Language and Proofs in Algebra

MATH135

Jaiden Ratti

Prof. J.P. Pretti

1229

Contents

1 Introduction to the Language of Mathematics

1.1 Sets

Sets are not ordered.

$\{7, \pi\} = \{\pi, 7\}$

Denote element of set by $7 \in \{2, 7, 3\}$. $\{7\} \notin \{7, 3, 2\}$, but $\{7\} \in \{\{7\}, 3, 2\}$.

$\{\} = \emptyset$, $\emptyset \neq \{\emptyset\}$

$\emptyset \notin \{7, 3\}$, $\emptyset \notin \emptyset$

$\mathbb{Z} \rightarrow$ set of integers.
$\mathbb{N} \rightarrow$ set of natural numbers.
$\mathbb{Q} \rightarrow$ set of rational numbers.
$\mathbb{R} \rightarrow$ set of real numbers.

1.2 Mathematical Statements and Negation

Statements are true or false.

$9 + 6 = 15$ is a statement

$x > 2$ is not a statement (Open sentence. If you knew x, it would be a statement)

$10 > 7$ is a statement

Open sentence $\neq$ statement.

Negation

P is a statement

Negation of $P(\neg P)$ is true when P is false.

1.3 Quantifiers and Quantified Statements

1.3.1 Universal and Existential Quantifiers

$x^2 - x \geq 0$ is an open statement.

$\forall x \in \mathbb{N}, x^2 - x \geq 0$. This is "for all natural numbers $x, x^2 - x \geq 0$" We know this is true.

Changing the domain makes it false.

$\forall x \in \mathbb{R}, x^2 - x \geq 0$

When domain is empty $(\forall x \in \emptyset)P(x)$ is always true.

$\forall x \in \emptyset, x^2 - x \geq 0$ is true. All elephants in the room have 20 legs $\ddot\smile$

Let $x \in \mathbb{R} \leftarrow$ universally quantifying the following statement.

Existential Quantifier

$\exists x \in S, P(x)$. This is "there exists a number x in the set S such that $P(x)$ is true." There just has to be one such case.

$\exists m \in \mathbb{Z}, \frac{m-7}{2m+4} = 5, m = -3. \therefore true.$

Once again, domain matters.

$\exists x \in \emptyset, P(x)$ is always false.

Exercises

$$\begin{aligned}
64 \text{ is a perfect square} &\iff \exists x \in \mathbb{Z}, x^2 = 64 \\
y = x^3 - 2x + 1 \text{ has no } x\text{-ints} &\iff \forall x \in \mathbb{R}, x^3 - 2x + 1 \neq 0 \\
&\iff \neg(\exists x \in \mathbb{R}, x^3 - 2x + 1 = 0) \\
2^{2a-4} = 8 \text{ has a rational solution} &\iff \exists a \in \mathbb{Q}, 2a - 4 = 3 \\
\frac{n^2+n-6}{n+3} \text{ is an integer as long as } n \text{ is an integer} &\iff \forall n \in \mathbb{Z}, \frac{n^2+n-6}{n+3} \in \mathbb{Z}
\end{aligned}$$

1.3.2 Negating Quantifiers

Everybody in this room was born before 2010 $\leftarrow$ Universal

Somebody in this room was born after 2010, or on 2010 $\leftarrow$ Existential

$\forall x \in S, P(x)$ is false when there is at least one $x \in S$ for which $P(x)$ is false.

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

We cannot just change all the signs since $P(x)$ might be complicated.

$\forall x \in \mathbb{R}, |x| < S$. Negation: $\exists x \in \mathbb{R}, |x| \geq S$

Someone in this room was born before 1990. Everyone in this room was born after or during 1990 is the negation.

$\exists x \in \mathbb{Q}, x^2 = S$. Negation: $\forall x \in \mathbb{Q}, x^2 \neq S$.

1.4 Nested Quantifiers

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

$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$ is true. $\exists$ is in the open statement

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

$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$ is false. If x was fixed, there is no way every y will work.

2 Logical Analysis of Mathematical Statements

2.1 Logical Operators

Statement represented by A.

A	$\neg A$
T	F
F	T

Conjunction and Disjunction

A and $B \equiv A \wedge B$ is

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

$\sqrt{2}$ is irrational and $3 > 2$ is true.

10 is even and $1 = 2$ is true.

$\forall x \in \mathbb{N}, (x > x - 1) \wedge (2x > x)$ is true.

$\forall x \in \mathbb{Z}, (x > x - 1) \wedge (2x > x)$ is false.

A or $B \equiv A \vee B$ is

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

$5 \leq 6$ is true.

87 is a prime number of $14x = 25$ has $x \in \mathbb{Z}$ is false.

16 is a perfect square or 15 is a multiple of 3 is true.

Logical Equivalence

$A \equiv \neg(\neg A)$. A is logically equivalent to not not A.

De Morgan's Laws

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

A	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

Example, show

$$\begin{aligned}
&\neg(A \wedge (\neg B \wedge C)) \equiv \neg(A \wedge C) \vee B \\
&\neg(A \wedge (\neg B \wedge C)) \\
&\equiv (\neg A) \vee \neg(\neg B \wedge C) \\
&\equiv (\neg A) \vee (B \vee \neg C) \\
&\equiv (\neg A) \vee (\neg C \vee B) \\
&\equiv (\neg A \vee \neg C) \vee B \\
&\equiv \neg(A \wedge C) \vee B
\end{aligned}$$

2.2 Implication

"If H then C", $H \implies C$

Equivalent to $(\neg H) \vee C$

$H =$ hypothesis, C is conclusion

H	C	$H \implies C$
T	T	T
T	F	F
F	T	T
F	F	T

$\sqrt{2}$ is irrational, $3^3 = 27 \leftarrow$ True.

$\sqrt{2}$ is irrational, $3^3 = 28 \leftarrow$ False.

$\sqrt{2}$ is rational, $3 + 4 = 6 \leftarrow$ True.

$\sqrt{2}$ is rational, $3 + 4 = 7 \leftarrow$ True.

For all real numbers x, if $x > 2, x^2 > 4 \leftarrow$ True.

For all real numbers x, if $x \geq 2, x^2 > 4 \leftarrow$ True.

$\forall k \in \mathbb{Z}$, if $k > 3$, then $2k + 1 \geq 9$ is true.

$\forall k \in \mathbb{Z}$, if $k > 3$, then $2k + 1 \geq 10$ is false.

$\forall k \in \mathbb{Z}$, if $k > 3$, then $2k + 1 \geq 8$ is true.

$\forall x \in \mathbb{R}(x \geq 7 \implies x + \frac{1}{x} \geq 2)$

For all $x \in \mathbb{R}$, if $x \geq 7$, then $x + \frac{1}{x} \geq 2$

$x \in \mathbb{R} \wedge x \geq y \implies x + \frac{1}{x} \geq 2$

$x + \frac{1}{x} \geq 2$ whenever $x \in \mathbb{R}$ and $x \geq 7$

Negation of Implication

$$\neg(H \implies C) \equiv \neg((\neg H) \vee C) \equiv (\neg(\neg H)) \wedge (\neg C)) \equiv H \wedge (\neg C)$$

Negation of implication is not an implication.

If 7 is a prime and $5 \leq 6$, then 24 is a perfect square (false).

7 is prime and $5 \leq 6$ and 24 is not a perfect square (true).

Negation of implication is and. Hypothesis is not always first.

Implication Examples

For all $a, b, x, \in \mathbb{R}$

1. If $a < b$, then $a \leq b$ (true)
2. If $|x| = 3$, then $x^2 = 9$ (true)

2.3 Contrapositive and Converse

Contrapositive

The contrapositive of $A \implies B$ is the implication $\neg B \implies \neg A$

1. If $a > b$, then $a \geq b$ (true)
2. If $x^2 \neq 9$, then $|x| \neq 3$ (true)

Logically equivalent with $A \implies B$

Converse

The converse of $A \implies B$ is the implication $B \implies A$

1. If $a \leq b$, then $a < b$ (false)
2. If $x^2 = 9$, then $|x| = 3$ (true)

Not logically equivalent with $A \implies B$

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

2.4 If and Only If

Logical operator $\iff$

For all $x \in \mathbb{R}, |x| = 3$ iff $x^2 = 9$

True both ways.

$2 + 2 = 5$ iff $3 + 3 = 7$ is True

3 Proving Mathematical Statements

Prove:

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

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

$$\begin{aligned} 0 &\leq (x^2 - 2y)^2 \\ &= x^4 - 4x^2y + 4y^2 \\ &= x^4 - 5x^2y + x^2y + 5y^2 + y^2 \end{aligned}$$

Faulty logic: Prove $7 = -7$ by squaring both sides

3.1 Proving Universally Quantified Statements

Proving $\forall x \in S, P(x)$

We can consider arbitrary $x \in S$, and argue that $P(x)$ must be true (direct proof).

Prove an identity

Prove

$max\{x, y\} = \frac{x+y+|x-y|}{2}$ for all $x, y \in \mathbb{R}$

Case 1: $x \geq y$. In this case $max\{x, y\} = x$. And $\frac{x+y+x-y}{2} = x$

Case 2: $x < y$. In this case $max\{x, y\} = y$. And $\frac{x+y+(-x+y)}{2} = y$

In both cases, LHS = RHS ■

Disprove Universally Quantified Statement

$\forall x \in \mathbb{R}, (x^2 - 1)^2 \geq 0$

A counter example is $1 \in \mathbb{R}$.

Single example doesn't prove $\forall x \in S, P(x)$ is true.

Single counter example does prove $\forall x \in S, P(x)$ is false.

3.2 Prove Existentially Quantified Statements

There exists a perfect square k such that $k^2 - \frac{31}{2}k = 8$.

Consider $k = 16$. Since $k = 4^2, k$ is a perfect square. Also $k^2 - \frac{31}{2}k = 256 - 248 = 8$ completing the proof.

Disprove Existential Statement

We will prove the negation is true.

"There exists a real number x such that $\cos 2x + \sin 2x = 3$"

"For all real numbers x such that $\cos 2x + \sin 2x \neq 3$"

$x \in \mathbb{R}$

Since $\cos 2x, \sin 2x \leq 1$, then

$\cos 2x + \sin 2x \leq 2\blacksquare$

For all $k \in \mathbb{N}$, there exists $x \in \mathbb{R}$, such that $\log_k x^5 = \frac{1}{2}$

Proof

Let $k \in \mathbb{N}$. Consider $x = k^{\frac{1}{10}}$. Clearly $x \in \mathbb{R}$. Moreover, $\log_k x^5 = \log_k (k^{\frac{1}{10}})^5 = \log_k k^{\frac{1}{2}} = \frac{1}{2}$

3.3 Proving Implications

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

Proof

Assume m is an even integer.

That is $m = 2k$ for some integer $k \in \mathbb{Z}$

We must show $\exists \ell \in \mathbb{Z}, 7m^2 + 4 = 2\ell$

We have $7m^2 + 4 = 7(2k)^2 + 4 = 2(14k^2 + 2)$

Since $k \in \mathbb{Z}$, then $14k^2 + 2 \in \mathbb{Z}$. That is, picking $\ell = 14k^2 + 2$ completes the proof.

For all integers k, if k^5 is a perfect square, then $9k^19$ is a perfect square

$$
\begin{aligned}
&\text{Let } k \in \mathbb{Z} \\
&\text{Assume } k^2 \text{ is a prefect square} \\
&\text{That is } k^5 = n^2 \text{for some } n \in \mathbb{Z} \\
&\text{then } 9k^{19} = (9k^{14})k^5 \\
&= (9k^{14})n^2 \\
&= (3k^7)^2 n^2 \\
&= (3k^7 n)^2
\end{aligned}
$$

Since $k, n \in \mathbb{Z}$, then $3k^7 n \in \mathbb{Z}$. Thus $9k^{19}$ is a perfect square. $\blacksquare$

3.4 Divisibility of Integers

An integer m divides an integer n if there exists an integer k so that $n = km$.

We write $m|n$ is m divides n

$7|56, 7|-56, 7|0, 0|0$

$7 \nmid 55, 0 \nmid 7$

$\frac{7}{56}$ is a number, $7|56$ is a statement.

