$

①: Soln are 3, 4. Show these are only solns: assume $a^2 \equiv 16 \bmod 17$.

Then $7 \mid a^2 - 16$. $7 \mid (a-4)(a+4)$, by EL,

$7 \mid a-4$ or $7 \mid a+4$.

Therefore $a \equiv 4 \bmod 7$ or $a \equiv -4 \bmod 7$

$a \equiv 3 \bmod 7$.

②: The sdn are $x \equiv 4 \bmod 11$ or $x \equiv 7 \bmod 11$

Now, we "glue" (un-split): given that $x^2 \equiv 16 \bmod 77$, one of 4 following is true.

$x \equiv 4 \bmod 7$ ∨ $x \equiv 4 \bmod 7$ ∨

$x \equiv 4 \bmod 11$ $x \equiv 7 \bmod 11$

⇓ ⇓

CRT: $x \equiv 4 \bmod 77$ $x \equiv 18 \bmod 77$

has 18 ⇒ has -18

-4

$x \equiv 3 \bmod 7$ $x \equiv 3 \bmod 7$

$x \equiv 4 \bmod 11$ $x \equiv 7 \bmod 11$

⇒ $-4 \bmod 77$

⇒ $73 \bmod 77$

$x \equiv -18 \bmod 77$ or $x \equiv 59 \bmod 77$ $\quad -4 \quad$ $x \equiv 73 \bmod 77$

E.x. Solve $x^7 + 7x^2 + x \equiv 15 \bmod 35$

Soln 1 Test 0 - 34 (test $[-17, 17] \cap \mathbb{Z}$)

Soln 2 "Solve mod 5, mod 7, then lift to 35"

① $x^7 + 7x^2 + x \equiv 15 \bmod 5$

FLT: $x^5 \equiv x \bmod 5$

So $x^7 \equiv x^3 \bmod 5$

$x^3 + 2x^2 + x \equiv 0 \bmod 5$

$x(x^2 + 2x + 1) \equiv 0 \bmod 5$

$x(x+1)^2 \equiv 0 \bmod 5$

EL$\Rightarrow$ $x \equiv 0 \bmod 5$ $\vee$ $x+1 \equiv 0 \bmod 5$

$x \equiv -1 \bmod 5$

$x \equiv 4 \bmod 5$

② $x^7 + 7x^2 + x \equiv 0 \bmod 15$

FLT $\Rightarrow x^7 \equiv x \bmod 7$

$2x \equiv 1 \bmod 7$

$\rightarrow x \equiv 4 \bmod 7$

③ Lift Either

$x \equiv 0 \bmod 5$ $\quad \vee \quad$ $x \equiv 4 \bmod 5$

$x \equiv 4 \bmod 7$ $\quad\quad$ $x \equiv 4 \bmod 7$

$x \equiv 25 \mod 35$ $\quad\quad$ $x \equiv 4 \mod 35$

RSA Public Key : no secret meeting in advance.

A wants to send a secret message to B, but E is eavesdropping. (A, B hasn't already met)
Assume "Message" mean "Number"

A: Yo B, I want to send you a message.
B: Ok, give me a minute.

B's Job Part 1:

1. Choose distinct primes p, q
2. Let $n = pq$. Let $\phi = (p-1)(q-1)$
3. Choose $1 \leq e \leq \phi$ such that $\gcd(e, \phi) = 1$.
4. Find $1 \leq d \leq \phi$ such that $ed \equiv 1 \mod \phi$.
5. Publish (e, n). (Keep p, q, ϕ, d secret)

A's Job

Suppose message is $M \in \mathbb{N}$.

① Check then $M < n$

② Find $0 \leq c \leq n \ni M^e \equiv c \mod n$

③ Publish c (c is the encrypted message)

B's Job Part 2:

① Find $0 \leq R \leq n$ such that $c^d \equiv R \mod n$

② Profit (Since $R = M$)

E.x Bob chooses $p = 13$, $q = 17$. So $n = 13 \cdot 17 = 221$, and $\phi = (13-1)(17-1) = 192$. Bob chose $e = 71$.

Solve $71d \equiv 1 \mod 192$ to get $d = 119 \mod 192$.
Now Bob publishes $(e, n) = (71, 221)$

Alice Suppose $M = 37$. A must find $0 \leq C < 221$ such that $M^{71} \equiv C \mod 221$

$M^1 \equiv 37 \mod 221$

$M^2 \equiv 37^2 \equiv 43 \mod 221$

$M^4 \equiv (37^2)^2 \equiv 43^2 \equiv 81 \mod 221$

$M^8 \equiv 81^2 \equiv 152 \mod 221$

$M^{16} \equiv 120 \mod 221$

$M^{32} \equiv 35 \mod 221$

$M^{64} \equiv 120 \mod 221$

So $M^{71} = M^{64} \cdot M^4 \cdot M^2 \cdot M^1$

$\equiv 120 \cdot 81 \cdot 43 \cdot 37 \mod 221$

$\equiv 45 \mod 221$

$\Rightarrow c = 45$

A publishes $c = 45$

Back to B

Find $0 \le R < 221$ such that

$$45^{119} \equiv R \mod 221$$

Get $R = 37$

Why can't E find p, q from n?

