Claim: If n is a positive integer, then n^2+1 is not a perfect square.

Pf: As $n^2 < n^2+1 < n^2+2n+1 = (n+1)^2$ and since there are no squares b/w n^2 and $(n+1)^2$, we are done. ☒.

Q: What if we change n^2+1 to n^2+13?

A: FALSE! Consider $n=6$.

Q: What if we change n^2+1 to $1141n^2+1$?

A: True for $n<10^{24}$. HOWEVER, if

$n = 3069338532276565719739720$

then $1141n^2+1$ is a perfect square.

Def'n: A <u>statement</u> is a sentence that is True or False.

A <u>proposition</u> is a claim that requires a proof.

<u>Theorem</u>: Strong proposition

<u>Lemma</u>: Weak proposition

<u>Corollary</u>: Follows immediately from a propositi

<u>Axiom</u>: A given truth.

Show: $\sin(3\theta) = 3\sin\theta - 4\sin^3\theta$
for $\theta \in \mathbb{R}$
theta in Real numbers

Pf: Recall: (1) $\sin^2\theta + \cos^2\theta = 1$

(2) $\sin(\overset{\theta}{x} \overset{+}{\pm} \overset{\theta}{y}) = \sin x \cos y \pm \sin y \cos x$

(3) $\cos(x \pm y) = \cos x \cos y \mp \sin x \sin y$

$LHS = \sin(3\theta) = \sin(2\theta + \theta)$

Use (2) with $x = 2\theta$, $y = \theta$.

$= \sin(2\theta)\cos\theta + \sin\theta\cos(2\theta)$

$(\sin\theta\cos\theta + \sin\theta\cos\theta)$

Use$^{(2)}$(3) with $x = y = \theta$.

$= (2\sin\theta\cos\theta)\cos\theta + \sin\theta(\cos^2\theta - \sin^2\theta)$

$= 3\sin\theta\cos^2\theta - \sin^3\theta$

By Pythagorean identity.

$= 3\sin\theta(1 - \sin^2\theta) - \sin^3\theta$

$= 3\sin\theta - 4\sin^3\theta = RHS$

Find the flaw in the following arguments:

(i) For $a, b \in \mathbb{R}$,

$$
\begin{aligned}
a &= b \\
a^2 &= ab \\
a^2 - b^2 &= ab - b^2 \\
(a-b)(a+b) &= b(a-b) \\
a + b &= b \\
b + b &= b \\
2b &= b \\
2 &= 1
\end{aligned}
$$

DIVIDE BY ZERO

$a = b$ so $a - b = 0$.

(ii)

$$
\begin{aligned}
x &= \frac{\pi + 3}{2} \\
2x &= \pi + 3 \\
2x(\pi - 3) &= (\pi + 3)(\pi - 3) \\
2\pi x - 6x &= \pi^2 - 9 \\
9 - 6x &= \pi^2 - 2\pi x \\
9 - 6x + x^2 &= \pi^2 - 2\pi x + x^2 \\
(3 - x)^2 &= (\pi - x)^2 \\
|3 - x| &= |\pi - x| \\
3 &= \pi
\end{aligned}
$$

$\sqrt{a^2} = |a|$

$3 - x = x - \pi$

(iii) For $x \in \mathbb{R}$,

$$
\begin{aligned}
(x-1)^2 &\geq 0 \\
x^2 - 2x + 1 &\geq 0 \\
x^2 + 1 &\geq 2x \\
x + \tfrac{1}{x} &\geq 2
\end{aligned}
$$

$x \neq 0$

$x > 0$ for this to work.

if $x < 0$, flip to $\leq$

Q: Let $x, y \in \mathbb{R}$. Prove that

$$x^4 + x^2y + y^2 \geq 5x^2y - 3y^2.$$

Pf: Since $0 \leq (x^2 - 2y)^2$, we have

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

$$5x^2y - 3y^2 \leq x^4 - 4x^2y + 4y^2 + 5x^2y - 3y^2$$

$$5x^2y - 3y^2 \leq x^4 + x^2y + y^2 \qquad \blacksquare.$$

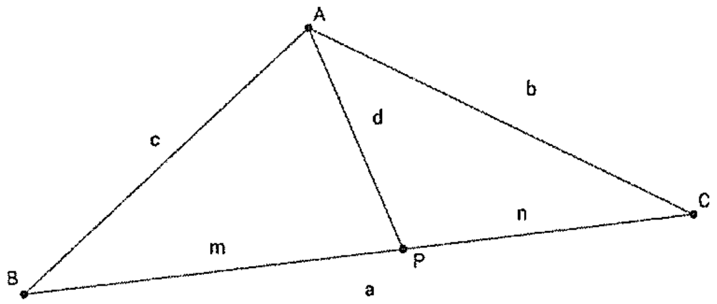
Alt. Pf:

Keep m

$$\begin{aligned} LHS = x^4 + x^2y + y^2 &= x^4 + x^2y + y^2 \boxed{+5x^2y} - 5x^2y \boxed{+3y^2} - \\ &= x^4 - 4x^2y + 4y^2 + 5x^2y - 3y^2 \\ &= (x^2 - 2y)^2 + 5x^2y - 3y^2 \\ &\geq 5x^2y - 3y^2 = RHS. \quad \blacksquare \end{aligned}$$

LS 92

Theorem 0.1. *Stewart's Theorem Let ABC be a triangle with $AB = c$, $AC = b$ and $BC = a$.*
If P is a point on BC with $BP = m$, $PC = n$ and $AP = d$,
then $dad + man = bmb + cnc$.



Proof. **Proof A**

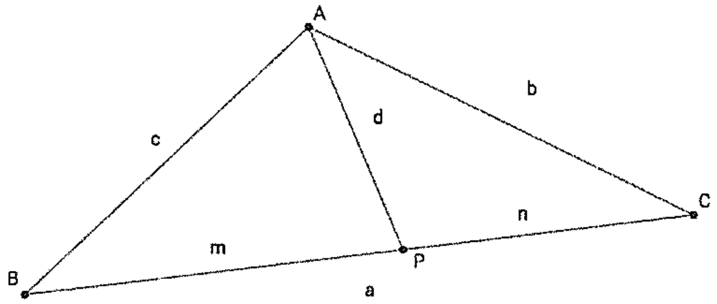
NO EXPLANATION
WHAT IS θ & θ'?

$$c^2 = m^2 + d^2 - 2md\cos\theta$$
$$b^2 = n^2 + d^2 - 2nd\cos\theta'$$
$$b^2 = n^2 + d^2 + 2nd\cos\theta$$
$$\frac{m^2 - c^2 + d^2}{-2md} = \frac{b^2 - n^2 - d^2}{2nd}$$
$$nc^2 - nm^2 - nd^2 = -mb^2 + mn^2 + md^2$$
$$nc^2 - mb^2 = mn^2 + md^2 + nm^2 + nd^2$$
$$cnc + bmb = nm(n + m) + d^2(m + n)$$
$$cnc + bmb = man + dad$$

$\square$

L3 P3

Theorem 0.2. *Stewart's Theorem Let ABC be a triangle with $AB = c$, $AC = b$ and $BC = a$.*
If P is a point on BC with $BP = m$, $PC = n$ and $AP = d$, then $dad + man = bmb + cnc$.



Proof. **Proof B**

The Cosine Law on $\triangle APB$ tells us that

$$c^2 = m^2 + d^2 - 2md\cos(\angle APB).$$

Subtracting c^2 from both sides gives

$$0 = -c^2 + m^2 + d^2 - 2md\cos(\angle APB).$$

Adding $2md\cos\angle APB$ to both sides gives

$$2md\cos(\angle APB) = -c^2 + m^2 + d^2.$$

Dividing both sides by $2md$ gives

$$\cos(\angle APB) = \frac{-c^2 + m^2 + d^2}{2md}.$$

Now, the Cosine Law on $\triangle APC$ tells us that

$$b^2 = n^2 + d^2 - 2nd\cos\angle APC.$$

Since $\angle APC$ and $\angle APB$ are supplementary angles, then

$$\cos\angle APC = \cos(\pi - \angle APB) = -\cos(\angle APB).$$

Substituting into our previous equation, we see that

$$b^2 = n^2 + d^2 + 2nd\cos\angle APB.$$

Subtracting n^2 from both sides gives

$$b^2 - n^2 = d^2 + 2nd\cos(\angle APB).$$

L3 P2

Then subtracting d^2 from both sides gives

$$b^2 - n^2 - d^2 = 2nd\cos(\angle APB).$$

Dividing both sides by $2nd$ gives

$$\frac{b^2 - n^2 - d^2}{2nd} = \cos(\angle APB).$$

Now we have two expressions for $\cos(\angle APB)$ and equate them to yield

$$\frac{-c^2 + m^2 + d^2}{2md} = \frac{b^2 - n^2 - d^2}{2nd}.$$

Multiplying both sides by $2mnd$ shows us that

WAY TOO MUCH WRITING.

$$n(-c^2 + m^2 + d^2) = m(b^2 - n^2 - d^2).$$

Next we distribute to get

$$-nc^2 + nm^2 + nd^2 = mb^2 - mn^2 - md^2.$$

Adding $nc^2 + mn^2 + md^2$ to both sides gives

$$nm^2 + mn^2 + nd^2 + md^2 = mb^2 + nc^2.$$

Factoring twice gives:

$$nm(m+n) + d^2(m+n) = mb^2 + nc^2.$$

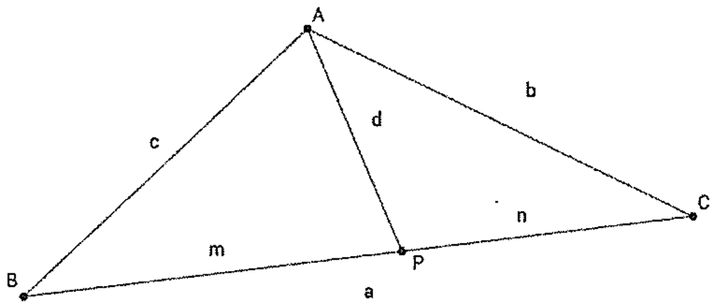
Since P lies on BC, then $a = m + n$ so we substitute to yield

$$nma + d^2a = mb^2 + nc^2.$$

Finally, we can rewrite this as $bmb + cnc = dad + man$.. □

L3 P8

Theorem 0.3. *Stewart's Theorem Let ABC be a triangle with $AB = c$, $AC = b$ and $BC = a$.*
If P is a point on BC with $BP = m$, $PC = n$ and $AP = d$, then $dad + man = bmb + cnc$.



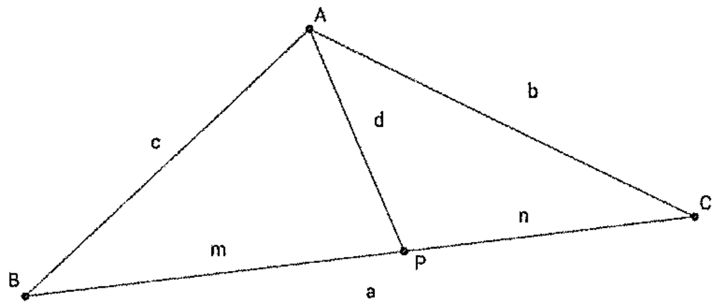
Proof. **Proof C**

Needs more steps.

Using the Cosine Law for supplementary angles $\angle APB$ and $\angle APC$, and then clearing denominators and simplifying gives $dad + man = bmb + cnc$ as required. $\square$

L3 P6

Theorem 0.4. *Stewart's Theorem Let ABC be a triangle with $AB = c$, $AC = b$ and $BC = a$.*
If P is a point on BC with $BP = m$, $PC = n$ and $AP = d$, then $dad + man = bmb + cnc$.



Proof. **Proof D**

The Cosine Law on $\triangle APB$ tells us that

$$c^2 = m^2 + d^2 - 2md \cos \angle APB.$$

Similarly, the Cosine Law on $\triangle APC$ tells us that

$$b^2 = n^2 + d^2 - 2nd \cos \angle APC.$$

Since $\angle APC$ and $\angle APB$ are supplementary angles, we have

$$b^2 = n^2 + d^2 + 2nd \cos \angle APB.$$

Equating expressions for $\cos \angle APB$ yields

$$\frac{-c^2 + m^2 + d^2}{2md} = \frac{b^2 - n^2 - d^2}{2nd}.$$

Clearing the denominator and rearranging gives

$$nm^2 + mn^2 + nd^2 + md^2 = mb^2 + nc^2.$$

Factoring yields

$$mn(m + n) + d^2(m + n) = mb^2 + nc^2.$$

Substituting $a = (m + n)$ gives $dad + man = bmb + cnc$ as required. $\square$

Throughout the lecture, let A, B, C be statements.

Def'n: $\neg A$ is NOT A.

A	$\neg A$
T	F
F	T

Def'n: $A \wedge B$ is A AND B.
$A \vee B$ is A OR B.

A	B	$A \wedge B$	$A \vee B$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

L3 P8

Which of the following are true?

- π is irrational and $3 > 2$ TRUE
- 10 is even and $1 = 2$ FALSE
- 7 is larger than 6 or 15 is a multiple of 3 TRUE
- $5 \leq 6$ TRUE
- 24 is a perfect square or the vertex of parabola $x^2 + 2x + 3$ is $(1, 1)$ FALSE.
- 2.3 is not an integer TRUE.
- 20% of 50 is not 10 FALSE.
- 7 is odd or 1 is positive and $2 \neq 2$

ORDER OF OPERATIONS.

$\neg$, $\wedge$, $\vee$.

LAST BULLET IS TRUE.

Def'n: The symbol $\equiv$ in logic means logically equivalent, that is, in a truth table, the LHS & RHS are equal.

Ex: Show $\neg(\neg A) \equiv A$.

A	$\neg A$	$\neg(\neg A)$
T	F	T
F	T	F

Since first & last columns are equal, $A \equiv \neg(\neg A)$.

Theorem: (De Morgan's Law).

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

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

Pf:

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

Since $\neg(A \vee B)$ has the same truth as $\neg A \wedge \neg B$, we have $\neg(A \vee B) \equiv \neg A \wedge \neg B$.

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

Implication $(A \Rightarrow B)$

Def'n:

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

In $A \Rightarrow B$, A is called the hypothesis
B is called the conclusion.

nota bene

$\boxed{NB}$ To <u>prove</u> $A \Rightarrow B$, we assume A is true and show B is true.

To <u>use</u> $A \Rightarrow B$, we <u>prove</u> A is true and use B as true.

In the following, identify the hypothesis, the conclusion and state whether the statement is true or false.

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

- If $\sqrt{2}$ is rational then $2 < 3$ TRUE
- If (1+1=2) then $5 \cdot 2 = 11$ FALSE.
- If C is a circle, then the area of C is πr^2 TRUE.
- If 5 is even then 5 is odd TRUE.
- If $4 - 3 = 2$ then $1 + 1 = 3$ TRUE.

Proposition: $A \Rightarrow B \equiv \neg A \vee B$.

Pf:

A	B	$A \Rightarrow B$	$\neg A$	$\neg A \vee B$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

equal

∎

Divisibility.

Def'n: Let $m, n \in \mathbb{Z}$ (integers) Zählen. We say that m divides n and write $m \mid n$ if (and only if) there exists a $k \in \mathbb{Z}$ such that

$$mk = n.$$

Ex: $3 \mid 6$, $2 \mid 2$, $7 \mid 49$, $55 \mid 0$, $0 \mid 0$.

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

CODE
BC

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Suppose A, B and C are all true statements.
The compound statement $(\neg A) \vee (B \wedge \neg C)$ is

A) True

B) False ←

$F \vee (T \wedge F)$
$F \vee F$

Q4. In class, I would prefer the use of

A) Document Camera

B) Blackboard

Divisibility: Let $m, n \in \mathbb{Z}$. Then $m | n$ if (and only if) there exists a $k \in \mathbb{Z}$ such that

$$mk = n.$$

Ex: $5 | 15$ $\because$ $5 \cdot 3 = 15$.

$-7 | 0$ $\because$ $(-7) \cdot 0 = 0$.

$0 | 0$ $\because$ $0 \cdot 0 = 0$.

$3 | -27$ $\because$ $3 \cdot (-9) = -27$

If m does not divide n, we write $m \nmid n$

Ex: $5 \nmid 7$ since there no integer satisfying

$$5k = 7.$$

$\boxed{NB}$ $\pi | 3\pi$ doesn't make sense since in the def'n of "$|$", $m, n \in \mathbb{Z}$.

Q: (Direct Proof) $n \in \mathbb{Z} \wedge 14 | n \Rightarrow 7 | n$.

"there exists"

Sol'n: Let $n \in \mathbb{Z}$ and suppose $14 | n$. Then $\exists$ $k \in \mathbb{Z}$ s.t. $14k = n$. Then $(7 \cdot 2)k = n$. By

such that.

associativity, $7(2k) = n$. Since $2k \in \mathbb{Z}$, $7 | n$ $\blacksquare$.

Q: Let $x \in \mathbb{Z}$. Suppose 2^{2x} is an odd integer. Show that 2^{-2x} is odd.

Pf: Recall: An integer n is...

(i) Even if $2 | n$.

(ii) Odd if $2 | (n-1)$

First, note $x \geq 0$ for 2^{2x} to be an integer. If $x \geq 1$ then $2^{2x} = 2 \cdot (\underbrace{2^{2x-1}}_{\in \mathbb{Z}})$ so $2 | 2^{2x}$ and thus, 2^{2x} is not odd.

$\therefore$ $x=0$. Hence $2^{2x}=1$ and $2^{-2x}=1$ is odd!
//

Def'n: An integer p is said to be prime if (and only if) $p>1$ and its only positive divisors are 1 and p.

Ex: Show p & $p+1$ are prime only when $p=2$.

Prop: Bounds by Divisibility (BBD).

$$a|b \wedge b\neq 0 \Rightarrow |a|\leq |b|.$$

Pf: Let $a,b\in\mathbb{Z}$ s.t.: $a|b$ and $b\neq 0$. Then $\exists\, k\in\mathbb{Z}$ s.t. $ak=b$. Since $b\neq 0$ we know that $k\neq 0$. Thus $a=\frac{b}{k}$. Also $|a|=\left|\frac{b}{k}\right|\leq |b|$ since $|k|\geq 1$ $\boxed{\times}$

(Alt: $|a|\leq |a||k|=|b|$)
since $k\neq 0$.

Prop: Transitivity of Divisibility
If $a|b \wedge b|c \Rightarrow a|c$.

Pf: $\exists k \in \mathbb{Z}$ s.t. $ak = b$; $\exists l \in \mathbb{Z}$ s.t. $bl = c$
$\Rightarrow (ak)l = c \Rightarrow a(\underbrace{kl}_{\in \mathbb{Z}}) = c$ so $a|c$ ∎

Prop: Divisibility of Integer Combinations (DIC)
Let $a,b,c \in \mathbb{Z}$. If $a|b \wedge a|c$ then for any $x,y \in \mathbb{Z}$
we have $a|(bx+cy)$

Divisibility of Integer Combinations (DIC)

If $a \mid b$ and $a \mid c$ then for all integers x, y we have $a \mid (bx+cy)$

Pf: Since $a|b$, $\exists k \in \mathbb{Z}$ s.t. $ak=b$.

Since $a|c$, $\exists l \in \mathbb{Z}$ s.t. $al=c$.

Then, $$bx+cy = akx + aly = a(kx+ly)$$

Since $kx+ly \in \mathbb{Z}$, by def'n $a|(bx+cy)$ ∎.

Ex: Prove that if $m \in \mathbb{Z}$ and $14|m$ then $7|135m+693$

Pf: Suppose $m \in \mathbb{Z}$ and $14|m$. Since $7|14$ $(7 \cdot 2 = 14)$ by transitivity, $7|m$. As $7|693$ $(7 \cdot 99 = 693)$ we have, by DIC

$$7 \mid \overset{b}{m}(\overset{x}{135}) + \overset{c}{693}(\overset{y}{1})$$

$$\Rightarrow 7 \mid 135m + 693$$ ∎.

Converse

Def'n: Let A, B be statements. The converse of $A \Rightarrow B$ is $B \Rightarrow A$

Ex: If $p, p+1$ are prime, then $p=2$

Converse: If $p=2$ then $p, p+1$ are prime.

(BBD) $a|b \wedge b \neq 0 \Rightarrow |a| \leq |b|$

Converse: $|a| \leq |b| \Rightarrow a|b \wedge b \neq 0$

NB: the converse is false!

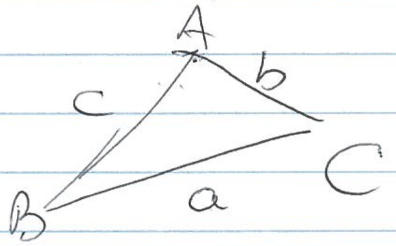
If and only if (iff)

Def'n: $A \Leftrightarrow B$, A iff B, A if and only if B

A	B	A <=> B
T	T	T
T	F	F
F	T	F
F	F	T

Ex: Show $A \Leftrightarrow B$
$\equiv A \Rightarrow B \wedge B \Rightarrow A$.

Ex: In $\triangle ABC$, $b = c \cdot \cos A$ iff $\angle C = \frac{\pi}{2}$



Pf: Suppose $b = c \cdot \cos A$. By the cosine law,

$$a^2 = b^2 + c^2 - 2bc \cos A$$

$$a^2 = b^2 + c^2 - 2b \cdot b$$

$$a^2 = c^2 - b^2$$

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

Using the cosine law again.

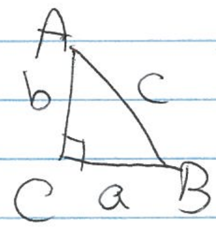
$$c^2 = a^2 + b^2 - 2ab\cos(\angle c)$$

$$\cancel{c^2} = \cancel{c^2} - 2ab\cos(\angle c)$$

$$0 = -2ab\cos(\angle C)$$

Thus $\cos(\angle C) = 0$. Since $0 < \text{angle}\, C < \pi$, we have $\angle C = \pi/2$.

Suppose now that $\angle C = \frac{\pi}{2}$.



Then, $\cos(A) = \frac{b}{c}$. Hence $c \cdot \cos A = b$ $\boxed{}$.

Prove the following. Suppose $x, y \geq 0$. Show that $x = y$ if and only if $\frac{x+y}{2} = \sqrt{xy}$.

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

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

$x^2+2xy+y^2 = 4xy$

$x^2-2xy+y^2 = 0$

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

Thus, $x-y=0 \Rightarrow x=y$.

Suppose $x=y$.

LHS $= \frac{x+y}{2}$

$= \frac{y+y}{2}$

$= \frac{2y}{2}$

$= y$.

RHS $= \sqrt{xy}$

$= \sqrt{y^2}$

$= y$ $(\because y \geq 0)$

LHS = RHS. $\boxtimes$

Set.

Def'n: A set is a collection of elements.

Ex: $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{R}$, $\mathbb{Q}$ (set of rational numbers)

$\{5, A\}$, $S = \{1, 2, \diamond, \}$.

$x \in S$ x in S $x \notin S$ x not in S.

$\{\}$, $\emptyset$ empty set.

nota bene

NB: $\{\emptyset\}$ is NOT the same as the empty set.

This is a set that contains the empty set

§8 Sets

$\{\}$ is different from $\{\emptyset\}$.

$\mathbb{Q} = \{ a/b \in \mathbb{R} : a, b \in \mathbb{Z} \text{ and } b \neq 0 \}$.

In the above example, $\mathbb{R}$ is called the "universe [of discourse]".

Ex: In set notation, write the set of positive integers less than 1000 and which are multiples of 7

Soln: $\{ n \in \mathbb{N} : n < 1000 \wedge 7 \mid n \}$.

$\{ 7k : k \in \mathbb{N} \text{ and } k \leq 142 \}$

↑ such that, s.t. $\ni$. $|$

Describe the following sets using set-builder notation:

1. Set of even numbers between 5 and 14 (inclusive).

$\{6, 8, 10, 12, 14\}$ or $\{n \in \mathbb{N} : 5 \leq n \leq 14 \wedge 2 \mid n\}$

2. All odd perfect squares.

$\boxed{\text{or } \mathbb{N}}$

$\{(2k+1)^2 : k \in \mathbb{Z}\}$.

3. Sets of three integers which are the side lengths of a (non-trivial) triangle.

$\frac{1,1}{2}$

$\{(a, b, c) : a, b, c \in \mathbb{N} \quad a < b+c \wedge b < a+c \wedge c < a+b\}$

4. All points on a circle of radius 8 centred at the origin.

$\{(x, y) : x, y \in \mathbb{R} \wedge x^2 + y^2 = 8^2\}$.

Set Operations:

Let S, T be sets. Define:

$S \cup T = \{x : x \in S \vee x \in T\}$ (union)

$S \cap T = \{x : x \in S \wedge x \in T\}$ (intersection)

$\overline{S}$ or S^c (with respect to Universe $\mathcal{U}$)

$= \{x \in \mathcal{U} : x \notin S\} = \mathcal{U} - S$ (complement)

$S - T = \{x : x \in S \wedge x \notin T\}$ (set difference)

$S \times T = \{(x,y) : x \in S \wedge y \in T\}$. (Cartesian Product).

Ex: $(1,2) \in \mathbb{Z} \times \mathbb{Z}$, $(2,1) \in \mathbb{Z} \times \mathbb{Z}$

BUT $(1,2) \neq (2,1)$.

$\boxed{\text{NB}}$ $\mathbb{Z} \times \mathbb{Z}$ and $\{(n,n) : n \in \mathbb{Z}\}$ are DIFFERENT sets!

Ex: $\mathbb{Z} = \overbrace{\{m \in \mathbb{Z} : 2 \mid m\}}^{\text{EVEN}} \cup \overbrace{\{2k+1 : k \in \mathbb{Z}\}}^{\text{ODD}}$.

& $\emptyset = \{m \in \mathbb{Z} : 2 \mid m\} \cap \{2k+1 : k \in \mathbb{Z}\}$

Def'n: $S \subseteq T$: S is a subset of T.

ie Every element of S is in T

$S \subsetneq T$: Proper/Strict subset

$S \supseteq T$: S contains T

$T \subseteq S$

ie Every element of T is in S.

$S \supsetneq T$: Proper/Strict containment.

S contains T AND $S \neq T$.

Def'n: $S = T$ means $S \subseteq T$ AND $T \subseteq S$.

Ex: $\{1,2\} = \{2,1\}$.

Ex: Prove $\{n \in \mathbb{N} : 4 \mid n+1\} \subseteq \{2k+1 : k \in \mathbb{Z}\}$

Pf: Let $m \in \{n \in \mathbb{N} : 4 \mid n+1\}$. Then $4 \mid m+1$. Thus, $\exists\, l \in \mathbb{Z}$ s.t. $4l = m+1$. Now, $m = 2(2l) - 1$

$$= \underline{2(2l) - 2} + 2 - 1$$
$$= 2(2l-1) + 1$$

Thus, $m \in \{2k+1 : k \in \mathbb{Z}\}$ $\blacksquare$

Ex: Show $S=T$ iff $S\cap T = S\cup T$.

Pf: Suppose $S=T$. Then I claim $S\cap T = S$.
Now, $S\cap T \subseteq S$ since if $x\in S\cap T$, then by def'n $x\in S$. Similarly, if $x\in S$, then $x\in T$ (since $S=T$) and thus $x\in S\cap T$.

Claim 2: $S\cup T = S$.

"$\supseteq$" is clear.