3.4.1 Transitivity of Divisibility

For all $a, b, c \in \mathbb{Z}$ if $a|b$ and $b|c$ then $a|c$.

Proof

Let $a, b, c \in \mathbb{Z}$. Assume $a|b$ and $b|c$ then $b = ak$ and $c = b\ell$ for some $k, \ell \in \mathbb{Z}$.

Substituting gives $c = (ak)\ell = (k\ell)a$

Notice that $k\ell \in \mathbb{Z}$ because $k, \ell \in \mathbb{Z}$. Thus $a|c$ by the definition of divisibility.

3.4.2 Divisibility of Integer Combinations

For all a, b, c if $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x, y.

e.g. $a = 5, b = 10, c = 25$

DIC $\rightarrow 5|(10x + 25y)$ for all $x, y, \in \mathbb{Z}$

Proof

Let $a, b, c \in \mathbb{Z}$. Assume $a|b$ and $a|c$. Then $ak = b$ and $a\ell = c$ for some $k, \ell \in \mathbb{Z}$. Now $bk + cy = akx + a\ell y = a(kx + \ell y)$

Since $k, x, \ell, y \in \mathbb{Z}$, then $kx + \ell y \in \mathbb{Z}$.

Proposition

For all $a, b, c \in \mathbb{Z}$ if $a|b$ or $a|c$, then $a|bc$

Note

Let P, Q, and R be statement variables

$$(P \vee Q) \implies R \equiv (P \implies R) \wedge (Q \implies R)$$

Proof

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

First we prove $a|b \implies a|bc$

So suppose $b = ak$ for some $k \in \mathbb{Z}$

Then $bc = (ak)c = a(kc)$

Since $k, c \in \mathbb{Z}$, then $kc \in \mathbb{Z}$. Hence $a|bc$

To complete this proof, we must show $a|c \implies a|bc$. The argument in this case is similar ■.

Another Example

For all $a, b, c \in \mathbb{Z}$ if for all $x \in \mathbb{Z}, a|(bx + c)$ then $a|(b + c)$

Proof

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

Assume $\forall x \in \mathbb{Z}, a|(bx + c)$

Choosing $x = 1$, gives $a|(b + c)$

This is not choosing a number for all integers x. We are assuming the hypothesis is correct.

For all $a, b, c, x \in \mathbb{Z}$ if $a|(bx + c)$, then $a|(b + c)$

This is false. Counter example

$3|(2(3) + 3)$ and $3 \nmid (2 + 3)$

TD: $\forall a, b, c \in \mathbb{Z}, (a|b \wedge b|c) \implies a|c$

$11|55$ and $55|n$, we know $11|n$, by TD.

3.5 Proof of Contrapositive

Example

For all integers x, if $x^2 + 4x - 2$ is odd, then x is odd.

Proof

Let $x \in \mathbb{Z}$. We will show the contrapositive is true.

Assume x is even. That is $x = 2k$ for some integer k. Substitute to get

$x^2 + 4x - 2 = 4k^2 + 8k - 2 = 2(2k^2 + 4k - 1)$

Since k is an integer, then $2k^2 + 4k - 1 \in \mathbb{Z}$. That is $x^2 + 4x - 2$ is even $\blacksquare$.

Example

If $a, b \in \mathbb{R}$. If ab is irrational then a is irrational or b is irrational.

Proof

Let $a, b \in \mathbb{R}$. We will use the contrapositive.

Assume $a = \frac{p}{q}$ and $b = \frac{r}{s}$ for some integers $p, q, r, s \in \mathbb{Z}$ where $q, s \neq 0$.

Then $ab = \frac{rp}{qs}$ moreover since $p, q, r, s \in \mathbb{Z}$ then $rp, qs \in \mathbb{Z}$. Also $qs \neq 0$. That is ab is rational.

Example

Let $x \in \mathbb{R}$. If $x^3 + 7x^2 < 9$, then $x < 1.1$.

Proof

Let $x \in \mathbb{R}$. Suppose $x \geq 1.1$ then $x^3 + 7x^2 \geq (1.1)^3 + 7(1.1)^2 > 9.8 > 9$.

We get that $x^3 + 7x^2 \geq 9$. Therefore the contrapositive is true, proving the original statement is true as well.

Example

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

If $a|b$ then $b \nmid c$ or $a|c$.

Proof

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

Using "elimination", assume $a|b$ and $b|c$. By TD $a|c$.

Why does this work?

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

3.6 Proof by Contradiction

A or $\neg A$ must always be false.

$A \wedge (\neg A)$ is always false, calling it true is a contradiction.

We can prove that statement P is true by, assuming $\neg P$ is true then based on this assumption, prove that both Q and $\neg Q$ are true for some statement P.

Prove that $\neg(\exists a, b \in \mathbb{Z}, 10a + 15b = 12)$

By way of contradiction (BWOC), assume that $10a + 15b = 12$ for some $a, b, \in \mathbb{Z}$. Then $5(2a + 3b) = 12$. Since $2a + 3b \in \mathbb{Z}$, then $5|12$. However we know that $5 \nmid 12$. This is a contradiction, completing the proof.

Prove $\sqrt{2}$ is irrational.

Assume it is rational, $\sqrt{2} \in \mathbb{Q}$.

$\sqrt{2} = \frac{a}{b}$ where a, b are integers > 0.

Assume they are not even. If they were even, $a = 2c$ and $b = 2d$ and thus $c < a$ and $d < b$.

$\frac{a}{b} = \frac{2c}{2d} = \frac{c}{d}$

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

$a^2 = 2b^2$

$2|a^2$, so a^2 is even.

Assume its odd

$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. a must be even.

$\exists$ an integer m such that $a = 2m$,

$b^2 = 2m^2$. b must be even then which is a contradiction.

$\therefore \sqrt{2}$ is irrational.

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

Proving $A \implies B$ is true by contradiction, we assume $A \implies B$ is false. A is true, B is false. If we can prove this is a contradiction, $A \implies B$ is true.

$\forall a, b, c \in \mathbb{Z}$ if $a|(b+c)$ and $a \nmid b$, then $a \nmid c$.

For sake of contradiction, there exists integers a, b, c such that $a|(b+c)$ and $a \nmid b$ and $a|c$.

By DIC we have $a|[(1)(b+c) + (-1)c] = a|b$ contradiction.

3.7 Proving If and Only If Statements

Example

Let $x, y \in \mathbb{R}$ where $x, y \geq 0$. Then $x = y$ iff $\frac{x+y}{2} = \sqrt{xy}$

Proof

Let $x, y \in \mathbb{R}$ where $x, y \geq 0$.

We will prove this in both directions $(\rightarrow)$

Assume $x = y$, $\frac{y+y}{2} \rightarrow y \leftarrow \sqrt{yy}$.

$(\leftarrow)$ Assume $\frac{x+y}{2} = \sqrt{xy}$

$\implies x + y = 2\sqrt{xy}$
$\implies (x+y)^2 = 4xy$
$\implies x^2 - 2xy + y^2 = 0$
$\implies (x-y)^2 = 0$
$\implies x - y = 0$
$\implies x = y$

4 Mathematical Induction

4.1 Notation for Summations, Products and Recurrences

Summation Notation

$$\sum_{k=3}^{7} k^2 = 3^2 + 4^2 + 5^2 + 6^2 + 7^2 = 135$$

Product Notation

$$\prod_{k=1}^{3}(5-k)! = 4! \cdot 3! \cdot 2! = 288$$

4.2 Proof by Induction

Statement

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

Proof

We will proceed by induction on n.

Base Case

We consider when $n = 1$

Then

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

And

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

That is, the statement is true when $n = 1$.

Inductive Step

Let k be an arbitrary natural number.

Assume

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

Consider when $n = k+1$

Then

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

And

$$\begin{aligned}
\sum_{i=1}^{n} i(i+1) &= \sum_{i=1}^{k+1} i(i+1) \\
&= (\sum_{i=1}^{k} i(i+1)) + (\sum_{i=k+1}^{k+1} i(i+1)) \\
&= \frac{1}{3}k(k+1)(k+2) + (k+1)(k+2) \text{ by our inductive hypothesis} \\
&= \frac{1}{3}k(k+1)(k+2) + \frac{3}{3}(k+1)(k+2) \\
&= \frac{1}{3}(k+1)(k+2)(k+3)
\end{aligned}$$

That is, the statement is true when $n = k+1$. Therefore by POMI, the proof is complete.

POMI

Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$. If statement 1 and 2 are true

1. $P(1)$
2. For all $k \in \mathbb{N}$, if $P(k)$, then $P(k+1)$

Then statement 3 is true.

3. For all $n \in \mathbb{N}, P(n)$

$P(1) \implies P(2) \implies P(3) \implies P(4)$

POMI doesn't have to start at 1.

Let $P(n)$ be the open sentence

$6|(2n^3 + 2n^2 + n)$

Prove $P(n)$ is true for all n.

<u>Base Case</u> $P(1), 6|6\checkmark$

Assume $P(k)$ is true

$6|(2k^3 + 3k^2 + k)$

<u>Inductive Step</u> $6|(2(k+1)^3 + 3(k+1)^2 + (k+1))$

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

$\underbrace{2k^3 + 3k^2 + k}_{\text{6 divides this}} + \underbrace{6k^2 + 6k + 6k + 6}_{\text{6 divides this}}$

6 divides the sum by DIC.

4.3 Binomial Coefficients

$\binom{5}{2} \implies 5C2 \implies$ "5 choose 2" $= \frac{5!}{3! \cdot 2!} = 10$

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

$\binom{n}{m} = 0$ when $m > n$.

<u>Pascals Identity</u>

$$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m} \quad \text{for all positive integers } n, m \text{ with } m < n.$$

<u>Binomial Theorem</u>

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

BT1

$$(1+x)^n = \sum_{m=0}^{n} \binom{n}{m} x^m$$

BT2

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

<u>Practice</u>

Prove that for all integers $n \geq 0$, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Let $x = 1$ in BT1

$(1+1)^n = \sum_{k=0}^{n} \binom{n}{0} (1)^0$

What is the coefficient of x^{18} in $(x^2 - 2x)^{12}$

By BT2

$$\begin{aligned}(x^2-2x)^{12} &= \sum_{m=0}^{12}\binom{12}{m}(x^7)^{12-m}(-2x)^m \\ &= \sum_{m=0}^{12}\binom{12}{m}(-2)^m x^{24-m} \\ \text{Choosing } m=6 \text{ gives the coefficient of } &\binom{12}{6}(-2)^6 \\ &= 59136\end{aligned}$$

Example

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

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

Proof by Induction on n.

Base Case: True when $n = 1, n = 2$

Inductive Step:

Let k be an arbitrary natural number where $k \geq 2$.

Let $P(n)$ be the open sentence.

Assume $P(1), P(2), P(3), \ldots, P(k)$ are all true. Then what happens to $k + 1$?

Consider $n = k + 1$

Then

$$\begin{aligned}x_n = x_{k+1} &= 2x_k + 15x_{k-1} \\ &= 2[2(-3)^k + 10 \cdot 5^{k-1}] + 15[2(-3)^{k-1} + 10 \cdot 5^{k-2}] \\ &= 4(-3)^4 + 30(-3)^{k-1} + 20 \cdot 5^{k-1} + 150 \cdot 5^{k-2} \\ &= 4(-3)^k - 10(-3)^k + 4 \cdot 5^k + 6 \cdot 5^k \\ &= -6(-3)^k + 10 \cdot 5^k \\ &= 2(-3)^{k+1} + 10 \cdot 5^k\end{aligned}$$

Hence the proof is done by POSI. Difference between POMI and POSI is not base cases.

4.4 Principal of Strong Induction

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

1. $P(1)$ is true, and
2. $\forall k \in \mathbb{N}, [(P(1) \wedge P(2) \wedge \ldots \wedge P(k)) \implies P(k+1)]$

Example

Prove that $nm - 1$ breaks are needed to break an $n \times m$ chocolate bar into individual pieces.

Proof

$N = nm$. We will proceed by induction on N.

Base Case

When $N = 1$, no breaks are needed.

Since $N - 1 = 0$, the statement is true for $N = 1$.

Inductive Step

Let $k \in \mathbb{N}$.