Suppose $p, q \approx 10^{50}$. So $pq \approx 10^{100}$, so $\sqrt{pq} \approx 10^{50}$

$$\#\text{ primes} \le 10^{50} \approx \frac{10^{50}}{\ln(10^{50})} \approx 10^{48}$$

Pretend u have a list of all these primes.
And ur laptop can compute 10^6 primes / second.

$$\frac{10^{48}}{10^6} = 10^{42} \text{ seconds} \Rightarrow 10^{37} \text{ days}$$

- Eve knows $M^{71} \equiv 45 \mod 221$

E guess number one at a time $\longrightarrow O(n \log n)$

Theorem (RSA). Let p, q be distinct primes. Let $n = pq$, let $\phi = (p-1)(q-1)$. Let $e, d \in \mathbb{N}$ such that $ed \equiv 1 \mod \phi$. Let M, C, R satisfy $0 \leq M, C, R < n$ and $M^e \equiv C \mod n$ and $C^d \equiv R \mod n$. Then $R = M$.

Proof: Since $0 \leq M, R < n$, it suffices to prove $R \equiv M \mod n$. Since $n = pq$, and $\gcd(p,q) = 1$, it suffices to prove $R \equiv M \mod p$ and $R \equiv M \mod q$. We just prove $R \equiv M \mod p$.

Note $M^e \equiv C \mod p$ & $C^d \equiv R \mod p$. Write $ed = 1 + k\phi$ for some $k \in \mathbb{N}$.

Assume $p \mid M$. Then $M \equiv 0 \mod p$. Then

$$C \equiv M^e \mod p \equiv 0^e \mod p \equiv 0 \mod p$$

Then also $R \equiv 0 \mod p$. So $M \equiv R \mod p$.

Assume $p \nmid M$. By FLT, $M^{p-1} \equiv 1 \mod p$. Then

$$R \equiv C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\phi} \equiv M^{1+k(p-1)(q-1)}$$
$$\equiv M^1 \cdot (M^{p-1})^{1 \cdot (q-1)}$$
$$\equiv M \mod p.$$

Complex Number

$\mathbb{N} \subsetneq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

$x + 7 = 5$ equation over $\mathbb{N}$, no solution in $\mathbb{N}$

$3x = 4$ equation over $\mathbb{Z}$, no solution in $\mathbb{Z}$

$x^2 - 3 = \frac{5}{9}$ equation over $\mathbb{Q}$, no solution in $\mathbb{Q}$

$x^2 = 7$ equation over $\mathbb{R}$, no solution in $\mathbb{R}$

$\mathbb{CN}$

Defn: Complex number (in standard form) is an expression of form $a + bi$, $a, b \in \mathbb{R}$.

The set of all complex number is $\mathbb{C}$.

Ex. Complex Numbers:

$3 + (-\pi)i$ (written as $3 - \pi i$)

$0 + 7i$ (written $7i$)

$135 + 0i$ (written 135) $\rightarrow \mathbb{R} \in \mathbb{C}$

$0 + 0i$ (written 0)

The real part of $a + bi$ is a. $\mathrm{Re}(3+4i) = 3$

The imaginary part of $a + bi$ is b. $\mathrm{Im}(3-4i) = -4$

Two complex number are equal if their real parts are equal, and their imaginary parts are equal. $(a+bi) = (c+di)$

$a = c$, $b = d$

Let $z \in \mathbb{C}$. So $z = a+bi$ for some $a, b \in \mathbb{R}$.
(easier to write z instead of $a+bi$).

Defn: z is purely real if $\text{Im}(z) = 0$
z is purely imaginary if $\text{Re}(z) = 0$

$0+0i$ is both PR and PI
$2+3i$ is neither PR or PI

Defn: Let $z, w \in \mathbb{C}$. Write $z = a+bi$ for some $a,b,c,d \in \mathbb{R}$.
$w = c+di$

Addition → G.3 addition

① $z+w \overset{\text{defn}}{=} (a+c) + (b+d)i$.

when writting CN

Multiplication

② $zw \overset{\text{defn}}{=} (ac-bd) + (ad+bc)i$

Ex $(2-7i) + (4+3i) = 6+4i$

$(2-7i)(4+3i) = (2\cdot 4 - (-7)\cdot 3) + (2\cdot 3 + (-7)\cdot 4)$

$= 29 - 22i$

Ex. $4(5) = (4+0i)(5+0i) = (4(5) - 0\cdot 0) + (4\cdot 0 + 0\cdot 5)i$

$= 20 + 0i = 20$

(complex mult is real result if $z, w \in \mathbb{R}$)

Ex. $i^2 = i \cdot i = (0+1i)(0+1i) = (0\cdot 0 - 1\cdot 1) + (0\cdot 1 + 1\cdot 0)i$

$= -1 + 0i = -1$

Mult → Binomial Expression

$(1+5i)(2-2i) = (1\cdot 2 - 5\cdot -2) + (1\cdot -2 + 5\cdot 2)i$

$= 12 - 8i$

$(1+5i)(2-2i) = 1\cdot 2 - 1\cdot 2i + 5i\cdot 2 + 5i(-2i)$

$= 2 - 2i + 10i - 10i^2$

$= 2 - 8i + 10 = 12 - 8i$

- Addition / Multiplication are commutative:

$\forall z, w \in \mathbb{C}, [z+w = w+z \wedge zw = wz]$

- $\forall z \in \mathbb{C}, 0 + z = z$, 0 is the additive identity of $\mathbb{C}$.
- $\forall z \in \mathbb{C}, \exists w \in \mathbb{C}, z + w = 0$, every CN has an additive inverse. (Add Inverse of z is $-z$)

$\forall z \in \mathbb{C}, z \cdot 1 = z$, 1 is mult identity of $\mathbb{C}$.