"$\subseteq$" Let $x\in S\cup T$ then either $x\in S$ and we are done OR $x\in T$ and since $S=T$, $x\in S$.

Thus, $S\cap T = S = S\cup T$.

For the converse, suppose $S\cap T = S\cup T$. ~~Let~~

Claim 3: $S\subseteq T$	Claim 4: $T\subseteq S$.
Pf: Let $x\in S$. Then $x\in S\cup T = S\cap T$	Pf: Let $x\in T$. Then $x\in S\cup T = S\cap$
So $x\in T$.	So $x\in S$.

Claims 3 & 4 $\Rightarrow$ $S=T$ $\blacksquare$.

Quantified Statements.

$\boxed{1}$ For every natural number n, $2n^2+11n+15$ is composite.

$\boxed{2}$ There is an integer k such that $6=3k$

$\forall$: For all symbol.

$\boxed{1}$ $\forall n \in \mathbb{N}$, $2n^2+11n+15$ is composite.

$\boxed{2}$ $\exists k \in \mathbb{Z}$ s.t. $6=3k$.

Quantifiers Variables domains Open sentence (involving the variable)

$\forall x \in S, P(x)$: For all x in S, statement $P(x)$ holds

$x \in S \Rightarrow P(x)$

Pf of $\boxed{1}$. Let n be an arbitrary natural number. Then factoring gives $2n^2+11n+15=(2n+5)(n+3)$

Since $2n+5>1$ and $n+3>1$, we have $2n^2+11n+15$ is composite. $\blacksquare$

L7P2

$\exists k \in \mathbb{Z}$ s.t. $6 = 3k$

Pf of $\boxed{2}$ Since $3 \cdot 2 = 6$, $k=2$ satisfies the statement. $\blacksquare$

Ex: $S \subseteq T \equiv \forall x \in S, x \in T$.

L7P3

Prove there is an $x \in \mathbb{R}$ such that $\frac{x^2+3x-3}{2x+3} = 1$.

When $x=2$, note $\frac{2^2+3(2)-3}{2(2)+3} = \frac{7}{7} = 1$. ⊿

$\frac{x^2+3x-3}{2x+3} = 1 \iff x^2+3x-3 = 2x+3 \iff x$

(PROVIDED $x \neq -\frac{3}{2}$)

Note: Vacuously true statement(s)

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

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

Pf: Assume $\forall x \in \mathbb{Z}, a \mid (bx+c)$. For example, when $x=1$, $a \mid (b(1)+c)$. Thus $a \mid (b+c)$ $\blacksquare$.

Q: $\exists\, m \in \mathbb{Z}$ s.t. $\frac{m-7}{2m+4} = 5$.

A: When $m=-3$, note $\frac{m-7}{2m+4} = \frac{-3-7}{2(-3)+4} = \frac{-10}{-2} = 5$ $\blacksquare$

L7P5

Show that for each $x \in \mathbb{R}$, $x^2 + 4x + 7 > 0$.

Let $x \in \mathbb{R}$ be arbitrary. Then

$$\begin{aligned} x^2+4x+7 &= x^2+4x+4-4+7 \\ &= (x+2)^2+3 \\ &> 0. \end{aligned}$$

$\boxtimes$.

Sometimes $\forall$ and $\exists$ are hidden! If you encounter a statement with quantifiers, take a moment to make sure you understand what the question is saying/asking.

Examples:

1. $2n^2 + 11n + 15$ is never prime when n is a natural number. $\forall n \in \mathbb{N},\ 2n^2+11n+15$ is not prime.
2. If n is a natural number, then $2n^2 + 11n + 15$ is composite. $\forall n \in \mathbb{N},\ 2n^2+11n+15$ is Composite.
3. $\frac{m-7}{2m+4} = 5$ for some integer m. $\exists m$ s.t. $\frac{m-7}{2m+4} = 5$.
4. $\frac{m-7}{2m+4} = 5$ has an integer solution. $\nearrow$.

Domain is Important!

Let $P(x)$ be the statement $x^2 = 2$.

Let $S = \{-\sqrt{2}, \sqrt{2}\}$.

Which of the following are true?

$\exists x \in \mathbb{Z}, P(x)$ FALSE $\quad\quad$ $\forall x \in \mathbb{Z}, P(x)$ FALSE.

$\exists x \in \mathbb{R}, P(x)$ TRUE $\quad\quad$ $\forall x \in \mathbb{R}, P(x)$ FALSE.

$\exists x \in S, P(x)$ TRUE. $\quad\quad$ $\forall x \in S, P(x)$ TRUE.

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2.When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Consider the following statement.

$$\{2k : k \in \mathbb{N}\} \supseteq \{n \in \mathbb{Z} : 8 \mid (n+4)\}$$

A well written and correct direct proof of this statement could begin with

A) We will show that the statement is true in both directions.

B) Assume that $8 \mid (n+4)$ where n is an integer. (CORRECT)

C) Let $m \in \{n \in \mathbb{Z} : 8 \mid (n+4)\}$.

D) Let $m \in \{2k : k \in \mathbb{N}\}$.

E) Assume that $8 \mid (2k+4)$.

Notes:

1. A single counter example proves that $(\forall x \in S, P(x))$ is false.

   Claim: Every positive even integer is composite.

   This claim is false since 2 is even but 2 is prime.

2. A single example does not prove that $(\forall x \in S, P(x))$ is true.

   Claim: Every even integer at least 4 is composite.

   This is true but we cannot prove it by saying "6 is an even integer and is composite." We must show this is true for an arbitrary even integer x. (Idea: $2 \mid x$ so there exists a $k \in \mathbb{N}$ such that $2k = x$ and $k \neq 1$.)

3. A single example does show that $(\exists x \in S, P(x))$ is true.

   Claim: Some even integer is prime.

   This claim is true since 2 is even and 2 is prime.

4. What about showing that $(\exists x \in S, P(x))$ is false?

   Idea: $(\exists x \in S, P(x))$ is false $\equiv \forall x \in S, \neg P(x)$ is true. This idea is central for proof by contradiction which we will see later.

Negating Quantifiers.

~~Q~~: Negate the following.

1: Everybody in this room was born before 2010.

Negation: Somebody in this room was NOT born before 2010.

2: Someone in this room was born before 1990. (1987).

Negate: Everyone in this room was born after 1990.

3. $\forall x \in \mathbb{R}, |x| < 5$

Negate: $\exists x \in \mathbb{R}, |x| \geq 5 \equiv \neg(\forall x \in \mathbb{R}, |x| < 5)$

4. $\exists x \in \mathbb{R}, |x| \leq 5$

$\forall x \in \mathbb{R}, |x| > 5$.

NB: A proof that a statement is false is called a disproof.

L894

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

Q: Prove or disprove: If $a | bc$ then $a | b \vee a | c$.

Sol'n: This is false! A counter example is given by $a = 6$, $b = 2$, $c = 3$. Then $a | bc$. BUT $6 \nmid 2$ and $6 \nmid 3$.

Fix: Include that a must be prime. Proof is an exercise.

Which of the following are true?

1. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$ FALSE (Choose $x=0$, $y=0$)
2. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$ TRUE ($x=1, y=0$)
3. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$
4. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$

$\boxed{3}$ TRUE: Pf: Let $x \in \mathbb{R}$ be arbitrary. Then Choose $y = \sqrt[3]{x^3-1}$. Then

$$x^3 - y^3 = x^3 - \left(\sqrt[3]{x^3-1}\right)^3 = x^3 - (x^3-1) = 1. \qquad \blacksquare$$

$\boxed{4}$ FALSE. Idea: Negate and show the negation is true.

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

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

Let $x \in \mathbb{R}$ be arbitrary. Take $y = x$. Then

$$x^3 - y^3 = x^3 - x^3 = 0 \neq 1. \qquad \blacksquare$$

L8P6

Notation Cheat Sheet

1. $+$ Addition
2. $-$ Subtraction
3. $\times$, $\cdot$ Multiplication
4. $\div$,/ Division
5. $\mathbb{N}$ Natural Numbers
6. $\mathbb{Z}$ Integers (Zählen)
7. $\mathbb{Q}$ Rational Numbers (Quoziente)
8. $\mathbb{R}$ Real Numbers
9. $\neg$ Not, Negation
10. $\vee$ Or
11. $\wedge$ And
12. $|$ Divides
13. $\Rightarrow$ Implies (If... Then)
14. $\Leftrightarrow$, (iff) If and Only If
15. $\in$ In
16. $\notin$ Not In
17. $\{\}$, $\emptyset$ Empty Set
18. $\cap$ Intersection (Of Sets)
19. $\cup$ Union (Of Sets)
20. $\subset$ Subset
21. $\subseteq$ Subset Or Equal
22. $\subsetneq$ Proper/Strict Subset (Subset Not Equal)
23. $\supset$ Contains
24. $\supseteq$ Contains Or Equal
25. $\supsetneq$ Properly/Strictly Contains (Contains Not Equal)
26. $\forall$ For All
27. $\exists$ There Exists

L8P7

List all elements of the set:

$$\{n \in \mathbb{Z} : n > 1 \land ((m \in \mathbb{Z} \land m > 0 \land m \mid n) \Rightarrow (m = 1 \lor m = n))\} \\ \cap \{n \in \mathbb{Z} : n \mid 42\}$$

L8P7
L9P1

List all elements of the set: if m is a positive divisor of n then $m=1$ or $m=n$.

$$S = \{n \in \mathbb{Z} : n > 1 \wedge ((m \in \mathbb{Z} \wedge m > 0 \wedge m \mid n) \Rightarrow (m = 1 \vee m = n))\}$$

$$\cap \underbrace{\{n \in \mathbb{Z} : n \mid 42\}}_{\{\cancel{\pm 1}, \pm 2, \pm 3, \cancel{\pm 6}, \pm 7, \cancel{\pm 14}, \cancel{\pm 21}, \cancel{\pm 42}\}}$$

Set of all Primes!

Thus, $S = \{2, 3, 7\}$.

L9 P2

Rewrite the following using as few English words as possible.

1. No multiple of 15 plus any multiple of 6 equals 100.
2. Whenever three divides both the sum and difference of two integers, it also divides each of these integers.

1. $\forall m, n \in \mathbb{Z}, \ (15m + 6n \neq 100)$.

2. $\forall m, n \in \mathbb{Z} \ ((3 \mid (m+n) \wedge 3 \mid (m-n)) \Rightarrow 3 \mid m \wedge 3 \mid n)$.

L9 P3

Write the following statements in (mostly) plain English.

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

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

1. If m is an even integer, then $7m^2+4$ is even.

2. For every integer, ~~there~~ there exists a greater integer.

There is no greatest integer.

Contrapositive.

<u>Moral</u>: Direct proofs are not always easy to find.

Eg: $7 \nmid n \Rightarrow 14 \nmid n \equiv 14 \mid n \Rightarrow 7 \mid n$.

Contrapositive Def'n:

The contrapositive of $H \Rightarrow C$ is $\neg C \Rightarrow \neg H$

Note: $H \Rightarrow C \equiv \neg C \Rightarrow \neg H$.

$$H \Rightarrow C \equiv \neg H \vee C \equiv C \vee \neg H$$
$$\equiv \neg(\neg C) \vee \neg H$$
$$\equiv \neg C \Rightarrow \neg H.$$

H	C	$H \Rightarrow C$	$\neg C$	$\neg H$	$\neg C \Rightarrow \neg H$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Ex: Let $x \in \mathbb{R}$. Prove $x^3 - 5x^2 + 3x \neq 15 \Rightarrow x \neq 5$.

Pf: We prove the contrapositive. Let $x = 5$. Then

$$x^3 - 5x^2 + 3x = (5)^3 - 5(5)^2 + 3(5)$$
$$= \cancel{5^3} - \cancel{5^3} + 15$$
$$= 15.$$

Irrationals.

Ex: Suppose $a, b \in \mathbb{R}$ and $ab \in \underbrace{\mathbb{R} - \mathbb{Q}}$. Show either $a \in \mathbb{R} - \mathbb{Q}$ OR $b \in \mathbb{R} - \mathbb{Q}$.

Pf: Proceed by contrapositive. Suppose a is rational and b is rational. Then, $\exists\, k, l, m, n \in \mathbb{Z}$ s.t. $a = \frac{k}{l}$ and $b = \frac{m}{n}$ with $l, n \neq 0$. Then

$$ab = \frac{km}{ln} \in \mathbb{Q}.$$

L10P0

Announcements

1. Office hours Thursday moved to 12 - 1:30.
2. Away Friday - Tuesday. Office hours covered by Shane Bauman (M: 9:30 - 10:30 & Tu 2 - 3:30).
3. A3 posted. Make sure by Thursday you have the link!
4. Clicker Thursday!

Prove that if $x \in \mathbb{R}$ is such that $x^3 + 7x^2 < 9$, then $x < 1.1$.

Pf: We prove the contrapositive.

Suppose $x \geq 1.1 \geq 1$. Then since $x > 0$,

$$x^3 + 7x^2 \geq (1.1)^3 + 7(1.1)^2$$

$$= \left(\frac{11}{10}\right)^3 + 7\left(\frac{11}{10}\right)^2$$

$$= \frac{1331}{1000} + 7\left(\frac{121}{100}\right)$$

$$= \frac{1331}{1000} + \frac{8470}{1000}$$

$$= \frac{9801}{1000} \geq 9. \quad \blacksquare$$

PASCAL'S Δ.

1

1 1

1 2 1

1 3 3 1

Types of Implications.

Let A, B, C be statements.

1. $A \wedge B \Rightarrow C$ (Seen: DIC. Trans. BBD)
2. $A \Rightarrow B \wedge C$

Ex: Let S, T, U be sets. If $(S \cup T) \subseteq U$ then $S \subseteq U$ and $T \subseteq U$.

Pf: Suppose $S \cup T \subseteq U$. If $x \in S$, then $x \in S \cup T \subseteq U$ so $x \in U$. Thus $S \subseteq$
By symmetry (similarly) $T \subseteq U$. $\square$.

3. $A \vee B \Rightarrow C$

Ex:* $x=1 \vee y=2 \Rightarrow x^2y + y - 2x^2 + 4x - 2xy = 2$.

Pf: If $x=1$, then LHS $= y + y - 2 + 4 - 2y = 2 =$ RHS.
If $y=2$, then LHS $= 2x^2 + 2 - 2x^2 + 4x - 4x = 2 =$ RH
$\square$

4. $A \Rightarrow B \vee C$. (Elimination).

Ex: If $x^2 - 7x + 12 \geq 0$ then $x \leq 3 \vee x \geq 4$

Pf: Suppose $x^2 - 7x + 12 \geq 0$ and $x > 3$.

Then, $0 \leq x^2 - 7x + 12 = \underbrace{(x-3)}_{+}\underbrace{(x-4)}_{\therefore \geq 0}$.

$\therefore x - 4 \geq 0$ hence $x \geq 4$. ∎.

L10P4

How many years has it been since the Toronto Maple Leafs have won the Stanley Cup?

A) ~~-3~~

$\boxed{\text{B) 48}}$

C) ~~1000000~~

D) ~~1500~~

Proof By Contradiction.

Let S be a statement. Then $S \wedge \neg S$ is false.

Ex: There is no largest integer.

Pf: Assume towards a contradiction that M_0 is the largest integer. Then since $M_0 < M_0 + 1$ and $M_0 + 1 \in \mathbb{Z}$, we have contradicted the def'n of M_0. $\#$ Thus, no largest integer exists. $\blacksquare$

Well Ordering Principle: (Axiom)

Every subset of the natural numbers that is nonempty contains a least element.

Example: Let $n \in \mathbb{Z}$ such that n^2 is even. Show that n is even.

Direct Proof: As n^2 is even, there exists a $k \in \mathbb{Z}$ such that

$$n \cdot n = n^2 = 2k.$$

Since the product of two integers is even if and only if at least one of the integers is even, we conclude that n is even.

Proof By Contradiction: Suppose that n^2 is even. Assume towards a contradiction that n is odd. Then there exists a $k \in \mathbb{Z}$ such that $n = 2k + 1$. Now,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Hence, n^2 is odd, a contradiction since we assumed in the statement that n^2 is even. Thus n is even.

Example: Prove that $\sqrt{2}$ is irrational.

Proof: Assume towards a contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ with $a, b \neq 0$ and $a, b \in \mathbb{N}$ (Think: Why is it okay to use $\mathbb{N}$ instead of $\mathbb{Z}$?).

Proof 1 (Well Ordering Principle): Let

$$S = \{n \in \mathbb{N} : n\sqrt{2} \in \mathbb{N}\}.$$

Since $b \in S$, we have that S is nonempty. By the Well Ordering Principle, there must be a least element of S, say k. Now, notice that

$$k(\sqrt{2} - 1) = k\sqrt{2} - k \in \mathbb{N}$$

(positive since $\sqrt{2} > \sqrt{1} = 1$). Further,

$$k(\sqrt{2} - 1)\sqrt{2} = 2k - k\sqrt{2} \in \mathbb{N}$$

and so $k(\sqrt{2} - 1) \in S$. However, $k(\sqrt{2} - 1) < k$ which contradicts the definition of k. Thus, $\sqrt{2}$ is not rational.

Proof 2 (Infinite Descent): Isolating from $\sqrt{2} = \frac{a}{b}$, we see that $2b^2 = a^2$. Thus a^2 is even hence a is even. Write $a = 2k$ for some integer k. Then $2b^2 = a^2 = (2k)^2 = 4k^2$. Hence $b^2 = 2k^2$ and so b is even. Write $b = 2\ell$ for some integer ℓ. Then repeating the same argument shows that k is even. So $a = 2k = 4m$ for some integer m. Since we can repeat this argument indefinitely and no integer has infinitely many factors of 2, we will (eventually) reach a contradiction. Thus, $\sqrt{2}$ is not rational.

Proof 3 (Simplified proof 2): Assume further that a and b share no common factor (otherwise simplify the fraction first). Then $2b^2 = a^2$. Hence a is even. Write $a = 2k$ for some integer k. Then $2b^2 = a^2 = (2k)^2 = 4k^2$ and canceling a 2 shows that $b^2 = 2k^2$. Thus b^2 is even and hence b is even. However, then a and b share a common factor, a contradiction.

41P1

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Let $n \in \mathbb{Z}$. Consider the following implication.

$$\text{If } \overbrace{(\forall x \in \mathbb{R},\ x \leq 0 \ \vee \ x+1 > n)}^{H}, \text{ then } \underbrace{n = 1}_{C}.$$

The contrapositive of this implication is

A) If $n = 1$, then $(\forall x \in \mathbb{R},\ x \leq 0 \ \vee \ x+1 > n)$.

B) If $n = 1$, then $(\exists x \in \mathbb{R},\ x > 0 \ \wedge \ x+1 \leq n)$.

C) If $n \neq 1$, then $(\exists x \in \mathbb{R},\ x \geq 0 \ \wedge \ x+1 < n)$.

D) If $n \neq 1$, then $(\forall x \in \mathbb{R},\ x \leq 0 \ \vee \ x+1 > n)$.

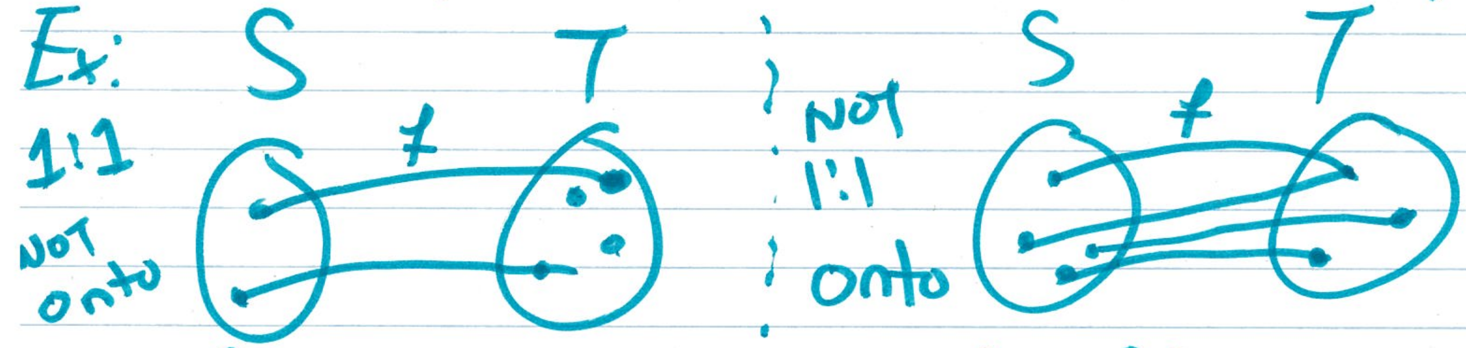
E) None of the above.

Injections & Surjections. 41 P2

Def'n: Let S & T be sets. A function $f: S \to T$ is said to be

(i) Injective (or one to one or 1:1) iff $\forall x, y \in S \quad f(x) = f(y) \Rightarrow x = y$.

Ex:



(ii) Surjective (or onto) iff $\forall y \in T \ \exists x \in S$ s.t. $f(x) = y$.

Ex: Prove $f: \mathbb{R} \xrightarrow{\text{to}} \mathbb{R}$ is not injective
$x \mapsto x^2$

$f(x) = x^2$

maps to

Pf: Note that
$f(-1) = (-1)^2 = 1 = (1)^2 = f(1)$ BUT $-1 \neq 1$. Thus, f is not 1:1. $\blacksquare$

Ex: Prove that $f: \mathbb{R} \to \mathbb{R}$ is 1:1.

$$x \mapsto 2x^3+1$$

Pf: Let $x, y \in \mathbb{R}$ s.t. $f(x) = f(y)$. Then

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

$$x^3 = y^3$$

$$\sqrt[3]{x^3} = \sqrt[3]{y^3}$$

$x = y$. Thus, f is injective $\blacksquare$.

Ex: Prove that $f: \mathbb{R} \to (-\infty, 1)$ is onto

$$x \mapsto 1 - e^{-x}$$

Need to show every $y \in (-\infty, 1)$ has some $x \in \mathbb{R}$ with $f(x) = y$.

Pf: Take $x = -\ln(1-y)$ for any $y \in (-\infty, 1)$.

Then $f(x) = 1 - e^{-x} = 1 - e^{-(-\ln(1-y))}$

$= 1 - e^{\ln(1-y)} = 1 - (1-y)$

$= y$. $\therefore f$ is onto $\blacksquare$.

Uniqueness: $\exists!$ "There exists a unique."

To prove uniqueness, either
(i) Assume $\exists\, x, y \in S$ s.t. $P(x) \wedge P(y)$ is true and show $x = y$. statement
(ii) Show $\exists\, x \in S$ s.t. $P(x)$ is true. Then use contradiction to show that if $\exists\, x, y \in S$ distinct s.t. $P(x) \wedge P(y)$ is true, then derive a contradiction.

Ex: Suppose $x \in \mathbb{R} - \mathbb{Z}$ and $m \in \mathbb{Z}$ s.t. $x < m < x+1$. Show m is unique.

Pf: Assume towards a contradiction that $\exists\, m, n \in \mathbb{Z}$ distinct s.t.

$$x < m < x+1 \text{ and } x < n < x+1.$$

Now, $0 < m - n < 1$ BUT $m - n \in \mathbb{Z}$. #. Thus, m is unique. ∎

Division Algorithm (Grade school division).

$$\overset{a}{51} = \overset{b}{7}(\overset{q}{7}) + \overset{r}{2}$$

$$-35 = 6(-6) + 1$$

"$\frac{a}{b}$ ="

Thm: Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Then $\exists!$ $q, r \in \mathbb{Z}$ s.t. $a = bq + r$ where $0 \leq r < b$.

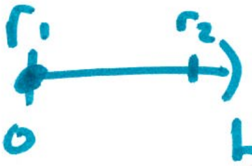
Pf: Existence: Use Well Ordering Principle on $S = \{a - bq : a - bq \geq 0 \wedge q \in \mathbb{Z}\}$

Division Algorithm Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then $\exists!\, q, r \in \mathbb{Z}$ such that $a = qb + r$ where $0 \leq r < b$.

Proof of the division algorithm (UNIQUENESS):
Suppose that $a = q_1 b + r_1$ with $0 \leq r_1 < b$. Also, suppose that $a = q_2 b + r_2$ with $0 \leq r_2 < b$ and $r_1 \neq r_2$. Without loss of generality, we can assume $r_1 < r_2$. WLOG

(if $r_1 \neq r_2$ then one is bigger!)

Then $0 < r_2 - r_1 < b$ and $\underbrace{(q_1 - q_2)b = r_2 - r_1}$. (Take difference of a's).



biggest gap. By def'n

Hence $b \mid (r_2 - r_1)$. By Bounds By Divisibility, $b \leq r_2 - r_1$ which contradicts the fact that $r_2 - r_1 < b$. # no $|b|$ $\because b \in \mathbb{N}$.

Therefore, the assumption that $r_1 \neq r_2$ is false and in fact $\underbrace{r_1 = r_2}$. But then $(q_1 - q_2)b = \underbrace{r_2 - r_1}_{=0}$ implies $q_1 = q_2$.

Oct 2nd, 15

$f(\mathbb{Z}) = \{y \in \mathbb{Z} : f(x) = y \text{ For some } x \in \mathbb{Z}\}$
$= \{f(x) : x \in \mathbb{Z}\}$

$f : \mathbb{Z} \to \mathbb{Z}$

$$f(n) = \max\{1001, n\} = \begin{cases} 1001 & n \le 1001 \\ n & n \geq 1001 \end{cases}$$

is f injective?
is f surjective?

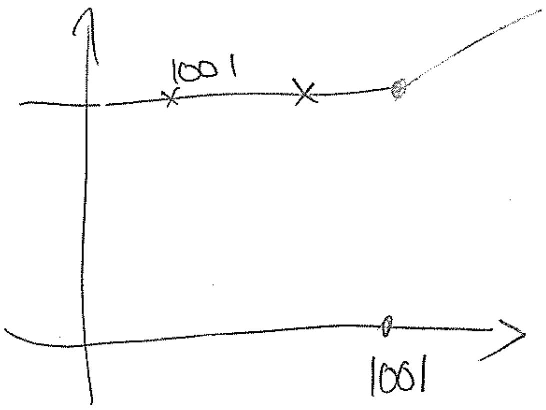
$\forall m, n \in \mathbb{Z}, m \neq n \Rightarrow f(m) \neq f(n)$

$\equiv$

$\forall m, n \in \mathbb{Z}, f(m) = f(n) \Rightarrow m = n$

No!

$f(1) = f(2) = 1001,$
$1 \neq 2, \; 1, 2 \in \mathbb{Z}$



$\forall y \in \mathbb{Z}, \; \exists x \in \mathbb{Z}, \text{ s.t } f(x) = y$

NO! E.g. $1000 \in \mathbb{Z}$
But $f(n) \neq 1000$ For any $n \in \mathbb{Z}$

Let $n \in \mathbb{Z}$, either $n \geq 1001$ OR $n \le 1001$. If $n \le 1001$, then $f(n) = 1001 \neq 1000$.
If $n \geq 1001$, Then $f(n) = n \geq 1001 > 1000$.

E.g $f: \mathbb{R} \to \mathbb{R}$

$f(x) = x^2$

$f(-1) = f(1) = 1 \quad \because -1 \neq 1, \quad -1, 1 \in \mathbb{R}$

not injective

not surjective: $-1 \neq f(x) = x^2$ for any $x \in \mathbb{R}$.