Suppose the statement is true when $N = 1, N = 2, N = 3, \ldots, N = k$.

Consider $N = k + 1$ and the first break. We are left with 2 smaller bars. Let x and y be the number of pieces in these smaller bars.

Then $1 \leq x, y \leq k$. Also $x + y = N$. Breaking these two bars requires $(x - 1) + (y - 1) = N - 2$ breaks by our IH.

For the original bar, we require

$1 + N - 2 = N - 1$ breaks. By POSI this completes the proof.

5 Sets

5.1 Introduction

The number of elements in a set is cardinality. Denoted by $|S|$.

$S = \{1, 2, 4, 6\}.|S| = 4$

$|\emptyset| = 0$ but $|\{\emptyset\}| = 1$

$\emptyset = \{\}$ empty set but ...

$\{\emptyset\}$ is not an empty set

5.2 Set-Builder Notation

Universal set $\mathcal{U}$ contains the objects we are concerned with (universe of discourse $\rightarrow$ universal set).

Notation:

$\{x \in \mathcal{U} : P(x)\} =$ "The set of all x in $\mathcal{U}$ such that $P(x)$ is true".

$Q = \{x \in \mathbb{R} : x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}, b \neq 0\}$

Set of positive factors of 12 $\{x \in \mathbb{N} : n|12\}$

Set of even integers $\{x \in \mathbb{Z} : x = 2k, k \in \mathbb{Z}\}$

Set-Builder Notation Type 2

$\{f(x) : x \in \mathcal{U}\}$ "all objects in $\mathcal{U}$ of the form $f(x)$"

Even set of integers $\{2k : k \in \mathbb{Z}\}$

Perfect squares $\{x^2 : x \in \mathbb{R}\}$

Multiples of 12 $\{12n : n \in \mathbb{Z}\}$

Set-Builder Notation Type 3

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

Set consisting of all objects of the form $f(x)$ such that x is an element of $\mathcal{U}$ and $P(x)$ is true.

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

Integer powers of $2 : \{2^k : k \in \mathbb{Z}, k \geq 0\}$

Perfect squares larger than $50 : \{x^2 : x^2 > 50, x \in \mathbb{Z}\}$

Multiples of $7 : \{7x : x \in \mathbb{Z}\}$

Odd perfect squares: $\{x^2 : x^2 = 2k + 1, k \in \mathbb{Z}\}$

5.3 Set Operations

Union of 2 sets S & $T, S \cup T$ is the set of all elements in either

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

e.g. $\{2k : k \in \mathbb{Z}\} \cup \{k \in \mathbb{Z} : 0 \leq k \leq 10\} = \{0, 1, 2, 3, 4, \ldots, 10, 12, 14, \ldots\}$

Intersection of 2 sets S & $T, S \cap T$ is the set of elements in both

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

Set Difference of 2 sets S & $T, S - T$ or $S \setminus T$ is the set of all elements in S but not in T.

$$S \setminus T = \{x : (x \in S) \vee (x \notin T)\}$$

The complement of a set $S, \overline{S}$ or $S^{\complement}$ is the set of elements in the universal set but not in S.

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

(When $\mathcal{U} = \mathbb{Z}$) Let $S = \{x \in \mathbb{Z} : x \geq 0\}, \overline{S} = \{x \in \mathbb{Z} : x < 0\}$

5.4 Subsets of a Set

Two sets are disjoint when $S \cap T = \emptyset$.

Any set S and its complement $\overline{S}$ are disjoint.

Any set S and $\emptyset$ are disjoint.

A set S is a subset of set T if every element of S is an element of T. Denoted by: $S \subseteq T$. If S is not a subset of T, that is denoted by $S \nsubseteq T$.

$\{2k : k \in \mathbb{Z}\} \subseteq \mathbb{Z}$
$\{2, 5, 6, 8, 10\} \nsubseteq \{2k : k \in \mathbb{Z}\}$
$\emptyset \subseteq S$ and $S \subseteq S$
$\mathbb{N} \subseteq \mathbb{Z}, \mathbb{Z} \subseteq \mathbb{Q}, \mathbb{Q} \subseteq \mathbb{R}$

A set S is a proper set of T if there is at least one element of T that is not in S. (S must be a subset). $S \subsetneq T$.

$A = \{2k : k \in \mathbb{Z}\}, B = \{2k + 1 : k \in \mathbb{Z}\}, C = A \cup B$

$A \subsetneq \mathbb{Z}, B \subsetneq \mathbb{Z}$

$C \subset \mathbb{Z}$ (not a proper subset since $C = \mathbb{Z}$)

$\{1, 2, 3\} \subset \{1, 2, 3, 4\}$ and $\{1, 2, 3\} \subsetneq \{1, 2, 3, 4\}$

All proper subsets are subsets

If $A \subset B \wedge B \subset A$, then $B = A$.

5.5 Subsets, Set Equality, and Implications

Given S and T, prove $S \subseteq T$

Prove the implication $\forall x \in \mathcal{U}, (x \in S) \implies (x \in T)$

Example: Let $S = \{8m : m \in \mathbb{Z}\}$ and $T = \{2n : n \in \mathbb{Z}\}$. Show that $S \subseteq T$.

Proof: Let $x \in \mathbb{Z}$ and assume $x \in S$. Then $8m$ for $m \in \mathbb{Z}$. Then $x = 2(4m)$. $4m \in \mathbb{Z}$, set $n = 4m$ and we can see $x = 2n$. Thus $x \in T$, $S \subseteq T$.

Let $A = \{n \in \mathbb{N} : 4|(n - 3)\}$ and $B = \{2k + 1 : k \in \mathbb{Z}\}$. Prove $A \subseteq B$.

Let $x \in \mathbb{N}$ since $x \in A$. Then $4|(x-3)$, such that $j \in \mathbb{Z}$

$$\begin{aligned} 4j &= x - 3 \\ x &= 4j + 3 \\ &= 4j + 2 + 1 \\ &= 2\underbrace{(2j+1)}_{\mathbb{Z}} + 1 \end{aligned}$$

since $j \in \mathbb{Z}, 2j + 1 \in \mathbb{Z}.k = 2j + 1, x = 2k + 1, x \in B$

Given S & T, prove $S = T$.

Prove $S \subseteq T$ and $T \subseteq S$.

Show $\forall x \in \mathcal{U}, (x \in S) \implies (x \in T) \wedge (x \in T) \implies (x \in S)$ or $(x \in S) \iff (x \in T)$

Let $S = \{1, -1, 0\}$ and $T = \{x \in \mathbb{R} : x^3 = x\}$. Prove $S = T$

$\subseteq$ Let $x \in S$. Then $x = 1, -1, 0$. When $x = 1, (1)^3 = 1 \ldots$. So $x \in S \implies x \in T$

$\supseteq$ Let $x \in T$. Then $x^3 = x$ or $x^3 - x = 0, x(x-1)(x+1) = 0$. x must be $0, -1$, or $1 \ldots x \in S$. $T \subseteq S$.

Since we have shown both $S \subseteq T$ and $S \supseteq T, S = T$.

Proving General Statements

Prove $A \cap B \subseteq A$

Proof: Let $x \in A \cap B$, then $x \in A$ and $x \in B$. Thus $x \in A \cap B \implies x \in A$ so $A \cap B \subseteq A$.

Prove that $S = T$ if and only if $S \cap T = S \cup T$

$(\rightarrow)$ Assume $S = T$. Then $S \subseteq T$ and $T \subseteq S$.

$\subseteq$ Let $x \in S \cap T$. Then $x \in S$ and $x \in T$ so $x \in S \cup T$

$\supseteq$ Let $x \in S \cup T$. Then $x \in S$ or $x \in T$. If $x \in S$, since $S \subseteq T$, then $x \in T$ and vice versa.

Thus $x \in S \cup T, x \in S \cap T$.

$(\leftarrow)$ Assume $S \cap T = S \cup T$

$\subseteq$ Let $x \in S$. Then $x \in S \cup T \implies x \in S \cap T$ so $x \in T$.

$\supseteq$ Let $x \in T$. Then $x \in S \cup T \implies x \in S \cap T$ so $x \in S$.

We have shown it both ways so $S \subseteq T$ and $T \subseteq S, S = T$.

6 The Greatest Common Divisor

Bounds by Divisibility

For all $a, b \in \mathbb{Z}$, if $b|a$ and $a \neq 0$, then $b \leq |a|$

Proof

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

Assume $b|a$ and $a \neq 0$

Then there exists $q \in \mathbb{Z}$ such that $bq = a$.

From this we get $|bq| = |a|$

This tells us $|b||q| = |a|$

Since $a \neq 0$m then $q \neq 0$.

Since $q \in \mathbb{Z}, q \neq 0$, then $|q| \geq 1$

Sub into equation to get $|b| \leq |a|$

Since $b \leq |b|$, so $b \leq |a|$.

6.1 Division Algorithm

For all $a \in \mathbb{Z}$ and for all $b \in \mathbb{N}$ there exists unique integers q and r such that

$$a = bq + r \quad \text{where } 0 \leq r < b$$

Examples

$$\begin{aligned} a = 50, b = 8 \quad & 50 = 8 \cdot \underbrace{6}_{q} + \underbrace{2}_{r} \\ a = 40, b = 8 \quad & 40 = 8 \cdot 5 + 0 \\ a = -50, b = 8 \quad & -50 = 8 \cdot (-7) + 6 \end{aligned}$$

6.2 Greatest Common Divisor (GCD)

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 $60 : \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60$

$gcd(84, 60) = 12$

Formal Definition

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

When a and b are not both zero, we say an integer $d > 0$ is the greatest common divisor of a and b, and write $gcd(a, b)$ iff

- $d|a \wedge d|b$
- for all integers c, if $c|a$ and $c|b$ then $c \leq d$

Otherwise, we say $gcd(0, 0) = 0$

Examples

- $gcd(84, 60) = 12$
- $gcd(-84, 60) = 12$
- $gcd(84, -60) = 12$
- $gcd(-84, -60) = 12$
- $gcd(84, 0) = 84$
- $gcd(-84, 0) = 84$

Fact

For all $a, b \in \mathbb{Z}, gcd(3a + b, a) = gcd(a, b)$

Proof

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

Case 1 $a = b = 0$

In this case, by definition, $d = 0$

Also $3a + b = 0$ and $a = 0$ in this case, thus $gcd(3a + b, a) = 0$ as well.

Case 2 $a \neq 0$ or $b \neq 0$

Note that $3a + b \neq 0$ or $a \neq 0$ in this case as well. Since $d = gcd(a, b)$, we know $d > 0$ and $d|a$. We get $d|(3a + b)$ by DIC since we also know $d|b$.

To complete the proof we let $c \in \mathbb{Z}$ and assume $c|(3a + b)$ and $c|a$

All we must show is $c \leq d$. Using DIC again we get

$c|[(3a+b)(1)+a(-3)]$

$c|b$

Hence by definition of $gcd(a,b) c \leq d$.

<u>GCD with Remainders (GCD w R)</u>

For all $a,b,q,r \in \mathbb{Z}$, if $a = bq + r$ then $gcd(a,b) = gcd(b,r)$

Example $86 = 20(7) - 54$

$gcd(86,20) = 2$
$gcd(20,-54) = 2$

Alternative proof of our fact

Clearly $3a + b = 3a + b$

By GCD w R, $gcd(3a+b,a) = gcd(a,b)$

<u>Euclidean Algorithm (EA)</u>

Process to compute $gcd(a,b)$ for $a,b \in \mathbb{N}$

$$\begin{aligned} 84 &= 60(1) + 24 & gcd(84,60)& \\ 60 &= 24(2) + \underline{12} & = gcd(60,24)& \\ 24 &= 12(2) + 0 & = gcd(24,12)& \\ & & gcd(12,0) = \underline{12}& \end{aligned}$$

The last non-zero will be GCD since remainder is non-negative and $< b$.