Mult Inverse?

E.x. Does $2+3i$ have a mult inverse?

$(2+3i)(a+bi) = 1$

$(2a-3b)(2b+3a) = 1 + 0i$

$$\Rightarrow \begin{matrix} 2a - 3b = 1 \\ 2b + 3a = 0 \end{matrix} \Rightarrow a = \frac{2}{13}, \quad b = \frac{-3}{13}$$

(check $(2+3i)\left(\frac{2}{13} - \frac{3}{13}i\right) = 1$)

Prop Let $z \in \mathbb{C}$, $z \neq 0$. Then z has a mult inverse in $\mathbb{C}$.
If $z = a+bi$, with $a, b \in \mathbb{R}$, then $z^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$

$$= \frac{a-bi}{a^2+b^2}$$

Conjugate & Modulus

Conjugate of a CN $z = x+yi$, written $\bar{z}$ is CN $z = x-yi$.

Properties of Conjugate

1. $\overline{(\bar{z})} = z$
2. $\overline{z+w} = \bar{z} + \bar{w}$
3. $z + \bar{z} = 2\,\mathrm{Re}(z)$ and $z - \bar{z} = 2\,\mathrm{Im}(z)i$
4. $\overline{zw} = \bar{z}\,\bar{w}$
5. If $z \neq 0$, then $\overline{(z^{-1})} = (\bar{z})^{-1}$

The modulus of the complex number $z = x + yi$, written $|z|$, is non-negative real number $|z| = \sqrt{x^2 + y^2}$

Properties of Modulus (PM)

1. $|z| = 0 \iff z = 0$ / $|z| \in \mathbb{R}$, $|z| \geq 0$
2. $|\bar{z}| = |z|$
3. $\bar{z}z = |z|^2$, so $\bar{z}z \in \mathbb{R}$ ★
4. $|zw| = |z|\,|w|$
5. If $z \neq 0$, then $|z^{-1}| = |z|^{-1}$

Corollary 5.

$\forall\, n \in \mathbb{N}$, and $\mathbb{C}$ $z_1, z_2, \ldots, z_n$, we have:

1. $\overline{z_1 + z_2 + \ldots + z_n} = \bar{z}_1 + \bar{z}_2 + \ldots + \bar{z}_n$
2. $\overline{z_1 \cdot z_2 \cdot \ldots \cdot z_n} = \bar{z}_1 \cdot \bar{z}_2 \cdot \ldots \cdot \bar{z}_n$
3. $|z_1 z_2 \ldots z_n| = |z_1|\,|z_2| \ldots |z_n|$

Triangle Inequality: TIQ

$\forall\, z, w \in \mathbb{C}$, $|z + w| \leq |z| + |w|$.

E.x. Write $\dfrac{1+2i}{3-4i}$ in standard form.

Soln #1: $\dfrac{1+2i}{3-4i} = (1+2i)(3-4i)^{-1}$

$= (1+2i)\left(\frac{3}{25} + \frac{4}{25}i\right)$

$$= \frac{1}{25}(1+2i)(3+4i)$$
$$= \frac{1}{25}(-5+10i) = \frac{-1}{5} + \frac{2}{5}i$$

Soln#2: $\frac{1+2i}{3-4i} = \frac{1+2i}{3-4i} \cdot \frac{3+4i}{3+4i}$

$$= \frac{(1+2i)(3+4i)}{25}$$

Prove PC:

Proof to 5. If $z \neq 0$, then $\overline{(z^{-1})} = (\bar{z})^{-1}$

#1

Pf: Write $z = a+bi$ with $a,b \in \mathbb{R}$. Assume $a \neq 0$ V $b \neq 0$.

Write down $\overline{z^{-1}}$ in terms of a,b

Write down $\bar{z}^{-1}$ in terms of a,b

Check they're equal.

#2.

Pf: Know $z z^{-1} = 1$. Then $\overline{zz^{-1}} = \bar{1}$

So $\bar{z}\,\overline{z^{-1}} = 1$ by ④

So $\bar{z}, \overline{z^{-1}}$ are inverse of each other. So $\bar{z}^{-1} = \overline{z^{-1}}$

E.x. Solve $z^2 = i\bar{z}$

Write $z = a+bi$ for $a, b \in \mathbb{R}$

Then $z^2 = (a+bi)(a+bi) = (a^2-b^2)+2abi$

Also $i\bar{z} = i(a-bi) = b+ai$

So ① $a^2-b^2 = b$

② $2ab = a \longrightarrow a(2b-1) = 0 \longrightarrow a=0 \vee b=\frac{1}{2}$

$\underline{a=0}$ ① $-b^2 = b$

$b(b+1) = 0 \rightarrow b=0 \vee b=-1$

$\therefore z = 0 \vee z = 0-1i$

$\underline{b=\frac{1}{2}}$ ① $a^2 = \frac{3}{4} \rightarrow a = \frac{\pm\sqrt{3}}{2}$

$\therefore z = \frac{\sqrt{3}}{2}+\frac{1}{2}i \vee z = \frac{-\sqrt{3}}{2}+\frac{1}{2}i$

If z is real, mod z is equal to $|z|$.

