MATH 135 - F21
Abstract Algebra
Full Course Notes

With Prof Ali Assem Abdelkader Mahmoud

Ali is the GOAT. He is an exceptional professor. He bought his class pizza, by golly.
Future Josiah here: He also gave me a job ❤️

Josiah Plett

MATH 135 FALL 2021 #1

① Warm-up Lecture

sentence with definite state of being either true or false.

① **Statements**: sequence of ideas that give meaning; are true or false

② **Sets**: a group of elements "axiom of set theory" $\emptyset$ – no elements $\{\emptyset\}$ – one element

③ **Proof**: something that gives evidence of truth to everyone. ⓐ proof ⓑ restatement ⓒ QED

any math 135 student

eg: for any positive integer n, n^2+1 is not a perfect square.

proof:

let n be a positive integer. Now, notice that:
$n^2 < n^2+1 < n^2+2n+1 = (n+1)^2$
where the last inequality is true since n is positive. Finally, notice that there cannot be perfect squares between n and $(n+1)^2$. This completes the proof. = ■ = QED

eg: for any positive integer n, n^2+13 is not a perfect square; Prove or disprove

proof:

It is false. $n=6$ is a counter-example.

④ **Quantifiers**:

$\forall$ = all, any, every.

$\exists$ = exists at least 1.

$\boxed{\forall x \in S \; P(x)}$

quantifier, domain, statement dependin on x

OPEN SENTENCE: contains a variable where the truth of the sentence is determined by the value of the variable chosen, within the variable's domain.

eg: Are the following statements quantified?

① 64 is a perfect square. YES

because: there exists an integer n such that $64 = n^2$, and this integer happens to be 8.

eg: NESTED QUANTIFIERS

– $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \; x^3 - y^3 = 1$ FALSE

– $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, \; x^3 - y^3 = 1$ ($x=1$, $y=0$) TRUE

– $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \; x^3 - y^3 = 1$ ($y = \sqrt[3]{x^3-1}$) TRUE

– $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \; x^3 - y^3 = 1$ ($x^3 - x^3 \neq 1$) FALSE

proof:

Assume x is such a real number; pick y to be x. Thus, $x^3 - x^3$ must equal 1, yet it does not. QED.

② Lecture 2

Method of Negation: $\boxed{\text{1 step at a time.}}$

$\exists \leftrightarrow \forall$

$\geq \leftrightarrow <$

or $\leftrightarrow$ and

Truth Table

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

Used to prove that two statements are logically equivalent

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

DeMorgan's law

$\wedge$ = conjunction (and)

$\vee$ = disjunction (or)

$\Rightarrow$ = implies (if _ then)

LAWS

$A \equiv \neg\neg A$ } double negation

$A \wedge B \equiv B \wedge A$, $A \vee B \equiv B \vee A$ } commutative law

$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$ } Associative law (works with or)

$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$, $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ } Distributive law

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

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

Contrapositive (logically equivalent)

You can express Everything using only $\neg$ and $\wedge$ (or $\neg$ and $\vee$)

③ Lecture 3

$\underset{\text{Hypothesis}}{A} \Rightarrow \underset{\text{conclusion}}{B}$ **Converse**: $B \Rightarrow A$ (of $A \Rightarrow B$)

If and only if: $\boxed{A \Leftrightarrow B} \equiv (A \Rightarrow B \wedge B \text{ only if } A)$

A is sufficient, A is Necessary

Read On Own

something short. no worries!

Proving Mathematical Statements

$a \mid b$: a divides b: $\exists m \in \mathbb{Z}\ [b = ma]$, $a \neq \emptyset$

(4) Lecture 4

recap:
- universally quantified: prove for all
- disproving universals: 1 counterexample
- proof by cases! ← disproving?

Proving Existentially Quantified Statements: Find 1 example. $\exists$

Proving Implicative Statements: Natural steps of a proof

Perturbation: add then subtract the same thing

fun fact: $\frac{0}{0}$ = undefined

(5) Divisibility of Integers

Definition of Divisibility: $m \in \mathbb{Z}$ divides $n \in \mathbb{Z}$ if $\exists k \in \mathbb{Z}$ such that $n = km$.