Bigger example: Compute $gcd(1239,735)$

$$\begin{aligned} 1239 &= (735)(1) + 504 \\ 735 &= 504(1) + 231 \\ 504 &= 231(2) + 42 \\ 231 &= 42(4) + \underline{21} \\ 42 &= 21(2) + 0 \\ &\implies gcd(1239,735) = 21 \end{aligned}$$

<u>Back Substitution</u>

$$\begin{aligned} 21 &= 231 + 42(-5) \\ &= 231 + (-5)(504 + 231(-2)) \\ &= 504(-5) + 231(11) \\ &= 504(-5) + (11)(735 - 504) \\ &= 735(11) + 504(-16) \\ &= 735(11) + (-16)(1239 - 735) \\ &= 1239(-16) + 735(27) \end{aligned}$$

6.3 Certificate of Correctness and Bézout's Lemma

For all $a,b,d \in \mathbb{Z}$ where $d \geq 0$. If $d|a$ and $d|b$ and there exists $s,t \in \mathbb{Z}$ such that $as + bt = d$ then $d = gcd(a,b)$.

Example

$d = 6, a = 30, b = 42$

$b \geq 0, 6|30, 6|42$

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

$\implies 6 = gcd(30, 42)$

Bézout's Lemma

For all integers $a, b \in \mathbb{Z}$, there exists $s, t \in \mathbb{Z}$ such that $as + bt = gcd(a, b)$

GCD w R

$a = bq + r$ then $gcd(a, b) = gcd(b, r)$

GCD CT

If $d \geq 0, d|ad|b$ and s, t exists $as + bt = d$, then $d = gcd(a, b)$

BL

If $d = gcd(a, b)$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = d$

Example

For all $n \in \mathbb{Z}, gcd(n, n + 1) = 1$

Proof 1

Since $n + 1 = n(1) + 1$, GCD w R gives us

$gcd(n + 1, n) = gcd(n, 1)$. However

$gcd(n, 1) = 1$ because 1 is the only positive divisor of 1

Proof 2

Since $(n + 1)(1) + n(-1) = 1, 1 \geq 0$

$1|n + 1$ and $1|n$, then $gcd(n + 1, n) = 1$ by GCD CT.

Proof 3

Suppose $d \in \mathbb{Z}, d|(n + 1)$ and $d|n$ then by DIC, $d|1[(n + 1)(1) + n(-1) = 1]$ Thus 1 is the only divisor, that is GCD = 1.

Example

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

Proof

Let $a, b, x, y \in \mathbb{Z}$. Assume $gcd(a, b) \neq 0$ and $ax + by = gcd(a, b)$

Division gives

$(\frac{a}{gcd(a,b)})x + (\frac{b}{gcd(a,b)})y = 1$ since $gcd(a, b) \neq 0$

Since $\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)} \in \mathbb{Z}$

Moreover $1 \geq 0, 1|xand1|y$

Thus by GCD LT, $gcd(x, y) = 1$

Example

For all $a, b, c \in \mathbb{Z}$

If $gcd(a, c) = 1$ then $gcd(ab, c) = gcd(b, c)$

Proof

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

By BL, there are integers x, y, s, t such that

$ax + cy = 1$ and $bs + ct = d$

multiply to get

$(ax + cy)(bs + ct) = d$

Thus

$ab(xs) + c(axt + ybs + yct) = d$

Since $xs, axt+ybs+yct$ are integers, $d \geq 0$ (by definition), $d|c$ (by definition), $d|ab$, we get $d = gcd(ab, c)$ by GCD CT.

6.4 Extended Euclidian Algorithm

Solve $56x + 35y = gcd(56, 35)$ for $x, y \in \mathbb{Z}$

x	y	r	q
1	0	56	$\leftarrow 56 = 35(1) + 21$
0	1	35	$\vdots$
1	-1	21	1
-1	2	14	1
<u>2</u>	<u>-3</u>	<u>7</u>	1
		0	2

Thus $gcd(36, 35) = 7, x = 2, y = -3$

EEA with 408 and 170

x	y	r	q
1	0	408	$\leftarrow 408 = 170(2) + 68$
0	1	170	$\vdots$
2	-2	68	2
-2	5	34	2
		0	

Solve $-170x + 408y = d$ for $x, y \in \mathbb{Z}$ and $d = gcd(-170, 408)$

Order is irrelevant for gcd.

From before $d = 34$ and $x = -5, y = -2$

6.5 Further Properties of the Greatest Common Divisor

<u>Proof of CDD GCD (Common Divisor Divides)</u>

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

By BL, $ax + by = gcd(a, b)$ for some $x, y \in \mathbb{Z}$

By DIC, $c|ax + by$. That is $c|gcd(a, b)$.

<u>Definition</u>

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

When $gcd(a, b) = 1$, we say a and b are coprime.

<u>Coprimeness Characterization Theorem</u>

a and b are coprime iff there exists integers s and t with $as + bt = 1$.

Sketch of CCT Proof

$\implies$ BL

$\impliedby$ GCD CT

Exercise

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

If $gcd(a, b, c) = 1$, then $gcd(a, c) = 1$ and $gcd(b, c) = 1$

a) Prove or disprove

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

By CCT, $(ab)s + ct = 1$ for some $s, t \in \mathbb{Z}$

Since $bs, t \in \mathbb{Z}, gcd(a, c) = 1$ by CCT

Since $as, t \in \mathbb{Z}, gcd(b, c) = 1$ by CCT

b) Prove or disprove the converse

If $gcd(a, c)$ and $gcd(b, c)$, then $gcd(ab, c) = 1$

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

By CCT, $as + ct = 1$ and $bx + cy = 1$ for some $s, t, x, y \in \mathbb{Z}$

Multiply to yield

$(as + ct)(bx + cy) = 1$

After expanding and rearranging, CCT gives us $gcd(a, b) = 1$ because $sx, asy + tbx + txy \in \mathbb{Z}$.

Division by GCD (DB GCD)

If $gcd(a, b) = d \neq 0$ then $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

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

By BL, $ax + by = d$ for some $x, y \in \mathbb{Z}$.

Divide by d

$\frac{a}{d}x + \frac{b}{d}y = 1$, since $d \neq 0$

Note $d|a$ and $b|d$ by definition of d, so $\frac{a}{d}, \frac{b}{d}$ are $\mathbb{Z}$. Thus $(\frac{a}{d}, \frac{b}{d}) = 1$ by CCT

Proof of Coprimeness and Divisibility (CAD)

If a, b and c are integers and $c|ab$ and $gcd(a, c) = 1$, then $c|b$.

Proof

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

Assume $c|ab$ and $gcd(a, c) = 1$

$ax + cy = 1$ by CCT for some $x, y \in \mathbb{Z}$

Multiply both sides by b to get

$abx + cby = b$

We know $c|c$ and we assumed $c|ab$ so by DIC, $c|[(ab)x + (c)by]$ (because $x, by \in \mathbb{Z}$).

That is, $c|b$

Note

$\forall a, b, c \in \mathbb{Z}, (c|ab) \implies (c|a \vee c|b)$ is false.

6.6 Prime Numbers

Prime Factorization

Every integer greater than 1, can be written as the product of primes.

Proof

Proceed by Strong Induction (can't use POMI) to prove that an integer $n > 1$ can always be written as a product of primes.

Base Case

When $n = 2$, n by itself is a product of primes since 2 is prime.

Inductive Step

Let k be an arbitrary integer greater than 2.

Assume i can be written as the product of primes for all integers i such that $2 \leq i \leq k$.

We will consider cases for $n = k + 1$

When $k + 1$ is prime, there is nothing to prove.

Otherwise, $k + 1$ is composite.

That is $k + 1 = ab$ for some $a, b \in \mathbb{Z}$ satisfying $1 < a, b < k + 1$

By our inductive hypothesis, a and b can each be written as the product of primes. Multiplying these products gives a product of primes equal to $k + 1$. Hence the statement is true by POSI.

Euclid's Theorem

There are infinitely many primes.

Proof

By way of contradiction, assume there are a finite number of primes. We will name them $p_1, p_2, \ldots, p_k$ for some $k \in \mathbb{N}$.

Consider $N = (p_1 \cdot p_2 \ldots p_k) + 1$

By PF, $p_i | N$ for some $i \in \{1, 2, \ldots, k\}$

However, also $p_i | (p_1 \cdot p_2 \ldots p_k)$ by definition.

By DIC, we get $p_i | N - (p_1 \cdot p_2 \ldots p_k)$

That is, $p|1$. This is a contradiction because 1 is the only positive divisor of 1.

Euclid's Lemma

For all $a, b \in \mathbb{Z}$ and primes p, if $p|ab$, then $p|a$ or $p|b$.

Proof

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

Assume $p|ab$ and $p \nmid a$ (elimination).

Since the only positive divisors of p are 1 and p, and $p \nmid a, gcd(a, p) = 1$.

Thus $p|b$ by CAD.

6.7 Unique Factorization Theorem

Every natural number > 1 can be written as a product of prime factors uniquely, apart from order.

Example

Let p be prime. Prove that $13p + 1$ is a perfect square iff $p = 11$.

If $p = 11, 13(11) + 1 = 144 = 12^2 \checkmark$

Other direction:

$13p + 1 = k^2$

$13p = (k + 1)(k - 1)$

UFT $\rightarrow 13 = k + 1$ or $13 = k - 1$

$k = 12 \checkmark$ or $k = 14$ (wrong).

6.8 Prime Factorization and the Greatest Common Divisor

If $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \dots b = p_k^{\beta_k}$ where $p_1, p_2, \dots, p_k$ are primes and all exponents are non-negative.

$$gcd(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots \text{ where } \gamma_i = min\{\alpha_i, \beta_1\} \text{ for } i \dots k$$

Examples

$$\begin{aligned}
&gcd(13^2 \cdot 7^{100}, 16^3 \cdot 7^{44}) \\
&gcd(7^{100} 11^0 13^2, 7^{44} 11^3 13^0) \\
&= 7^{44} \cdot 11^0 \cdot 13^0 \\
&= 7^{44}
\end{aligned}$$

And

$$\begin{aligned}
&gcd(20000, 30000) \\
&gcd(2^5 5^4, 2^4 3^1 5^4) \\
&= 2^4 \cdot 5^4 \cdot 3^0 \\
&= 2^4 \cdot 5^4 \\
&= 10000
\end{aligned}$$

7 Linear Diophantine Equations

7.1 The Existence of Solutions in Two Variables

Given $a, b, c \in \mathbb{Z}$, find $x, y \in \mathbb{Z}$ such that $ax + by = c$

- Is there a solution? LDET 1
- If so, how can we find one? EEA
- And can we find all solutions? LDET 2

Examples of

1. $143x + 253y = 11$
2. $143x + 253y = 155$
3. $143x + 253y = 154$

1) Use EEA

y	x	r	q
1	0	253	
0	1	143	
1	-1	110	1
-1	2	33	1
4	-7	11	3
-13	23	3	0

Thus $\{(-7 + 23n, 4 - 13n) : n \in \mathbb{Z}\}$

Thus $143(-7) + 253(4) = 11$, $(-7, 4)$ is a solution.

2) There is no solution because $x, y \in \mathbb{Z}$, $11|(143x + 253y)$ but $11|155$ (not a multiple of 11).

3) Multiply equation in 1) by $\frac{154}{11} = 14$ to get:

$143(-98) + 153(56) = 154$

Other solutions to 1)?

Rewrite as $y = \frac{-13}{23}x + \frac{1}{23}$

LDET 1

Let $a, b \in \mathbb{Z}$ (both not zero) and let $d = gcd(a, b)$ the LDE $ax + by = c$ has a solution if and only if $d|c$.

First, suppose there exists $x, y \in \mathbb{Z}$ such that $ax + by = c$.

We know $d|a$ and $d|b$ (by definition of gcd), so $d|c$ by DIC.

Next we suppose $d|c$ to prove the other direction.

By BL there exists $s, t \in \mathbb{Z}$ such that $as + bt = d$.

Now we also know $dk = c$ for some integer k. Multiplying by k gives

$a(bk) + b(tk) = dk = c$

Since sk and $tk, \in \mathbb{Z}$, the proof is complete.

7.2 Finding All Solutions in Two Variables

LDET 2

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

If $(x, y) = (x_0, y_0)$ is one solution to the LDE $ax + by = c$, then the complete solution is

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

LDET 2 Example

We found that $(x, y) = (-7, 4)$ was a particular solution to $143x + 253y = 11$.