Prove PM:

Proof # 1 of ④: 4. $|zw| = |z||w|$

Let $z = a+bi$, $w = c+di$, with $a, b, c, d \in \mathbb{R}$

Then, $|zw|^2 = |(a+bi)(c+di)|^2$

$= (ac-bd)^2 + (ad+bc)^2 = |(ac-bd)+(ad+bc)i|^2 = |z|^2|w|^2$

Since $|zw|, |z|, |w| \geq 0$, we get $|zw| = |z||w|$

Proof #2.

$$\begin{aligned} |zw|^2 &= (zw)(\overline{zw}) \quad \text{by } ③ \\ &= zw\bar{z}\bar{w} \\ &= z\bar{z}\,w\bar{w} \\ &= |z|^2|w|^2 \end{aligned}$$

Proof of ⑤: If $z \neq 0$, then $|z^{-1}| = |z|^{-1}$

know $zz^{-1} = 1$, $\therefore |zz^{-1}| = |1|$

So, by ④, $|z||z^{-1}| = 1$. So $|z^{-1}| = \frac{1}{|z|}$

E.x. Prove:

① $\forall z,w \in \mathbb{C}$, $|z+w|^2 + |z-w|^2 = 2(|z|^2+|w|^2)$

Let $z, w \in \mathbb{C}$. Then

$$|z+w|^2 + |z-w|^2 = (z+w)\overline{(z+w)} + (z-w)\overline{(z-w)}$$

$$= z\bar{z} + z\bar{w} + \bar{z}w + w\bar{w} + z\bar{z} - z\bar{w} - w\bar{z} + w\bar{w}$$

$$= 2(z\bar{z} + w\bar{w})$$

$$= 2(|z|^2 + |w|^2)$$

E.x. Prove:

③ Let $z \in \mathbb{C}$ s.t. $z^2+1 \neq 0$.

Prove $\frac{z}{z^2+1} \in \mathbb{R} \iff (z \in \mathbb{R} \vee |z| = 1)$

$$\frac{z}{z^2+1} \iff \frac{z}{z^2+1} = \overline{\left(\frac{z}{z^2+1}\right)}$$

$$\iff \frac{z}{z^2+1} = \frac{\bar{z}}{\bar{z}^2+1}$$

$$\iff z(1+\bar{z}^2) = \bar{z}(1+z^2)$$

$$\iff z + z\bar{z}^2 = \bar{z} + \bar{z}z^2$$

$$\iff z - \bar{z} = z^2\bar{z} - z\bar{z}^2$$

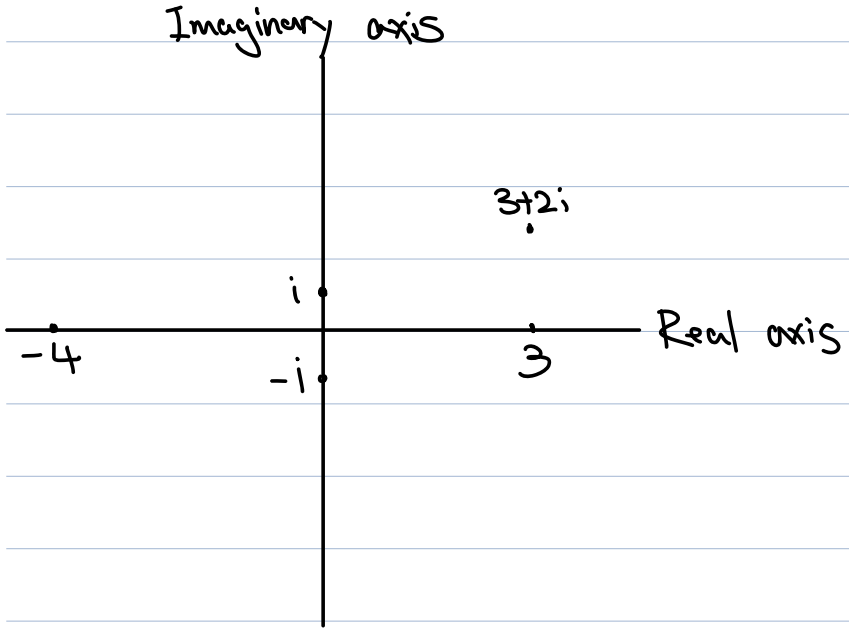
$$\iff z - \bar{z} = z\bar{z}(z - \bar{z})$$

$$\iff z - \bar{z} = |z|^2(z - \bar{z})$$

$\Longrightarrow \quad z \in \mathbb{C} = |z| \; (z \in \mathbb{C})$

$\Longleftrightarrow \quad z - \bar{z} = 0 \quad \vee \quad |z|^2 = 1$

$\Longleftrightarrow \quad z \in \mathbb{R} \quad \vee \quad |z| = 1$

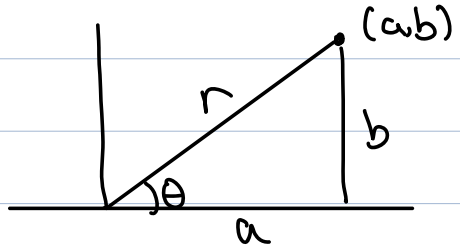


Complex plane	Thing	Geometry?
	Addition	"Parrallelogram Law"
	Multiplication	
	Conjugation	Reflect thru real axis
	Modulus	Distance to origin

When writing $z = a + bi$, with $a, b \in \mathbb{R}$, "describing" z in terms of horizontal and vertical distance.

- can instead describe z by giving r, θ
- relationship between a, b and r, θ??