$\left.\frac{d|x|}{dy}\right|_{0,0}$ = undefined

PROPOSITIONS $\quad m \mid n \Rightarrow \exists k \in \mathbb{Z},\ n = km$

Check a proof/disproof: Not violate the negation

1. (Transitivity of divisibility) $\forall a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.
2. (proposition two) $\forall a, b, c \in \mathbb{Z}$, if $a \mid b$ or $a \mid c$, then $a \mid bc$.
3. (Divisibility of integer combinations OR DIC) $\forall a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $\forall x, y \in \mathbb{Z}$, $a \mid (xb + yc)$.

(6) Proving implications

BIG LONG CONFUSION TO FINALLY FIND

TO PROVE AN IMPLICATION ⇨ ASSUME THE HYPOTHESIS

(7) Proving by contrapositive

if $A \Rightarrow B$ is hard to prove, try proving $\neg B \Rightarrow \neg A$ (contrapositive)!

Proving by Contradiction

if A is hard, prove $\neg A$.

(8) (3.6) Proof by Contradiction

You can be creative and create new things.

if $1 \in \emptyset$, then $1 = 2$

(9) Method of Elimination

$A \Rightarrow B \vee C$

prove

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

Proving Uniqueness..

Group $(G, \otimes, e)$ such that for all $a, b, c \in G$,

(G: set, $\otimes$: operation, e: identity element)

1. $a \otimes b \in G$
2. $a \otimes (b \otimes c) = (a \otimes b) \otimes c$
3. $a \otimes e = a$
4. $\exists a' \in G,\ a \otimes a' = e$

Proving a' is unique

$a' = a' \otimes e = a' \otimes (a \otimes a'')$
$= (a' \otimes a) \otimes a'' = e \otimes a'' = a''$

(10) Summation...

$\sum_{j=0}^{10} i = 1 + 2 + \ldots + 10 = 55$

$S = \frac{n(n+1)}{2}$ ← simple summation

sum of squares: $\frac{n(n+1)(2n+1)}{6}$

$\sum_{i=m}^{n} cx_i + \sum_{j=m}^{n} y_j \Rightarrow \sum_{k=m}^{n} (cx_k + y_k)$

$\Downarrow$

$c\sum_{i=m}^{n} x_i$

(10.1) Products...

$\prod_{i=1}^{n} x_i = x_1 \cdot x_2 \cdot \ldots \cdot x_n$

(10.2) Proof by Mathematical Induction (POMI)

1. Prove that a base value is true. $\exists k \in \mathbb{N},\ P(k)$
2. Prove that $P(k) \Rightarrow P(k+1)$
3. Therefore, $P(n)$ is true for all $n \in \mathbb{N}$ → $\mathbb{Q}$ or $\mathbb{Z}$, NOT $\mathbb{R}$!!!

MATH 135 FALL 2021 $\boxed{\#2}$

(11) Lecture 11

Lemma: Something you need before going into your proof.

Corralary: Consequence of a proof.

☆ **Principle of Strong Induction (POSI)**

1. **Base Case:** Prove that $P(i)$ is true.
2. **Induction Step:** Assume $P(i)$ is true for all $1 \le i \le k$, and use this to prove $P(k+1)$.

(12) Binomial Theorem

For any non-negative integer n and $x \in \mathbb{R}$,

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^{n-m} b^m$$

$\binom{n}{m}$:
- n choose m
- binomial coefficient
- C^n_m (combinations)

$$\binom{n}{m} = \frac{n!}{m! \cdot (n-m)!}$$

$\binom{0}{0} = 1$

0!

"Such that" → $:$, or $|$

Fact: $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$

Sets

- Set-builder notation: $\{x \in \overset{\text{Universal Set}}{U} \mid \overset{\text{Condition}}{P(x)}\}$
- Union: $S \cup T = \{x \mid x \in S \vee x \in T\}$
- Intersection: $S \cap T = \{x : x \in S \wedge x \in T\}$
- Difference: $S - T = S \setminus T = \{x : x \in S \wedge x \notin T\}$

(13) BIG BRAIN Summations

A summation can be *logically* (not mathematically) broken up how you like (even/odd, perhaps), and after more algebra, re-index to finish mathematically.