LDET 2 tells us the complete solution is

$\{(-7 + \frac{253}{11}n, 4 - \frac{143}{11}n) : n \in \mathbb{Z}\}$

$= \{(-7 + 23n, 4 - 13n) : n \in \mathbb{Z}\}$

Examples of some solutions are:

$n = 0 \quad (-7, 4)$
$n = 1 \quad (16, -9)$
$n = -1 \quad (-30, 17)$

Exercise

Solve the following LDEs:

1) $28x + 35y = 60$

$7 \nmid 60$, no solutions.

2) $343x + 259y = 658$

$$343(-3) + 259(4) = 7$$
$$343(-3 \cdot 94) + 259(4 \cdot 94) = 7 \cdot 94$$
$$343(282) + 259(376) = 658$$
$$\{(-3 + 37n, 4 + 49n) : n \in \mathbb{Z}\}$$

LDET 2 Proof

Let $a, b, c \in \mathbb{Z}$ where $d = gcd(a, b), a \neq 0$ and $b \neq 0$.

Assume $ax_0 + by_0 = c$ for some $x_0, y_0 \in \mathbb{Z}$.

Define $S = \{(x, y) : ax + by = c \text{ and } x, y \in \mathbb{Z}\}$ and $T = \{(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n) : n \in \mathbb{Z}\}$

Must show how $S = T(S \subseteq T, T \subseteq S)$

We begin by showing $T \subseteq S$.

Let $n \in \mathbb{Z}$.

We must show $(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n) \in S$.

To do this we substitute into $ax + by$ to get

$$a(x_0 + \frac{b}{d}n) + b(y_0 - \frac{a}{d}n) = ax_0 + by_0 = c$$

Indeed $T \subseteq S$.

Now we must show $S \subseteq T$.

Let $(x, y) \in S$. Then $ax + by = c$.

We also know $ax_0 + by_0 = c$.

Equating gives $ax - ax_0 = -by + by_0$

Thus $a(x - x_0) = -b(y - y_0)(\star)$

Since $d \neq 0$, we divide and get the following.

$\frac{a}{d}(x - x_0) = \frac{-b}{d}(y - y_0)$

This tells us $\frac{b}{d} | \frac{a}{d}(x - x_0)$

By DBGCD, $gcd(\frac{a}{d}, \frac{b}{d}) = 1$. By CAD, we know $\frac{b}{d} | (x - x_0)$. Thus $\frac{b}{d} | (x - x_o)$. Thus $\frac{b}{d}n = x - x_0$ for some $n \in \mathbb{Z}$.

That is $x = x_0 + \frac{b}{d}n$. Substitution into $(\star)$ yields $y = y_0 - \frac{a}{d}n$. Thus $(x, y) \in T$.

<u>Exercise</u>

Find all $x, y \in \mathbb{Z}$ satisfying

$15x - 24y = 9 \quad 0 \leq x, y \leq 20$.

We will solve the LDE first.

Note that it is equivalent to

$5x - 8y = 3$

By inspection, a solution (7,4).

So by LDET 2, the complete solution is

$x = -1 - 8n$ and $y = -1 - 5n$ where $n \in \mathbb{Z}$

We also need

$$\begin{aligned} -1 - 8n \geq 0 &\implies n \leq -1 \\ -1 - 8n \leq 20 &\implies n \geq -2 \\ -1 - 5n \geq 0 &\implies n \leq -1 \\ -1 - 5n \leq 20 &\implies n \geq -4 \end{aligned}$$

Thus $n = -1$ or $n = -2$.

Thus the final answer is $\{(7, 4), (15, 9)\}$

8 Congruence and Modular Arithmetic

8.1 Congruence

-1 is congruent to 7 modulo 8.

<u>Definition</u>

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

We say a is congruent to b module m when

$m|(a-b)$.

We write

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

Otherwise we write $a \not\equiv b \pmod{m}$.

Examples

$-1 \equiv 7 \pmod{8}$
$-1 \equiv -1 \pmod{8}$
$-1 \equiv 15 \pmod{8}$
$15 \equiv -1 \pmod{8}$
$15 \equiv 7 \pmod{8}$

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

$$\begin{aligned} & a \equiv b \pmod{m} \\ \iff & m|(a-b) \\ \iff & \exists k \in \mathbb{Z}, mk = a-b \\ \iff & \exists k \in \mathbb{Z}, a = mk+b \end{aligned}$$

8.2 Elementary Properties of Congruence

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

Reflexive: $a \equiv a \pmod{m}$
Symmetric: $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$
Transitivity: $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$

Proof of Reflexivity:

Since $a - a = 0$ and $m0 = 0$, we have $m|(a-a)$. That is $a \equiv a \pmod{m}$.

Proof of Symmetric:

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

This means $mk = a - b$ for some $k \in \mathbb{Z}$. $m(-k) = b - a$.

Since $-k \in \mathbb{Z}, m|(b-a)$.

That is $b \equiv a \pmod{m}$.

Proof of Transitivity:

Assume $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.

$m|(a-b), m|(b-c)$.

By DIC, $m|(a-c)$.

That is $a \equiv c \pmod{m}$.

Proposition 2

If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$
2. $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$
3. $a_1 a_2 \equiv b_1 b_2 \pmod{m}$

Proof of 1.

$mk = a_1 - b_1 \quad m\ell = a_2 - b_2$

$$\begin{aligned} a_1 + a_2 &= (mk + b_1) + (m\ell + b_2) \\ &= m\underbrace{(k+\ell)}_{\in\mathbb{Z}} + b_1 + b_2 \end{aligned}$$

Proof of 3.

$$\begin{aligned} a_1 a_2 &= (mk + b_1) + (m\ell + b_2) \\ &= (b_1 \cdot b_2) + m \quad \underbrace{(\ldots)}_{\text{some integer}} \end{aligned}$$

CAM (Generalization of Proposition 2)

For all positive integers n, for all integers $a_1 \ldots a_n$ and $b_1 \ldots b_n$, if $a_i \equiv b_i \pmod{m}$ for all $1 \leq i \leq n$ then

$$\begin{aligned} a_1 + a_2 + \ldots + a_n &\equiv b_1 + b_2 \ldots + b_n \pmod{m} \\ a_1 a_2 \ldots a_n &\equiv b_1 b_2 \ldots b_n \pmod{m} \end{aligned}$$

Congruence of Power

For all positive integers n and $a, b \in \mathbb{Z}$.

$a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m}$.

Question: Does 7 divide $5^9 + 62^{2000} - 14$

Is $5^9 + 62^{2000} - 14 \equiv 0 \pmod{7}$?

We will "reduce modulo 7"

$$\begin{aligned} -14 &\equiv 0 \pmod{7} \\ \implies 5^9 + 62^{2000} - 14 &\equiv 5^9 + 62^{2000} + 0 \pmod{7} \\ &\equiv 5^9 + (-1)^{2000} \pmod{7} \leftarrow \text{ by CP} \\ &\equiv 5^9 + 1 \pmod{7} \\ &\equiv (-2)^9 + 1 \pmod{7} \\ &\equiv (-2)^3(-2)^3(-2)^3 + 1 \pmod{7} \\ &\equiv (-1)(-1)(-1) + 1 \\ &\equiv 0 \pmod{7} \end{aligned}$$

Congruence and Division

Examples

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

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

Examples

1)
$3 \equiv 24 \pmod{7}$
$1 \equiv 8 \pmod{7}$

2)
$3 \equiv 27 \pmod{6}$
$1 \not\equiv 9 \pmod{6}$

Exercise

Does 72 divide $4(-66)^{2022} + 800$

By CAR, CAM and CP:

$$\begin{aligned} 4(-66)^{2022} + 800 &\equiv 2(-6)^2 2(-11)^2(-66)^{2020} + 800 \\ &\equiv 0 + 8 \pmod{72} \\ &\equiv 8 \pmod{72} \end{aligned}$$

But $8 \not\equiv 0 \pmod{72}$

Thus by CER, our number is not congruent to 0 modulo 72. Thus it does not.

Proof of CD

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

Assume $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$.

Then $m|(ac - bc)$ or equivalently $m|c(a - b)$.

By CAD, $m|(a - b)$. That is, $a \equiv b \pmod{m}$.

8.3 Congruence and Remainders

Congruent iff Same Remainder (CISR) and Congruent to Remainder (CTR) Examples

1) What is the remainder when $x = 77^{100}(999) - 6^{83}$ is divided by 4.

We will find r such that $0 \le r < 4$ and $x \equiv r \pmod{4}$. By CTR, this will be our answer.

By CER, CAM, and CP:

$$\begin{aligned} x &\equiv 1^{100}(-1) - 36 \cdot 6^{81} \pmod{4} \\ x &\equiv -1 \pmod{4} \\ &\equiv 3 \pmod{4} \end{aligned}$$

The answer is 3.

2) What is the last digit (units) of $x = 5^{32}3^{10} + 9^{22}$

The answer will be r such that $x \equiv r \pmod{10}$ and $0 \le r < 10$ (By (TR)).

By CER, CAM, and CP

$$\begin{aligned} x &\equiv (5^2)^{16}(3^2)^5 + (-1)^{22} \pmod{10} \\ &\equiv (5^2)^8(-1)^5 + 1 \pmod{10} \\ &\equiv (5^2)^4(-1) + 1 \\ &\equiv -5 + 1 \pmod{10} \\ &\equiv 6 \pmod{10} \end{aligned}$$

The answer is 6.

Proof of CISR

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

By DA,

$a = mq_a + r_a, \quad 0 \le r_a < m$
$b = mq_b + r_b, \quad 0 \le r_b < m$

Then, $a - b = m(q_a - q_b) + (r_a - r_b)$

where $-m < r_a - r_b < m$

Now we assume $r_a = r_b$.

Thus, $m|(a-b)$ by our equation for $a-b$. That is $a \equiv b \pmod{m}$.

Next, we assume $a \equiv b \pmod{m}$.

Then $mk = a - b$ for some $k \in \mathbb{Z}$.

Substituting and rearranging gives,

$m(k - q_a + q_b) = r_a - r_b$

So $m|(r_a - r_b)$ since $k - q_a + q_b \in \mathbb{Z}$. Thus $r_a - r_b = 0$ by our inequality for $r_a - r_b$. We get $r_a = r_b$, completing the proof.

<u>CTR</u>

For all a, b with $0 \leq b < m$, $a \equiv b \pmod{m}$ iff a has remainder b when divided by m.

$m|(a-b)$ if $a = mr + b$

<u>Divisibility Tests</u>

Let $n \geq 0$ be an integer. Then we can write.

$n = d_k 10^k + d_{k-1} 10^{k-1} + \ldots d_1 10 + d_0$ for digits $d_k, d_{k-1}, \ldots, d_1, d_0$

What about 3?

Since $10 \equiv 1 \pmod{3}$. $n \equiv d_k + d_{k-1} + \ldots + d_1 + d_0 \pmod{3}$

Thus, by CER

$n \equiv 0 \pmod{3}$ iff $d_k + d_{k-1} + \ldots + d_1 + d_0 \equiv 0 \pmod{3}$.

9?

$10 \equiv 1 \pmod{9}$ so we can deduce that n is divisibly by 9 iff the sum of its digits are divisible by n.

e.g. 4456217395

$4+4+5+6+2+1+7+3+9+5 = 46$. 46 is not divisible by 9, the number is not divisible by 9.

11?

8217993

$8 - 2 + 1 - 7 + 9 - 9 + 3 = 3$

$10 \equiv -1 \pmod{11}$

8.4 Linear Congruences

Let $m \in \mathbb{N}$.

Let $a, c \in \mathbb{Z}$ where $a \neq 0$.

Find all $x \in \mathbb{Z}$ such that

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

- Is there a solution?
- If so can we find one?
- If so can we find them all?

<u>Example</u>

Solve $4x \equiv 5 \pmod{8}$

$$\begin{aligned}
&\iff 8|(4x-5) \\
&\iff 8k = 4x - 5 \text{ for some } k \in \mathbb{Z} \\
&\iff 4x - 8k = 5 \text{ for some } k \in \mathbb{Z} \\
&\iff 4x = 8y = 5 \text{ for some } y \in \mathbb{Z}
\end{aligned}$$

Linear Diophantine $\implies gcd(4,8) = 4.\ 4 \nmid 5.\ \therefore$ no solution, $\therefore$ no $x-$values.