$(r, \theta) \to (a, b)$ $\quad a = r\cos\theta$, $\quad b = r\sin\theta$



$(a, b) \to (r, \theta)$ $\quad r = \sqrt{a^2 + b^2}$ $\quad (= |a + bi|)$

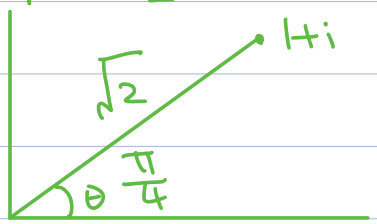
$$\theta = \begin{cases} \tan^{-1}\left(\frac{b}{a}\right) & a > 0 \\ \pi + \tan^{-1}\left(\frac{b}{a}\right) & a < 0 \\ \pi/2 & a = 0 \wedge b > 0 \\ -\pi/2 & a = 0 \wedge b < 0 \\ \text{any angle} & a = 0 \wedge b = 0 \end{cases}$$

$$\begin{aligned} z &= a + bi \\ &= r\cos\theta + r\sin\theta\, i \\ &= r(\cos\theta + \sin\theta i) \end{aligned}$$

Defn: Let $z \in \mathbb{C}$. Suppose $r, \theta \in \mathbb{R}$ and $r \geq 0$ and $z = r(\cos\theta + i\sin\theta)$ Call polar form of z.

Call (r, θ) polar coordinates of z).

E.x. Put $1+i$ in polar form.



$1+i = \sqrt{2}\left(\cos\frac{\pi}{4} + \sin\frac{\pi}{4}\, i\right)$

PC's are $\left(\sqrt{2}, \frac{\pi}{4}\right)$ or $\left(\sqrt{2}, \frac{9\pi}{4}\right)$

E.x. $z = 5$ $\quad 5 = 5(\cos 0 + i\sin 0)$

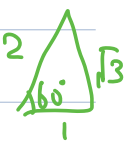
$z = -5$ $\quad -5 = 5(\cos\pi + i\sin\pi)$

$z = 5i$ $\quad 5i = 5\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)$

$z = 0$ $\quad 0 = 0\left(\cos\frac{12\pi}{9} + i\sin\frac{12\pi}{9}\right)$

If $(r_1, \theta_1), (r_2, \theta_2)$ are PC's of z, then $r_1 = r_2$.
If $r_1 \neq 0$, then $\theta_1 - \theta_2 = 2\pi k$ for some k.

$$1 + i = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$$



E.x. Let $z = 1 + \sqrt{3}\, i = 2\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)$

$w = -3 + 3i = 3\sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)$

$$zw = 2\left(\cos\tfrac{\pi}{3} + i\sin\tfrac{\pi}{3}\right)\cdot 3\sqrt{2}\left(\cos\tfrac{3\pi}{4} + i\sin\tfrac{3\pi}{4}\right)$$

$$= 6\sqrt{2}\left[\left(\cos\tfrac{\pi}{3}\cdot\cos\tfrac{3\pi}{4}\right) - \left(\sin\tfrac{\pi}{3}\cdot\sin\tfrac{3\pi}{4}\right) + \left(\cos\tfrac{\pi}{3}\cdot\sin\tfrac{3\pi}{4} + \sin\tfrac{\pi}{3}\cdot\cos\tfrac{3\pi}{4}\right) i\right]$$

$= 6\sqrt{2}\left(\cos\left(\frac{\pi}{3}+\frac{3\pi}{4}\right) + i\sin\left(\frac{\pi}{3}+\frac{3\pi}{4}\right)\right]$ Add angle and multiply by modulus

Short hand: $\cos\theta + i\sin\theta \Rightarrow \text{cis}\,\theta = e^{i\theta}$

PMC: Let $z_1 = r_1\text{cis}\theta_1$, $z_2 = r_2\text{cis}\theta_2$

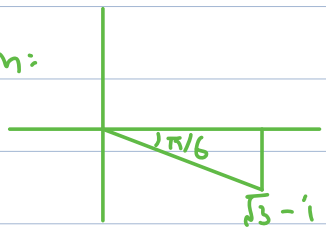
then $z_1 \cdot z_2 = r_1 r_2 \cdot \text{cis}(\theta_1 + \theta_2)$

Demoivre's Theorem: for all $n \in \mathbb{Z}$.

$$(r\,\text{cis}\,\theta)^n = r^n \cdot \text{cis}(n\theta)$$

E.X. Write $(\sqrt{3}-i)^{10}$ in standard form.

Soln:



$$\sqrt{3} - i = 2\,\text{cis}\left(\frac{-\pi}{6}\right)$$

$$(\sqrt{3}-i)^{10} = 2^{10} \cdot \text{cis}\left(\frac{-10\pi}{6}\right)$$

$$= 2^{10} \cdot \text{cis}\left(\frac{\pi}{3}\right)$$

$$\text{cis}\frac{\pi}{3} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + \frac{\sqrt{3}\,i}{2}$$

$$\Rightarrow (\sqrt{3}-i)^{10} = 2^{10}\cdot\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$$

$$= 2^9 + \sqrt{3}\,i \cdot 2^9$$

E.X. $(\text{cis}\,\theta)^3 = (\cos^2\theta - \sin^2\theta + (2\cos\theta\sin\theta)i)(\cos\theta + i\sin\theta)$

$= (\cos^3\theta - \cos\theta\sin^2\theta - 2\cos\theta\sin^2\theta) + (\text{thing})\,i$

$(\text{cis}\,\theta)^3 = \cos 3\theta + \sin 3\theta\, i$

$\rightarrow \quad \cos 3\theta = 4\cos^3\theta - 3\cos\theta$

$\sin 3\theta = 3\sin^3\theta - 4\sin\theta$

PMC: $\text{cis}\theta_1 \cdot \text{cis}\theta_2 = \text{cis}(\theta_1 + \theta_2)$