(14) TEXTBOOK (5.1) Set intro...

$\emptyset = \{\}$

- Cardinality: # of elements in S... $= |S|$

(5.2) Set builder Notation. See section (12)

eg $\{3a : 2|a, a \in \mathbb{Z}\}$

(5.3) see operations above $\boxed{\text{PLUS}}$:

- Complement: $\overline{S} = \{x \in U : x \notin S\}$

(5.4)

- Disjoint: $S \cap T = \emptyset$ (are disjoint) don't share any elements.

(5.5) Subsets

$S \subseteq T \equiv \forall x \in U, (x \in S) \Rightarrow (x \in T)$

- Subset: S subset of T: $S \subseteq T$
- Proper Subset: $S \subsetneq T$ → when $\exists x \in T \ (x \notin S)$
- Superset: T superset of S: $S \subseteq T$
- Proper Superset: same same

- Equality: $S \subseteq T \wedge T \subseteq S \Rightarrow S = T$

- # of Subsets: $n = |S|$ ... S has 2^n subsets

(15) GCD - Greatest Common Divisor.

BBD: Bounds By Divisibility

$\forall a, b \in \mathbb{Z}, (b|a \wedge a \neq 0) \Rightarrow b \le |a|$

Proof:
1. Use definition of divisibility
2. Use inequality, cause $k \ge 1$

Theorem: Division Algorithm

$\forall a \in \mathbb{Z} \ \forall b \in \mathbb{N}, \exists \underset{\text{quotient}}{q} \text{ and } \exists \underset{\text{remainder}}{r} \in \mathbb{Z} \ [a = qb + r \wedge 0 \le r < b]$

Another Theorem: Remainder Theorem

$\forall a, b, q, r \in \mathbb{Z}, a = qb + r \Rightarrow \gcd(a,b) = \gcd(b,r)$ ($a > b$)

(16) Greatest Common Divisor

GCD With Remainders: $\forall a, b, q, r, \ a = qb + r \Rightarrow \gcd(a,b) = \gcd(b,r)$

Finding GCD: Euclidean Algorithm

GCD Characterization Theorem (alternative way to define gcd) ← GCDCT

$\gcd(a,b)$ → for $a, b \in \mathbb{Z}$ and $d \in \mathbb{Z}$ with $d \ge 0$:
1. if $d|a$ and $d|b$, and
2. if $\exists s, t \in \mathbb{Z}$, $d = sa + bt$, then $d = \gcd(a,b)$

Converse is also true here. Called Bézout's Lemma.

BL: $\exists s, t \in \mathbb{Z} \ [as + bt = \gcd(a,b)]$

GCD
1. $d|a$ and $d|b$
2. $\forall c \in \mathbb{Z} \ [c|a \wedge c|b \Rightarrow c \le d]$

GCD → $\gcd(a,b) = d$

$\gcd(0, 5) = 5$

(17) Extended Euclidian Algorithm

assume $a \geq b > 0$ without loss of generality.

x	y	r	q
1	0	a	0
0	1	b	0
x	y	d	
s	t	0	
↑	↑	↑	↑
x_i	y_i	r_i	q_i

$ax+by=d$

$as+bt=0$

1. $q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$
2. $Row_i = Row_{i-2} - q_i Row_{i-1}$

Stop when $r_i = 0$.

Output: $\gcd(a,b) = r_{i-1}$, $s = x_{i-1}$, $t = y_{i-1}$

S and t are called the Certificate of Correctness

Coprime: $\gcd(a,b) = 1$

(18) More GCD Theorems:

CDDGCD: Common Divisor Divides GCD

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

CCT: Coprimeness Characterization Theorem

$\forall a,b \in \mathbb{Z}, [\gcd(a,b)=1 \Leftrightarrow \exists s,t \in \mathbb{Z}, \ as+bt=1]$

DBGCD: Division by the GCD

$\forall a,b \in \mathbb{Z}, \neg(a=b=0) \Rightarrow \left(d=\gcd(a,b) \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1\right)$

CAD: Coprimenes and Divisibility [IMPORTANT]

$\forall a,b,c \in \mathbb{Z}, \ c|ab \wedge \gcd(a,c)=1 \Rightarrow c|b$

(19) Primes

Prime Factorisation (PF):

$\forall n \in \mathbb{N}, \ n>1 \Rightarrow n$ is a product of primes

Unique Factorisation Theorem (UFT): [IMPORTANT]

PF, except the solution is unique up to order.