$x^2 \geq 0 > -1$

continued: Let $x_1, x_2 \in \mathbb{R}_{\geq 0}$. suppose $f(x_1) = f(x_2)$

so $x_1^2 = x_2^2$

$x_1^2 - x_2^2 = 0$

$(x_1 + x_2)(x_1 - x_2) = 0$

$x_1 + x_2 = 0$ OR $x_1 - x_2 = 0$

$x_1 = -x_2$ OR $x_1 = x_2$

$\because x_2 \geq 0, \; x_1 < 0$, not part of domain

$\therefore x_1 = x_2$.

3. Show that if $r \in \mathbb{R} - \mathbb{Q}$ then $\frac{1}{r} \in \mathbb{R} - \mathbb{Q}$

prove by contrapositive

$\frac{1}{r} \in \mathbb{Q} \Rightarrow r \in \mathbb{Q}$

Suppose $\frac{1}{r}$ is rational.

Then $\exists\, a, b \in \mathbb{Z}, \underline{a, b \neq 0}$ such that $\frac{1}{r} = \frac{a}{b}$.

Then $\frac{r}{1} = \frac{b}{a} \in \mathbb{Q}$

Let $x \in \mathbb{R}$, show that $x^2 - x > 0 \iff x \notin [0,1]$.

2. $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$ $\qquad$ $P \iff Q \equiv \neg P \iff \neg Q$

$Q \Rightarrow P \equiv \neg P \Rightarrow \neg Q$

$x^2 - x \leq 0 \iff x \in [0,1]$

5. Contrapositive:

IF $a \mid c$ then either $a \mid b$ OR $a \nmid b+c$.

$$\equiv P \Rightarrow (Q \cup R)$$
$$(P \wedge \neg Q) \Rightarrow R$$

suppose $a \mid c$, suppose also $a \mid b+c$

We want to conclude that $a \mid b$.

Since $a \mid c$, and $a \mid b+c$, $a \mid (b+c-c) = b$

By divisibility of integer combination.

$$P \Rightarrow (Q \wedge R) \equiv (P \wedge \neg Q) \Rightarrow R$$

5. prove by contradiction:

suppose $a \nmid b$ and $a \mid b+c$

Want: $a \nmid c$

assume towards contradiction, $a \mid c$.

$a \mid b+c$ & $a \mid c$, so $a \mid b+c-c = b$

contradiction.

6. Show that the sum of the first n odd positive integer equals n^2.

$1+2+3 \cdots +100$

$1+3+5 \cdots +2n-1$

$2n-1 + 2n-3 + 2n-5 \cdots + 1$

$2n \quad 2n \quad 2n \cdots \quad 2n$

$2n \cdot n = 2n^2$ $\Rightarrow$ divides by 2: n^2.

tn times

sum & product notation

$$\sum_{1\le i\le n} = \sum_{i=1}^{n} x_i = x_1 + x_2 \dots + x_n$$

$$\sum_{S} = \text{Sum of elements of } S$$

$$\sum_{x\in\emptyset} = 0 \text{ ; convention} \qquad \prod_{x\in\emptyset} x = 1$$

$$\sum_{j=k}^{2k} \frac{1}{j} = \frac{1}{k} + \frac{1}{k+1} + \dots \frac{1}{2k}$$

$$\sum_{j=2} j = 0 \rightarrow \prod_{j=2} j = 1$$

$$\prod_{\substack{p \text{ prime} \\ p\le 3}} \left(1-\frac{1}{p^2}\right) = \left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)$$

Factorial :

$$n! = \prod_{j=1}^{n} j \qquad n \in \mathbb{N} \cup \{0\}$$

$0! = 1$

$1! = 1$ $\qquad (n+1)! = (n+1)\,n!$

$2! = 2\times 1$

$3! = 3\times 2\times 1$

Challenge: Find $n \in \mathbb{N}$ s.t. $(1!+2! \dots + n!) \mid (n+1)!$

principle of mathematical induction (form 1)

Recall sum & product notation from Friday:

$$\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + \dots + n^3$$

$$\prod_{j=n}^{2n} \frac{1}{j-1} = \frac{1}{n-1} \cdot \frac{1}{n+1-1} \cdots \frac{1}{2n-1} \text{ etc}$$

"Factorial" $0! = 1$, $n! = n \times (n-1)! = n(n-1) \dots 2(1)$
$\{n \geq 1\}$

A sequence $P(1), P(2) \dots$ are true if (i)

(i) $\to$ $P(1)$ is true

(ii) $\to$ For any $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

(P_1) is true by (i)

$(P_1) \Rightarrow P(2)$ is true by (ii) w/ $(k=1)$

$\therefore P(2)$ is true

$P(2) \Rightarrow P(3)$ by (ii) w/ $(k=2)$

$\therefore P(3)$ is true

In practice, induction argument proceeds as follows:

1. base case: verify $P(1)$ is true
2. inductive hypothesis: Let $k \in \mathbb{N}$ be ARBitrary. Assume $P(k)$ is true
3. ind conclusion deduce $P(k+1)$ is true.

$\therefore$ by pmi 1 $P(n)$ holds $\forall n \in \mathbb{N}$.

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

2. $\forall n \in \mathbb{N}$,

$$\sum_{j=1}^{n} j^2 = \frac{1}{6}n(n+1)(2n+1) \cdots (P(n))$$

Base case :

For $n=1$, Have

$$\sum_{j=1}^{1} j^2 = 1^2 = 1 = \frac{1}{6}(1)(1+1)(2(1)+1) \checkmark \therefore P(1) \text{ holds.}$$

IH : Let k be arbitrary

Assume $P(k)$ holds. I.E.

$$\sum_{j=1}^{k} j^2 = \frac{1}{6}k(k+1)(2k+1) \cdots (1+1)$$

ind conclusion:

we want to show $P(k+1)$ holds, i.e.

$$\sum_{j=1}^{k+1} j^2 = \frac{1}{6}(k+1)(k+2)(2k+3)$$

Now,

$$\sum_{j=1}^{k+1} j^2 = \sum_{j=1}^{k} j^2 + (k+1)^2$$

$\parallel$ (IH)

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2$$

By inductive hypothesis

$$= (k+1)\left[\frac{1}{6}k(2k+1) + (k+1)\right]$$

$$= \frac{1}{6}(k+1)\left[k(2k+1) + 6(k+1)\right]$$

$$= \frac{1}{6}(k+1)\left[2k^2 + k + 6k + 6\right]$$

$$= \frac{1}{6}(k+1)(k+2)(2k+3) \triangleleft$$

principle of mathematical induction

∴ Hence $P(k+1)$. holds
By POMI $P(n)$ holds $\forall n \in \mathbb{N}$

3 $\forall n \in \mathbb{N}$

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

<u>Base case</u>, For $n = 1$, have

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

so $P(1)$ holds.

<u>IH</u> Let $k \in \mathbb{N}$ be Arbitrary, assume $P(k)$ holds. I.E

$$\prod_{j=2}^{k} \left(1 - \frac{1}{j^2}\right) = \frac{k+1}{2k} \qquad \text{.... (IH)}$$

Induction conclusion: want to show $P(k+1)$ holds I.E

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

want to be the same

Now

$$\prod_{j=2}^{k+1} \left(1 - \frac{1}{j^2}\right) = \underbrace{\left[\prod_{j=2}^{k} \left(1 - \frac{1}{j^2}\right)\right]}_{\text{IH}} \cdot \left[1 - \frac{1}{(k+1)^2}\right]$$

$$= \left(\frac{k+1}{2k}\right) \times \left[1 - \frac{1}{(k+1)^2}\right] \qquad \text{By IH}$$

⋮

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

∴ Hence $P(k+1)$ holds.

4. $\forall n \in \mathbb{N}$, $n \geqslant 4$,

$n! > 2^n$ ... $P(n)$

Base case: For $n = 4$,

$4! = 24$ $\quad 24 > 16 = 2^4$ ✓

$2^4 = 16$

$\therefore$ $P(4)$ holds

<u>IH</u> Let $k \in \mathbb{N}$, $k \geqslant 4$. Assume $P(k)$ holds.

I.E. $k! > 2^k$ ... (IH)

<u>Ind Conc</u> We want to show $P(k+1)$ holds, I.E.

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

Now,

$$(k+1)! = (k+1)\,k!$$

$\vee$

2^k

$\begin{bmatrix} a, b, c \geqslant 0 \\ b \geqslant c \\ ab \geqslant ac \end{bmatrix}$

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

$\geqslant \cancel{2 \cdot 2}$

$\because k+1 \geqslant 2$ Since $k+1 \geqslant 2$

(In fact, $k+1 \geqslant 5$)

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

POMI "Take 2"

A sequence $P(1)$, ... of statement are all true if

(i) $P(1) \wedge P(2)$ is true.

(ii) For $k \in \mathbb{N}$, if $P(k)$ & $P(k+1)$ are true, then $P(k+2)$ is true.

6. Let $a_1 = 2$, $a_2 = 3$, & $a_{n+2} = 3a_{n+1} - 2a_n$ $\forall n \in \mathbb{N}$

prove: $a_n = 2^{n-1} + 1$ $(P(n))$

$\forall n \in \mathbb{N}$

Base cases: For $n=1$

$a_1 = 2 = 2^{1-1} + 1$ ✓

For $n=2$

$a_2 = 3 = 2^{2-1} + 1$ ✓

So $P(1)$ & $P(2)$ hold.

IH: Let $k \in \mathbb{N}$. Assume $P(k)$ & $P(k+1)$ hold.

I.E. $a_k = 2^{k-1} + 1$ & $a_{k+1} = 2^k + 1$ ... (IH)

Ind Conclusion: we want to show $P(k+2)$ holds, I.E.

$$a_{k+2} = 2^{k+1} + 1$$

Now,

$$a_{k+2} = 3a_{k+1} - 2a_k \quad \text{by definition}$$

$$= 3(2^k+1) - 2(2^{k-1}+1) \quad \text{By (IH)}$$

$$= 3 \times 2^k + 3 - 2 \times 2^{k-1} - 2$$

$$= 3 \times 2^k - 2 \cdot 2^{k-1} + 1$$

$$= 2^k(3-1) + 1 \qquad \boxed{2 \cdot 2^{k-1} = 2^k}$$

$$= 2^k \cdot 2 + 1$$

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

L14 P1
(Survey Lecture)

Ex: Prove $P(n)$: $6 \mid 2n^3+3n^2+n \quad \forall n \in \mathbb{N}$.

Base Case: $n=1$

$2n^3+3n^2+n = 2+3+1 = 6$ and $6 \mid 6$ ✓.

Induction Hypothesis (IH):

Assume $P(k)$ is true for some $k \in \mathbb{N}$.

ie. $\exists \ell \in \mathbb{Z}$ s.t. $6\ell = 2k^3+3k^2+k$.

Inductive Step: Prove $P(k+1)$ is true.

$$2(k+1)^3+3(k+1)^2+(k+1)$$
$$= 2k^3+6k^2+6k+2+3k^2+6k+3+k+1$$
$$= \underbrace{2k^3+3k^2+k}+6k^2+12k+6.$$
$$\overset{IH}{=} 6\ell+6k^2+12k+6$$
$$= 6\underbrace{(\ell+k^2+2k+1)}_{\in \mathbb{Z}}.$$

$\therefore 6 \mid 2(k+1)^3+3(k+1)^2+(k+1)$

$\therefore P(k+1)$ is true

So, by POMI, $P(n)$ is true $\forall n \in \mathbb{N}$. ∎

L14P7

Let $\{x_n\}$ be a sequence defined by $x_1 = 4$, $x_2 = 68$ and

$$x_m = 2x_{m-1} + 15x_{m-2} \qquad \text{for all } m \geq 3$$

Prove that $x_n = 2(-3)^n + 10 \cdot 5^{n-1}$ for $n \geq 1$.

Solution: We proceed by induction.

Base Case: For $n = 1$, we have

$$x_1 = 4 = 2(-3)^1 + 10 \cdot 5^0 = 2(-3)^n + 10 \cdot 5^{n-1}.$$

Inductive Hypothesis: Assume that

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

is true for some $k \in \mathbb{N}$.

Inductive Step: Now, for $k + 1$,

$$\begin{aligned} x_{k+1} &= 2x_k + 15x_{k-1} \\ &= 2(2(-3)^k + 10 \cdot 5^{k-1}) + 15x_{k-1} \\ &= 4(-3)^k + 20 \cdot 5^{k-1} + 15x_{k-1} \\ &= \ldots? \end{aligned}$$

Principle of Strong Induction.

Let $P(n)$ be a statement. If

(i) $P(1), P(2), \dots, P(b)$ are true for some $b \in \mathbb{N}$

(ii) $P(1) \wedge P(2) \wedge \dots \wedge P(k)$ true $\Rightarrow P(k+1)$ is true $\forall k \in \mathbb{N}$

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

Q: Let $\{x_n\}$ be a sequence s.t.

$x_1 = 4$, $x_2 = 68$ and

$$x_m = 2x_{m-1} + 15x_{m-2} \quad \forall m \geq 3.$$

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

Pf: Base Cases.

$n=1$ $\quad x_1 = 4 = 2(-3)^1 + 10 \cdot 5^{1-1} = 2(-3)^n + 10 \cdot 5^{n-1}$

$n=2$ $\quad x_2 = 68$ & $2(-3)^2 + 10 \cdot 5^{2-1} = 18 + 50 = 68$.

IH: $P(i)$ is true for all $i \in \{1, 2, \dots k\}$ for some $k \in \mathbb{N}$ $(k \geq 2)$.

IStep: For $k \in \mathbb{N}$ with $k \geq 2$,

$$x_{k+1} = 2x_k + 15x_{k-1} \quad (\because k+1 \geq 3)$$

$$\overset{IH}{=} 2\left(2(-3)^k + 10 \cdot 5^{k-1}\right) + 15\left(2(-3)^{k-1} + 10 \cdot 5^{k-2}\right)$$

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

$$= (-3)^{k-1}(-12 + 30) + 5^{k-2}(100 + 150)$$

$$= (-3)^{k-1}(18) + 5^{k-2}(250)$$

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

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

Thus $P(k+1)$ is true.

Hence $P(n)$ is true $\forall n \in \mathbb{N}$ by POSI. $\blacksquare$

Suppose $x_1 = 3$, $x_2 = 5$ and

$$x_m = 3x_{m-1} + 2x_{m-2} \quad \forall m \geq 3.$$

Prove $x_n < 4^n$ $\forall n \in \mathbb{N}$.

Pf: Let $P(n)$ be the given statement. We prove $P(n)$ by strong induction.

Base cases:

$n=1$ $x_1 = 3 < 4$ $\quad$ $n=2$ $x_2 = 5 < 16 = 4^2$

IH: Assume $P(i)$ is true forall $i \in \{1, 2, \ldots, k\}$ for some $k \in \mathbb{N}$ $(k \geq 2)$.

I. Step: For $k \geq 2$,

$$\begin{aligned} x_{k+1} &= 3x_k + 2x_{k-1} \\ &\overset{IH.}{<} 3 \cdot 4^k + 2 \cdot 4^{k-1} \\ &= 4^{k-1}(3 \cdot 4 + 2) \end{aligned}$$

L14 P6

*

$$= 4^{k-1}(14)$$
$$< 4^{k-1} \cdot 16$$
$$= 4^{k+1}.$$

$\therefore P(k+1)$ is true. Thus, $P(n)$ is true $\forall n \in \mathbb{N}$. ∎

Fibonacci Sequence

Define a sequence

$f_1 = 1 \quad f_2 = 1$ and

$f_n = f_{n-1} + f_{n-2} \quad \forall n \geq 3.$

So $f_3 = 2, \; f_4 = 3, \; f_5 = 5, \ldots$

Tool - Lateralus

L15P1

Fibonacci sequence: $f_1 = 1$, $f_2 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 3$.

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

$$LS = f_1^2 + f_2^2 + \cdots + f_n^2$$

Pf: Use POMI

Base Case: $n=1$ $\quad LHS = \sum_{r=1}^{n} f_r^2 = \sum_{r=1}^{1} f_r^2 = f_1^2 = 1^2 = 1$

$RHS = f_n f_{n+1} = f_1 f_2 = 1 \cdot 1 =$

$LHS = RHS$.

IH: Assume $\sum_{r=1}^{k} f_r^2 = f_k f_{k+1}$ for some $k \in \mathbb{N}$.

IStep.: $\boxed{\underline{\text{WANT}} \quad \sum_{r=1}^{k+1} f_r^2 = f_{k+1} f_{k+2}.}$

$$\sum_{r=1}^{k+1} f_r^2 = \sum_{r=1}^{k} f_r^2 + f_{k+1}^2 \overset{IH}{=} f_k f_{k+1} + f_{k+1}^2 = f_{k+1}(f_k + f_{k+1})$$
$$= f_{k+1} f_{k+2}$$

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

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

45P2

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

Exercise (see video).

Closed Form: "Easy to put into a calculator"

Ex: Find a closed form expression for

$$P_n = \prod_{r=2}^{n} \left(1 - \frac{1}{r^2}\right) \qquad (n \geq 2)$$

and prove true by induction.

WARMUP: $n=2$ $\quad P_2 = \prod_{r=2}^{2} \left(1-\frac{1}{r^2}\right) = \left(1-\frac{1}{2^2}\right) = 1-\frac{1}{4} = \frac{3}{4}$

$n=3$ $\quad P_3 = \prod_{r=2}^{3} \left(1-\frac{1}{r^2}\right) = \left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right) = \frac{3}{4}\cdot\frac{8}{9} = \frac{2}{3} = \frac{4}{6}$

$n=4$ $\quad P_4 = \prod_{r=2}^{4} \left(1-\frac{1}{r^2}\right) = \underbrace{\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)}\left(1-\frac{1}{4^2}\right)$

$$= \frac{2}{3}\cdot\frac{15}{16} = \frac{5}{8}$$

Claim: $\boxed{n=5 \quad P_5 = \frac{6}{10}}$ $\cdot$ Claim: $P_n = \dfrac{n+1}{2n}$

L16P01

CODE BC

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. A statement $P(n)$ is proved true for all $n \in \mathbb{N}$ by induction.

In this proof, for some natural number k, we might:

A) Prove $P(1)$. Prove $P(k)$. Prove $P(k+1)$.

B) Assume $P(1)$. Prove $P(k)$. Prove $P(k+1)$.

C) Prove $P(1)$. Assume $P(k)$. Prove $P(k+1)$.

D) Prove $P(1)$. Assume $P(k)$. Assume $P(k+1)$.

E) Assume $P(1)$. Prove $P(k)$. Assume $P(k+1)$.

46P2

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

Solution: Last class, we hypothesized that the product above is equal to $\frac{n+1}{2n}$. Let $P(n)$ be the statement that

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

We prove $P(n)$ is true for all values of $n \geq 2$ by induction.

Base Case: $n=2$

$$\prod_{r=2}^{2}\left(1-\frac{1}{r^2}\right) = 1-\frac{1}{2^2} = \frac{3}{4} = \frac{2+1}{2(2)} \checkmark.$$

IH: $P(k)$ is true for some $k \geq 2$, $k \in \mathbb{N}$.

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

IStep: $\underline{\text{WANT}}$ $\prod_{r=2}^{k+1}\left(1-\frac{1}{r^2}\right) = \frac{(k+1)+1}{2(k+1)}$

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

$$\overset{IH}{=} \frac{\cancel{k+1}}{2k}\cdot\frac{(k+1)^2-1}{(k+1)^2}$$

$$= \frac{k^2+2k+\cancel{1}-\cancel{1}}{2k(k+1)}$$

L6P3

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

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

$\therefore$ $P(k+1)$ is true.

$\therefore$ $P(n)$ is true $\forall n \in \mathbb{N}$ $n \geq 2$ by POMI. $\square$

L16 P4

Examine the following induction "proofs". Find the mistake

Question: For all $n \in \mathbb{N}$, $n > n + 1$.

Proof: Let $P(n)$ be the statement: $n > n + 1$. Assume that $P(k)$ is true for some integer $k \geq 1$. That is, $k > k + 1$ for some integer $k \geq 1$. We must show that $P(k + 1)$ is true, that is, $k + 1 > k + 2$. But this follows immediately by adding one to both sides of $k > k + 1$. Since the result is true for $n = k + 1$, it holds for all n by the Principle of Mathematical Induction. NO BASE CASE.

Question: All horses have the same colour. (Cohen 1961).

Proof:

Base Case: If there is only one horse, there is only one colour.

Inductive hypothesis and step: Assume the induction hypothesis that within any set of n horses for any $n \in \mathbb{N}$, there is only one colour. Now look at any set of $n + 1$ horses. Number them: $1, 2, 3, ..., n, n + 1$. Consider the sets $\{1, 2, 3, ..., n\}$ and $\{2, 3, 4, ..., n + 1\}$. Each is a set of only n horses, therefore by the induction hypothesis, there is only one colour. But the <u>two sets overlap</u>, so there must be only one colour among all $n + 1$ horses. FALSE when $n=1$!

Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be factored "uniquely" as a product of primes up to reordering.

Pf: Existence

Assume towards a contradiction that not every number can be factored into primes. Let n be the smallest such number (Well Ordering Principle). Either n is prime #

OR $n = ab$ with $1 < a, b < n$. However, since $a, b < n$, a & b can be written as a product of primes. Thus, $n = ab$ is a product of primes, contradicting the def'n of n.

Uniqueness

Assume towards a contradiction that $\exists\, n>1,\ n\in\mathbb{N}$ s.t.

$$n = p_1 p_2 \cdots p_K = q_1 q_2 \cdots q_m$$

By def'n $p_1 \mid n = q_1 \cdots q_m$. Thus, $p_1 \mid q_j$ for some $1 \le j \le m$. Thus $p_1 = q_j$. WLOG assume $j=1$. So $p_1 = q_1$ (otherwise rearrange)

Then, $p_2 \cdots p_K = q_2 \cdots q_m$. Take n to be minimal (Well ordering Principle)

As $p_2 \cdots p_K < n$ and $q_2 \cdots q_m < n$,

Thus, $K=m$ and $p_i = q_j$ in some order

Thus, $p_2 \cdots p_K = q_2 \cdots q_K$ (up to reordering)

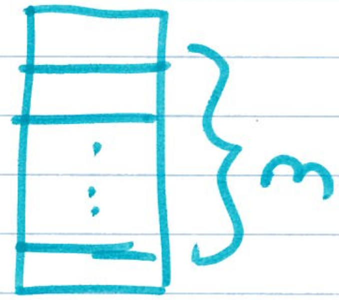
$$p_1 p_2 \cdots p_K = p_1 q_2 \cdots q_K = q_1 q_2 \cdots q_K.$$

This contradicts the existence of n. $\blacksquare$.

Q: Exactly $mn-1$ breaks are always needed to break a $m \times n$ chocolate rectangle into unit squares.

Pf: Fix $m \in \mathbb{N}$. Use induction on n.

Base Case $n=1$



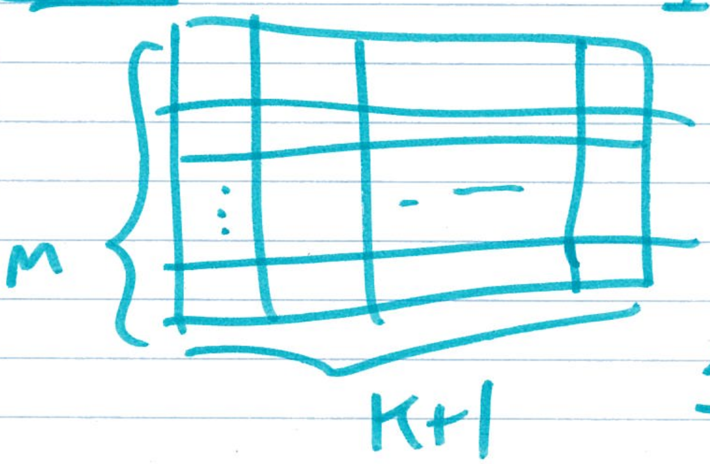
Takes $m-1$ cracks. ✓

$= m(1)-1$

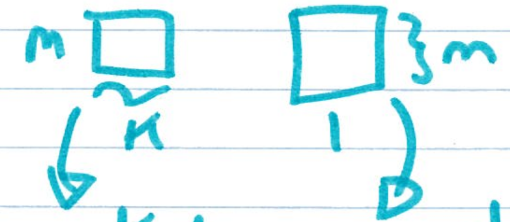
$= mn-1$

IH: $\boxed{\text{HW}}$

I Step:



1: Break last column



$1 + mK - 1 + m - 1$

$= m(K+1) - 1$. ∎

Theorem (Euclid) There exists infinitely many primes.

Pf. Assume towards a contradiction that $\exists$ finitely many primes

$$p_1, p_2, \dots p_n.$$

Consider $N = \prod_{i=1}^{n} p_i + 1$. By FTArithmetic, N can be written as a product of primes. In particular, $\exists$ a prime $p \mid N$. So $p = p_i$ for some $1 \leq i \leq n$. As $p \mid N \wedge p \mid \prod_{i=1}^{n} p_i$, we conclude by DIC, $p \mid N - \prod_{i=1}^{n} p_i = 1$ #.

L17P2

Gap in FT Arithmetic

Need: $p \mid \prod_{i=1}^{k} n_i$ for $n_1, n_2, \dots n_k \in \mathbb{Z}$ then $p \mid n_i$ for some $1 \le i \le k$.
To prove this, need Euclid's Lemma

p is a prime $\wedge\ p \mid ab \Rightarrow p \mid a \vee p \mid b$.

To prove this we need Bēzout's Lemma and gcds.

// GCD (Greatest Common Divisor)

Divisors of 84:
$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 12, \pm 14, \pm 21, \pm 28, \pm 42, \pm 84$

Divisors of 120:
$\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 8, \pm 10, \pm 12, \pm 15, \pm 20, \pm 24, \pm 30, \pm 40, \pm 60, \pm 120$.

So the greatest common divisor of 84 and 120 is 12.

Def'n: The greatest common divisor of integers a and b with $a \neq 0$ or $b \neq 0$ is an integer $d > 0$ such that

(i) $d \mid a \wedge d \mid b$

(ii) If $c \mid a \wedge c \mid b$ then $c \leq d$.

We write $d = \gcd(a,b)$.

Notes:

- $\gcd(a,a) = |a| = \gcd(a,0)$
- Define $\gcd(0,0) = 0$. Note

$$\gcd(a,b) = 0 \iff a = b = 0.$$

- Ex: $\gcd(a,b) = \gcd(b,a)$

L17P4

Prove that $\underbrace{\gcd(3a+b,a)}_{d} = \underbrace{\gcd(a,b)}_{e}$ using the definition directly.

So $d \mid 3a+b$ $\wedge$ $d \mid a$. Then

DIC $\Rightarrow$ $d \mid (3a+b)-3a = b$

Since e is the maximal divisor of a and b, $d \leq e$.

So $e \mid a$ and $e \mid b$. Then

DIC $\Rightarrow$ $e \mid 3a+b$. Since d is maximal, $e \leq d$.

Hence $d=e$. $\blacksquare$

Claim: $\gcd(a,b)$ exists.

Pf: Suppose $a \neq 0$ or $b \neq 0$.
Clearly $1 | a$ and $1 | b$.
So a divisor exists.

There is a greatest common divisor
Since $\gcd(a,b) | a$ and $\gcd(a,b) | b$
so $\gcd(a,b) \leq \min\{|a|,|b|\}$ by BBD.
Thus, $1 \leq \gcd(a,b) \leq \min\{|a|,|b|\}$. $\blacksquare$

Claim: $\gcd(a,b)$ is unique.