$\rightarrow e^{i(\theta_1+\theta_2)}$

DMT: $(\text{cis}\theta)^n = \text{cis}(n\theta) \rightarrow (e^{i\theta})^n = e^{i(n\theta)}$

When use $e^{i\theta}$ notation, PMC & DMC exacty state grade 9 exponential rules.

$$-1 = \text{cis}(\pi) \longrightarrow -1 = e^{i\pi}$$

$r_1 e^{i\theta_1} = r_2 e^{i\theta_2} \Leftrightarrow [r_1 = r_2 \wedge (r_1 \neq 0) \Rightarrow \theta_1 - \theta_2 = 2\pi k)]$ for some $k \in \mathbb{Z}$

Ex. Solve $z^4 = 16$

Write $z = re^{i\theta}$ (solve for r, θ)

Then $z^4 = r^4 e^{i(4\theta)}$

$16 = 16e^{i0}$ For $z^4 = 16$, need $r^4 = 16$

Since $r \in \mathbb{R}$, $r \geq 0$, $r^4 = 16 \Rightarrow r = 2$

Also need $4\theta - 0 = 2\pi k$ for some $k \in \mathbb{Z}$.

k	z (polar)	z (standard)
0	$2e^{i0}$	2
1	$2e^{i\cdot\frac{\pi}{2}}$	$2i$
2	$2e^{i\pi}$	-2
3	$2e^{i\frac{3\pi}{2}}$	$-2i$
4	$2e^{i2\pi}$	2

$e^{i\pi k_1/2} = e^{i\pi k_2/2} \iff k_1 \equiv k_2 \bmod 4$

Ex. Solve $z^3 = (2+2i)$

Ex. Solve $z^3 = 5+5i$

$5+5i = \sqrt{50}\, e^{i(\frac{\pi}{4})}$

$z = re^{i\theta}$

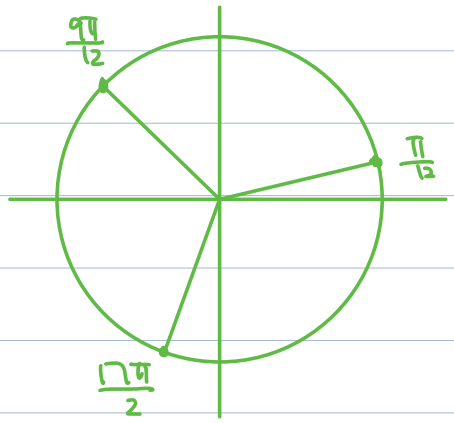
$z^3 = r^3 \cdot e^{i(3\theta)}$

$z^3 = 5+5i \Rightarrow r^3 = \sqrt{50} \Rightarrow r = \sqrt[6]{50}$

$3\theta - \frac{\pi}{4} = 2\pi k, \; k \in \mathbb{Z}.$

$\theta = \frac{2\pi k + \frac{\pi}{4}}{3} = \frac{8\pi k + \pi}{12}$

k	z
0	$\sqrt[6]{50} \cdot e^{i\pi/12}$
1	$\sqrt[6]{50} \cdot e^{i\frac{9\pi}{12}}$
2	$\sqrt[6]{50} \cdot e^{i\frac{17\pi}{12}}$



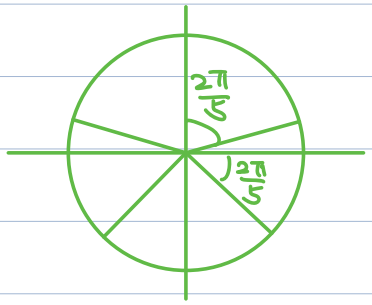
Defn: Let $n \in \mathbb{N}$, let $a \in \mathbb{C}$. The solns to $z^n = a$ are called the n^{th} roots of a.

CNRT: Assume $a = te^{i\psi}$ where $t, \psi \in \mathbb{R}$, and $t \geq 0$

The n^{th} root of a are precisely n complex numbers.

$$\sqrt[n]{t}\, e^{i\left(\frac{2\pi k + \psi}{n}\right)} \text{ with } 0 \leq k \leq n-1$$

if $a \neq 0$, these n solutions live on a circle of radius of $\sqrt[n]{r}$ and are equally spaced.



E.x. Solve $z^5 = 32i$

Soln: $32i = 32e^{i\frac{\pi}{2}}$

CNRT: 5 solutions are $\sqrt[5]{32}\, e^{i\left(\frac{2\pi k + \frac{\pi}{2}}{5}\right)}$ with $0 \leq k \leq 4$.

E.x. Solve $z^3 = i\overline{z}$ (CNRT doesn't directly apply)

$z = r \cdot e^{i\theta}$ $\quad \overline{z} = r \cdot e^{i(-\theta)}$ $\quad i = r \cdot e^{i\frac{\pi}{2}}$

$z^3 = r^3 \cdot e^{i(3\theta)}$ $\quad i\overline{z} = re^{i(\frac{\pi}{2} - \theta)}$

$\Rightarrow r^3 e^{i(3\theta)} = r \cdot e^{i(\frac{\pi}{2} - \theta)}$

$\Rightarrow r^3 = r \Rightarrow r = 0 \vee r = 1$

$r = 0 \Rightarrow z = 0$

$r = 1 \Rightarrow 3\theta - (\frac{\pi}{2} - \theta) = 2\pi k$

$\theta = \frac{2\pi k + \frac{\pi}{2}}{4} = \frac{4\pi k + \pi}{8}$

k	z
0	$e^{i\frac{\pi}{8}}$
1	$e^{i\frac{5\pi}{8}}$
2	$e^{i\frac{9\pi}{8}}$
3	$e^{i\frac{13\pi}{8}}$
4?	$e^{i\frac{17\pi}{8}} = e^{i\frac{\pi}{8} + 2\pi}$