Euclid's Lemma (EL):

$p \in P: \ p|ab \Rightarrow p|a$ or $p|b$

(generalized Euclid's Lemma; $p|q_1q_2\cdots q_k \Rightarrow p|q_1$ or $p|$other)

(20) More Primes

Euclid's Theorem (ET):

The number of Primes is Infinite.

Finding a Prime Factor (FPF):

Every natural n, $n>1$, is either prime or has a prime factor less than or equal to $\sqrt{n}$.

DFPF: Divisors from prime factorization → Use: find divisors: $p_1^{\beta} \ldots p_k^{\beta}$ → all β! $\quad 0 \leq \beta \leq \alpha_i$ $\quad \alpha > 0$

Integer c is a positive divisor of n if and only if c can be written as $p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ when $p = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

UNKOWN Lemma → if $p, q \in P$, and $p|q$, then $p = q$

positive divisors: $(\beta_1 + 1) \ldots (\beta_k + 1)$

(21) More Primeness Theorems

Let a, b be expressed as

GCD PF: GCD from prime Factorization: $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \ldots p_k^{\beta_k}$. Then, $\gcd(a,b) = p_1^{\min\{\alpha_1, \beta_1\}} \ldots p_k^{\min\{\alpha_k, \beta_k\}}$

(22) Diophantine Equations in Two Variables:

$ax + by = c; \quad a,b,c,x,y \in \mathbb{Z}$

LDET1 Linear Diophantine Equation Theorem 1: $\forall a,b,c \in \mathbb{Z}$, $ax+by=c$ has solutions $\Leftrightarrow \gcd(a,b) \mid c$

LDET2 " 2: (x_0, y_0) is solution to $ax+by=c$. ($d = \gcd(a,b)$) Then all solutions is $\{(x,y) \mid x = x_0 + \frac{b}{d}n, \ y = y_0 - \frac{a}{d}n, \ n \in \mathbb{Z}\}$!

Finding a Particular solution: EEA to get $as+bt=d$, so $\frac{c}{d}s = x$, $\frac{c}{d}t = y$, iff $d|c$.

(23) Congruence and Modular Arithmetic

$A \equiv B$ if $m \mid a-b$

modulo: produces remainder

modulus: is remainder

1. $a \equiv a$ $\{\forall m \in \mathbb{N}\}$
2. $a_1 \equiv a_2 \wedge b_1 \equiv b_2 \Rightarrow a_1 + b_1 \equiv a_2 + b_2$
3. $a \equiv b \Leftrightarrow b \equiv a$

eg • $42 \not\equiv -11 \pmod 3$

• $13 \not\equiv -13 \pmod 4$

(Congruence is an) Equivalence Relation;

Let S be a set, and Δ be an equivalence relation. Then:

1. $\forall a \in S, \ a \Delta a$ (Reflexivity)
2. $\forall a,b \in S, \ a \Delta b \Leftrightarrow b \Delta a$ (Symmetry)
3. $\forall a,b,c \in S, \ a \Delta b \wedge b \Delta c \Rightarrow a \Delta c$ (transitivity)

If $a_1 \equiv a_2 \pmod m$ & $b_1 \equiv b_2 \pmod m$

then $a_1 + b_1 \equiv a_2 + b_2 \pmod m$

AND $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod m$

MATH 135

FALL 2021 #3

24 More Congruence

Use congruence EXACTLY as you do equality! Since $7^2 \equiv -1 \pmod{10}$, we can sub in -1 for 7^2!