Pf: Suppose d and e are both the greatest common divisor of a and b.
Then $d | a \wedge d | b$ so since e is maximal $d \leq e$. Similarly $e \leq d$. Hence $d = e$. $\blacksquare$

L17P6

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

Pf: Suppose $n = ab$ and $a > \sqrt{n}$.

$ab > b\sqrt{n}$

$n > b\sqrt{n}$

$\sqrt{n} > b \Rightarrow b \leq \sqrt{n}$ ☆.

GCD with Remainder (GCDWR)

If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$ then $\gcd(a,b) = \gcd(b,r)$

Ex: $\gcd(72, 40) = 8$

Now, $72 = 40(1) + 32$

So GCDWR says $\gcd(72, 40) = \gcd(40, 32)$

Again: $40 = 32(1) + 8$ so

$\gcd(40, 32) = \gcd(32, 8)$

4 7 P 7

Pf of GCDWR:

If $a = b = 0$, then $r = a - bq = 0$

So $\gcd(a,b) = 0 = \gcd(b,r)$

If $a \neq 0$ or $b \neq 0$ . . .

(Continued from last class...)

GCDWR

If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

Proof: If $a = b = 0$, then since $r = a - bq$, $r = 0$. Hence $\gcd(a, b) = 0 = \gcd(b, r)$. Thus, assume that $a \neq 0$ or $b \neq 0$.

Let $d = \gcd(a,b)$ and $e = \gcd(b,r)$

Since $a = bq+r$ and $d \mid a$ and $d \mid b$

By DIC $d \mid a - bq = r$. Thus,

$d \leq e$ (1) since e is the largest divisor of b & r. Now, $e \mid b$ and $e \mid r$ so by DIC $e \mid bq + r = a$. Thus $e \leq d$ (2) since d is the largest common divisor of a & b. By (1) and (2) $d = e$. $\boxtimes$.

L18P2

Prove that $\gcd(3a+b, a) = \gcd(a, b)$ using GCDWR.

$$\overset{\text{"}a\text{"}}{3a+b} = \overset{\text{"}q\text{"}}{(3)}\,\overset{\text{"}b\text{"}}{a} + \overset{\text{"}r\text{"}}{b}$$

GCDWR $\Rightarrow$ $\gcd(\text{"}a\text{"}, \text{"}b\text{"}) = \gcd(\text{"}b\text{"}, \text{"}r\text{"})$

$\gcd(3a+b, a) = \gcd(a, b)$

Euclidean Algorithm

Idea: Compute GCDs quickly by using GCD WR & Division Algorithm.

Ex: Compute $\gcd(1239, 735)$

(DA)
$$1239 = 735(1) + 504 \quad (1)$$
$$735 = 504(1) + 231 \quad (2)$$
$$504 = 231(2) + 42 \quad (3)$$
$$231 = 42(5) + 21 \quad (4)$$
$$42 = 21(2) + 0$$

Thus, by GCDWR,

$$\gcd(1239, 735) = \gcd(735, 504)$$
$$= \gcd(504, 231) = \gcd(231, 42)$$
$$= \gcd(42, 21) = \gcd(21, 0) = 21$$

NB: This process stops $\because$ remainders form a sequence of non-negative decreasing integers.

Q: What is the runtime of Euclidean Alg'm?

Back Substitution

Q: Do there exist integers x, y s.t. $ax + by = \gcd(a, b)$? A: YES!

$$21 = 231 + 42(-5) \quad (\text{by } (4))$$

by (3) $= 231 + (504 + 231(-2))(-5)$

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

by (2) $= (735 + 504(-1))(11) + 504(-5)$

$= 735(11) + 504(-16)$

by (1) $= 735(11) + (1239 + 735(-1))(-16)$

$= 735(27) + 1239(-16).$

L18 P5

Use the Euclidean Algorithm to compute gcd$(120, 84)$ and then use back substitution to find integers x and y such that gcd$(120, 84) = 120x + 84y$.

$120 = 84(1) + 36$

$84 = 36(2) + 12$

$36 = 12(3) + 0$

By E.A. & GCDWR.

gcd$(120, 84) = 12$.

$12 = 84 + 36(-2)$

$= 84 + (120 + 84(-1))(-2)$

$= 84(3) + 120(-2)$

$84(3 + 120) + 120(-2 - 84)$

$84 \cdot 3 = 252$

$120 \cdot (-2) = -240$

12

Bézout's Lemma (GCDCT in the notes)

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

(i) If $d = \gcd(a,b)$ then $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = d$.

(ii) If $d > 0$, $d | a$, $d | b$ and $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = d$ then $d = \gcd(a,b)$

Pf: (i) Painful. Use Back Substitution

(ii) Let $e = \gcd(a,b)$. Since $d | a \wedge d | b$ by maximality, $d \leq e$. Now, $e | a \wedge e | b$ so by DIC, $e | ax + by = d$. So by BBD, $|e| \leq |d|$ and $\because e, d > 0$ $e \leq d$. Thus, $d = e$. ☒.

L19P1

CODE
BC

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Which of the following statements is false?

A) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \leq b \ \wedge \ \gcd(a,b) \leq a)$

B) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \neq 0 \implies (a \neq 0) \ \vee \ (b \neq 0))$

C) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \mid a \ \wedge \ \gcd(a,b) \mid b)$

D) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (((c \mid a) \ \wedge \ (c \mid b)) \implies c \leq \gcd(a,b))$

E) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \gcd(a,b) \geq 0$

A is False $a=-12$ $b=0$ $\gcd(-12,0)=12 > 0 > -12$.
B True $\gcd(a,b)=0 \iff a=b=0$.
C True
D is false $a=b=0$ and $c=10$
E is true.

L19 P2

Recall:

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

1. (Bezout's Lemma/Identity) If $d = \gcd(a, b)$ then $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$.
2. (GCDCT - GCD Characterization Theorem) If $d > 0$, $d \mid a$, $d \mid b$ and $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$, then $d = \gcd(a, b)$.

Ex: $6 > 0$, $6 \mid 30$, $6 \mid 42$ and

$$30(3) + 42(-2) = 6$$

GCDCT $\Rightarrow \gcd(30, 42) = 6$

Q: Prove if $a, b, x, y \in \mathbb{Z}$ are s.t. $\gcd(a,b) \neq 0$ and $ax + by = \gcd(a,b)$ then $\gcd(x,y) = 1$

Pf: Since $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ we divide by $\gcd(a,b) \neq 0$ to see that

$$\underbrace{\left(\frac{a}{\gcd(a,b)}\right)}^{\text{"}x\text{"}} \overset{\text{"}a\text{"}}{x} + \underbrace{\left(\frac{b}{\gcd(a,b)}\right)}^{\text{"}y\text{"}} \overset{\text{"}b\text{"}}{y} = 1$$

Since $1 \mid x$, $1 \mid y$, $1 > 0$, GCDCT $\Rightarrow \gcd(x, y) = 1$. ∎

Euclid's Lemma (PAD Primes and Divisibility)

If p is a prime and $p|ab$ then $p|a$ or $p|b$.

Pf: Suppose p is prime, $p|ab$ and $p\nmid a$. Since $p\nmid a$, $\gcd(p,a)=1$. By Bézout's Lemma, $\exists x,y\in\mathbb{Z}$ s.t.

$p|ab$ so $\exists k\in\mathbb{Z}$ s.t. $ab=pk$

$$px+ay=1$$
$$pbx+aby=b$$
$$pbx+pky=b$$
$$p\underbrace{(bx+ky)}_{\in\mathbb{Z}}=b \Rightarrow p|b$$

41914

Prove or disprove the following:

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

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

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

1. $n+1 = n(1) + 1$ TRUE

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

2. $\gcd(a,b) \mid a$ TRUE

$\gcd(a,b) \mid b$

DIC $\Rightarrow$ $\gcd(a,b) \mid ax^2 + by^2 = c$. ✓

3.

Def'n: For $x \in \mathbb{R}$, define the floor function $\lfloor x \rfloor$ to be the greatest integer less than or equal to x.

Ex: $\lfloor 2.5 \rfloor = 2 = \lfloor 2 \rfloor$

$\lfloor \pi \rfloor = 3$ $\qquad \lfloor 0 \rfloor = 0$

$\lfloor -2.5 \rfloor = -3$

//

Find $\gcd(56, 35)$

$[1]$ $\quad 56(1) + 35(0) = 56$

$[2]$ $\quad 56(0) + 35(1) = 35$ $\qquad q_1 = \lfloor \frac{56}{35} \rfloor = 1$

$[3] = [1] - q_1[2]$ $\quad 56(1) + 35(-1) = 21$ $\qquad q_2 = \lfloor \frac{35}{21} \rfloor = 1$

$[4] = [2] - q_2[3]$ $\quad 56(-1) + 35(2) = 14$ $\qquad q_3 = \lfloor \frac{21}{14} \rfloor = 1$

$[5] = [3] - q_3[4]$ $\quad 56(2) + 35(-3) = 7$ $\qquad q_4 = \lfloor \frac{14}{7} \rfloor = 2$

$[6] = [4] - q_4[5]$ $\quad 56(-5) + 35(8) = 0.$

$\therefore \gcd(56, 35) = 7 = 56(2) + 35(-3).$

Ex: Find $x, y \in \mathbb{Z}$ s.t.

$$506x + 391y = \gcd(506, 391)$$

	x	y	r	q
[1]	1	0	506	0
[2]	0	1	391	0
[3]=[1]-[2]	1	-1	115	$\lfloor \frac{506}{391} \rfloor = 1$
[4]=[2]-3[3]	-3	4	46	$\lfloor \frac{391}{115} \rfloor = 3$
[5]=[3]-2[4]	7	-9	23	$\lfloor \frac{115}{46} \rfloor = 2$
[6]=[4]-2[5]	-17	22	0	$\lfloor \frac{46}{23} \rfloor = 2$

$\therefore\ 506(7) + 391(-9) = 23 = \gcd(506, 391)$

This is called the Extended Euclidean Algorithm (EEA).

L20P3

Use the Extended Euclidean Algorithm to find integers x and y such that $408x + 170y = \gcd(408, 170)$.

x	y	r	q
1	0	408	0
0	1	170	0.
1	-2	68	2
-2	5	34	$\lfloor \frac{170}{68} \rfloor = 2$
5	-12	0	$\frac{68}{34} = 2$

$\therefore 408(-2) + 170(5) = 34 = \gcd(408, 170)$

Quick Notes:

- Bézout's Lemma is EEA in textbook.
- With $\gcd(a,b)$ what if
  - $b>a$? Swap a & b. Works since $\gcd(a,b)=\gcd(b,a)$.
  - What if $a<0$ or $b<0$?
    Sol'n: Make it positive. Works since
    $$\gcd(a,b)=\gcd(-a,b)=\gcd(a,-b)$$
    $$=\gcd(-a,-b).$$

L20 P5

Use the Extended Euclidean Algorithm to find integers x and y such that $399x - 2145y = \gcd(399, -2145)$.

Find $\tilde{x}, \tilde{y} \in \mathbb{Z}$ s.t. $\cancel{399\tilde{x} + 2}$

$2145\tilde{x} + 399\tilde{y} = \gcd(2145, 399)$

$\tilde{x}$	$\tilde{y}$	r	q
1	0	2145	0
0	1	399	0
1	-5	150	5
-2	11	99	2
3	-16	51	1
-5	27	48	1
8	-43	3	1
-5-16(8)	27-(16)(-43)	0	16

$\therefore\ 2145(8) + 399(-43) = 3 = \gcd(2145, 399)$

$\therefore\ -2145(-8) + 399(-43) = 3 = \gcd(399, -2145)$

GCD Characterization Theorem GCD CT: If d is positive common divisor of the integers a and b, and $\exists\ x,y \in \mathbb{Z}$ s.t. $ax+by=d$, then $d=\gcd(a,b)$

ex. $ab, c \in \mathbb{Z}$. Prove if $\gcd(ab,c)=1$, then $\gcd(a,c), \gcd(b,c)=1$.
By the EEA, $\exists\ x,y \in \mathbb{Z}$ s.t. $ab(x)+c(y)=1$.

Since $1|a$ and $1|c$ and $a(bx)+c(y)=1$, by GCD CT.
where $bx, y \in \mathbb{Z}$

thus, $\gcd(a,c)=1$

Since $1|b$ and $1|c$ and $b(ax)+c(y)=1$
where $ax, y \in \mathbb{Z}$

ex. 2. State converse and prove/disprove. If $\gcd(a,c)=\gcd(b,c)=1$ then $\gcd(ab,c)=1$

~~gcd(17, 59) = gcd(34~~ true. If a,c are relatively prime if b,c are relatively prime then a,b,c are pairwise prime. $\therefore$ true.

Proof: If $\gcd(a,c)=1$ then by EEA there exist $x,y \in \mathbb{Z}$ s.t. $ax+cy=1$. Likewise, if $\gcd(b,c)=1$ then by EEA $\exists\ k,m \in \mathbb{Z}$ s.t. $bk+cm=1$ Multiplying these gives: $(ax+cy)(bk+cm)=1$
$axbk+axcm+cybk+c^2ym=1$

Since $1|ab$ and $1|c$ and $ab(\quad)+c(\quad)=1$, Then by GCD CT
$\gcd(ab,c)=1$

$ab(xk)+c(axm+ybk+cym)=1$ where $xk, axm+ybk+cym \in \mathbb{Z}$

Observation: EEA is useful with gcd in the hypothesis, GCD CT is useful with GCD in the conclusion

Proposition: (GCD of One (GCDOO))
Let $a,b \in \mathbb{Z}$. Then $\gcd(a,b)=1$ iff $\exists x,y \in \mathbb{Z}$ with $ax+by=1$

Proof of GCDOO

1. ($\Rightarrow$) Suppose $GCD(a,b)=1$. Then by EEA $\exists x,y\in\mathbb{Z}$ s.t. $ax+by=d$ $=1$.

($\Leftarrow$) Suppose $\exists x,y\in\mathbb{Z}$ s.t. $ax+by=1$
Since $1|a$ and $1|b$, by GCDCT, $\gcd(a,b)=1$. ■

Division by the GCD (DB GCD)
Let $a,b\in\mathbb{Z}$. If $\gcd(a,b)=d$ and $d\neq 0$, then $\gcd(\frac{a}{d},\frac{b}{d})=1$

ex. Let $a=91$ and $b=70$. Then $\gcd(a,b)=7$ and by DBGCD, $\gcd(\frac{a}{d},\frac{b}{d})$ $=\gcd(\frac{91}{7},\frac{70}{7})=\gcd(13,10)=1$

Pf: Suppose $\gcd(a,b)=d\neq 0$. Then by EEA, $\exists x,y\in\mathbb{Z}$ s.t. $ax+by=d$
Dividing by d gives $\frac{a}{d}x+\frac{b}{d}y=1$

By GCDOO, since $\frac{a}{d}(x)+\frac{b}{d}(y)=1$, where $x,y\in\mathbb{Z}$
thus $\gcd(\frac{a}{d},\frac{b}{d})=1$.
//

Def'n: Coprime : Two integers a and c are coprime if $\gcd(a,c)=1$

Proposition: Coprimeness and Divisibility (CAD)
If $a,b,c\in\mathbb{Z}$ and $c|ab$ and $\gcd(a,c)=1$ then $c|b$.
ex. (CAD). Let $a=14$, $b=30$, $c=15$. Then $c|ab$ since $15|420$ and $\gcd(a,c)=1$ $=\gcd(14,15)=1$. Thus by CAD, $c|b$ or $15|30$.

Proof of CAD: Suppose $\gcd(a,c)=1$ and $c|ab$. Since $\gcd(a,c)=1$ then by EEA $\exists x,y\in\mathbb{Z}$ s.t. $ax+cy=1$.
Multiplying by b gives $abx+cby=b$
Since $c|ab$, $\exists k\in\mathbb{Z}$ s.t. $ab=ck$. Substituting into * gives

$ckx + cby = b$

$c(kx+by) = b$ where $(kx+by) \in \mathbb{Z}$ $\therefore c \mid b$ ∎

(DFPF)

Let $n > 1$ be an integer and $d \in \mathbb{N}$. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$ where $\alpha_i \in \mathbb{Z}$ are each ≥ 1, then d is a positive divisor of n iff a prime factorization of d is given by

$$d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$$

where $\delta_i \in \mathbb{Z}$, $0 \leq \delta_i \leq \alpha_i$ for $1 \leq i \leq k$.

Ex: Divisors (positive) of $63 = 3^2 \cdot 7$

$3^0 \cdot 7^0$, $3^0 \cdot 7^1$, $3^1 \cdot 7^0$, $3^1 \cdot 7^1$, $3^2 \cdot 7^0$, 3^2

$1, 7, 3, 21, 9, 63.$

Pf is extra reading.

L22P2

How many multiples of 12 are positive divisors of 2940? What are they?

$$
\begin{array}{r}
245 \\
12\,\overline{)\,2940} \\
\underline{24} \\
54 \\
\underline{48} \\
60
\end{array}
$$

$2940 = 12 \cdot 245$

$245 = 5 \cdot 49$

$= 5 \cdot 7^2$

Total number is $(1+1)(2+1) = 6$

Multiples are:

$12,\ 12\cdot 5,\ 12\cdot 7,\ 12\cdot 5\cdot 7,\ 12\cdot 7^2,\ 12\cdot 5\cdot 7^2$

L22P3

Q: Prove $a^2 | b^2$ iff $a | b$.

Pf: Assume $a|b$. Then $\exists K \in \mathbb{Z}$ s.t. $aK = b$. Now, $a^2K^2 = b^2$ and hence $a^2 | b^2$ by def'n.

Now, assume $a^2 | b^2$. For convenience, $a, b > 0$ Write (Exer: prove true when $a \in \{0, \pm 1\}$)

$$a = \prod_{i=1}^{K} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{K} p_i^{\beta_i}$$

with $0 \le \alpha_i, \beta_i$ integers. Since $a^2 | b^2$, $\prod_{i=1}^{K} p_i^{2\alpha_i} \mid \prod_{i=1}^{K} p_i^{2\beta_i}$. DFPF implies $2\alpha_i \le 2\beta_i \Rightarrow \alpha_i \le \beta_i$ for $1 \le i \le K$.

DFPF again implies

$$a = \prod_{i=1}^{K} p_i^{\alpha_i} \mid \prod_{i=1}^{K} p_i^{\beta_i} = b.$$

■.

GCD PF

Ex: $\gcd(2^5 \cdot 3^0 \cdot 5^4, 2^4 \cdot 3^1 \cdot 5^4)$

$= 2^{\min\{4,5\}} \cdot 3^{\min\{0,1\}} \cdot 5^{\min\{4,4\}}$

$= 2^4 \cdot 5^4 = 10000$

Statement: If

$$a = \prod_{i=1}^{\ell} p_i^{\alpha_i} \quad \text{and} \quad b = \prod_{i=1}^{\ell} p_i^{\beta_i}$$

where $0 \leq \alpha_i, \beta_i$ are integers and p_i are distinct primes. Then

$$\gcd(a,b) = \prod_{i=1}^{\ell} p_i^{m_i}$$

where $m_i = \min\{\alpha_i, \beta_i\}$ for $1 \leq i \leq \ell$

Pf is extra reading.

Let $lcm(a,b)$ represent the least common multiple of a & b.

Ex: 1. Write a formal defn for $lcm(a,b)$

2. Show
$$lcm(a,b) = \prod_{i=1}^{l} p_i^{e_i}$$
where $e_i = \max\{\alpha_i, \beta_i\}$

3. Prove $\gcd(a,b) \cdot lcm(a,b) = ab$

L22 P6
(EXTRA).

Linear Diophantine Equations.

Common DE: $x^2+y^2=z^2$ (NOT Linear)

Pythagoreen triples

$$\left.\begin{array}{l} ax=b \\ ax+by=c=\gcd(a,b) \end{array}\right\} \text{Linear.}$$

$$56x+249y=31$$

$$2x+4y=3$$

DFPF (Divisors from Prime Factorization)

Solving GCD Problems.

- Bézout's Lemma (EEA)
- GCD CT
- GCD WR
- Definition
- GCD PF

L23P2

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Let $a, b, x, y \in \mathbb{Z}$.

Which one of the following statements is true?

~~A)~~ If $ax + by = 6$, then $\gcd(a, b) = 6$.

B) If $\gcd(a, b) = 6$, then $ax + by = 6$. X

~~C)~~ If $a = 12b + 18$, then $\gcd(a, b) = 6$.

D) If $ax + by = 1$, then $\gcd(6a, 6b) = 6$. $\to \gcd(a,b)=1 \Rightarrow \gcd(6a, 6b) = 6$

E) If $\gcd(a, b) = 3$ and $\gcd(x, y) = 2$, then $\gcd(ax, by) = 6$.

L2373

Linear Diophantine Equations (LDE

Want to solve

$$ax + by = c$$

where $a, b, c \in \mathbb{Z}$.

Catch! $x, y \in \mathbb{Z}$.

Ex: Solve $143x + 253y = 11$

Solve using EEA!

x	y	r
0	1	253
1	0	143
-1	1	110
2	-1	33
-7	4	11
23	-13	0

$\therefore 143(-7) + 253(4) = 11$

Questions about LDEs.

- Is there a solution?.
- ~~Is~~ What is it?
- Is there more than one?.

Q: Solve the LDE

$$143x + 253y = 155$$

Assume towards a contradiction that $\exists\, x_0, y_0 \in \mathbb{Z}$ s.t.

$$143x_0 + 253y_0 = 155$$

By before, $11 \mid 143$ & $11 \mid 253$. Hence by DIC $143x_0 + 253y_0$ is divisible by 11. BUT $11 \nmid 155 = 143x_0 + 253y_0$ #. Hence the original LDE has no integer solutions.

What about
$$143x + 253y = 154$$
$154 = 11 \cdot 14$.
$$143(-7) + 253(4) = 11$$
Multiply by 14
$$143(-7\cdot 14) + 253(4\cdot 14) = 154$$
$$143(-98) + 253(56) = 154.$$

LDE T1

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

Pf: $\Rightarrow$ Assume $ax+by=c$ has an integer solution, say $x_0, y_0 \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, by DIC
$$d \mid ax_0 + by_0 = c.$$

$\Leftarrow$ Assume $d \mid c$. Then $\exists k \in \mathbb{Z}$ s.t. $dk = c$. By Bézout's Lemma $\exists u, v \in \mathbb{Z}$ s.t.

$$au + bv = \gcd(a,b) = d.$$

Mult by k

$$a(uk) + b(vk) = dk = c$$

$\therefore$ a solution is $x = uk$, $y = vk$

Ex: $20x + 35y = 5$ (Solve the LDE)

Simplify: $4x + 7y = 1$

A solution is $x = 2$ $y = -1$

Look at $x_2 = 2 + 7(2)$ $y_2 = -1 - 4(2)$

$$\begin{aligned} 4x_2 + 7y_2 &= 4(2 + 7(2)) + 7(-1 - 4(2)) \\ &= 4 \cdot 2 + \cancel{4 \cdot 7(2)} + 7(-1) - \cancel{7 \cdot 4(2)} \\ &= 4x + 7y \\ &= 1 \end{aligned}$$

LDET2

Let $d = \gcd(a,b)$ where $a \neq 0$ and $b \neq 0$. If $(x,y) = (x_0, y_0)$ is a solution to the LDE

$$ax + by = c$$

Then all solutions are given by

$$x = x_0 + \frac{b}{d}n \qquad y = y_0 - \frac{a}{d}n$$

for all $n \in \mathbb{Z}$. (Alternatively:

$$\{(x_0 + \tfrac{b}{d}n,\ y_0 - \tfrac{a}{d}n) : n \in \mathbb{Z}\}.$$

Pf: Note the above are actually solutions to the LDE.

Now, let (x,y) be another solution to the LDE. Thus

$$ax + by = c$$

$$ax_0 + by_0 = c$$

Subtract: $a(x - x_0) + b(y - y_0) = 0$

$$a(x-x_0) = -b(y-y_0)$$

$$\frac{a}{d}(x-x_0) = -\frac{b}{d}(y-y_0) \quad (1)$$

Now, since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ (by DBGCD) ~~we have that~~ and since

$$\frac{b}{d} \mid -\frac{b}{d}(y-y_0) = \frac{a}{d}(x-x_0)$$

we use CAD to see that $\frac{b}{d} \mid x-x_0$.
Thus, $\exists n \in \mathbb{Z}$ s.t. $x-x_0 = \frac{b}{d}n$ and thus $x = x_0 + \frac{b}{d}n$. Plug into (1):

$$\frac{a}{d}\left(\frac{b}{d}n\right) = -\frac{b}{d}(y-y_0)$$

$$-\frac{a}{d}n = y-y_0$$

$$\Rightarrow y = y_0 - \frac{a}{d}n.$$

Q: Alice has a lot of mail to send. She wishes to spend exactly 100 dollars buying 49-cent & 53-cent stamps. In how many ways can she do this?

Sol'n: Let x be the number of 49 cent stamps. Let y be the number of 53 cent stamps. Note $x, y \in \mathbb{Z}$ and $x, y \geq 0$.

WANT to solve

$$0.49x + 0.53y = 100$$

$$49x + 53y = 10000$$

x	y	r	q
0	1	53	0
1	0	49	0
-1	1	4	1
13	-12	1	12
		0	4.

$\therefore$ $49(13) + 53(-12) = 1$

$49(130000) + 53(-120000) = 10000$

Thus, by LDET2

$$x = 130000 - 53n \qquad \forall n \in \mathbb{Z}$$
$$y = -120000 + 49n$$

Since $x \geq 0$, we have

$$130000 - 53n \geq 0$$
$$2452 + \frac{44}{53} = \frac{130000}{53} \geq n$$

Since $y \geq 0$, we have

$$-120000 + 49n \geq 0$$
$$\Rightarrow \quad n \geq \frac{120000}{49} = 2448 + \frac{48}{49}$$

Since $n \in \mathbb{Z}$,

$$2449 \leq n \leq 2452$$

Thus, there are 4 possible solutions. $\blacksquare$

Find all non-negative integer solutions to $15x - 24y = 9$ where $x \leq 20$ and $y \leq 20$.

$\div 3$ $$5x - 8y = 3$$

Note $x_0 = -1$ & $y_0 = -1$ is a solution.

Since $\gcd(5, -8) = 1$, by LDET2.

$$x = -1 - (-8)n = -1 + 8n \quad \forall n \in \mathbb{Z}$$
$$y = -1 + 5n \quad = -1 + 5n$$

is the solution set. By the statement

$0 \leq x \leq 20$ & $0 \leq y \leq 20$

$0 \leq -1 + 8n \leq 20$ & $0 \leq -1 + 5n \leq 20$

$1 \leq 8n \leq 21$ & $1 \leq 5n \leq 21$

$\Rightarrow n = 1, 2$ $\qquad$ $\Rightarrow n = 1, 2, 3, 4$

Thus, $n = 1, 2$ gives the only solutions of

$(7, 4)$ & $(15, 9)$ $\blacksquare$.

Congruences.

Idea: Simplify problems in Divisibility.

Q: Is 156723 divisible by 11?

What angle do you get after a 1240° rotation?

What time is it 40 hours from now

Idea: We only care ~~b~~ about the above answers up to multiples of 11, 360, and 24.

Def'n: Let $m \in \mathbb{N}$. We say that two integers a, b are congruent modulo m iff $m \mid (a-b)$ and we write

$$a \equiv b \bmod m$$

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

If $m \nmid a-b$ we write $a \not\equiv b \bmod m$.