} solution to $z^4 = i$

Soln 2. $z^3 = i\bar{z}$

$|z|^3 = |i\bar{z}|$

$\Rightarrow |z| = 0 \vee |z| = 1$

$|z| = 1$: $z^4 = iz\cdot z$

$z^4 = i|z|^2 = i$

Practice: Redo $z^2 = i\bar{z} \longrightarrow z^3 = i$

Consider equation $x^2 - 12x + 27 = 0$

$$x = \frac{12 \pm \sqrt{12^2 - 4(27)}}{2} = \frac{12 \pm 6}{2}$$

36 has 2 square roots, $+6$ & -6. Doesn't matter which one we use.

QF: Consider $az^2 + bz + c = 0$ where $a, b, c \in \mathbb{C}$, $a \neq 0$

Let $w \in \mathbb{C}$ such that $w^2 = b^2 - 4ac$

Then $z = \frac{-b \pm w}{2a}$

Ex. Solve $z^2 + \sqrt{7}\, z + 3 - 3i = 0$

Soln 1: $z = x + iy$, $x, y \in \mathbb{R}$,

$b^2 - 4ac = (\sqrt{7})^2 - 4(1)(3-3i) = -5 + 12i$

Solve $w^2 = -5 + 12i$

$w = x + yi \Rightarrow x^2 + y^2 = -5 \Rightarrow x^2 - \left(\frac{6}{x}\right)^2 = -5$

$2xy = 12$ $\Rightarrow x^4 + 5x^2 - 36 = 0$

Let $v = x^2 \Rightarrow v^2 + 5v - 36 = 0$

Choose $v = 4$

$(-9 = x^2$ no R soln$) \rightarrow x = 2 \Rightarrow y = 3$

So $(2+3i)^2 = -5 + 12i$

So $z = \dfrac{-\sqrt{7} \pm (2+3i)}{2}$

Polynomials.

Let x be a variable. A polynomial in x over $\mathbb{R}$ (over $\mathbb{C}$) is an expression of the form

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x + a_0$$

$$= \sum_{k=0}^{n} a_k x^k, \quad n \in \mathbb{Z}, n \geq 0, \text{ each } a_i \in \mathbb{R} \text{ or } \in \mathbb{C}.$$

- a_i is a coefficient of $f(x)$
- $a_i x^i$ is a term of $f(x)$
- $R[x]$ ← Set of all real polynomials in x
  $C[x]$
- Zero Polynomial has $a_k = 0$ for all k.
- Degree is largest k such that $a_k \neq 0$.

Ex $f(x) = x^5 + 2x + \pi$ $\quad f(x) \in R[x]$, $f(x) \in C[x]$
$\deg(f) = 5$

$g(x) = 0x^4 + 2x^2 + 3ix + (2 - 5i)$ $\quad g(x) \notin R[x]$, $g(x) \in C[x]$

2 is the coefficient of x in $f(x)$.
$2x$ is a term of $f(x)$.

Ex. $(x^2 + ix + 3) + (ix^2 - 1) = (1+i)x^2 + ix + 2$

$$(x^2 + ix + 3)(ix^2 - 1) = ix^4 - x^2 + i^2x^3 + 3ix^2 - 3$$
$$= ix^4 - x^3 + (3i - 1)x^2 - ix - 3$$

Given $f(x), g(x) \in \mathbb{R}[x]$, say f divides g or f is a factor of g, written $f(x) \mid g(x)$, if $f(x)h(x) = g(x)$ for some $h(x) \in \mathbb{R}[x]$.

Ex. $x-1 \mid x^3-1$ since $(x-1)(x^2+x+1) = x^3-1$

$x+i \mid x^2+1$ since $(x+i)(x-i) = x^2+1$

Ex. Determine if $x^2+x+3 \mid x^4-x^3+6x^2-x+15$

$$
\begin{array}{r}
x^2-2x+5 \\
x^2+x+3 \;\overline{)\; x^4-x^3+6x^2-x+15} \\
-(x^4+x^3+3x^2) \\
\hline
-2x^3+3x^2-x \\
-(-2x^3-2x^2-6x) \\
\hline
5x^2+5x+15 \\
-(5x^2+5x+15) \\
\hline
0
\end{array}
$$

$\Rightarrow f \mid g$ and $f(x)(x^2-2x+5) = g(x)$

Ex. Determine if $ix^2+2x+(3+i) \mid 3ix^3+7x^2+(9+i)x+(3-2i)$

$$
\begin{array}{r}
3x-i \\
ix^2+2x+(3+i) \;\overline{)\; 3ix^3+7x^2+(9+i)x+(3-2i)} \\
-(3ix^3+6x^2+(9+3i)x) \\
\hline
x^2-2ix+3-2i \\
-(x^2-2ix+1-3i) \\
\hline
2+i
\end{array}
$$

Stop since $\deg(2+i) < \deg(f)$

So $f(x) \nmid g(x)$. In fact, $g(x) = f(x)\underbrace{(3x-i)}_{q(x)} + \underbrace{2+i}_{r(x)}$

Given $c \in \mathbb{C}$, c is a root of $f(x)$ if $f(c) = 0$.