$5x \equiv 3 \pmod 7$

Rewrite

$$\begin{aligned} 5x + 7y = 3 &\implies x \in \{2 + 7n : n \in \mathbb{Z}\} \\ &gcd(5,7) = 1 \quad 1|3\checkmark \end{aligned}$$

Answer in congruence is $x \equiv 2 \pmod 7$.

By CTR, every integer is congruent to $\{0,1,2,3,4,5,6\}$.

Try all of them and see which one works.

By CER, CAM, if x_0 is a solution, $x \equiv x_0 \pmod 7$ are solutions.

GCD is the number of solutions in the set $\{0,1,2,\ldots\}$

$$\begin{aligned} 2x &\equiv 4 \pmod 6 \\ 2(0) &\not\equiv 4 \pmod 6 \\ &\vdots \\ 2(2) &\equiv 4 \pmod 6 \\ &\vdots \\ 2(5) &\equiv 4 \pmod 6 \end{aligned}$$

Complete solution is $x \equiv 2, 5 \pmod 6$.

Using LDE's we get $\{2 + 3n : n \in \mathbb{Z}\}$.

Complete solution is $x \equiv 2 \pmod 3$.

$x \equiv 2, 5 \pmod 6$ and $x \equiv 2 \pmod 4$ represent the exact same set of integers.

<u>Linear Congruence Theorem (LCT)</u>

Complete solution $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{d}}\}$ equivalently,

$$\{x \in \mathbb{Z} : x \equiv x_0, \underbrace{x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}}_{d \text{ number of solutions}}\}$$

Informally, LCT tells us there

- is one solution modulo $\frac{m}{d}$ or
- d solutions modulo m

Solve $9x \equiv 6 \pmod{15}$

$d = gcd(9,15) = 3, 3|6\checkmark$

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

8.5 Congruence Classes and Modular Arithmetic

<u>Definition</u>

Let $m \in \mathbb{N}$. Let $a \in \mathbb{Z}$.

The congruence class of a modulo m is

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

Example

Let $m = 5$

The congruence class of 3 modulo 5 is:

$$\begin{aligned}[3] &= \{x \in \mathbb{Z} : x \equiv 3 \pmod 5\} \\ &= \{\ldots, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\} \text{ infinite set of integers}\end{aligned}$$

- $[3]$ is an infinite set
- $[3] = [23] = [-7]$ (both subsets of each other)
- $[3]$ is our most common representative from this set because $0 \leq 3 \leq 5$

Operations

Let $m \in \mathbb{N}$. Let $a, b \in \mathbb{Z}$. We define

$$\begin{aligned}[a] + [b] &= [a + b] \\ [a][b] &= [ab]\end{aligned}$$

Examples ($m = 5$)

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Note

Addition is well-defined

$[8] + [31] = [39] = [4]$

$[-7] + [16] = [9] = [4]$

Multiplication is as well.

Definition

Let $m \in \mathbb{N}$. The integers modulo m are

$$\begin{aligned}\mathbb{Z}_m &= \{[0], [1], [2], \ldots, [m-1]\} \quad |\mathbb{Z}_m| = m \text{ finite} \\ &= \{[x] : x \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}a \equiv b \pmod m \iff m \mid (a - b) \iff \exists k \in \mathbb{Z}, a - b = km \iff \exists k \in \mathbb{Z}, a = km + b \\ \iff a \text{ and } b \text{ have the same remainder when divided by } m \iff [a] = [b] \text{ in } \mathbb{Z}_m\end{aligned}$$

Let $[a] = \mathbb{Z}_n$ where $m \in \mathbb{N}$.

$[0]$ is the additive identity $[a] + [0] = [a]$
$[1]$ is the multiplication identity $[a][1] = [a]$
$[-a]$ is the additive inverse of $[a] \implies [a] + [-a] = [0]$

Multiplicative inverse of $[a]$ (if exists) is an elem $[b]$ such that $[a][b] = [b][a] = [1]$ and we write $[b] = [a]^{-1}$.

Examples

In $\mathbb{Z}_{12}$ does $[5]^{-1}$ exist? Does $[6]^{-1}$ exist?

$[5][x] = [1]$

$[x] = [5]$ is a solution, so $[5]^{-1} = [5]$

$[6][x] = [1]$. Only 12 combinations, none where $6x \equiv 1 \pmod{12}$.

Modular Arithmetic Solution

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

The equation $[a][x] = [c]$ in $\mathbb{Z}_n$ has a solution iff $d|c$.

If $[x] = [x_0]$ is one solution, then there are d solutions given by,

$$\{[x_0], [x_0 + \frac{m}{d}], [x_0 + 2\frac{m}{d}], \ldots, [x_0 + (d-1)\frac{m}{d}]\}$$

Review

$\mathbb{Z}_{10}, [3] = [13] = [23] = [-17]$

In $\mathbb{Z}_{10}$, solve

1) $[12][x] + [3] = [8]$
$[2][x] = [5]$ has no solution.

2) $[15][x] + [7] = [12]$
$[5][x] = [5]$. $gcd(5, 10) = 5 \implies 5$ solutions. $\frac{10}{5} = 2$, spanned by $2 \downarrow$

$[1], [3], [5], [7], [9]$

3) $[9][x] + [1] = [8]$

$[9][x] = [7]$. $gcd(9, 10) = 1 \implies 1$ solution.

$x = 3, 3 \cdot 9 = 27, 27 - 7 = \underline{20}$.

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

Let $a \in \mathbb{Z}$ with $0 \leq a \leq m - 1$. $[a] \in \mathbb{Z}_m$ has a multiplicative inverse iff $gcd(a, m) = 1$. Multiplicative inverse is unique.

Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$)

For all prime numbers p and $[a] \in \mathbb{Z}_p$ have a unique multiplicative inverse.

8.6 Fermat's Little Theorem (FℓT)

Let p be prime. Let $a \in \mathbb{Z}$.

If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Examples

$4^6 \equiv 1 \pmod 7$ $\quad 39^6 \equiv 1 \pmod 7$

$13^2 \equiv 1 \pmod 7$ but not by FℓT.

Exercise

What is the remainder when 7^{92} is divided by 11?

Since 11 is prime and $11 \nmid 7$, $7^{10} \equiv 1 \pmod{11}$.

$$7^{92} \equiv (7^{10})^9 \cdot 7^2 \equiv 1^9 \cdot 7^2 \equiv 49 \equiv 5 \pmod{11}$$

By CAM, CER, CP. Thus, the remainder is 5.

Notes

We can write $a^{p-1} \equiv 1 \pmod p$ as $[a^{p-1}] = [1]$ in $\mathbb{Z}_p$. In this case $[a]^{-1} = [a^{p-2}]$

Idea of Proof of FℓT

Let $a = 4$ and $p = 7$.

$\{[4], [2 \cdot 4], [3 \cdot 4], [4 \cdot 4], [5 \cdot 4], [6 \cdot 4]\}$

$= \{[4], [1], [5], [2], [6], [3]\}$

No zero, all distinct.

Corollary to FℓT

Let p be prime. Let $a \in \mathbb{Z}$.

Then $a^p \equiv a \pmod p$

Proof

Let p be prime. Let $a \in \mathbb{Z}$. We will use cases.

When $p \nmid a$, by FℓT, $a^{p-1} \equiv 1 \pmod p$. Multiplying gives $a^p \equiv a \pmod p$ by CAM.

When $p|a$, $a \equiv 0 \pmod p$. Thus $a^p \equiv 0 \pmod p$ by CP. Thus $a^p \equiv a \pmod p$ by CER.

The statement is true in all cases. ■

Exercise

What is the remainder when $8^{(9^7)}$ is divided by 11.

$$\begin{aligned} 9^7 &\equiv -1 \pmod{10} \\ &\equiv 9 \pmod{10} \\ 8^{9^7} \equiv 8^{10q+r} &\equiv (8^{10})^q 8^r \equiv 8^r \pmod{11} \end{aligned}$$

Simultaneous Congruences Examples

Solve $x \equiv 2 \pmod{13}, x \equiv 17 \pmod{29}$. If moduli are coprime, always get one solution.

Rewrite the second statement as $x = 17 + 29k$ where $k \in \mathbb{Z}$.

Thus we want to find all k satisfying:

$$\begin{aligned} &17 + 29j \equiv 2 \pmod{13} \\ &\iff 29k \equiv 11 \pmod{13} \\ &\iff 3k \equiv 11 \pmod{13} \\ &\iff k \equiv 8 \pmod{13} \\ &\iff k = 8 + 13\ell \text{ for some } \ell \in \mathbb{Z} \end{aligned}$$

Sub to get

$$\begin{aligned} x &= 17 + 29(8 + 13\ell) \\ x &= 17 + 29 \cdot 8 + 29 \cdot 13\ell \\ x &= 249 + 377\ell \end{aligned}$$

The solution is $x \equiv 249 \pmod{377}$

8.7 Chinese Remainder Theorem

Suppose $gcd(m_1, m_2) = 1$ and $a_1, a_2 \in \mathbb{Z}$

There is a unique solution module m_1m_2 to the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

That is, once we have one solution $x = x_0$, CRT also tells us the full solution is $x \equiv x_0 \pmod{m_1m_2}$

Generalized CRT

If $m_1, m_2, \ldots, m_k \in \mathbb{N}$ and $gcd(m_i, m_j) = 1$ then for any integers there exists a solution to simultaneous congruences.

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

The complete solution is $n \equiv n_0 \pmod{m_1m_2\ldots m_k}$

Exercises

$x \equiv 4 \pmod 6, x \equiv 2 \pmod 8$.

Rewrite the second equation as $x = 2 + 8k$ where $k \in \mathbb{Z}$. Sub into the first equation to get

$$\begin{aligned} 2 + 8k &\equiv 4 \pmod 6 \\ 8k &\equiv 2 \pmod 6 \\ 2k &\equiv 2 \pmod 6 \end{aligned}$$

Since 1 is a solution, the full solution is $k \equiv 1 \pmod 3$ by LCT.

Rewrite as $k = 1 + 3\ell$ where $\ell \in \mathbb{Z}$. Sub to get $x = 2 + 8(1 + 3\ell), x = 10 + 24\ell$.

Final answer is $x \equiv 10 \pmod{24}$.

8.8 Splitting the Modulus

Let m_1 and m_2 be coprime positive integers. For any two integers x and a,

$$x \equiv a \pmod{m_1}, x \equiv a \pmod{m_2} \iff x \equiv a \pmod{m_1m_2}$$

Exercise

What is the units digit of $8^{(9^7)}$?

Rough

$$\begin{aligned} 8^{(9^7)} &\equiv r \pmod{10} \\ r &\equiv 8^{(9^7)} \pmod 2 \\ r &\equiv 8^{(9^7)} \pmod 5 \\ r &\equiv 0 \pmod 2 \\ 8^{(9^7)} &\equiv 3^{(9^7)} \pmod 5 \\ 9 &\equiv 1 \pmod 4 \\ \therefore 9^7 &\equiv 1 \pmod 4 \\ \therefore 9^7 &\equiv 4\ell + 1 \text{ for some } \ell \in \mathbb{Z} \end{aligned}$$

So we get

$$8^{(9^7)} \equiv 3^{4k+1} \equiv (3^4)^k \cdot 3 \equiv 1^k 3 \equiv 3 \pmod 5$$

To complete the problem, we solve

$$\begin{aligned} r &\equiv 0 \pmod{2} \\ r &\equiv 3 \pmod{5} \\ r &\equiv 8 \pmod{10} \end{aligned}$$

$8^{(9^7)} \equiv r \pmod{11}, 8^{10} \equiv 1 \pmod{11}$ by FℓT

9 The RSA Public-Key Encryption Scheme

Cool history lesson about William Tutte

Message $\rightarrow$ encrypt *to* transmit cipher *to* decrypt *to* message

Math functions (easy to encrypt), hard to decrypt (invert) without info.