L25P7.

Ex: $7 \equiv 4 \mod 3$ $\quad 7 \not\equiv 4 \mod 4$

$4 \equiv 7 \mod 3$ $\quad 2 \equiv 2 \mod 3$

$10 \equiv 15 \mod 5$ & $15 \equiv 30 \mod 5$

& $10 \equiv 30 \mod 5$.

L2SP1

Quick! For $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, define what it means for a to be congruent to b modulo n.

We say that a is congruent to b modulo n and write $a \equiv b \pmod{n}$ if and only if $n \mid (a-b)$. This is equivalent to saying there exists an integer k such that $a-b = kn$ or $a = b+kn$.

L25P2

Congruence is an Equivalence Relation (CER)

Let $n \in \mathbb{N}$. Let $a, b, c \in \mathbb{Z}$. Then

1. (Reflexivity) $a \equiv a \pmod{n}$.
2. (Symmetry) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.
3. (Transitivity) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Proofs:

1. Since $n \mid 0 = (a - a)$, we have that $a \equiv a \pmod{n}$.
2. Since $n \mid (a - b)$, there exists an integer k such that $nk = (a - b)$. This implies that $n(-k) = b - a$ and hence $n \mid (b - a)$ giving $b \equiv a \pmod{n}$.
3. Since $n \mid (a - b)$ and $n \mid (b - c)$, by Divisibility of Integer Combinations, $n \mid ((a - b) + (b - c))$. Thus $n \mid (a - c)$ and hence $a \equiv c \pmod{n}$

L25P3

Without a calculator, is $167 \equiv 2015 \mod 4$

Sol'n: $2015 \equiv 3 \mod 4 \because 4 \mid 2012 = 2015-3$

$167 \equiv 3 \mod 4 \because 4 \mid 164 = 167-3$

By symmetry $3 \equiv 2015 \mod 4$

By transitivity $167 \equiv 2015 \mod 4$.

Alt Sol'n: Does $4 \mid 2015-167 = 1848$

L25 P4

Properties of Congruence (PC) Let $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then

1. $a + b \equiv a' + b' \pmod{m}$
2. $a - b \equiv a' - b' \pmod{m}$
3. $ab \equiv a'b' \pmod{m}$

Proofs:

1. Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid (a - a' + (b - b'))$. Hence $m \mid (a + b - (a' + b')$ and so $a + b \equiv a' + b' \pmod{m}$.

2. Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid (a - a' - (b - b'))$. Hence $m \mid (a - b - (a' - b')$ and so $a - b \equiv a' - b' \pmod{m}$.

3. Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid ((a - a')b + (b - b')a')$. Hence $m \mid ab - a'b'$ and so $ab \equiv a'b' \pmod{m}$.

Corollary If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for $k \in \mathbb{N}$.

Example: Since $2 \equiv 6 \mod 4$, we have that $2^2 \equiv 6^2 \mod 4$, that is, $4 \equiv 36 \mod 4$.

L25 P5

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

Sol'n: Reduce mod 7. By (PC)

$$5^9 + 62^{2000} - 14 \equiv (-2)^9 + (-1)^{2000} - 0 \mod 7$$
$$\equiv -2^9 + 1 \mod 7$$
$$\equiv -(2^3)^3 + 1 \mod 7$$
$$\equiv -(8)^3 + 1 \mod 7$$
$$\equiv -(1)^3 + 1 \mod 7$$
$$\equiv 0 \mod 7$$

$\therefore$ the number is divisible by 7.

Divisibility Rules

A positive integer n is divisible by

(a) 2^k iff the last k digits are divisible by 2^k.

(b) 3 (or 9) iff the sum of the digits is divisible by 3 (or 9)

(c) 5^k iff the last k digits are divisible by 5^k.

(d) 7 (or 11 or 13) iff the alternating sum of triples of digits is divisible by 7 (or 11 or 13)

Ex: $n = 123\,456\,333$

$$333 - 456 + 123 = 0$$

$\therefore 7, 11, 13 \mid 0 \overset{(d)}{\Rightarrow} 7, 11, 13 \mid n$.

L26P2

Proof of (b)

Let $n \in \mathbb{N}$. Write

$$n = d_0 + 10d_1 + 10^2 d_2 + \dots + 10^k d_k$$

where $d_i \in \{0, 1, \dots 9\}$

(Ex: $213 = 3 + 10(1) + 100(2)$)

<u>So</u>: $9 \mid n \iff n \equiv 0 \mod 9$

$\iff 0 \equiv d_0 + 10d_1 + 10^2 d_2 + \dots + 10^k d_k \mod 9$

By PC $\iff 0 \equiv d_0 + d_1 + d_2 + \dots + d_k \mod 9$

Thus, $9 \mid n \iff$ 9 divides the sum of the digits of n. $\blacksquare$

"Random" Examples

$3 \equiv 24 \mod 7$ and $1 \equiv 8 \mod 7$

$3 \equiv 27 \mod 6$ and $1 \not\equiv 9 \mod 6$

Proposition (Congruences & Division - CD)

Let $a, b, c \in \mathbb{Z}$ & $n \in \mathbb{N}$

If $ac \equiv bc \mod n$ and $\gcd(c,n) = 1$ then $a \equiv b \mod n$.

Pf: By assumption, $n \mid ac - bc$ so $n \mid c(a-b)$. Since $\gcd(c,n) = 1$, by CAD, $n \mid a-b$. Hence $a \equiv b \mod n$. ◮

L26P4

What is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4?

$$77 = 19(4) + 1$$

$$999 = 249(4) + 3$$

By CISR, $77 \equiv 1 \mod 4$

$999 \equiv 3 \mod 4$

Thus, by PC

$$77^{100}(999) - 6^{83}$$

$$\equiv (1)^{100}(3) - 2^{83} \mod 4$$

$$\equiv 3 - 2^2 \cdot 2^{81} \mod 4$$

$$\equiv 3 - 4 \cdot 2^{81} \mod 4$$

$$\equiv 3 - 0 \cdot 2^{81} \mod 4$$

$$\equiv 3 \mod 4.$$

By CISR, 3 is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4.

Proposition (Congruent iff Same Remainder CISR). Let $a,b\in\mathbb{Z}$. Then
$a\equiv b \mod n \iff a$ & b have the same remainder after division by n.

Pf: By the Division Algorithm, write

$$a = nq_a + r_a$$
$$b = nq_b + r_b$$

where $0 \le r_a, r_b < n$. Subtracting

$$a-b = n(q_a - q_b) + r_a - r_b \quad (1)$$

$\Rightarrow$ Assume $a\equiv b \mod n$ ie. $n \mid a-b$.
Since $n \mid n(q_a - q_b)$ by DIC,

$$n \mid r_a - r_b.$$

By our restriction

$$-n+1 \le r_a - r_b \le n-1$$

L26P6

BUT only 0 is divisible by n in this range! Since $n \mid r_a - r_b$, we must have that $r_a - r_b = 0$. Hence $r_a = r_b$.

$\Leftarrow$ Assume $r_a = r_b$. By (1),

$$a - b = n(q_a - q_b)$$
$$\Rightarrow n \mid a - b \Rightarrow a \equiv b \bmod n. \blacksquare$$

What is the last digit of $5^{32}3^{10} + 9^{22}$?

Homework:

READ CHAPTER 26!

L27 P2

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Which of the following satisfies $x \equiv 40 \pmod{17}$?

$x \equiv 6 \mod 17$

(Do not use a calculator.)

A) $x = 173$ $\equiv 3 \mod 17$

B) $x = 15^5 + 19^3 - 4$ $\equiv (-2)^5 + 2^3 - 4 \equiv -32 + 8 - 4 \equiv 2 + 4 \equiv 6 \mod 17$

C) $x = 5 \cdot 18^{100}$ $\equiv 5(1)^{100} \equiv 5 \mod 17$

D) $x = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ $\equiv 6 \cdot 35 \cdot \cancel{143} (-6)(-4) \equiv 6 \cdot 1 \cdot 24 \equiv 6 \cdot 7 \equiv 42 \equiv 8 \mod 17$

E) $x = 17^0 + 17^1 + 17^2 + 17^3 + 17^4 + 17^5 + 17^6$ $\equiv 1 \mod 17$

What is the last digit of $5^{32}3^{10} + 9^{22}$?

Sol'n: Reduce mod 10.

$$
\begin{aligned}
5^{32} \cdot 3^{10} + 9^{22} &\equiv (5^2)^{16} (9)^5 + (-1)^{22} \mod 10 \\
&\equiv 5^{16} (-1)^5 + 1 \mod 10 \\
&\equiv (5^2)^8 (-1) + 1 \mod 10 \\
&\equiv -5^8 + 1 \mod 10 \\
&\equiv -(5^2)^4 + 1 \mod 10 \\
&\equiv -5^4 + 1 \mod 10 \\
&\equiv -5^2 + 1 \mod 10 \\
&\equiv -5 + 1 \mod 10 \\
&\equiv -4 + 10 \mod 10 \\
&\equiv 6
\end{aligned}
$$

Linear Congruences.

Q: Solve $ax \equiv c \mod m$
(for $a, c \in \mathbb{Z}$, $m \in \mathbb{N}$) for $x \in \mathbb{Z}$.

Compare to $ax = c$ (sol'n when $a | c$).

Ex: $4x \equiv 5 \mod 8$
Sol'n 1: By def'n $\exists y' \in \mathbb{Z}$ s.t.
$4x - 5 = 8y'$ $\iff$ $\exists y' \in \mathbb{Z}$ s.t.
$4x - 8y' = 5$.
Let $y = -y'$. Thus, the original question is equivalent to solving the LDE

$$4x + 8y = 5$$

Since $\gcd(4,8) = 4 \nmid 5$, by LDET1, this LDE has no sol'n.

$$4x \equiv 5 \mod 8$$

Sol'n 2: Try all numbers from 0 to 7.

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

Now, let $x \in \mathbb{Z}$. By the Div Alg'm

$$x = 8q + r$$

for some $0 \leq r \leq 7$. By CISR

$$4x \equiv 5 \mod 8 \iff 4r \equiv 5 \mod 8$$

Above we tried all numbers from 0 to 7 and saw that there was no solution.

Sol'n 3: Assume towards a contradiction that $\exists x \in \mathbb{Z}$ s.t. $4x \equiv 5 \mod 8$. Multiply both sides by 2 to get (by PC)

$$0 \equiv 0x \equiv 8x \equiv 10 \mod 8$$

Thus $8 \mid 10$. __BUT__ $8 \nmid 10$ #. So there are no integer solutions to $4x \equiv 5 \mod 8$.

Ex: $5x \equiv 3 \bmod 7$

Sol'n1:

x	0	1	$\boxed{2}$	3	4	5	6
$5x \bmod 7$	0	5	$\boxed{3}$	1	6	4	2

$\therefore$ $x \equiv 2 \bmod 7$ gives the solutions.

Sol'n2: Equivalent to solving the LDE

$$5x + 7y = 3.$$

By LDET2 $x = 2 + 7n$ $y = -1 - 5n$ $\forall n \in \mathbb{Z}$ gives the solutions.

Sol'n3: $5x \equiv 3 \bmod 7 \underset{\text{mult. by } 3}{\overset{\text{mult. by } 5}{\Longleftrightarrow}} x \equiv 2 \bmod 7$

Ex: $2x \equiv 4 \bmod 6$

Sol'n

x	0	1	$\boxed{2}$	3	4	$\boxed{5}$
$2x \bmod 6$	0	2	$\boxed{4}$	0	2	$\boxed{4}$

$\therefore$ $x \equiv 2, 5 \bmod 6 \Longleftrightarrow x \equiv 2 \bmod 3$

Summary: LCT1 (Linear Congruence Theorem 1)

Let $a, c \in \mathbb{Z}$, $m \in \mathbb{N}$ and $\gcd(a,m) = d$ Then

$ax \equiv c \bmod m$ has a solution $\iff d \mid c$.

NB: Have d solutions modulo m.
Have 1 solution modulo $\frac{m}{d}$.

Moreover, if $x = x_0$ is a solution, then $x \equiv x_0 \bmod \frac{m}{d}$ forms the complete sol'n

OR $x = x_0 + \frac{m}{d} n$ for all $n \in \mathbb{Z}$

OR $x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \bmod m$

Pf: Read p. 180.

L28P1

Solve $9x \equiv 6 \pmod{15}$.

Equivalent to solving the LDE

$$9x + 15y = 6.$$

$$3x + 5y = 2$$

By LDET2 $x = -1 + 5n$

$y = 1 - 3n$ $\forall n \in \mathbb{Z}$.

$\therefore$ Sol'n is $x \equiv -1 \bmod 5$

OR $x \equiv 4 \bmod 5$

OR $x \equiv 4, 9, 14 \bmod 15$.

Ex: Show that there are no integer solutions to

$$x^2+4y=2.$$

Sol'n: Assume towards a contradiction that $\exists\, x, y \in \mathbb{Z}$ s.t.

$$x^2+4y=2.$$

$$\Leftrightarrow \quad x^2-2=-4y$$

$$\Rightarrow \quad 4 \mid x^2-2 \quad \text{so } x^2-2\equiv 0 \bmod 4$$

$$\underline{\text{OR}} \quad x^2\equiv 2 \bmod 4$$

x	0	1	2	3
$x^2 \bmod 4$	0	1	0	1

$\#$

none equal 2.

$\therefore\ x^2-4y=2$ has no integer solutions! ■

$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ Integers modulo m.

The congruence / equivalence class modulo m of an integer a is the set of integers:

$$[a] := \{x \in \mathbb{Z} : x \equiv a \bmod m\}$$

"defined as"

Further, define

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

We make $\mathbb{Z}_m$ a "ring" by defining addition, subtraction and multiplication by

$$\underbrace{[a] \pm [b]}_{\text{adding sets}} := [\underbrace{a \pm b}_{\substack{\text{adding}\\ \text{integers}}}] \qquad \underbrace{[a] \cdot [b]}_{\substack{\text{mult}\\ \text{of sets}}} := [\underbrace{a \cdot b}_{\substack{\text{mult.}\\ \text{integers.}}}]$$

Issue: Well <u>defined</u>.

How do we know that this

addition didn't depend on our representation of [a] & [b]?.

Ex: Does $[2][5] = [14][-13]$ in $\mathbb{Z}_6$?.

Sol'n: $[2]\cdot[5] = [2\cdot 5] = [10] = [4]$ in $\mathbb{Z}_6$

$[14][-13] = [14\cdot(-13)] = [-182] = [-2]$

$= [4]$ ✓

The members $0, 1, \ldots m-1$ are called representative members.

Addition table for $\mathbb{Z}_4$

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

Notes:

- We call $[0]$ the additive identity of $\mathbb{Z}_m$.
- We call $[1]$ the multiplicative identity of $\mathbb{Z}_m$.

L28P6

Solve the following equations in $\mathbb{Z}_{14}$. Express answers as $[x]$ where $0 \leq x < 14$.

i) $[75] - [x] = [50]$

ii) $[10][x] = [1]$

iii) $[10][x] = [2]$

(i) $[75] - [x] + [x] - [50] = [50] + [x] - [50]$

$[25] = [x] \quad \Rightarrow [x] = [11].$

$[25] = \{\bar{x} \in \mathbb{Z} : \bar{x} \equiv 25 \bmod 14\}$

$= \{\bar{x} \in \mathbb{Z} : \bar{x} \equiv 11 \bmod 14\}$

$= [11].$

Solve the following equations in $\mathbb{Z}_{14}$. Express answers as $[x]$ where $0 \leq x < 14$.

ii) $[10][x] = [1]$ $\iff 10x \equiv 1 \mod 14$

iii) $[10][x] = [2]$

$\because \gcd(10, 14) = 2 \nmid 1$

by LCT 1, this has no solutions

(iii) $[10][x] = [2] \iff 10x \equiv 2 \mod 14$

Since $10(3) \equiv 30 \equiv 2 \mod 14$

LCT1 says $x \equiv 3 \mod \frac{14}{\gcd(10,14)}$

is the complete solution.

ie $x \equiv 3 \mod 7$

ie $x \equiv 3, 10 \mod 14$

ie $[x] = [3]$ or $[10]$ in $\mathbb{Z}_{14}$.

Solve the following equations in $\mathbb{Z}_{14}$. Express answers as $[x]$ where $0 \leq x < 14$.

ii) $[10][x] = [1]$ $\iff 10x \equiv 1 \mod 14$

iii) $[10][x] = [2]$

$\because \gcd(10,14) = 2 \nmid 1$

by LCT 1, this has no solutions.

(iii) $[10][x] = [2] \iff 10x \equiv 2 \mod 14$

$\iff$ Solve the LDE

$$10x + 14y = 2$$

$$5x + 7y = 1$$

By LDET2 $x = 3 + 7n$
$y = -2 - 5n$ $\forall n \in \mathbb{Z}$

$\therefore x \equiv 3 \mod 7$

$\therefore x \equiv 3, 10 \mod 14$

$\therefore [3]$ & $[10]$ ~~are our~~ are our solutions.

Inverses

- $[-a]$ is the additive inverse of $[a]$, that is,

$$[a]+[-a]=[0].$$

- If $\exists\, b \in \mathbb{Z}$ s.t. $[a][b]=[1]=[b][a]$

we call $[b]$ the multiplicative inverse of $[a]$ and write $[b]=[a]^{-1}$

Ex: $[5][11]=[1]$ in $\mathbb{Z}_{18}$

$\therefore [5]^{-1}=[11]$ & $[11]^{-1}=[5]$

WARNING: Multiplicative inverses do <u>NOT</u> always exist!

Ex: $[9][x]=[1]$ in $\mathbb{Z}_{18}$

LHS is <u>always</u> $[0]$ or $[9]$.

So $[9]^{-1}$ does not exist in $\mathbb{Z}_{18}$.

Find the additive and multiplicative inverses of $[7]$ in $\mathbb{Z}_{11}$. Give your answers in the form $[x]$ where $0 \leq x \leq 10$.

Sol'n: Additive inverse

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

Multiplicative Inverse: Want to Solve

$$[7][x] = [1]$$

$$\iff 7x \equiv 1 \mod 11$$

$$7 \cdot 3 \equiv 21 \equiv 10 \equiv -1 \mod 11$$

$$\therefore 7(-3) \equiv 1 \mod 11$$

$$\therefore [x] = [-3] = [8]$$

L29P4

Proposition: Let $a \in \mathbb{Z}$, $m \in \mathbb{N}$.

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

(b) $[a]^{-1}$ is unique if it exists.

Pf: (a) $[a]^{-1}$ exists

$\iff [a][x]=[1]$ is solvable in $\mathbb{Z}_m$

$\iff ax+my=1$ is a solvable LDE

$\iff \gcd(a,m)=1$ (GCDOO)

(b) Assume $[a]^{-1}$ exists. Suppose $\exists$ $b \in \mathbb{Z}$ s.t. $[a][b]=[1]=[b][a]$.

Then $[a]^{-1}[a][b]=[a]^{-1}[1]$

$$[1][b]=[a]^{-1}$$

$$[b]=[a]^{-1} \quad \blacksquare.$$

Solve $[15][x] + [7] = [12]$ in $\mathbb{Z}_{10}$.

Solution: This is equivalent to solving

$$15x + 7 \equiv 12 \pmod{10}.$$

Isolating for x gives

$$15x \equiv 5 \pmod{10}.$$

Since $15 \equiv 5 \pmod{10}$, Properties of Congruences states that

$$5x \equiv 5 \pmod{10}.$$

This clearly has the solution $x = 1$. Hence, by Linear Congruence Theorem 1, we have that

$$x \equiv 1 \mod \tfrac{10}{\gcd(5,10)}$$

gives the complete set of solutions. Thus, $x \equiv 1 \pmod 2$ or $x \equiv 1, 3, 5, 7, 9 \pmod{10}$. Since the original question is framed in terms of congruence classes, our answer should be as well and hence

$$[x] \in \{[1], [3], [5], [7], [9]\}.$$

For extra practice, see if you can phrase this argument using Linear Congruence Theorem 2.

L29P5

Practice problem: Solve $[15][x] + [7] = [12]$ in $\mathbb{Z}_{10}$.

The following are equivalent (TFAE)

- $a \equiv b \pmod{m}$
- $m \mid (a - b)$
- $\exists k \in \mathbb{Z}, a - b = km$
- $\exists k \in \mathbb{Z}, a = km + b$
- a and b have the same remainder when divided by m
- $[a] = [b]$ in $\mathbb{Z}_m$.

Theorem (LCT 2). *Let $a, c \in \mathbb{Z}$ and let $m \in \mathbb{N}$. Let $\gcd(a, m) = d$. The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$. Moreover, if $[x] = [x_0]$ is one particular solution, then the complete solution is*

$$\left\{[x_0], [x_0 + \tfrac{m}{d}], [x_0 + 2\tfrac{m}{d}], \ldots, [x_0 + (d-1)\tfrac{m}{d}]\right\}$$

Fermat's Little Theorem (FℓT)

If p is a prime number and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$. Equivalently, $[a^{p-1}] = [1]$ in $\mathbb{Z}_p$.

Ex: $5^6 \equiv 1 \bmod 7$, $4^6 \equiv 1 \bmod 7$, $39^6 \equiv 1 \bmod 7$

Note 1: $p-1$ is in the exponent! Note

$$6^3 \not\equiv 1 \bmod 7$$

Note 2: $p-1$ is not necessarily the smallest exponent s.t. $a^k \equiv 1 \bmod p$. Ex: $6^2 \equiv 1 \bmod 7$.

Lemma: Modulo p, the sets $S = \{a, 2a, \dots (p-1)a\}$ & $T = \{1, 2, -- p-1\}$ consist of the same elements provided

$$\gcd(a,p) = 1.$$

Pf: We show that S has $p-1$ distinct non zero elements modulo p. Let $1 \le k, m \le p-1$ be integers. Now if $ka \equiv ma \mod p$ then $p \mid a(k-m)$.
Since $\gcd(a,p)=1$, $p \mid (k-m)$ by (A).
Since $-p < 2-p \le k-m \le p-2 < p$ and $p \mid k-m$, we see that $k-m=0$ ie $k=m$.
Lastly, if $ka \equiv 0 \mod p$ then $p \mid ka$.
By Euclid's Lemma, $p \mid k$ (# $1 \le k \le p-1$ and p is prime) OR $p \mid a$ (# since $\gcd(a,p)=1$
Thus, S has $(p-1)$ distinct non zero elements modulo p.

Lemma proof recap:

(1) Start with $ka, ma \in S$

(2) Show $ka \equiv ma \mod p \Leftrightarrow k = m$

(3) Show if $ka \in S$ is s.t. $ka \equiv 0 \mod p$ then we have a contradiction.

Pf of FlT:

Using the lemma, valid since $p \nmid a \iff \gcd(a,p)=1$ (GCDPF), we have

$$\underbrace{\prod_{k=1}^{p-1} ka}_{\text{product of elets of } S} \equiv \underbrace{\prod_{k=1}^{p-1} k}_{\text{product of elets. of } T.} \mod p$$

Let $Q = \prod_{k=1}^{p-1} k = (1)(2)\cdots(p-1)$. Then

$$Qa^{p-1} \equiv Q \mod p$$

Since $\gcd(Q,p)=1$ ($\because$ Q is a product of terms less than a prime p), Q^{-1} exists hence

$$Q^{-1}Qa^{p-1} \equiv Q^{-1}Q \mod p$$

$$a^{p-1} \equiv 1 \mod p. \quad \blacksquare$$

Find the remainder when 7^{92} is divided by 11.

Recall (FlT): If $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$ (for p a prime)

By FlT $7^{10} \equiv 1 \mod 11$

$\Rightarrow 7^{90} \equiv 1 \mod 11$

$\Rightarrow 7^{92} \equiv 7^2 \equiv 49 \equiv 5 \mod 11.$

Option 2: $7^{92} \equiv 7^{9(10)+2} \mod 11$

$\equiv (7^{10})^9 \cdot 7^2 \mod 11$

FlT. $\equiv 1^9 \cdot 7^2 \mod 11$

$\equiv 49 \mod 11$

$\equiv 5 \mod 11$

Corollary: If p is a prime and $a \in \mathbb{Z}$ then $a^p \equiv a \bmod p$

Pf: If $p \mid a$ then $a \equiv 0 \bmod p$

$\Rightarrow a^p \equiv 0 \equiv a \bmod p$.

If $p \nmid a$ then by FlT:

$a^{p-1} \equiv 1 \bmod p \Rightarrow a^p \equiv a \bmod p$ ■

Corollary: If p is a prime number and $[a] \neq [0]$ in $\mathbb{Z}_p$, then $\exists [b] \in \mathbb{Z}_p$ s.t. $[a][b] = [1]$.

Pf: Since $[a] \neq [0]$, $p \nmid a$. Hence by FlT $a^{p-1} \equiv 1 \bmod p$

$a a^{p-2} \equiv 1 \bmod p$

Sensible since $p-2 \geq 0$. Thus, take $[b] = [a^{p-2}]$. ■

Corollary: If $r = s + kp$ then $a^r \equiv a^{s+k} \bmod p$ (p is a prime, $a, r, s, k \in \mathbb{Z}$)

Pf:
$$a^r \equiv a^{s+kp} \bmod p$$
$$\equiv a^s (a^p)^k \bmod p$$
(Cor. to FLT)
$$\equiv a^s (a)^k \bmod p$$
$$\equiv a^{s+k} \bmod p.$$

Prove that if $p \nmid a$ and $r \equiv s \mod (p-1)$ then $a^r \equiv a^s \mod p$.

Since $\cancel{p}$ $r \equiv s \mod (p-1)$

$(p-1) \mid r-s$

$\exists k \in \mathbb{Z}$ s.t. $(p-1)k = r-s$

$\Rightarrow r = s + (p-1)k$

$a^r \equiv a^{s+(p-1)k} \mod p$

$\equiv a^s (a^{p-1})^k \mod p$

(FLT) $\because p \nmid a$ $\equiv a^s (1)^k \mod p$

$\equiv a^s \mod p$

L30P5
Version1

Chinese Remainder Theorem (CRT)

Solve
$$x \equiv 2 \mod 7$$
$$x \equiv 7 \mod 11$$

Using the first condition, write
$$x = 2 + 7k$$
Plug into the second condition
$$2 + 7k \equiv 7 \mod 11$$
$$7k \equiv 5 \mod 11$$
Multiply both sides by 3

Used that $\gcd(7,11)=1$ to find 7^{-1}.

$$3 \cdot 7k \equiv 15 \mod 11$$
$$21k \equiv 4 \mod 11$$
$$-k \equiv 4 \mod 11$$
$$k \equiv -4 \equiv 7 \mod 11$$
$$\therefore k = 7 + 11\ell \text{ for some } \ell \in \mathbb{Z}$$

Version 1

Recall $x = 2 + 7k$

$= 2 + 7(7 + 11l)$

$= 51 + 77l$

$\therefore x \equiv 51 \mod 77$

L30 PS
Version 2

Chinese Remainder Theorem (CRT)

Solve: $x \equiv 2 \mod 7$

$x \equiv 7 \mod 11$

Condition 1 says

$x = 2 + 7k$ for some $k \in \mathbb{Z}$

Plug into condition 2:

$2 + 7k \equiv 7 \mod 11$

$7k \equiv 5 \mod 11$

This is equivalent to

$7k + 11y = 5$

k	y	r	q
0	1	11	
1	0	7	
-1	1	4	1
2	-1	3	1
-3	2	1	1
		0	3

$\therefore 7(-3) + 11(2) = 1$

$\therefore 7(-15) + 11(10) = 5$

LDET2: $k = -15 + 11n$ for all $n \in \mathbb{Z}$

~~Needed~~ Used $\gcd(7,11) = 1$.