CISR → Congruence iff Same Remainder

$\forall a,b \in \mathbb{Z}, \forall m \in \mathbb{N}$, $a \equiv b \pmod m \iff$ a and b have the same remainder when divided by m.

Linear Congruence $\leftarrow ax \equiv c \pmod m$

"linear congruence in the variable x"

LCT → Linear Congruence Theorem

$ax \equiv c \pmod m$ has solutions iff $\gcd(a,m) \mid c$ $(a \neq 0)$

$\hookrightarrow m \mid ax-c$

$\hookrightarrow ax-c = mk$

$\hookrightarrow ax - mk = c$

PLUS

if x_0 is a solution to the congruence, then all solutions is $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{d}}\}$

$d = \gcd(a, m)$

To find a particular solution to $ax \equiv c \pmod m$, we consider $ax + my = c$

$\{x \in \mathbb{Z} : x \equiv x_0,\ x \equiv x_0 + \frac{m}{d},\ \ldots,\ x \equiv x_0 + \frac{(d-1)m}{d} \pmod m\}$

25 More Congruence

CD → Congruence Divide

If $a,b,c \in \mathbb{Z}$, $ac \equiv bc \pmod m$, $\gcd(c,m) = 1$, then $a \equiv b$.

CP → Congruence Power

$a,b \in \mathbb{Z}$, $a \equiv b \implies a^n \equiv b^n$

26 More congruence

Exhaustive search!

example: $4x \equiv 6 \pmod 5$: $\to 1$

x	0	1	2	3	4
4x	0	4	3	2	1

we would list all congruencies here!

$\to \{x \in \mathbb{Z},\ x \equiv 4 \pmod 5\}$

Congruence Classes

- The Congruence Class of $a \in \mathbb{Z}$ modulo m is the set $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod m\}$, and we have

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

In $\mathbb{Z}_m$: algebra to ELIMINATE Y

Multiplication: $[a][b] = [ab]$

Addition: $[a]+[b] = [a+b]$

Multiplicative Inverse: $[a]^{-1}[a] = [1]$

INV $\mathbb{Z}_m$ Inverses in $\mathbb{Z}_m$

$\forall m \in \mathbb{Z}$ and $1 \le a \le m-1$, a multiplicative inverse for $[a]$ exists iff $\gcd(a,m) = 1$. (if $m \in \mathbb{P}$, then $\forall a$, $a \neq 0$, $[a]^{-1}$ exists)

27 Fermat's Little Theorem, & Chinese Remainder Theorem

FLT $\forall p \in \mathbb{P}, \forall a \in \mathbb{Z}$, $p \nmid a \implies a^{p-1} \equiv 1 \pmod p$

Actual Fact: $\forall c \in \mathbb{Z}$...

$\gcd(a,b) = 1 \implies (a \mid c \land b \mid c \implies ab \mid c)$

If $p \nmid a$, $[a]^{-1}$ in $\mathbb{Z}_p$ is $[a^{p-2}]$

also

$a^p \equiv a$

★★★★★★★

FLT corollary

CRT $\forall a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$,

$\gcd(m_1, m_2) = 1 \implies x \equiv a_1 \pmod{m_1} \land x \equiv a_2 \pmod{m_2}$ has a solution x_0.

Besides, x_0 is unique $\pmod{m_1 m_2}$

SMT Splitting the Modulus

$\forall a \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$ and m_1 and m_2 coprime, then

$x \equiv a \pmod{m_1}$, $x \equiv a \pmod{m_2} \iff x \equiv a \pmod{m_1 m_2}$

28 More Modulo

CRT

$m_1 k + m_2 l = 1$

$x_0 = a_2 m_1 k + a_1 m_2 l$

$\begin{cases} x_0 \equiv a_1 \pmod{m_1} \\ x_0 \equiv a_2 \pmod{m_2} \end{cases}$

↳ CRT says x_0 is unique $\pmod{m_1 m_2}$

GCRT — Generalized CRT

for $a_1, \ldots a_n \in \mathbb{Z}$ and $m_1, \ldots m_n \in \mathbb{N}$:

$\gcd(m_i, m_j) = 1$ all $i \neq j$ $\implies \exists$ a solution to $x \equiv a_1 \pmod{m_1} \ \ldots\ x \equiv a_n \pmod{m_n}$ and the solution is unique.