- $\sqrt{3}$ is root of $x^2 - 3$
- $2i$ is a root of $x^2 + 4$.

Let $c \in \mathbb{C}$, $f(x) \in \mathbb{C}[x]$

c is a root of $f(x)$ if $f(c) = 0$

FT $f(c) = 0 \iff x - c \mid f(x)$

Ex. $f(x) = x^2 + 1$

$x - i \mid f(x)$ $\quad x - 3 \mid x^2 + 1$ since $f(3) \neq 0$.

Th (Fundamental Theorem of Algebra

Let $f(x) \in \mathbb{C}[x]$ with $\deg f(x) \geq 1$

$\exists \alpha \in \mathbb{C}$, $f(x) = 0$.

CPN. Let $f(x) \in \mathbb{C}[x]$ with $\deg(f) = n \geq 1$

$\exists\ A \in \mathbb{C}, A \neq 0$, and $c_1, c_2, \ldots c_n \in \mathbb{C}$ such that

$f(x) = A(x - c_1)\cdot(x - c_2)\cdot(x - c_3)\cdot \ldots (x - c_n)$

The roots are exactly the c_i's. of f.

$\deg(f) = 3$ FTA $\rightarrow$ f has a root c_1

$\rightarrow f(x) = (x - c_1)\cdot f_1(x)$

FTA $\rightarrow$ f_1 has a root c_2

$\rightarrow f(x) = (x-c_1)\cdot(x-c_2)\cdot(Ax+B)$

$= A(x-c_1)\cdot(x-c_2)\cdot(x-\frac{B}{A})$

Ex. $3x^2-21 = 3(x^2-7)$

$= 3(x-\sqrt{7})(x-(-\sqrt{7}))$

Ex. $(x^2+1)^2 = (x-i)(x-i)(x-(-i))(x-(-i))$

<u>Consequence</u> $f(x)$ has at most n roots

Defn: Let $f(x) \in R[x]$. f is reducible in $R[x]$ if there exist $g, h \in R[x]$, with $\deg(g), \deg(h) \geq 1$, and $f = hg$. f is irreducible in $R[x]$ if it's not reducible. Same for $\mathbb{C}$.

Ex. $x^2-10 = (x-\sqrt{10})(x+\sqrt{10})$

reducible in $R[x]$ and $\mathbb{C}[x]$.

Ex. $x^2+1 = (x-i)(x+i)$

: Reducible in $\mathbb{C}[x]$, irreducible in $R[x]$.

Ex: $x-7 = (2x-14)(\frac{1}{2})$

- not show that $x-7$ is reducible.

E.x $(x^2+1)^2 = (x^2+1)(x^2+1)$

: Reducible in $\mathbb{R}[x]$ but has no roots in $\mathbb{R}$.

E.x. Let $f(x) \in \mathbb{C}[x]$

$f(x)$ is irreducible in $\mathbb{C}[x] \iff \deg(f) = 1$

CJRT Let $f(x) \in \mathbb{R}$. Let $c \in \mathbb{C}$.

If $f(c) = 0$ then $f(\bar{c}) = 0$

Proof: Assume $f(c) = 0$. Write

$f(x) = a_n x^n + \dots + a_1 x^1 + a_0$ with $a_i \in \mathbb{R}$ $\forall$ i.

Well, $f(\bar{c}) = a_n \bar{c}^n + \dots + a_1 \bar{c} + a_0$

$= \bar{a}_n \bar{c}^n + \dots + \bar{a}_1 \bar{c} + \bar{a}_0$ since each $a_i \in \mathbb{R}$.

$= \overline{a_n c^n + \dots + a_1 c + a_0} = \overline{f(c)} = \bar{0} = 0$

Two types of root in $\mathbb{R}[x]$,

- Real root $c \in \mathbb{R}$ ← c is "alone"
- nonreal root $c \in \mathbb{C}$, $c \notin \mathbb{R}$ ← $c, \bar{c}$ are a pair

Observe: $(x-c)(x-\bar{c}) = x^2 - (c+\bar{c})x + c\bar{c}$

$= 1x^2 - 2\mathrm{Re}(c)x + |c|^2$

(Real)

E.x. Let $f(x) = x^4 - 5x^3 + 16x^2 - 9x + 13$.

Told that $f(2-3i) = 0$

Write $f(x)$ as a product of irreducibles.

i) in $\mathbb{C}[x]$

ii) in $\mathbb{R}[x]$.

$(x-(2-3i))(x-(2+3i)) = x^2-4x+13$

$$x^2-4x+13 \;\big|\; x^4-5x^3+16x^2-9x+13$$

$$x^2-x-1$$

$\therefore f(x) = (x^2-4x+13)(x^2-x-1)$

roots of $(x^2-x-1) = \frac{1\pm\sqrt{5}}{2}$

Let $c = 2-3i$ $\quad \beta = \frac{1-\sqrt{5}}{2}$

$\alpha = \frac{1+\sqrt{5}}{2}$

i) $f(x) = (x-c)(x-\bar{c})(x-\alpha)(x-\beta)$

ii) $f(x) = (x^2-4x+13)(x-\alpha)(x-\beta)$

When factoring $f(x)$ in $\mathbb{R}[x]$, two types of factors:

i) $L(x) = x-a$, $a \in \mathbb{R}$

$Q(x) = (x-c)(x-\bar{c})$, $c \in \mathbb{C}$, $c \notin \mathbb{R}$

Odd must have linear roots

END OF MATH 135