L-30 p6

Version 2

$\therefore\ k \equiv -15 \equiv 7 \mod 11$

$k = 7 + 11\ell$ for some $\ell \in \mathbb{Z}$.

Recall!: $x = 2 + 7k$

$= 2 + 7(7 + 11\ell)$

$= 51 + 77\ell$.

$\therefore\ x \equiv 51 \mod 77$ is the sol'n.

L30P7

Theorem (Chinese Remainder Theorem (CRT)). *If* $\gcd(m_1, m_2) = 1$*, then for any choice of integers* a_1 *and* a_2*, there exists a solution to the simultaneous congruences*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

Moreover, if $n = n_0$ *is one integer solution, then the complete solution is* $n \equiv n_0 \pmod{m_1 m_2}$.

Theorem (Generalized CRT (GCRT)). *If* $m_1, m_2, \ldots, m_k$ *are integers and* $\gcd(m_i, m_j) = 1$ *whenever* $i \neq j$*, then for any choice of integers* $a_1, a_2, \ldots, a_k$*, there exists a solution to the simultaneous congruences*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

Moreover, if $n = n_0$ *is one integer solution, then the complete solution is*

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

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Which of the following is equal to $[53]^{242} + [5]^{-1}$ in $\mathbb{Z}_7$?

(Do not use a calculator.)

$\boxed{\text{A) } [5]}$

B) [4]

C) [3]

D) [2]

E) [1]

$$53^{242} \equiv 4^{242} \mod 7$$

$$\equiv (4^6)^{40} \cdot 4^2 \mod 7$$

FLT $(\because \gcd(4,7)=1)$ $\equiv 1^{40} \cdot 16 \mod 7$

$$\equiv 2$$

$$5^{-1} \equiv 3 \mod 7$$

$5 \cdot 3$
$\equiv 15$
$\equiv 1 \mod 7$

Sum: $5 \mod 7$

L31P2

Theorem (Chinese Remainder Theorem (CRT)). *If* $\gcd(m_1, m_2) = 1$, *then for any choice of integers* a_1 *and* a_2, *there exists a solution to the simultaneous congruences*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

Moreover, if $n = n_0$ *is one integer solution, then the complete solution is* $n \equiv n_0 \pmod{m_1 m_2}$.

Theorem (Generalized CRT (GCRT)). *If* $m_1, m_2, \ldots, m_k$ *are integers and* $\gcd(m_i, m_j) = 1$ *whenever* $i \neq j$, *then for any choice of integers* $a_1, a_2, \ldots, a_k$, *there exists a solution to the simultaneous congruences*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

Moreover, if $n = n_0$ *is one integer solution, then the complete solution is*

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

Solve $\quad x \equiv 5 \bmod 6 \quad (1)$

$x \equiv 2 \bmod 7 \quad (2)$

$x \equiv 3 \bmod 11 \quad (3)$

From (1) $x = 5 + 6k$ for some $k \in \mathbb{Z}$.

Plug into (2) $5 + 6k \equiv 2 \bmod 7$

$6k \equiv -3 \bmod 7$

$-k \equiv -3 \bmod 7$

$k \equiv 3 \bmod 7$

$k = 3 + 7l$ for some $l \in \mathbb{Z}$

$\therefore x = 5 + 6(3 + 7l)$

$= 23 + 42l. \quad (4)$

$\therefore x \equiv 23 \bmod 42$

Now, we need to solve

$x \equiv 23 \bmod 42$

$x \equiv 3 \bmod 11 \quad (3)$

Plug (4) into (3)

$$23+42l \equiv 3 \mod 11$$

$$-2l \equiv -20 \mod 11$$

Use CD valid $\because \gcd(-2,11)=1$

$$l \equiv 10 \mod 11$$

$\therefore l = 10 + 11m$ for some $m \in \mathbb{Z}$.

$\because x = 23 + \cancel{} 42l$,

$$\Rightarrow x = 23 + 42(10+11m)$$

$$= 443 + 462m$$

$$\therefore x \equiv 443 \mod 462$$

Twists

Solve $3x \equiv 2 \mod 5$

$2x \equiv 6 \mod 7$

Mult by 2 $6x \equiv 4 \mod 5$

$x \equiv 4 \mod 5$

mult. by 4 $8x \equiv 24 \mod 7$

$x \equiv 3 \mod 7$

Twist 2: $x \equiv 4 \mod 6$ (1)

$x \equiv 2 \mod 8$ (2)

(1) $\Rightarrow$ $x = 4 + 6k$ for some $k \in \mathbb{Z}$.

Into (2): $4 + 6k \equiv 2 \mod 8$

$6k \equiv -2 \mod 8$

$6k \equiv 6 \mod 8$

Clearly $k = 1$ is a solution.

LCT1 says $k \equiv 1 \mod \frac{8}{\gcd(6,8)}$ gives ALL solutions

$k \equiv 1 \mod 4$

$k = 1 + 4l$ for some $l \in \mathbb{Z}$.

$\therefore\ x = 4 + 6(1 + 4l)$

$= 10 + 24l$

$\therefore\ x \equiv 10 \mod 24$

Example: Solve $x^2 \equiv 34 \mod 99$

This implies $99 \mid x^2 - 34$

Note $9 \mid 99$ $\therefore\ 9 \mid x^2 - 34$ by transitivity

$\Rightarrow x^2 \equiv 34 \mod 9$

Note $11 \mid 99$ $\therefore\ 11 \mid x^2 - 34$ by transitivity

$\Rightarrow x^2 \equiv 34 \mod 11$

$\Rightarrow x^2 \equiv 1 \mod 11$

$\Rightarrow x \equiv \pm 1 \mod 11$

Similarly $x^2 \equiv 34 \equiv 7 \mod 9 \Rightarrow x \equiv \pm 4 \mod 9$.

This gives 4 systems of equations:

$$\begin{cases} x \equiv 1 \mod 11 \\ x \equiv 4 \mod 9 \end{cases} \qquad \begin{cases} x \equiv 1 \mod 11 \\ x \equiv -4 \mod 9 \end{cases}$$

$$\begin{cases} x \equiv -1 \mod 11 \\ x \equiv 4 \mod 9 \end{cases} \qquad \begin{cases} x \equiv -1 \mod 11 \\ x \equiv -4 \mod 9 \end{cases}$$

Use CRT 4 times.

(Sol'n $x \equiv 23, 32, 67, 76 \mod 99$)

Splitting the Modulus (SM)

Let m, n be coprime positive integers. Then for any integers x, a,

$$\begin{matrix} x \equiv a \mod m \\ x \equiv a \mod n \end{matrix} \text{ (simultaneously)} \iff x \equiv a \mod mn$$

Splitting the Modulus (SM)

L32P1

Let m, n be coprime positive integers. Then for any integers x, a,

$x \equiv a \bmod m$
$x \equiv a \bmod n$ (simultaneously) $\Leftrightarrow x \equiv a \bmod mn$

Pf: ($\Leftarrow$) $x \equiv a \bmod mn$

$\Rightarrow mn \mid x-a$

$\Rightarrow x \equiv a \bmod m$ $\because m \mid mn$ & $mn \mid x-a$ so by transitivity $m \mid x-a$

& $x \equiv a \bmod n$ similarly.

($\Rightarrow$) Assume $x \equiv a \bmod m$ & $x \equiv a \bmod n$

Note $x = a$ is a solution. Since $\gcd(m,n) = 1$ by CRT $x \equiv a \bmod mn$ gives all solutions.

$\blacksquare$.

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

Want to solve

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

By (SM)

$$x^5+x^3+2x^2+1 \equiv 0 \mod 2$$

$$x^5+x^3+2x^2+1 \equiv 0 \mod 3$$

Use equation 1 and plugin $x \equiv 0 \mod 2$ & $x \equiv 1 \mod 2$. In both cases

$$x^5+x^3+2x^2+1 \equiv 1 \mod 2.$$

$\therefore$ $x^5+x^3+2x^2+1$ is never divisible by 6.

L32 P3

Cryptography

- The practice/study of secure communication.

Eve

Alice ——┴—— Bob

<u>NB</u>: A cryptosystem should not depend on the secrecy of the methods of encryption & decryption (except for possibly secret keys).

Private Key Cryptography

∴ Agree before hand on a secret encryption & decryption key.

Ex! Caesar Cipher (ASCII Table)

Map plaintext M to

$$C \equiv M+3 \mod 26 \quad (0 \leq C < 26)$$

Ex: A P P L E

00 15 15 11 04

03 18 18 14 07

D S S O H

Cons of Private Key Cryptography.

- Tough to share private key before hand.
- Too many private keys to share.
- Difficult to communicate with strangers

Public Key Cryptography.

L32P5

Analogy: Pad lock
- Easy to lock
- Difficult to unlock without a Key

Eve

Alice ——— Bob

public Key e

Private Key d

$M \mapsto C$

Decrypt C to M using d.

Send C

using encryption Key

- Encryption & Decryption are inverses
- d & e are different
- Only d is secret.

Exponentiation Ciphers

Alice chooses a (large) prime p and an integer e satisfying

$1 < e < p-1$ & $\gcd(e, p-1) = 1$

Alice makes (e, p) public.

Alice computes d, an integer via

$1 < d < p-1$ & $ed \equiv 1 \mod p-1$

Note: d can be found quickly using EEA.

Note: Inverse exists $\because \gcd(e, p-1) = 1$.

To send a message $0 \leq M < p$ to Alice, Bob computes C s.t.

$0 \leq C < p$ & $C \equiv M^e \mod p$

Bob sends C to Alice & Alice computes $R \equiv C^d \mod p$ with $0 \leq R < p$.

Recall Corollary to FLT: If $p \nmid a$ and $r \equiv s \mod p-1$ then $a^r \equiv a^s \mod p$

Last Time: Let p be a prime, e an integer satisfying

$$1 < e < p-1 \qquad \text{and} \qquad \gcd(e, p-1) = 1.$$

Let d be an integer such that

$$1 < d < p-1 \qquad \text{and} \qquad ed \equiv 1 \mod p-1$$

Let M be an integer between 0 and $p-1$ inclusive. Compute C an integer satisfying

$$0 \leq C < p \qquad \text{and} \qquad C \equiv M^e \mod p.$$

and let $R \equiv C^d \mod p$ be an integer with $0 \leq R \leq p-1$.

Eve

Alice

Bob

(e,p)

Private d

$M \mapsto C \equiv M^e \mod p$

C

$R \equiv C^d \mod p$.

Proposition 1: $R \equiv M \mod p$.

Corollary: $R = M$

Pf of proposition 1:

If $p \mid M$ then $M = 0$. Since $0 \le M \le p-1$

Then $C \equiv M^e \equiv 0 \mod p$ and so $C = 0 \because 0 \le C < p$.

Then $R \equiv C^d \equiv 0 \mod p$ and so $R = 0 \because 0 \le R < p$.

If $p \nmid M$ then

$$\begin{aligned} R &\equiv C^d \mod p \\ &\equiv (M^e)^d \mod p \quad \left(\text{Recall } ed \equiv 1 \mod p-1\right) \\ &\equiv M^{ed} \mod p \\ &\equiv M \mod p \quad (\text{By corollary to FlT}) \end{aligned}$$

$\blacksquare$

Pf of Corollary: Since $0 \le R, M \le p-1$, and $p \mid R-M$, we have that $R - M = 0$ ie $R = M$.

$\blacksquare$

RSA

Alice chooses distinct primes p & q and an integer e satisfying

$$1 < e < (p-1)(q-1) \quad \& \quad \gcd(e,(p-1)(q-1))=1$$

Alice's private key d is an integer satisfying

$$1 < d < (p-1)(q-1) \quad \& \quad ed \equiv 1 \mod (p-1)(q-1)$$

Bob wants to send a message M, an integer between 0 & $pq-1$ inclusive. He computes C an integer satisfying

$$0 \leq C < pq \quad \text{and} \quad C \equiv M^e \mod pq$$

Alice computes $R \equiv C^d \mod pq$ with $0 \leq R \leq pq-1$.

Eve

Alice —— (e,pq) —— Bob

private d

Compute $R \equiv C^d \mod pq$. C $C \equiv M^e \mod pq$

Proposition 2: $R = M$

PF: Since $ed \equiv 1 \mod (p-1)(q-1)$, transitivity of divisibility says

$$ed \equiv 1 \mod p-1 \quad \& \quad ed \equiv 1 \mod q-1$$

Since $\gcd(e, (p-1)(q-1)) = 1$, GCDPF states that $\gcd(e, (p-1)) = 1 = \gcd(e, (q-1))$

Since $C \equiv M^e \mod pq$ (SM) states

$$C \equiv M^e \mod p \quad \& \quad C \equiv M^e \mod q.$$

Similarly, by (SM), $R \equiv C^d \mod p$ & $R \equiv C^d \mod q$

By Proposition 1:

$$R \equiv M \mod p \qquad \& \quad R \equiv M \mod q$$

By (SM) or (CRT) we have

$$R \equiv M \mod pq$$

<u>BUT</u> since $0 \leq R, M \leq pq-1$ we have that $R = M$. $\blacksquare$.

Why is this more secure?

Before: given (e, p) we can easily compute $p-1$. Hence can easily compute $d \equiv e^{-1} \bmod p-1$

Now: Given (e, pq) we cannot easily compute $(p-1)(q-1)$ UNLESS we factor pq.

Notes: We denote $n = pq$ and
$\phi(n) = (p-1)(q-1)$
(ϕ is called Euler's toitent function or phi-function)

$$\sum_{\substack{p \leq x \\ p \text{ is prime}}} 1 \sim \frac{x}{\log(x)}$$ PRIME NUMBER THEOREM

Let $p = 2$, $q = 11$ and $e = 3$

1. Compute n, $\phi(n)$ and d.
2. Compute $C \equiv M^e \mod n$ when $M = 8$
3. Compute $M \equiv C^d \mod n$ when $C = 6$

1. $n = 22$ $\quad \phi(n) = (2-1)(11-1) = 10$

$3d \equiv 1 \mod 10$

$d \equiv 7 \mod 10$ so $d = 7$.

2. $C \equiv M^e \mod 22$
$\equiv 8^3 \mod 22$
$\equiv 8 \cdot 64 \mod 22$
$\equiv 8(-2) \mod 22$
$\equiv -16 \mod 22$
$\equiv 6 \mod 22$.

3. $M \equiv C^d \mod 22$
$\equiv 6^7 \mod 22$
$\equiv 6 \cdot (6^3)^2 \mod 22$
$\equiv 6 \cdot (216)^2 \mod 22$
$\equiv 6(-4)^2 \mod 22$
$\equiv 6 \cdot 16 \mod 22$
$\equiv 6(-6) \mod 22$
$\equiv -36 \mod 22$
$\equiv 8 \mod 22$.

Complex Numbers

Current view $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

These sets can be thought of as helping us to solve polynomial equations.
However $x^2+1=0$ has no solution in <u>any</u> of these sets.

Def'n: A complex number (in standard form) is an expression of the form $x+yi$ where $x, y \in \mathbb{R}$ and i is the imaginary unit.
Denote the set of complex numbers by

$$\mathbb{C} := \{x+yi : x, y \in \mathbb{R}\}.$$

Ex: $1+2i$, $3i$, $\sqrt{13}+\pi i$, $2+0i$

Note: $\mathbb{R} \subseteq \mathbb{C}$.

If $z = x+yi$ then $x = \mathrm{Re}(z) = \Re(z)$ real part.
$y = \mathrm{Im}(z) = \Im(z)$ imaginary part.

L34P2

Two complex numbers $z = x + yi$ and $w = u + vi$ are equal iff

$$x = u \quad \& \quad y = v.$$

A complex number z is

- purely real if $\mathrm{Im}(z) = 0$ ie $z = x$
- Purely imaginary if $\mathrm{Re}(z) = 0$ ie $z = yi$.

We turn $\mathbb{C}$ into a ring by defining $+, -, \cdot$ b

$$(x+yi) \pm (u+vi) = (x \pm u) + (y \pm v)i$$

$$(x+yi)(u+vi) = (xu - vy) + (xv + uy)i$$

By this def'n:

$$i^2 = i \cdot i = (0+i)(0+i) = -1 + 0i = -1$$

<u>So</u> i is a solution to $x^2 + 1 = 0$.

With this, multiplication can be remembered b

$$(x+yi)(u+vi) = xu + xvi + uyi + vyi^2$$

$$= xu - vy + (xv + uy)i$$

Ex: $(1+2i)+(3+4i) = 4+6i$

$(1+2i)-(3+4i) = -2-2i$

$(1+2i)(3+4i) = 3-8+(4+6)i$

$= -5+10i$

Commutative
Rings (hence $\mathbb{C}$) have the following properties

1. Associativity (Let $v, w, z \in \mathbb{C}$ & $z = x+yi$)

$(v+w)+z = v+(w+z)$

& $(vw)z = v(wz)$

2. Commutativity

$w+v = v+w$ & $wv = vw$

3. Identities

$z+0 = z$ & $z \cdot 1 = z$ where

$0 = 0+0i$ & $1 = 1+0i$

4. Additive inverses

$z+(-z) = 0$ where $-z = -x-yi$

5. Distributive Property

$$z(w+v) = zw + zv$$

We turn $\mathbb{C}$ into a field by defining the inverse operation for nonzero complex numbers

$$(x+yi)^{-1} := \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2} i$$

Note: If $z \in \mathbb{C}$ & $z \neq 0$ then

$$z \cdot z^{-1} = 1 \quad \text{(Exercise)}$$

For complex numbers u, v, w, z with v, z nonzero, the above is consistent with the usual fraction rules:

$$\frac{u}{v} + \frac{w}{z} = \frac{uz+vw}{vz} \quad \& \quad \frac{u}{v} \cdot \frac{w}{z} = \frac{uw}{vz}$$

For $k \in \mathbb{N}$, $z \in \mathbb{C}$ define $(z \neq 0)$

$$z^0 = 1 \quad z^1 = z \;\; \& \;\; z^{k+1} = z \cdot z^k$$

Define $z^{-k} := (z^{-1})^k$

Usual exponent rules hold ie

$$(z^m)^n = z^{mn} \quad \& \quad z^m \cdot z^n = z^{m+n}$$

(for $m, n \in \mathbb{Z}$).

Ex: Write $\frac{1+2i}{3-4i}$ in standard form

Sol'n:

$$\begin{aligned}
\frac{1+2i}{3-4i} &= (1+2i)(3-4i)^{-1} \\
&= (1+2i)\left(\frac{3}{3^2+4^2} - \frac{(-4)}{3^2+4^2} i\right) \\
&= (1+2i)\left(\frac{3}{25} + \frac{4}{25} i\right) \\
&= \frac{3}{25} - \frac{8}{25} + \left(\frac{4}{25} + \frac{6}{25}\right) i \\
&= \frac{-5}{25} + \frac{10}{25} i \\
&= \frac{-1}{5} + \frac{2}{5} i
\end{aligned}$$

Express the following in standard form:

1. $\frac{(1-2i)-(3+4i)}{5-6i} = S$

2. $i^{2015} = T$

1. $S = ((1-2i)-(3+4i))(5-6i)^{-1}$

$= (-2-6i)\left(\frac{5}{5^2+6^2} - \frac{(-6)}{5^2+6^2}i\right)$

$= (-2-6i)\left(\frac{5}{61} + \frac{6}{61}i\right)$

$= \left(\frac{-10}{61} + \frac{36}{61}\right) + \left(\frac{-12}{61} - \frac{30}{61}\right)i$

$= \frac{26}{61} - \frac{42}{61}i$

2. $T = i^{2015}$

$i^2 = -1$
$i^4 = 1$

$= (i^4)^{503} \cdot i^3$

$= 1^{503} \cdot i^2 \cdot i$

$= -i = 0 - i$

L35 P1

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2.When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. How many integers x satisfy all of the following three conditions?

$$x \equiv 6 \pmod{13}$$
$$4x \equiv 3 \pmod{7}$$
$$-1000 < x < 1000$$

$x \equiv 6 \bmod 7$

A) 1

B) 7

C) 13

D) 22

E) 91

By CRT OR SM $x \equiv 6 \bmod 91$

$x = 6 + 91k$

$-1000 < 6 + 91k < 1000$

$-1006 < 91k < 994$

$91 \cdot 10 = 910$

$91 \cdot 11 = 1001$

$-11 \leq k \leq 10$

22 solutions!

Ex: Solve

$$z^2 - z + 1 = 0 \quad \text{for } z \in \mathbb{C}$$

Sol'n: $z = \dfrac{-(-1) \pm \sqrt{(-1)^2 - 4(1)(1)}}{2(1)}$

$= \dfrac{1 \pm \sqrt{-3}}{2}$

$= \dfrac{1 \pm \sqrt{3}\, i}{2}$

Q: What are the solutions to

$$z^2 = -r \quad \text{for } r \in \mathbb{R},\ r \geq 0?$$

Sol'n: Let $z = x + yi$ with $x, y \in \mathbb{R}$. Then

$-r = z^2 = (x+yi)^2 = x^2 - y^2 + 2xyi$

$\therefore \left.\begin{array}{l} 2xy = 0 \\ x^2 - y^2 = -r \end{array}\right\} \Rightarrow x = 0$ and $-y^2 = -r \Rightarrow y^2 = r$

$\Rightarrow y = \pm\sqrt{r}$

$\therefore z = \pm\sqrt{r}\, i$

Note: This validates the usage of

$$\sqrt{-r} = \pm\sqrt{r}\,i$$

Corollary: The quadratic formula still works for complex numbers.

Def'n: The complex conjugate of a complex number $z = x + yi$ is $\bar{z} := x - yi$

Solve $z^2 = i\bar{z}$ for $z \in \mathbb{C}$

Let $z = x + yi$ for $x, y \in \mathbb{R}$.

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

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

$x^2 - y^2 = y \quad (1)$

$2xy = x \Rightarrow 2xy - x = 0$

$x(2y-1) = 0$

$x = 0$ OR $y = \frac{1}{2}$.

Subinto (1)

$\boxed{x=0}$ $-y^2 = y \Rightarrow y^2 + y = 0 \Rightarrow y = 0$ or -1

$\boxed{y=\frac{1}{2}}$ $x^2 - (\frac{1}{2})^2 = \frac{1}{2} \Rightarrow x^2 = \frac{3}{4}$ $x = \pm\frac{\sqrt{3}}{2}$.

$\therefore z \in \{0, -i, \frac{\sqrt{3}}{2} + \frac{1}{2}i, -\frac{\sqrt{3}}{2} + \frac{1}{2}i\}$.

Find a real solution to

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

Take $z = r \in \mathbb{R}$

$6r^3 + r^2 + 3\sqrt{2}\,ir^2 - 11r + 2\sqrt{2}\,ir - 6 = 0$

$\Rightarrow 3\sqrt{2}\,r^2 + 2\sqrt{2}\,r = 0 \Rightarrow r(3r+2) = 0$

$r = 0$ OR $r = \frac{-2}{3}$

$6r^3 + r^2 - 11r - 6 = 0$

$r = 0$ is not a solution to $6r^3 + r^2 - 11r - 6 = 0$

$r = -\frac{2}{3}$ <u>is</u> a solution to $6r^3 + r^2 - 11r - 6 = 0$.

$\therefore z = \frac{-2}{3}$ is a real solution.

L35P6

Properties of Conjugates (PCJ)

Let $z, w \in \mathbb{C}$. Then

1. $\overline{z+w} = \bar{z} + \bar{w}$
2. $\overline{zw} = \bar{z}\,\bar{w}$
3. $\overline{\overline{z}} = z$
4. $z + \bar{z} = 2\,\mathrm{Re}(z)$
5. $z - \bar{z} = 2i\,\mathrm{Im}(z)$

Pf: Let $z = x+yi$ & $w = u+vi$.

(3) $\overline{\overline{z}} = \overline{\overline{(x+yi)}} = \overline{(x-yi)} = x+yi = z$.

(2) $\overline{zw} = \overline{(x+yi)(u+vi)}$

$= \overline{((xu-vy) + (xv+uy)i}$

$= xu - vy - (xv+uy)i$

$\bar{z}\bar{w} = (x-yi)(u-vi) = xu - vy + (-xv-uy)i$

$= \overline{zw}$

Properties of Conjugates (PCJ)

Let $z, w \in \mathbb{C}$.

1. $\overline{z+w} = \overline{z} + \overline{w}$
2. $\overline{zw} = \overline{z}\,\overline{w}$
3. $\overline{\overline{z}} = z$
4. $z + \overline{z} = 2\mathrm{Re}(z)$
5. $z - \overline{z} = 2i\mathrm{Im}(z)$

Prove the following for $z \in \mathbb{C}$

1. $z \in \mathbb{R}$ if and only if $z = \bar{z}$.

2. z is purely imaginary if and only if $z = -\bar{z}$.

1. $\Rightarrow$ Let $z = x + 0i \in \mathbb{R}$.

Then $\bar{z} = x - 0i = x = z$

$\Leftarrow$ Let $z = x + yi$ $x, y \in \mathbb{R}$. Assume

$$z = \bar{z}$$

$$x + yi = x - yi$$

$$\Rightarrow \quad y = -y$$

$$\Rightarrow \quad 2y = 0$$

$$\Rightarrow \quad y = 0 \qquad \therefore z = x + 0i \in \mathbb{R}.$$

2. z is purely imaginary

$\Leftrightarrow \quad iz \in \mathbb{R}$

By 1. $\Leftrightarrow \quad iz = \overline{iz}$

$\Leftrightarrow \quad iz = -i\bar{z}$

$\Leftrightarrow \quad z = -\bar{z}$

Def'n: The modulus of $z = x+yi$ is the non-negative real number

$$|z| = |x+yi| := \sqrt{x^2+y^2}$$

Properties of Modulus (PM)

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

Pf of 4: Let $z = x+yi$ & $w = u+vi$

Suffices to show $|zw|^2 = |z|^2|w|^2$

$$|zw|^2 = |(x+yi)(u+vi)|^2$$
$$= |(xu-vy) + (xv+uy)i|^2$$
$$= (xu-vy)^2 + (xv+uy)^2.$$

$$|zw|^2 = |(x+yi)(u+vi)|^2$$
$$= |(xu-vy)+(xv+uy)i|^2$$

By def'n of $|z|$. $\rightarrow$ $= (xu-vy)^2 + (xv+uy)^2$

$$= x^2u^2 - 2xuvy + v^2y^2 + x^2v^2 + 2xuvy + u^2y^2$$
$$= x^2u^2 + x^2v^2 + v^2y^2 + u^2y^2$$

$$|z|^2|w|^2 = |x+yi|^2\,|u+vi|^2$$
$$= (x^2+y^2)(u^2+v^2)$$
$$= x^2u^2 + x^2v^2 + y^2u^2 + y^2v^2 = |zw|^2$$

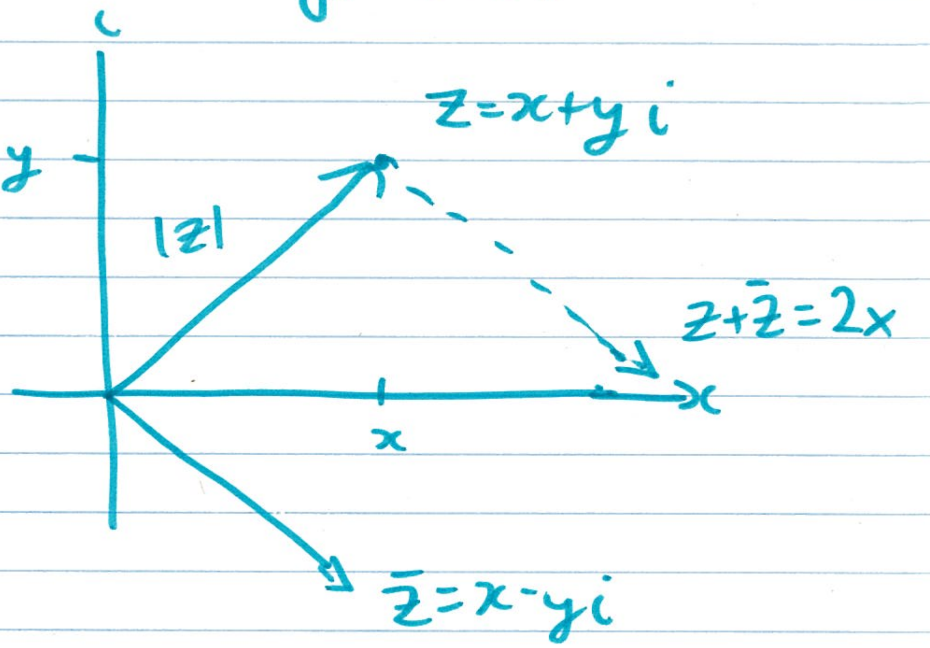
Pf of 5 (Exercise)

Revisit Inverses:

If $z = x+yi$ then $z^{-1} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}i$

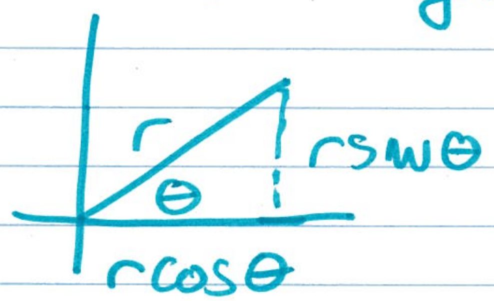
Note $z^{-1} = \frac{1}{z}\,\frac{\overline{z}}{\overline{z}} = \frac{\overline{z}}{z\cdot\overline{z}} = \frac{\overline{z}}{|z|^2}$.