(29) The RSA Cryptosystem

Public-key encryption
Private-key decryption

1970's!

$n=pq$

(a) Setting up RSA
(b) RSA Encryption
(c) RSA Decryption

[A] RSA Setup

① choose p,q, very large primes; let $n=pq$
② select e so $\gcd(e,(p-1)(q-1))=1$ and $1<e<(p-1)(q-1)$
③ solve $ed\equiv 1 \pmod{(p-1)(q-1)}$ for d with $1<d<(p-1)(q-1)$
④ Publish (e,n) — public key
⑤ Keep secret (d,n) p,q — private key. (keep p,q private)

important

(RSA) RSA Works
⑥ $R\equiv C^d \pmod n$
⑦ Then $R=M$.

[B] RSA Encryption

① obtain public (e,n)
② Plaintext message $=M$, $1\le M<n$
③ Ciphertext $C\equiv M^e \pmod n$ where $0\le C<n$
④ Send C!

[C] RSA Decryption

① Use the private key (d,n) to get $R\equiv C^d \pmod n$ with $1\le R<n$
② R is the original M!

(30) Complex numbers $\mathbb{C}$

$(x^2=-1!)$

$i^2=-1$

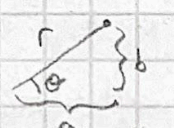
$w=z \iff \mathrm{Re}(z)=\mathrm{Re}(w)\ \wedge\ \mathrm{Im}(z)=\mathrm{Re}(z)$

- Standard form $z=\underline{a}+i\underline{b}$, $a,b\in\mathbb{R}$

$\mathrm{Re}(z)=a \quad \mathrm{Im}(z)=b$

- Multiplicative inverse: $\dfrac{a-bi}{a^2+b^2}=z^{-1}$
- Conjugate: $\overline{z}=a-bi$
- Modulus: $|z|=a^2+b^2$

Polar Form



$z=a+ib$,

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

$r=|z|$

$\cos\theta=\dfrac{a}{r}$ $\quad \sin\theta=\dfrac{b}{r}$

getting into polar form:

$z=a+ib=|z|(\cos\theta+i\sin\theta)$ and find θ!

$r\to$ radius
$\theta\to$ arguement

(31) More Complex Modulus

① $|z|=0 \iff z=0$
② $|\overline{z}|=|z|$
③ $|zw|=|z||w|$
④ $|z^{-1}|=\dfrac{1}{|z|}$
⑤ $z\overline{z}=|z|^2$ D!
⑥ $|z+w|\le|z|+|w|$

(PMC) — Polar Multiplication in $\mathbb{C}$

$$z_1z_2=r_1r_2(\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2))$$

(DMT) De Moivre's Theorem (any $n\in\mathbb{Z}$)

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

(32) More Complexes

$z^n=a$ has n roots, called an n^{th} root for a

(CNRT) $\sqrt[n]{r}\left(\cos\left(\frac{\theta+2\pi k}{n}\right)+\sin\left(\frac{\theta+2\pi k}{n}\right)\right)$

☆ $k\in\{0,1,\dots n-1\}$

★ helpful for the final ★

(CJRT) If $f(x)=a_nx^n+\dots+a_0x^0\in\mathbb{C}[x]$ with real coefficients (so $f(x)\in\mathbb{R}[x]$) and if $c\in\mathbb{C}$ is a root of $f(x)$ $(f(c)=0)$ then $\overline{c}$ is also a root!

a happy Ali to make you smile!

For studying for this class I recommend doing less note-rewriting and more practice problems. The course is testing your ability to try different proof methods, so an overpowered strategy is to write flash cards for yourself *while you do the problems* that contain notes specifically on **how to tie proof strategies to problem types**. At the end of the day it's more important to know which tools you should be using in a proof than it is to know how the tools work.

Oftentimes people think advice like this is wishy-washy and not helpful. I disagree! I followed nothing but that advice, and ended up acing this class.

fun fact the anagram in Ali's gallery was me hehe