RSA Scheme

Setup (Bob)

1. Randomly choose two large, distinct primes p and q and let $n = pq$
2. Select arbitrary integer e such that $gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$
3. Solve $ed \equiv 1 \pmod{(p-1)(q-1)}$ for an integer d where $1 < d < (p-1)(q-1)$
4. Publish the public key (e, n)
5. Keep the private key (d, n) secret, and the primes p and q

Encryption (Alice does the following to send a message as ciphertext to Bob)

1. Obtain a copy of Bob's public key (e, n)
2. Construct the message M, an integer such that $0 \leq M < n$
3. Encrypt M as the ciphertext C, given by $C \equiv M^e \pmod{n}$ where $0 \leq C < n$
4. Send C to Bob

Decryption (Bob does the following to decrypt)

1. Use the private key (d, n) to decrypt the ciphertext C as the received message R, given by $R \equiv C^d \pmod{n}$ where $0 \leq R < n$
2. Claim: $R = M$

Setup

$p = 2, q = 11, n = 22$

$\phi(n) = 10(1 \times 10)$

$e = 3 \quad gcd(3, 10) = 1$

$3d \equiv 1 \pmod{10} \leftarrow ed \equiv 1 \pmod{\phi(n)}$ where $0 < d < \phi(n)$. $d = 7$.

Public key $(e, n) \implies (3, 22)$.

Private key $(d, n) \implies (7, 22)$.

Encryption

Generate message M where $0 \leq M < n$

$M = 8$

$$\begin{aligned} C &\equiv 8^3 \pmod{22} \quad 0 \leq C < n \\ &\equiv (-2) \cdot 8 \pmod{22} \\ &\equiv 6 \pmod{22} \end{aligned}$$

Decryption

$$\begin{aligned} R &\equiv 6^7 \pmod{22} \quad 0 \le R < n \\ &\equiv (36)^3 6 \pmod{22} \\ &\equiv 14^3 \cdot 6 \pmod{22} \\ &\equiv 84 \cdot 2^2 \cdot 7^2 \pmod{22} \\ &\equiv (-4) \cdot 6 \cdot 7 \pmod{22} \\ &\equiv 8 \pmod{22} \end{aligned}$$

8 is the original message that Alice wanted to send.

Exercise

Let $p = 11, q = 13, e = 23$

- public key?
- private key?
- if $M = 13$ what is C?

Public key: $(c, n) \to (23, 143)$

Private key: solve $23d \equiv 1 \pmod{10 \cdot 12}$, $d \equiv 47$

$$\begin{aligned} C &\equiv 13^{23} \pmod{143} \\ &\equiv 13^{16} 13^4 13^2 13^1 \pmod{143} \\ &\quad 13^2 \equiv 169 \equiv 26 \pmod{123} \\ &\quad 13^4 \equiv 26^2 \equiv \dots \\ &\quad \vdots \end{aligned}$$

Square and multiply, then use SMT if you know p and q.

10 Complex Numbers

10.1 Standard Form

Complex Numbers

$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$

Examples

- $2 + 3i \leftarrow$ standard form $\quad \mathbb{C} = \{x + yi : x, y \in \mathbb{R}\}$
- $\frac{1}{2} + (-\sqrt{2})i$
- $0 + 0i = 0$
- $1 + 1i = 1 + i$

For $z = x + yi \in \mathbb{C}$, we call x the real part and y the imaginary part.

$Re(z)$ and $Im(z)$

$z = w$ means $Re(z) = Re(w)$ and $Im(z) = Im(w)$

$z = 7 + 0i = 7 \implies \mathbb{R} \subsetneq \mathbb{C} \implies z$ is purely real

$z = 7i \implies$ purely imaginary

Arithmetic

Addition:

$(a+bi)+(c+di)=(a+c)+(b+d)i$
$(2+3i)+(1+2i)=3+5i$

Multiplication:

$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i$
$(2+3i)\cdot(5+4i)=((2\cdot 5)-(3\cdot 4))+((2\cdot 4)+(3\cdot 5))i=-2+23i$
$(0+1i)\cdot(0+1i)=-1+0i$
$i^2=-1$

Informally we can treat elements of $\mathbb{C}$ as "normal" algebraic expressions where $i^2=-1$ and when we do that "everything works".

0 is the additive identity in $\mathbb{C}$.
$-z$ is the additive inverse of z in $\mathbb{C}$.

Subtraction

Let $w,z\in\mathbb{C}$. We define

$z-w=z+(-1+0i)w$

1 is the multiplicative identity in $\mathbb{C}$.
$\frac{a-bi}{a^2+b^2}$ is the unique multiplicative inverse of $a+bi\neq 0$

Division

$$\begin{aligned}\frac{3+4i}{1+2i}&=(3+4i)(1+2i)^{-1}\\&=(3+4i)(\frac{1-2i}{5})\\&=(3+4i)(\frac{1}{5}-\frac{2}{5}i)\\&=(\frac{3}{5}+\frac{8}{5})-\frac{2}{5}i\\&=\frac{11}{5}-\frac{2}{5}i\end{aligned}$$

Why is $(1+2i)^{-1}=\frac{1-2i}{5}$.

$$\begin{aligned}&\text{Let } (1+2i)^{-1}=x+yi \text{ where } x,y\in\mathbb{R}\\&\text{Then } (1+2i)(x+yi)=1+0i\\&=(x-2y)+(y+2x)i=1+0i\\&x-2y=1\\&\underbrace{\underbrace{y+2x=0}\\x=\frac{1}{5},y=-\frac{2}{5}}_{\text{multiplicative inverse}}\end{aligned}$$

Alternatively

$$\begin{aligned}\frac{3+4i}{1+2i}\cdot\frac{1-2i}{1-2i}&=\frac{(3+4i)(1-2i)}{5}\\&=11-2i\\&=\frac{11}{5}-\frac{2}{5}i\end{aligned}$$

Properties of Complex Arithmetic (PCA)

Let $u, v, z \in \mathbb{C}$ with $z = x + yi$

$$
\begin{aligned}
&(u+v)+z = u+(v+z) \\
&u+v = v+u \\
&z+0 = z \text{ where } 0 = 0+0i \\
&z+(-z) = 0 \text{ where } -z = -x-yi \\
&(uv)w = u(vw) \\
&z \cdot 1 = z \text{ where } 1 = 1+0i \\
&z \neq 0 \implies zz^{-1} = 1 \text{ where } z^{-1} = \frac{x-xi}{x^2+y^2} \\
&z(u+v) = zu+zv
\end{aligned}
$$

Proof that multiplicative inverses are unique in $\mathbb{C}$.

Let $z \in \mathbb{C}$ where $z \neq 0$.

Suppose $u \cdot z = 1$ and $v \cdot z = 1$ for $u, v \in \mathbb{C}$.

Then $uz = vz$

Thus

$$
\begin{aligned}
&(uz)u = (vz)u \\
\implies &u(zu) = v(zu) \text{ by PCA 5} \\
&u = v \quad \blacksquare
\end{aligned}
$$

10.2 Conjugate and Modulus

Warm-up

$\frac{(1-2i)-(3+4i)}{5-6i}$

$= \frac{-2-6i}{5-6i} \cdot \frac{5+6i}{5+6i}$

$i^{2022} = -1$ since $(i^2)^{1011}$

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

$$
\begin{aligned}
&6r^3 + (1+3\sqrt{2}i)r^2 - (11-2\sqrt{2}i)r - 6 = 0+0i \\
&6r^3 + r^2 - 11r - 6 = 0 \quad \text{a} \\
&3\sqrt{2}r^2 + 2\sqrt{2}r = 0 \qquad \text{b} \\
&\text{b} \implies \underbrace{r=0}_{\neg\checkmark}, \underbrace{r=-\frac{2}{3}}_{\checkmark}
\end{aligned}
$$

Definition

Let $z = a + bi$ be a complex number in standard form

The complex conjugate of z is $\overline{z} = a - bi$

Examples

$5+6i = 5-6i \quad \overline{5-6i} = 5+6i$

Properties of Complex Conjugate (PCJ)

Let $z, w \in \mathbb{C}$. Then,

1. $\overline{\overline{z}} = z$
2. $\overline{z+w} = \overline{z} + \overline{w}$

3. z + $\overline{z} = 2Re(z)$; $\quad z - \overline{z} = 2Im(z)i$
4. $\overline{zw} = \overline{z} \cdot \overline{w}$
5. $z \neq 0 \implies \overline{z^{-1}} = \overline{z}^{-1}$

$1-4$ can be proved by using standard form and showing $LHS = RHS$.

Proof of 5.

Suppose $z \in \mathbb{C}$ where $z \neq 0$.

Therefore z^{-1} exists and $zz^{-1} = 1$ by PCA.

We get $\overline{zz^{-1}} = \overline{1}$.

Thus $\overline{z}\overline{z^{-1}} = 1$. That is, $\overline{z^{-1}} = \overline{z}^{-1}$

<u>Exercise</u>

Solve $z^2 = i\overline{z}$

Rough work

$$\begin{aligned}(a+bi)^2 &= i(a-bi)\\ a^2 - b^2 + 2abi &= b + ia\\ a^2 - b^2 &= b\\ 2ab &= a\end{aligned}$$

When $a = 0, b = 0, b = i$.

When $a \neq 0, b = \frac{1}{2}, a = \frac{\sqrt{3}}{2}$, or, $a = -\frac{\sqrt{3}}{2}, b = \frac{1}{2}$.

Thus there are 4 solutions.

<u>Modulus</u>

Let $z = x + yi \in \mathbb{C}$.

The modulus of z is $|x + yi| = \sqrt{x^2 + y^2}$.

<u>Examples</u>

$|5 + 6i| = \sqrt{5^2 + 6^2} = \sqrt{61}$
$|5 - 6i| = \sqrt{61}$
$|135| = 135$
$|-135| = 135$

<u>Properties of Modulus</u>

$|z| = 0$ iff $z = 0$
$|\overline{z}| = |z|$
$z \cdot \overline{z} = |z|^2$
$|zw| = |z||w|$
if $z \neq 0$, then $|z^{-1}| = |z|^{-1}$

Proof of the fourth statement above.

Let $z, w \in \mathbb{C}$.

Consider

$$\begin{aligned}|zw|^2 &= (zw)(\overline{zw})\\ &= zw(\overline{z}\overline{w})\\ &= (z\overline{z})(w\overline{w})\\ &= |z|^2|w|^2\\ &= (|z||w|)^2\end{aligned}$$

Since the modulus of every complex number is a non-negative real number, we get

$$|zw| = |z||w| \quad \blacksquare$$

10.3 Complex Plane and Polar Form

Complex Plane

Imaginary axis is $y-$axis, real axis is $x-$axis.

$\overline{z}$ is the reflection of z in the real axis.

$|z|$ is the distance from z to the origin ($\sqrt{x^2+y^2}$)

$z+w$ is considered to be vector addition.

Polar Form

Standard form: $3+3i$
Cartesian Coordinates: $(3,3)$
Polar Coordinates: $(3\sqrt{2}, \frac{\pi}{4})$
Polar Form: $3\sqrt{2}cis(\frac{\pi}{4}) \downarrow$

$3\sqrt{2}(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4}))$ = Standard Form

Definition

The polar form of a complex number z is

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

where $r = |z|$ and θ (an argument) is an angle measured counter-clockwise from the real axis.

Note

Polar form is not unique (add multiples of 2π).

Examples

Convert to standard form $cis(\frac{\pi}{2})$
$r = 1, |z| = 1$
$= i$

$2cis(\frac{3\pi}{4})$
$r = 2, |z| = 2$
$= -\sqrt{2} + \sqrt{2}i$

Convert from standard form

$\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$

$(r,\theta) = (1, (\sqrt{\frac{1}{\sqrt{2}}^2 + \frac{1}{\sqrt{2}}^2}))$
$\theta = \frac{7\pi}{4}$
$= cis(\frac{7\pi}{4})$

$\sqrt{6} + \sqrt{2}i$
$r = \sqrt{8} = 2\sqrt{2}$
$\cos\theta = \frac{\sqrt{6}}{2\sqrt{2}}, \sin\theta = \frac{\sqrt{2}}{2\sqrt{2}}$
$\cos\theta = \frac{\sqrt{6}}{2\sqrt{2}}, \sin\theta = \frac{\sqrt{2}}{2\sqrt{2}}$
$= 2\sqrt{2}cis(\frac{\pi}{6})$

$cis(\frac{15\pi}{6})$ in standard form.
$cis(\frac{15\pi}{6}) = cis(\frac{3\pi}{6}) = \frac{\pi}{2} = 1(0+1i) = i$

Write $-3\sqrt{2} + 3\sqrt{6}i$ in polar form.