Pictures! (Argand Diagrams)

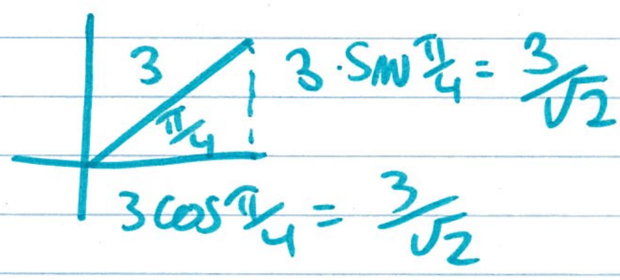


Polar Coordinates

A point in the plane corresponds to a length and ~~a~~ an angle.



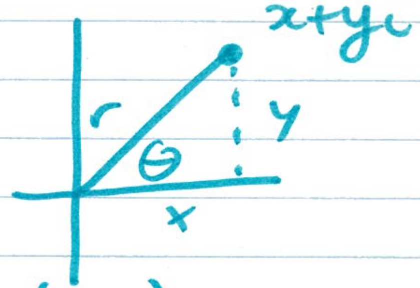
Ex: $(r, \theta) = (3, \frac{\pi}{4})$



Corresponds to $3\cos\frac{\pi}{4} + i \cdot 3\sin\frac{\pi}{4}$

$$= \frac{3}{\sqrt{2}} + \frac{3}{\sqrt{2}} i$$

Given $z = x + yi$



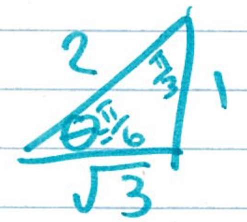
$r = |z| = \sqrt{x^2 + y^2}$

$\theta = \arccos\left(\frac{x}{r}\right) = \arcsin\left(\frac{y}{r}\right) = \arctan\left(\frac{y}{x}\right)$

Ex: $z = \sqrt{6} + \sqrt{2}\, i$

$r = \sqrt{\sqrt{6}^2 + \sqrt{2}^2} = \sqrt{8} = 2\sqrt{2}$.

$\theta = \arctan\left(\frac{\sqrt{2}}{\sqrt{6}}\right) = \arctan\left(\frac{1}{\sqrt{3}}\right) = \frac{\pi}{6}$.



$\therefore z$ corresponds to $(r, \theta) = (2\sqrt{2}, \frac{\pi}{6})$

Def'n: The polar form of a complex number z is $z = r(\cos\theta + i\sin\theta)$ where r is the modulus of z and θ is called <u>an</u> argument of z $(\arg(z) = \theta)$

Denote $\operatorname{cis}\theta := \cos\theta + i\sin\theta$

Ex: $z = \sqrt{6} + \sqrt{2}\, i = 2\sqrt{2}\,(\cos\pi/6 + i\sin\pi/6)$

L36P7.

Express the following in terms of polar coordinates:

1. -3

2. $1-i$

Triangle Inequality: Let $z, w \in \mathbb{C}$. Then $|z+w| \leq |z| + |w|$.

Proof: It suffices to prove that

$$|z+w|^2 \leq (|z|+|w|)^2 = |z|^2 + 2|zw| + |w|^2$$

since the modulus is a positive real number. Using the Properties of Modulus and the Properties of Conjugates, we have

$$\begin{aligned}
|z+w|^2 &= (z+w)\left(\overline{z+w}\right) && \text{PM} \\
&= (z+w)(\bar{z}+\bar{w}) && \text{PCJ} \\
&= z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} \\
&= |z|^2 + z\bar{w} + \overline{z\bar{w}} + |w|^2 && \text{PCJ and PM}
\end{aligned}$$

Now, from Properties of Conjugates, we have that

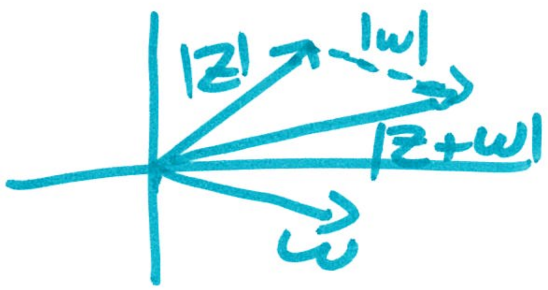
$$z\bar{w} + \overline{z\bar{w}} = 2\Re(z\bar{w}) \leq 2|z\bar{w}| = 2|zw|$$

and hence

$$|z+w|^2 = |z|^2 + z\bar{w} + \overline{z\bar{w}} + |w|^2 \leq |z|^2 + 2|zw| + |w|^2$$

completing the proof.

Diagram:



Express the following in terms of polar coordinates:

1. -3
2. $1 - i$

1. $z = -3$

$r = |-3| = 3$

$\theta = \arctan\left(\frac{0}{-3}\right) = 0$

$-3 = 3(\cos(0) + i\sin(0))$ ×

actually, $\theta = 0 + \pi$.

$-3 = 3(\cos\pi + i\sin\pi)$

2. $1-i$ $\quad r = |1-i| = \sqrt{1^2+1^2} = \sqrt{2}$

$1 - i = \sqrt{2}\left(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right)$

$= \sqrt{2}\left(\cos\left(\frac{7\pi}{4}\right) + i\sin\left(\frac{7\pi}{4}\right)\right)$

$= \sqrt{2}\,\mathrm{cis}\left(\frac{7\pi}{4}\right)$

1. Write $\operatorname{cis}(15\pi/6)$ in standard form.

2. Write $-3\sqrt{2}+3\sqrt{6}i$ in polar form.

1. $\text{CIS}(15\frac{\pi}{6}) = \cos(\frac{5\pi}{2}) + i\sin(\frac{5\pi}{2})$

$= i$

2. $r = |-3\sqrt{2}+3\sqrt{6}i|$

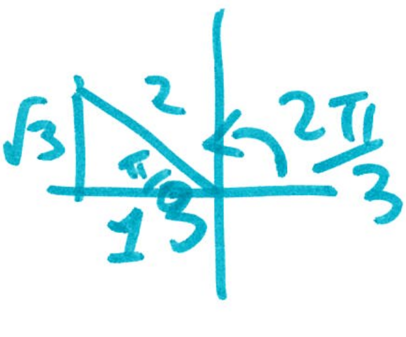
$= \sqrt{(-3\sqrt{2})^2 + (3\sqrt{6})^2}$

$= \sqrt{18+54}$

$= \sqrt{72}$

$= 6\sqrt{2}$

$-3\sqrt{2}+3\sqrt{6}i = 6\sqrt{2}\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)$



$= 6\sqrt{2}\,\text{CIS}(2\pi/3)$

L37 P4

(PMCN)

Polar Multiplication of Complex Numbers

If $z_1 = r_1 \operatorname{cis} \theta_1$ & $z_2 = r_2 \operatorname{cis} \theta_2$

Then $z_1 z_2 = r_1 r_2 \operatorname{cis}(\theta_1 + \theta_2)$

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

$= r_1 r_2 (\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2$

$+ i(\cos\theta_1 \sin\theta_2 + \sin\theta_1 \cos\theta_2$

trig identities. $= r_1 r_2 (\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$

Corollary: Multiplication by $i = \cos(\pi/2) + i\sin(\pi/2)$ gives a rotation by $\pi/2$.

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

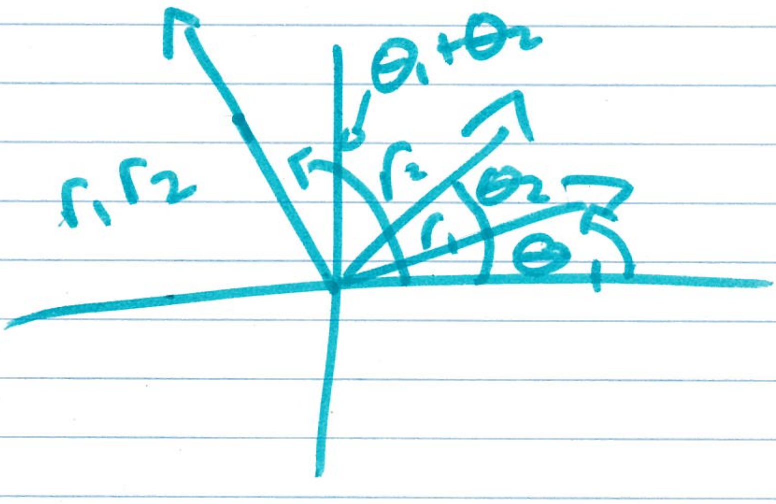
$= 2\sqrt{2}\,\text{CIS}\left(\frac{\pi}{6}\right) \cdot 6\sqrt{2}\,\text{CIS}\left(\frac{2\pi}{3}\right)$

PMCN $= 24\,\text{CIS}\left(\frac{\pi}{6} + \frac{2\pi}{3}\right)$

$= 24\,\text{CIS}\left(\frac{5\pi}{6}\right)$

$= 24\left(-\frac{\sqrt{3}}{2} + \frac{i}{2}\right)$

$= (-12\sqrt{3} + 12i)$



L37P6.

De Moivre's Theorem

If $\theta \in \mathbb{R}$ & $n \in \mathbb{Z}$ then

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

Pf: First note that when $n=0$,

$$(\cos\theta + i\sin\theta)^0 = 1$$

$$\cos(0\cdot\theta) + i\sin(0\cdot\theta) = 1$$

Now, if $n<0$, write $n=-m$ for some $m\in$

$$\begin{aligned}(\cos\theta + i\sin\theta)^n &= (\cos\theta + i\sin\theta)^{-m} \\ &= ((\cos\theta + i\sin\theta)^{-1})^m \\ &= \left(\frac{\cos\theta - i\sin\theta}{\cos^2\theta + \sin^2\theta}\right)^m \\ &= (\cos\theta - i\sin\theta)^m \\ &= (\cos(-\theta) + i\sin(-\theta))^m\end{aligned}$$

Thus, it suffices to prove DMT with a positive exponent.

De Moivre's Theorem

Let $\theta \in \mathbb{R}$ & $n \in \mathbb{Z}$. Then

$$(\text{cis}\,\theta)^n = \text{cis}(n\theta)$$

Pf: From work yesterday, it suffices to prove the claim for $n \in \mathbb{N}$.

Proof by induction on n.

Base Case: $n = 1$

$\text{cis}(n\theta) = \text{cis}\,\theta = (\text{cis}\,\theta)^1 = (\text{cis}\,\theta)^n$.

IH: Assume that

$$(\text{cis}\,\theta)^k = \text{cis}(k\theta)$$

for some $k \in \mathbb{N}$

I Step: WANT $(\text{cis}\,\theta)^{k+1} = \text{cis}((k+1)\theta)$

$$\begin{aligned} LH = (\text{cis}\,\theta)^{k+1} &= (\text{cis}\,\theta)^k (\text{cis}\,\theta) \\ &\overset{IH}{=} \text{cis}(k\theta)\,\text{cis}(\theta) \\ &\overset{PMCN}{=} \text{cis}(k\theta + \theta) \\ &= \text{cis}((k+1)\theta) \end{aligned}$$

$\therefore$ by POMI $(\text{cis}\,\theta)^n = \text{cis}(n\theta)$ $\forall n \in \mathbb{N}$. ∎

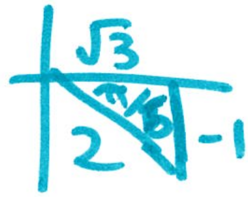
Corollary: If $z = r\,\text{cis}\,\theta$ then

$$z^n = r^n\,\text{cis}(n\theta)$$

Write $(\sqrt{3}-i)^{10}$ in standard form.

Convert $\sqrt{3}-i$ to polar coordinates.

$$\sqrt{3}-i = 2\left(\frac{\sqrt{3}}{2}-\frac{i}{2}\right) \quad \because 2=|\sqrt{3}-i|$$



$$= 2\,\mathrm{cis}\left(-\frac{\pi}{6}\right)$$

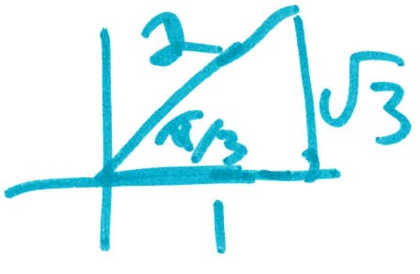
$$= 2\,\mathrm{cis}\left(\frac{11\pi}{6}\right)$$

DMT

$$\left(2\,\mathrm{cis}\left(\frac{11\pi}{6}\right)\right)^{10} = 2^{10}\,\mathrm{cis}\left(\frac{110}{6}\pi\right)$$

$$= 2^{10}\,\mathrm{cis}\left(\frac{55}{8}\pi\right)$$

$$= 2^{10}\,\mathrm{cis}\left(9(2\pi)+\frac{\pi}{3}\right)$$



$$= 2^{10}\,\mathrm{cis}\left(\frac{\pi}{3}\right)$$

$$= 2^{10}\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)$$

$$= 2^{9} + 2^{9}\sqrt{3}\,i$$

$$= 512 + 512\sqrt{3}\,i$$

Complex Exponential Function

For real θ, define

$$e^{i\theta} := \cos\theta + i\sin\theta = \text{cis}\,\theta$$

Note: Can write $z \in \mathbb{C}$ as $z = re^{i\theta}$ where $r = |z|$ & θ is an argument of z

Q: Why this def'n?

Reason 1: Exponent Laws Work!

$$e^{i\theta} \cdot e^{i\alpha} = e^{i(\theta+\alpha)} \quad \text{(PMCN)}$$

$$n \in \mathbb{Z} \qquad (e^{i\theta})^n = e^{in\theta} \quad \text{(DMT)}$$

Reason 2: Derivative wrt θ

$$\frac{d}{d\theta}(\cos\theta + i\sin\theta) = -\sin\theta + i\cos\theta$$
$$= i(\cos\theta + i\sin\theta)$$
$$= ie^{i\theta}$$

Reason 3: Power Series

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots$$

Using these,

$$e^{ix} = \cos x + i \sin x$$ Euler's Formula.

If $\theta = \pi$ then

$$e^{i\pi} = \cos \pi + i \sin \pi = -1$$

Ex: Write $(2e^{11\pi i/6})^6$ in standard form.

Sol'n: By exponent rules (DMT)

$$\begin{aligned} (2e^{11\pi i/6})^6 &= 2^6 e^{11\pi i} \\ &= 2^6(\cos(11\pi) + i\sin(11\pi)) \\ &= 2^6(-1 + 0 \cdot i) \\ &= -64. \end{aligned}$$

Solve: $z^6+2z^3-3=0$

$$(z^3)^2+2z^3-3=0$$
$$(z^3-1)(z^3+3)=0$$
$$z^3=1 \quad \underline{\text{OR}} \quad z^3=-3$$

Q: Can we solve $z^n=w$ for a fixed $w \in \mathbb{C}$?

Note: Saw this with $n=2$ & $w=-r$.

Ex: Solve $z^6=-64$

Sol'n: $2e^{11\pi i/6}$ was a solution.

$\pm 2i$ are 2 other examples.

How do we find solutions in general?

Ans: Write $z=re^{i\theta}$

$$z^6=r^6e^{i6\theta}=-64$$
$$|r|^6|e^{i6\theta}|=64$$
$$|r|^6=64$$
$$\Rightarrow r=2 \quad (\because r>0)$$

L39P1

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. What is the value of $\left|\left(\overline{-\sqrt{3}+i}\right)^5\right|$?

~~A) $16i$~~

B) 27

C) 32

~~D) -45~~

E) 64

$= |(-\sqrt{3}-i)^5|$

polar coord

$|(-\sqrt{3}-i)|^5$

$= |(2(-\frac{\sqrt{3}}{2}-\frac{i}{2}))^5|$

$= \sqrt{(-\sqrt{3})^2+(-1)^2}^{\,5}$

DMT $= |2^5 \operatorname{cis}(\frac{7\pi}{6}\cdot 5)|$

$= \sqrt{4}^{\,5}$

$= 32$

$= 32.$

Last Time: Solve $z^6 = -64$

- $z = re^{i\theta}$ $(r = |z|)$
- $64 = |z|^6 = r^6 |e^{i \cdot 6\theta}| = r^6 \Rightarrow r = 2$
- $r^6 e^{i \cdot 6\theta} = -64 \Rightarrow e^{i6\theta} = -1$

$\cos(6\theta) + i\sin(6\theta) = -1 = \cos\pi + i\sin\pi.$

Equating real parts gives

$\cos(6\theta) = \cos(\pi) \Rightarrow 6\theta = \pi + 2\pi k$ (for $k \in \mathbb{Z}$)

Solving for θ gives: $\theta = \frac{\pi + 2\pi k}{6} = \frac{\pi}{6} + \frac{\pi}{3}k.$

When do two θ values coincide with the same complex point? A: When they differ by multiples of 2π.

Claim: $\theta_1 = \frac{\pi}{6} + \frac{\pi}{3}k_1$ & $\theta_2 = \frac{\pi}{6} + \frac{\pi}{3}k_2$ are equal up to 2π rotations iff $k_1 \equiv k_2 \bmod 6$

Pf: $\theta_1 = \theta_2 + 2\pi m$ for some $m \in \mathbb{Z}$

$\iff \frac{\pi}{6} + \frac{\pi}{3}k_1 = \frac{\pi}{6} + \frac{\pi}{3}k_2 + 2\pi m$

$$\Longleftrightarrow \frac{\pi}{3}k_1 = \frac{\pi}{3}k_2 + 2\pi m$$

$$\Longleftrightarrow k_1 = k_2 + 6m$$

$$\Longleftrightarrow k_1 \equiv k_2 \bmod 6.$$

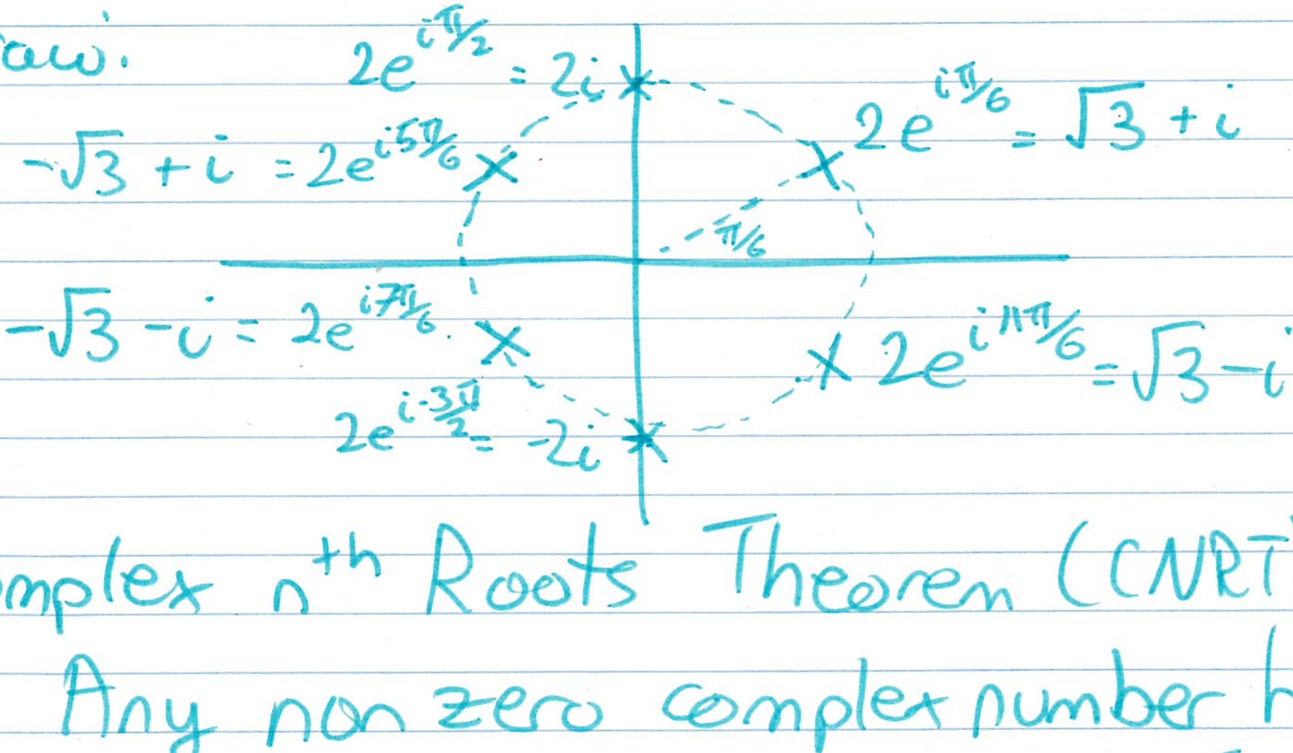
Hence $\theta = \frac{\pi}{6} + \frac{\pi}{3}k_1$ for $k_1 \in \{0,1,2,3,4,5\}$.

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

$\theta \in \left\{\frac{\pi}{6} + \frac{\pi}{3}k_1 : k_1 \in \{0,1,2,3,4,5\}\right\}.$

$\therefore z = re^{i\theta} \in \left\{2e^{i\left(\frac{\pi}{6}+\frac{\pi}{3}k\right)} : k \in \{0,1,2,3,4,5\}\right\}$

Draw:



Complex n^{th} Roots Theorem (CNRT)

Any non zero complex number has exactly $n \in \mathbb{N}$ distinct n^{th} roots. The roots lie on a circle (of radius $|z|$).

centred at the origin and spaced out evenly by angles of $\frac{2\pi}{n}$.

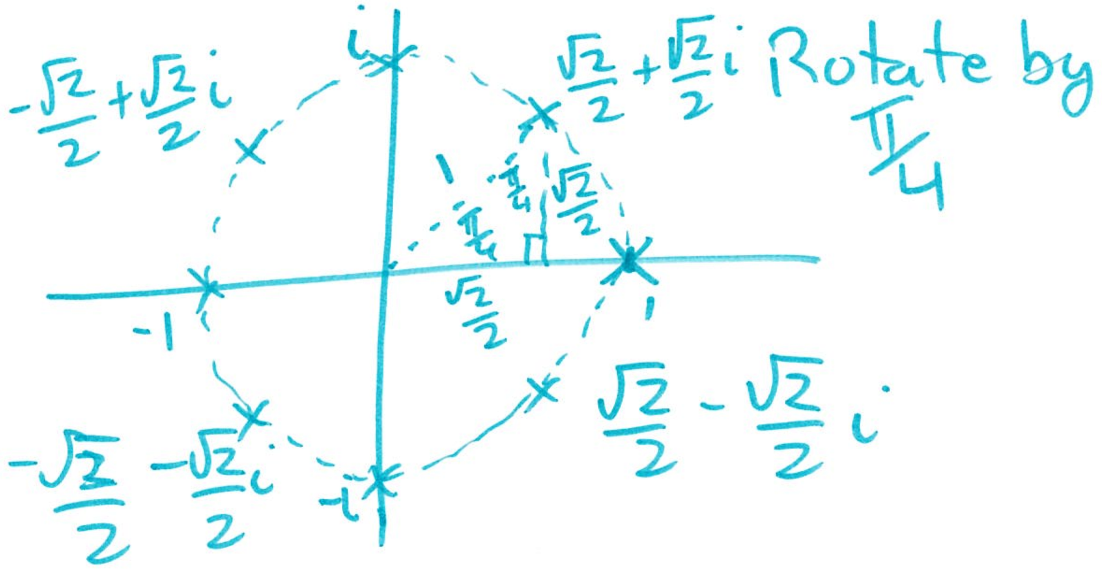
Def'n: An n^{th} root of unity is a complex number z s.t. $z^n = 1$.
(Sometimes denoted by ζ_n) (zeta).

Ex: -1 is a second root of unity (and fourth, and sixth, ...)

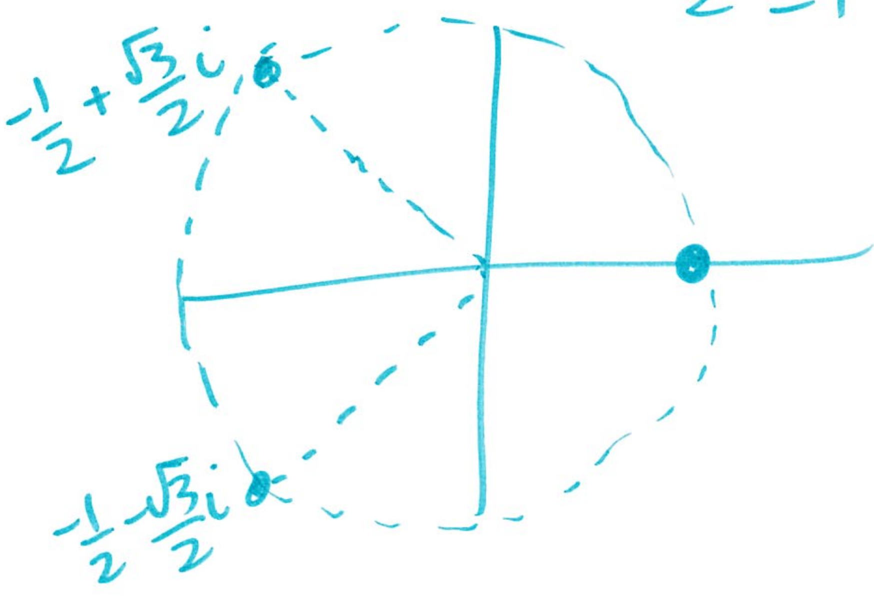
Find all eighth roots of unity in standard form. Draw.