$r^2 = 72, r = 6\sqrt{2}$.

$\cos\theta = \frac{-3\sqrt{2}}{6\sqrt{2}} = -\frac{1}{2}$
$\sin\theta = \frac{3\sqrt{6}}{6\sqrt{2}} = \frac{\sqrt{3}}{2}$

Thus $\theta = \frac{2\pi}{3}$

$6\sqrt{2}cis(\frac{2\pi}{3})$

Polar Multiplication of Complex Numbers

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

10.4 De Moivre's Theorem (DMT)

For all $n \in \mathbb{Z}$ and $\theta \in \mathbb{R}$

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

Proof of Polar Multiplication in $\mathbb{C}$ (PM$\mathbb{C}$)

Multiply in standard form and use trig identities.

Proof of DMT

When $n \geq 0$, this is induction
When $n < 0$, we can translate to the previous case.

Using rules for $cos(-x)$ and $sin(-x)$.

DMT Examples

Write $(cis\frac{3\pi}{4})^{-100}$ in standard form.

$$\begin{aligned} = cis(\frac{-300\pi}{4}) &= cis(-75\pi) \\ &= cis(\pi) \\ &= -1 \end{aligned}$$

Write $(\sqrt{3} - i)^{10}$ in standard form

$$\begin{aligned} (\sqrt{3} - i)^{10} &= (2cis\frac{11\pi}{6})^{10} \\ &= 2^{10}cis(\frac{55\pi}{3}) \\ &= 2^{10}cis(\frac{1}{2} + \frac{\sqrt{3}}{2}i) \\ &= 512 + 512\sqrt{3}i \end{aligned}$$

Note

Multiplying by i corresponds to rotating $90°$

10.5 Complex n-th Roots Theorem (CNRT)

N^{th} Root Examples

Solve $z^6 = -64$
Let $z = rcis\theta$ in polar form.

In polar form, $-64 = 64cis(\pi)$

Equating gives that

$$(rcis\theta)^6 = 64cis(\pi)$$
$$\implies r^6 cis6\theta = 64cis(\pi)$$

Since $r \in \mathbb{R}$ and $r \geq 0$, we get $r = 2$.

Also $\theta = \frac{\pi+2\pi k}{6}$ where $k \in \mathbb{Z}$.

We get $2cis\frac{\pi}{6}, 2cis\frac{3\pi}{6}, 2cis\frac{5\pi}{6}, 2cis\frac{7\pi}{6}, 2cis\frac{9\pi}{6}, 2cis\frac{11\pi}{6}$

Roots of Unity

Solve $z^8 = 1$

$i, \frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}, -1, \frac{-1}{\sqrt{2}} - \frac{i}{\sqrt{2}}, -i, \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}, 1, \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$

10.6 Square Roots and the Quadratic Formula

Quadratic Formula

For all $a, b, c \in \mathbb{C}, a \neq 0$, the solutions to $az^2 + bz + c = 0$ are,

$$\frac{-b \pm w}{2a} \quad \text{where } w^2 = b^2 - 4ac$$

11 Polynomials

11.1 Introduction

Fields

All non-zero numbers have a multiplicative inverse.

$ab = 0$ iff $a = 0$ or $b = 0$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ when p is prime.

11.2 Arithmetic of Polynomials

Polynomials

No negative exponents, no fractional exponents.

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_o \quad \text{is a polynomial over } \mathbb{F}.$$

when $n \geq 0 \in \mathbb{Z}, a_n, a_{n-1} \in \mathbb{F}$.

Terminology/Notation

$iz^3 + (2 + 3i)z + \pi, z$ is indeterminate.

- complex polynomial (not real)
- degree is 3
- cubic polynomial
- in $\mathbb{C}[z]$
- $f(x) = g(x)$ means corresponding coefficients are equal
- polynomial equation (if there was an equal sign). Solution to that is a root.

Degree of a Product

$$deg f(x)g(x) = deg f(x) + deg g(x)$$

Division Algorithm for Polynomials

If $f(x), g(x) \in \mathbb{F}[x]$, then $\exists q(x), p(x) \in \mathbb{F}[z]$ such that $f(x) = q(x)g(x) + r(x)$ where $r(x)$ is the 0 polynomial or $deg(r(x)) < deg(g(x))$

If r is 0, $g(x)|f(x)$

Polynomial Arithmetic

Let $g(z) = z + (i+1)$ and $q(z) = iz^2 + 4z - (1-i)$. Compute $q(z)g(z)$.

Find the q and r where

$f(z) = iz^3 + (i+3)z^2 + (5i+3)z + (2i-2)$
$g(z) = z + (i+1)$

$$
\begin{array}{r}
iz^2 + 4z + (i-1) \\
z + (1+i)\overline{\smash{)}\, iz^3 + (i+3)z^2 + (5i+3)z + (2i-2)} \\
-\ \ (iz^3 + (-1+i)z^2) \\
\hline
4z^2 + (5i+3) \\
-\ \ (4z^2 + (4+4i)z) \\
\hline
\vdots \\
2i
\end{array}
$$

Yields $q(z) = iz^2 + yz + (i-1)$
$r(z) = 2i$

Check

$f(z) = g(z)q(z) - r(z)$

Exercise 3

Prove $(x-1) \nmid (x^2+1)$

BWOC suppose $(x-1)|(x^2+1)$ in $\mathbb{R}[x]$.

Then by DP we have

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

for some $a, b \in \mathbb{R}$ and $a \neq 0$.

If they are equal, coefficients must be the same.

Comparing coefficients:

$1 = a, 0 = b - a, 1 = -b$

Second and third above $\implies b - a = -2$

11.3 Roots of Complex Polynomials and the Fundamental Theorem of Algebra

Remainder Theorem (RT)

For all fields $\mathbb{F}$, all polynomials $f(x) \in \mathbb{F}[x]$, and all $c \in \mathbb{F}$, the remainder polynomial when $f(x)$ is divided by $x - c$ is the constant polynomial $f(c)$.

Proof

Let $f(x) \in \mathbb{F}[x]$ where $\mathbb{F}$ is a field. Let $c \in \mathbb{F}$.

By DAP,

$f(x) = r(x-c)q(x) + r(x)$ for unique $g(x), r(x) \in \mathbb{F}[x]$ where $r(x)$ is the zero polynomial or $deg(r(x)) = 0$.

Regardless, $r(x) = r_0$ for some $r_0 \in \mathbb{F}$.

Alas, $f(x) = (c - c)q(c) + r_0 = r_0$

Takeaway

Finding roots corresponds to finding linear factors.

Fundamental Theorem of Algebra (FTA)

Every complex polynomial of complex degrees has a root.

Complex Polynomials of Degree n Have n Roots (CPN) Proof Discovery

Induction on n degrees.

Base Case

$az + b, a \neq 0$

$a(z - (-\frac{b}{a}))$

If $f(z)$ has degree $k + 1$

By FTA, $f(z)$ has a root. Name it c_{k+1}.

Then $f(z) = g(z)(z - c_{k+1})$

Multiplicity

The multiplicity of root c of a polynomial $f(x)$ is the largest possible integer k such that $(x - c)^k$ is a factor of $F(x)$.

Reducible and Irreducible Polynomial

Polynomial in $F[x]$ of positive degree is a reducible polynomial in $F[x]$ when it can be written as the product of 2 polynomials of positive degree.

Otherwise we say that the polynomial is irreducible in $P[x]$.

$x^2 + 1$ is irreducible in $R[x]$

BWOC suppose $x^2 + 1$ is the product of $(ax + b)(cx + d)$ where $a, b, c, d \in \mathbb{R}$. Then compare coefficients.

Prove that $x^4 + 2x^2 + 1$ has no roots in $\mathbb{R}$ but is reducible.

$x^4 + 2x^2 + 1$

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

Prove factors don't have roots to prove no roots (lots of ways to show no roots)

Write $x^2 + 1$ as a product of irreducible factors in $\mathbb{C}[x]$

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

Write $x^4 + 2x + 1$ as a product of irreducible factors

$$x^4 + 2x^2 + 1 = (x - i)^2(x + i)^2$$

Factor $ix^3 + (3 - i)x^2 + (-3 - 2i)x - 6$ as a product of linear factors.

Hint -1 is a root

$$\begin{array}{r|l} & ix^2 + (3-2i)x - 6 \\ \hline x+1 & ix^3 + (3-i)x^2 + (-3-2i)x - 6 \\ & -\ (ix^3 + ix^2) \\ \hline & (3-2i)x^2 + (-3-2i)x \\ & -\ (3-2i)x^2 + (3-2i)x \\ \hline & \vdots \\ & 0 \end{array}$$

The roots of this quotient are $\frac{(-3-2i)\pm w}{2i}$ where $w^2 = (3-2i)^2 + 24i$ by QF.

Let $wa + bi$ where $a, b \in \mathbb{R}$

Then $a^2 - b^2 = 5, 2ab = 12, a = 3, b = 2$

So the roots are $\frac{(-3-2i)\pm 3+2i}{2i}$.

That is

$$\begin{aligned} &\frac{(-3-2i)+3+2i}{2i} \\ &= \frac{4i}{2i} \\ &= 2 \end{aligned}$$

and

$$\begin{aligned} &\frac{(-3-2i)-3+2i}{2i} \\ &= \frac{-6}{2i} \\ &= 3i \end{aligned}$$

Roots are $-1, 2, 3$

Hence the final answer is

$$i(x+1)(x-2)(x-3i)$$

Write $x^4 - 5x^3 + 16x^2 - 9x - 13$ as a product of irreducible polynomials given that $2-3i$ is a root.

11.4 Real Polynomials and Conjugate Roots Theorem

$f(x)$, if $z \in \mathbb{C}$ and $f(z) = 0$, then $f(\overline{z}) = 0$. Depends on the fields.

By CJRT, $2+3i$ is also a root. Thus, $(x-(2-3i))(x-(2+3i))$ is a factor.

This quadratic factor equals, $x^2 - 4x + 13$

Now we use long division to yield, $x^2 - x - 1$

By QF, the roots of $x^2 - x - 1$ are $\frac{1\pm\sqrt{5}}{2}$

Therefore,

$$(x-(2-3i))(x-(2+3i))(x-\frac{1+\sqrt{5}}{2})(x-\frac{1-\sqrt{5}}{2}) \text{ over } \mathbb{C}.$$

or

$$x^2-4x+13)(x-\frac{1+\sqrt{5}}{2})(x+\frac{1-\sqrt{5}}{2}) \in \mathbb{R}$$

or

$$(x^2-4x+13)(x^2-x-1) \in \mathbb{Q}$$

<u>Real Quadratic Factors</u>

If $f(c) = 0$ for some $c \in \mathbb{C}$ with $Im(C) \neq 0$, $\exists$ real quadratic irreducible polynomial $g(x)$ and real polynomial $q(x)$ such that $f(x) = g(x)q(x)$

<u>Real Factors of Real Polynomials</u>

Every non-constant with real coefficients can be written as a product of real linear and quadratic factors.

Proof of CJRT

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Where $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{R}$.

Let $z \in \mathbb{C}$ and assume $f(z) = 0$

Now we get,

$$\begin{aligned} f(\overline{z}) &= a_n(\overline{z})^n + a_{n-1}(\overline{z})^{n-1} + \ldots + a_1\overline{z} + a_0 \\ &= a_n(\overline{z^n}) + a_{n-1}(\overline{z^{n-1}}) + \ldots + a_1\overline{z} + a_0 \text{ by PCJ} \\ &= \overline{a_n}(\overline{z^n}) + \overline{a_{n-1}}(\overline{z^{n-1}}) + \overline{a_1 z} + \overline{a_0} \\ &= \overline{a_n z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0} \text{ by PCJ} \\ &= \overline{0} = 0 \quad \blacksquare \end{aligned}$$