Want to solve $z^8 = 1$

Know $z \in \{\pm 1, \pm i\}$ are solutions.



$z^3 = 1$



Solve

$$z^5 = -16\bar{z}$$

Sol'n: Tricky! Take moduli (by PM)

$$|z^5| = |z|^5 = |-16\bar{z}| = 16|\bar{z}| = 16|z|$$

$$|z|^5 = 16|z|$$

$$|z|^5 - 16|z| = 0$$

$$|z|(|z|^4 - 16) = 0$$

$|z| = 0$ <u>OR</u> $|z|^4 = 16$.

$\iff z = 0$ <u>OR</u> $|z| = 2$

Let's revisit $z^5 = -16\bar{z}$

Multiply by z: $z^6 = -16z\bar{z} = -16|z|^2 = -6$

$\therefore z \in \{0, \pm 2i, \pm\sqrt{3} \pm i\}$

7 solutions!

Restatement of CNRT

If $a = re^{i\theta}$, then solutions to $z^n = a$ are given by

$$z = \sqrt[n]{r}\, e^{i\left(\frac{\theta + 2\pi k}{n}\right)}$$

for $k \in \{0, 1, \dots n-1\}$

Solve $z^6 + 2z^3 - 3 = 0$

Sol'n: $(z^3 - 1)(z^3 + 3) = 0$

$\Rightarrow z^3 = 1$ OR $z^3 = -3$

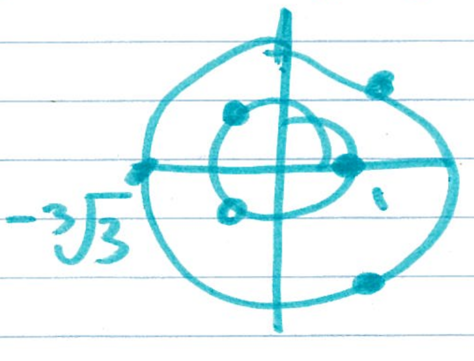
Note $1 = e^{i\cdot 0}$ & $-3 = 3e^{i\pi}$

By CNRT, sol'ns to $z^3 = 1$ are given by

$$z \in \{e^{i\cdot 0}, e^{i2\pi/3}, e^{i4\pi/3}\}.$$

and solutions to $z^3 = -3$ are given by

$$z \in \{\sqrt[3]{3}\, e^{i\pi/3}, \sqrt[3]{3}\, e^{i\pi}, \sqrt[3]{3}\, e^{i5\pi/3}\}$$



L40P2

Polynomials

For us fields include

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}_p$ for p a prime

Def'n: A polynomial in x over a field $\mathbb{F}$ is an expression of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_0, a_1, \ldots a_n \in \mathbb{F}$ and $n \geq 0$ is an integer. Denote the set/ring of all polynomials over $\mathbb{F}$ by $\mathbb{F}[x]$.

Ex:
- $(2\pi + i)z^3 - \sqrt{7}z + \frac{5i}{4} \in \mathbb{C}[z]$
- $[5]x^2 + [3]x + [1] \in \mathbb{Z}_7[x]$

  $5x^2 + 3x + 1 \in \mathbb{Z}_7[x]$
- $x^2 + \frac{1}{x}$ is <u>NOT</u> a polynomial.
- $x + \sqrt{x}$ is <u>NOT</u> a polynomial.

Definitions:

- The coefficient of x^n is a_n.
- The degree of a polynomial is n provided $a_n x^n$ is the largest non-zero term.
- A term of a polynomial is any $a_i x^i$.
- 0 is the zero polynomial
- A root of a polynomial $p(x) \in \mathbb{F}[x]$ is a value $a \in \mathbb{F}$ s.t. $p(a) = 0$.
- If the degree of a polynomial is
  - ↳ 1, the polynomial is linear
  - ↳ 2, the polynomial is quadratic
  - ↳ 3, the polynomial is cubic.

$\mathbb{C}[x]$	$\mathbb{R}[x]$	$\mathbb{Q}[x]$	$\mathbb{Z}[x]$
Complex polynomials	real	rational	integral

- Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$
  $g(x) = b_n x^n + \cdots + b_1 x + b_0$

be polynomials over $\mathbb{F}[x]$. Then $f(x) = g(x)$ iff $a_i = b_i$ for all $i \in \{0, 1, \ldots n\}$

- Operations:

  Addition, subtraction, multiplication

- x is an indeterminate (or a variable). It has no meaning on its own (but can be replaced with a value when this makes sense.

L40P5

Simplify $(x^5 + x^2 + 1)(x + 1) + (x^3 + x + 1)$ over $\mathbb{Z}_2[x]$

$= x^6 + x^5 + x^3 + x^2 + x + 1 + x^3 + x + 1$

$= x^6 + x^5 + 2x^3 + x^2 + 2x + 2$

$= x^6 + x^5 + x^2$

Prove $(ax+b)(x^2+x+1)$ over $\mathbb{R}$ is the zero polynomial iff $a=b=0$.

Pf: Expanding gives
$$(ax+b)(x^2+x+1)$$
$$= ax^3+(a+b)x^2+(a+b)x+b$$
This is 0 iff
$$a=0 \ \& \ (a+b)=0 \ \& \ b=0$$
which holds iff $a=0=b$. $\blacksquare$

(DAP) Division Algorithm for Polynomials
If $f(x), g(x) \in \mathbb{F}[x]$ & $g(x) \neq 0$ then $\exists!$ polynomials $q(x)$ & $r(x) \in \mathbb{F}[x]$ s.t.
$$f(x) = q(x)g(x) + r(x)$$
with $r(x)=0$ OR $\deg(r(x)) < \deg(g(x))$

Pf: Exercise.

L40P7

Notes:

- $q(x)$ is the quotient
- $r(x)$ is the remainder
- If $r(x)=0$ then $g(x)$ divides $f(x)$ and we write $g(x) \mid f(x)$. Otherwise, $g(x) \nmid f(x)$.

Ex: Show over $\mathbb{R}[x]$ that

$$(x-1) \nmid x^2+1$$

Pf: By DAP, $\exists$ $q(x), r(x) \in \mathbb{R}[x]$ s.t.

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

To show $r(x) \neq 0$ it suffices to show $r(a) \neq 0$ for some $a \in \mathbb{F}$. Take $x=1$.

Then $$(1)^2+1 = (1-1)q(1) + r(1)$$

$$2 = r(1)$$

$\therefore$ $r(x) \neq 0$ hence $(x-1) \nmid x^2+1$ ∎

Long Division

Let's Divide

$$f(z) = iz^3 + (i+3)z^2 + (5i+3)z + (2i-2)$$

by $g(z) = z + (i+1)$

$$\begin{array}{r l}
 & iz^2 + 4z + (i-1) \\
\hline
z+(i+1) \,\big) & iz^3 + (i+3)z^2 + (5i+3)z + (2i-2) \\
 & -\left(iz^3 + (i-1)z^2\right) \\
\hline
 & 4z^2 + (5i+3)z \\
 & -\left(4z^2 + (4i+4)z\right) \\
\hline
 & (i-1)z + (2i-2) \\
 & -\left((i-1)z \quad -2\right) \\
\hline
 & 2i
\end{array}$$

$\therefore\ q(z) = iz^2 + 4z + (i-1)$

$r(z) = 2i$

L41P1

Compute the quotient and the remainder when

$$x^4 + 2x^3 + 2x^2 + 2x + 1$$

is divided by $g(x) = 2x^2 + 3x + 4$ in $\mathbb{Z}_5[x]$.

$$3x^2 + 4x + 4 \quad \text{quotient.}$$

$$2x^2+3x+4 \,\overline{)\, x^4 + 2x^3 + 2x^2 + 2x + 1}$$

$$-(x^4 + 4x^3 + 2x^2)$$

$$3x^3 + 0x^2 + 2x$$

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

$$3x^2 + x + 1$$

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

$$4x$$

remainder

Proposition

Let $f(x), g(x) \in \mathbb{F}[x]$. If $f(x) \mid g(x)$ & $g(x) \mid f(x)$ then $f(x) = c \cdot g(x)$ for some $c \in \mathbb{F}$.

Pf: Note $f(x)=0$ iff $g(x)=0$. In this case, choose $c=1$. Now, assume neither are 0. By def'n $\exists$ $q(x), \hat{q}(x) \in \mathbb{F}[x]$ s.t.

(1) $f(x) = g(x) q(x)$

(2) $g(x) = f(x) \hat{q}(x)$

Substitute (2) into (1) giving:

$$f(x) = f(x) \hat{q}(x) q(x)$$

$$f(x)(1 - \hat{q}(x) q(x)) = 0$$

As $f(x) \neq 0$, we see that

$$1 = \hat{q}(x) q(x)$$

In fact, $\hat{q}(x)$ $q(x)$ are nonzero.

Now, $\deg(1) = 0$ & thus

$$0 = \deg(\hat{q}(x)q(x)) = \deg(\hat{q}(x)) + \deg(q(x))$$

(Exercise)

$\therefore \deg(q(x)) = 0 = \deg(\hat{q}(x))$

$\therefore q(x) = c \in \mathbb{F}$. Thus, by (1)

$$f(x) = c\,g(x).$$

Remainder Theorem (RT)

Suppose $f(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$. Then the remainder when $f(x)$ is divided by $x - c$ is $f(c)$.

Pf: By DAP, $\exists!\ q(x), r(x) \in \mathbb{F}[x]$ s.t

$$f(x) = (x-c)q(x) + r(x) \qquad (3)$$

with $r(x) = 0$ OR $\deg(r(x)) < \deg(x-c) = 1$

$\therefore \deg(r(x)) = 0$

Hence, in either case, $r(x) = K$ for some $K \in \mathbb{F}$. Plug $x=c$ into (3) to see that $f(c) = r(c) = K$

Hence $r(x) = f(c)$. ∎

Ex: Find the remainder when $f(z) = z^2+1$ is divided by

A) $z-1$ B) $z+1 = z-(-1)$ C) $z+i+1 = z-(-i-1)$

Sol'n: A) By RT, remainder is $f(1) = (1)^2+1 = 2$

B) By RT, remainder is $f(-1) = (-1)^2+1 = 2$

Note: $z^2+1 = (z-1)(z+1)+2$.

C) By RT, remainder is

$$f(-i-1) = (-i-1)^2+1 = -1+2i+1+1$$
$$= 2i+1.$$

LL1PS

In $\mathbb{Z}_7[x]$, what is the remainder when $4x^3 + 2x + 5$ is divided by $x + 6$?

Sol'n: $x+6 = x-1$. By RT, the remainder is

$$4(1)^3+2(1)+5 = 11$$
$$\equiv 4 \mod 7.$$

L41 P6

Factor Theorem (FT)

Suppose $f(x) \in \mathbb{F}[x]$ & $c \in \mathbb{F}$.
The polynomial $x-c$ is a factor of $f(x)$ iff $f(c)=0$ ie c is a root of $f(x)$

Pf: $x-c$ is a factor of $f(x)$

$\iff r(x)=0$

$\iff f(c)=0$ by RT. ∎

Prove that there does not exist a real linear factor of

$$f(x) = x^8 + x^3 + 1.$$

Pf: By FT, it suffices to show $f(x)$ has no real roots. We will show $f(x) > 0$ $\forall x \in \mathbb{R}$.

If $|x| \geq 1$, then $x^8 + x^3 \geq 0$

hence $f(x) > 0$

If $|x| < 1$, then $|x^3| < 1$

hence $x^3 + 1 > 0$

hence $f(x) > 0$.

L42P1

Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geqslant 1$ has at most n roots.

Let $P(n)$ be the statement that all polynomials over $\mathbb{F}$ of degree n have at most n roots.

Proof by induction on n

Base Case: If $n=1$ ie polynomials of the form $ax-b$ have at most a root over $\mathbb{F}$, with $a \neq 0$. Root is $x = b/a$.

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

I Step: Let $p(x) \in \mathbb{F}[x]$ of degree $k+1$. Either $p(x)$ has no root ✓ OR $p(x)$ has a root $c \in \mathbb{F}$. By FT, $x-c$ is a factor of $p(x)$. Write $p(x) = (x-c)\,q(x)$ for some $q(x) \in \mathbb{F}[x]$ of degree k. By IH, $q(x)$ has at most k roots. So $p(x)$ has at most $k+1$ roots

L42P7

$\therefore$ by POMI, $P(n)$ is true $\forall n \in \mathbb{N}$. $\square$

Ex: Factor $f(x) = x^4 - 2x^3 + 3x^2 - 4x + 2$ over $\mathbb{Z}_7$.

Pf: Note $f(1) = 0$ thus by FT $x-1$ is a factor. By long division,

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

Now, the sum of the coefficients of the cubic is still 0 hence $x-1$ is another root of $f(x)$! By long division

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

Factor theorem says if x^2+2 could be factored, it must have a root since the factors must be linear.

x	0	1	2	3	4	5	6
$x^2+2 \bmod 7$	2	3	6	4	4	6	3

The table shows x^2+2 has no root.

Def'n: The multiplicity of a root $c \in \mathbb{F}$ of $f(x) \in \mathbb{F}[x]$ is the largest $k \in \mathbb{Z}$ s.t. $(x-c)^k$ is a factor of $f(x)$.

Ex: The multiplicity of 1 in the last example was 2.

Note: $x^4+2x^2+1 = (x^2+1)^2$ over $\mathbb{R}[x]$ BUT does not split into linear factors over

Fundamental Theorem of Algebra

Every non-constant complex polynomial has a complex root.

Notes: Roots need not be distinct.

- x^2+1 over $\mathbb{R}$ shows this does not happen over all fields.

Pf: $\boxed{\text{Ξ}}$

Solve: $x^3-x^2+x-1=0$ over $\mathbb{C}$.

Note $x-1$ is a factor. Either do long division or note:

$$\begin{aligned} x^3-x^2+x-1 &= x^2(x-1)+(x-1) \\ &= (x-1)(x^2+1) \\ &= (x-1)(x-i)(x+i) \end{aligned}$$

Factor $iz^3 + (3-i)z^2 + (-3-2i)z - 6$ as a product of linear factors. Hint: There is an easy to find integer root!

Note $z=-1$ & $z=2$ are roots!

Hence $(z+1)(z-2)$ is a factor

$= z^2 - z - 2$

f(z)

$$
\begin{array}{r|l}
 & iz + 3 \\
z^2 - z - 2 & iz^3 + (3-i)z^2 + (-3-2i)z - 6 \\
 & \underline{iz^3 - iz^2 - 2iz} \\
 & 3z^2 - 3z - 6 \\
 & \underline{3z^2 - 3z - 6} \\
 & R\ 0
\end{array}
$$

$\therefore\ f(z) = (z+1)(z-2)(iz+3)$.

(CPN) Complex Polynomials of Degree n Have n Roots.

A complex polynomial $f(z)$ of degree $n \geq 1$ can be written as

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

for some $c \in \mathbb{C}$, for $c_1, c_2, \ldots c_n \in \mathbb{C}$. (not necessarily distinct) roots of $f(z)$

Ex: $2z^7 + z^5 + iz + 7$ can be written as

$$2(z-z_1)(z-z_2)\cdots(z-z_7)$$

for roots $z_1, z_2, \ldots, z_7 \in \mathbb{C}$.

Note: Factorization depends on the field!

Eg: $\mathbb{C}$: $(z-i)(z+i)(z-\sqrt{2})(z+\sqrt{2})(z-1)$

$\mathbb{R}$: $(z^2+1)(z-\sqrt{2})(z+\sqrt{2})(z-1)$

$\mathbb{Q}$: $(z^2+1)(z^2-2)(z-1)$

Pf of CPN: We prove the given statement by induction

Base case: $n=1$ take $az+b \in \mathbb{C}[z]$ rewrite as $a(z-(\frac{-b}{a}))$

IH: Assume all polynomials over $\mathbb{C}$ of degree k can be written in the given form. (for some $k \in \mathbb{N}$).

IStep: Take $f(z) \in \mathbb{C}[z]$ of degree $k+1$. By FTA & FT, $z-c_{k+1}$ is a factor of $f(z)$ for some $c_{k+1} \in \mathbb{C}$. Write

$$f(z) = (z-c_{k+1})\, g(z)$$

where degree $g(z)$ is k. By IH, write $g(z) = c(z-c_1)(z-c_2)\cdots(z-c_k)$ for $c, c_1, c_2, \dots c_k \in \mathbb{C}$. Combine toget

$$f(z) = c\prod_{i=1}^{k+1}(z-c_i).$$

L42P9

$\therefore$ by POMI, the given statement is true $\forall n \in \mathbb{N}$.

L43P1

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. How many of the following statements are true?

- TRUE FTA Every complex cubic polynomial has a complex root.
- FALSE When $x^3 + 6x - 7$ is divided by $ax^2 + bx + c$ in $\mathbb{R}[x]$, then the remainder has degree 1.
- TRUE If $f(x), g(x) \in \mathbb{Q}[x]$, then $f(x)g(x) \in \mathbb{Q}[x]$.
- FALSE Every polynomial in $\mathbb{Z}_5[x]$ has a root in $\mathbb{Z}_5$.

A) 0 $f(x) = 1$

B) 1

$\boxed{\text{C) } 2}$ $f(x) = x(x-1)(x-2)(x-3)(x-4)+1$

D) 3

E) 4

Rational Roots Theorem (RRT)

If $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ & $r = s/t \in \mathbb{Q}$ is a root of $f(x)$ over $\mathbb{Q}$ in lowest terms, then $s \mid a_0$ & $t \mid a_n$

Pf: Plug in $r = \frac{s}{t}$ into $f(x)$:

$$0 = a_n\left(\frac{s}{t}\right)^n + a_{n-1}\left(\frac{s}{t}\right)^{n-1} + \dots + a_1\left(\frac{s}{t}\right) + a_0$$

Multiply by t^n:

$$0 = a_n s^n + a_{n-1} s^{n-1} t + \dots + a_1 s t^{n-1} + a_0 t^n$$

$$a_0 t^n = -(a_n s^n + a_{n-1} s^{n-1} t + \dots + a_1 s t^{n-1})$$

$$= -s(a_n s^{n-1} + a_{n-1} s^{n-2} t + \dots + a_1 t^{n-1})$$

$\therefore$ $s \mid a_0 t^n$. Since $\gcd(s,t) = 1$, $\gcd(s, t^n) = 1$ hence $s \mid a_0$ by CAD.

Similarly $t \mid a_n$ $\blacksquare$.

Ex: Find the roots of
$$2x^3+x^2-6x-3 \in \mathbb{R}[x]$$

Sol'n: By RRT if r is a root then writing $r=\frac{s}{t}$, we have that $s \mid -3$ & $t \mid 2$

Thus, $r \in \{\pm 1, \pm 3, \pm\frac{3}{2}, \pm\frac{1}{2}\}$

Now, trying these one by one shows that $r=-\frac{1}{2}$ is a root since
$$2(-\tfrac{1}{2})^3+(-\tfrac{1}{2})^2-6(-\tfrac{1}{2})-3$$
$$=-\frac{1}{4}+\frac{1}{4}+3-3$$
$$=0.$$

$\therefore$ $(x+\frac{1}{2})$ or $(2x+1)$ is a factor!

By long division:
$$2x^3+x^2-6x-3=(2x+1)(x^2-3)$$
$$=(2x+1)(x-\sqrt{3})(x+\sqrt{3})$$

$\therefore$ All real roots are $-\frac{1}{2}$, $\pm\sqrt{3}$.

Fully factor $x^3 - \frac{32}{15}x^2 + \frac{1}{5}x + \frac{2}{15} \in \mathbb{Q}[x]$

$$= \frac{1}{15}(15x^3 - 32x^2 + 3x + 2) = f(x)$$

By RRT, Possible roots are

$$\pm 1, \pm \frac{1}{3}, \pm \frac{1}{5}, \pm \frac{1}{15}, \pm 2, \pm \frac{2}{3}, \pm \frac{2}{5}, \pm \frac{2}{15}.$$

Note: $x = 2$ is a root. By FT, $x-2$ is a factor.

$$
\begin{array}{r l}
 & 15x^2 - 2x - 1 \\
x-2 \,\big) & 15x^3 - 32x^2 + 3x + 2 \\
 & 15x^3 - 30x^2 \\
\hline
 & -2x^2 + 3x \\
 & -2x^2 + 4x \\
\hline
 & -x + 2
\end{array}
$$

$$\therefore f(x) = \frac{1}{15}(x-2)(15x^2 - 2x - 1)$$

$$= \frac{1}{15}(x-2)(5x+1)(3x-1).$$

Prove $\sqrt{7}$ is irrational.

Assume towards a contradiction that

$$\sqrt{7} = x \in \mathbb{Q}$$

Square both sides:

$$7 = x^2$$

$$0 = x^2 - 7$$

As a polynomial, $x^2 - 7$ has a rational root. By RRT, the only possible rational roots are given by $\pm 1, \pm 7$. None of these are roots. (Check!.) $\blacksquare$.

$(\pm 1)^2 - 7 = -6 \neq 0$ $\quad (\pm 7)^2 - 7 = 42 \neq 0.$

Prove that $\sqrt{5} + \sqrt{3}$ is irrational.

BWOC (By way of contradiction) suppose

$$\sqrt{5} + \sqrt{3} = x \in \mathbb{Q}$$

Squaring

$$5 + 2\sqrt{15} + 3 = x^2$$

$$2\sqrt{15} = x^2 - 8$$

Square again

$$60 = x^4 - 16x^2 + 64$$

$$0 = x^4 - 16x^2 + 4 = f(x)$$

RRT $\Rightarrow$ only possible roots are:

$$\pm 4, \pm 1, \pm 2$$

Checking shows none work. $\blacksquare$.

(Eg: $f(\pm 1) = -11 \neq 0$).

L43P7.

Conjugate Roots Theorem (CJRT)

If $c \in \mathbb{C}$ is a root of a polynomial $p(x) \in \mathbb{R}[x]$ (over $\mathbb{C}$) then $\bar{c}$ is a root of $p(x)$

Pf: Write $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ & $p(c) = 0$. Then

$$
\begin{aligned}
p(\bar{c}) &= a_n(\bar{c})^n + \cdots + a_1\bar{c} + a_0 \\
&= \overline{a_n c^n} + \cdots + \overline{a_1 c} + \overline{a_0} \\
&= \overline{a_n c^n + \cdots + a_1 c + a_0} \\
&= \overline{p(c)} \\
&= 0.
\end{aligned}
$$

PM

▲

Recall:

Conjugate Roots Theorem

If $c \in \mathbb{C}$ is a root of a real polynomial, then $\bar{c} \in \mathbb{C}$ is also a root.

Not true if coefficients are not real

Ex: $(x+i)^2 = x^2 + 2ix - 1$

Ex: Fully factor

$$f(z) = z^5 - z^4 - z^3 + z^2 - 2z + 2$$

over $\mathbb{C}$ given that i is a root.

Pf: Note by CJRT $\pm i$ are roots. By FT $(z-i)(z+i) = z^2+1$ is a factor. Note $z-1$ is also a factor hence $(z^2+1)(z-1) = z^3 - z^2 + z - 1$ is a factor.

$$\begin{array}{r|l} & z^2 - 2 \\ \hline z^3 - z^2 + z - 1 & z^5 - z^4 - z^3 + z^2 - 2z + 2 \\ & -(z^5 - z^4 + z^3 - z^2) \\ \hline & -2z^3 + 2z^2 - 2z + 2 \\ \hline & 0 \end{array}$$

L44 P2

$$\therefore f(z) = (z^3 - z^2 + z - 1)(z^2 - 2)$$
$$= (z - i)(z + i)(z - 1)(z - \sqrt{2})(z + \sqrt{2})$$

$\boxtimes$

Fully factor $f(z) = z^4 - 5z^3 + 16z^2 - 9z - 13$ over $\mathbb{C}$ given that $2 - 3i$ is a root.

Factors are (by FT & CJRT)

$$(z-(2-3i))(z-(2+3i))$$
$$= z^2 - 4z + 13$$

After long division

$$f(z) = (z^2 - 4z + 13)(z^2 - z - 1)$$

By the quadratic formula or $z^2 - z - 1$

$$z = \frac{-(-1) \pm \sqrt{(-1)^2 - 4(1)(-1)}}{2(1)}$$
$$= \frac{1 \pm \sqrt{5}}{2}$$

Hence $f(z) = (z-(2-3i))(z-(2+3i))$
$$\cdot \left(z - \left(\frac{1+\sqrt{5}}{2}\right)\right)\left(z - \left(\frac{1-\sqrt{5}}{2}\right)\right)$$

Real Quadratic Factors (RQF).

Let $f(x) \in \mathbb{R}[x]$. If $c \in \mathbb{C} \setminus \mathbb{R}$ & $f(c)=0$ then $\exists\, g(x) \in \mathbb{R}[x]$ s.t. $g(x)$ is a real quadratic factor of $f(x)$.

Pf: Take $g(x) = (x-c)(x-\bar{c})$

$$= x^2 - (c+\bar{c})x + c\bar{c}$$

$$= x^2 - 2\mathrm{Re}(c)\,x + |c|^2 \in \mathbb{R}[x]$$

It suffices to show that $g(x)$ is a factor of $f(x)$. By DAP, $\exists!\, q(x), r(x) \in \mathbb{R}[x]$ s.t. $f(x) = g(x)q(x) + r(x)$ (1).

with $r(x)=0$ or $\deg(r(x)) < \deg(g(x)) = 2$

Assume towards a contradiction that $r(x) \neq 0$ ie $\deg(r(x)) = 0$ or 1. Plug $x=c$ into (1)

$$0 = f(c) = g(c)q(c) + r(c) = r(c).$$

$$\therefore r(c) = 0.$$

Now, $r(x)$ is linear or constant real polynomial

If $r(x)$ was constant, $r(x)=0$ #
If $r(x)$ is linear, say $r(x)=ax+b$, then
$$r(c)=ac+b=0 \Rightarrow c=\frac{-b}{a}\in\mathbb{R} \ \#.$$
$\therefore$ $r(x)=0$ & $g(x) \mid f(x)$ ■.

Real Factors of Real Polynomials (RFPF).
Let $f(x)=a_n x^n+\cdots+a_1 x+a_0 \in \mathbb{R}[x]$.
Then $f(x)$ can be written as a product of real linear & real quadratic factors.
Pf: By CPN, $f(x)$ has n roots over $\mathbb{C}$.
Let $r_1, r_2, \ldots r_k$ be the real roots and let $c_1, c_2, \ldots c_\ell$ be the complex roots. By CJRT complex roots come in pairs say $c_2=\overline{c_1}$, $c_4=\overline{c_3}$, $\ldots$ $c_\ell=\overline{c_{\ell-1}}$. For each pair, by RQF, we have an associated quadratic factor, say $q_1(x), q_2(x), \ldots, q_{\ell/2}(x)$.

L44P6

By FT, each real root corresponds to a linear factor, say $g_1(x), g_2(x), \dots, g_k(x)$

Then $f(x) = c\, g_1(x) g_2(x) \cdots g_k(x) q_1(x) \cdots q_{\frac{\ell}{2}}(x)$

$\boxed{\text{}}$

L44P7

Prove that a real polynomial of odd degree has a real root.