Jan 7, 2020

Sets and statements (1.2 - 1.4)

A set is a collection of distinct objects. An object in a set is called an element of the set.

Ex. Natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$

Integers $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2 \ldots\}$

Rational numbers $\mathbb{Q}$ = set of all $\frac{a}{b}$ where a & b are integers, $b \neq 0$.

Real numbers $\mathbb{R}$

More examples

$\{\emptyset, \square\}$ .... $\{1, \{2, 3\}\}$

Empty set $\emptyset$ has no elements (of all)

Notation if x is an element of a set S, then we have $x \in S$, otherwise, we write $x \notin S$

Ex. $\pi \in \mathbb{R}$, $\pi \notin \mathbb{Q}$ $\quad \emptyset \notin \emptyset$

$2 \notin \{1, \{2, 3\}\}$ $\quad \emptyset \neq \{\emptyset\}$

$\{2, 3\} \in \{1, \{2, 3\}\}$

Statements

A statement is a sentence that is either true or false.

Ex. (a) 25 is a perfect square TRUE

(b) $4 > 7$ False

(c) Zack has a hedgedog named quantia. True.

If A is a statement, we define $\neg A$ to be the statement that asserts the opposite of A.

(we can call $\neg A$ the negation of A)

Let negate the statements in (a) (b) (c)

(a) 25 is not a perfect square (False)

(b) $4 \leq 7$ (true)

(c) zack doesn't have a hedgedog named quantia False

Remark: If A is true, then $\neg A$ is false (and vice versa) This means that $\neg(\neg A)$ is true exactly when A is true

We therefore say that A and $\neg(\neg A)$ are logically equivalent and write $A \equiv \neg(\neg A)$

Ex. Are these statements?

(a) " Is it a perfect square?' No

(b) $x^2 - 2x + 1 = 0$ No.

part (b) is what we can call an open sentence: a sentence $P(x)$ with a variable, where the truth of $P(x)$ depends on the variable.

We can turn an open sentence into a statement by quantifying it!

We need a domain: a set containing possible value of x.

We need a quantifier.

2 options

Universal quantifier.

$\forall$ "for all", "for every"

Existential quantifier:

$\exists$ "there exists" "there is"

Lets quantify $x^2-2x+1=0$

$\forall x \in \mathbb{R},\ x^2-2x+1=0$

" For every real number x, $x^2-2x+1=0$" FALSE

or. $\exists x \in \mathbb{R},\ x^2-2x+1=0$

" There exists a real number x such that $x^2-2x+1=0$" TRUE because it works for $x=1$

Exercise consider the open sentence $P(m): \frac{m-9}{2m+4}=5$ and the following quantifications.

a) $\exists m \in \mathbb{Z}\ \frac{m-9}{2m+4}=5$

b) $\exists m \in \mathbb{Q}\ \frac{m-9}{2m+4}=5$

(a) is false, then $m-9=5(2m+4)=10m+20$ $m=-\frac{29}{9}$ (no integer)

(b) is true, $-\frac{29}{9}$ is a rational number solves the equation.

Moral: The truth of a statement depends on the domain & quantifier

Exercise: Write each statement symbolically with the proper quantifier

(a) 64 is a perfect square

(b) $y=\sin x-\cos x$ has no x-intercept. $\exists x \in \mathbb{Z},\ y=\sin x-\cos x$ has no intercept

(c) There is an element of the empty set that squares to 3

Solution:

(a) $\exists k \in \mathbb{Z},\ k^2=64$ T

(b) $\forall x \in \mathbb{R},\ \sin x-\cos x \neq 0$ F

(c) $\exists x \in \emptyset,\ x^2=3$ F (Vacuously False)

Another example

$\forall x \in \emptyset,\ x^2=3$

↳ If this were false, then there is some $x \in \emptyset$ such that $x^2 \neq 3$

Therefore the statement is (vacuously) true.

In general,

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

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

Now, lets try to negate statements a & b

First do this in English and then in symbols

(a) 64 is not a perfect square $\forall k \in \mathbb{Z},\ k^2 \neq 64$

(b) $y=\sin x-\cos x$ has an x-intercept $\exists x \in \mathbb{R},\ \sin x-\cos x=0$

Multiple Quantifiers

Ex: (1) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$ False

(2) $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$ True

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

(4) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$ False

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

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

Shorthand: We sometimes write $\forall x \in S, \forall y \in S$, as $\forall x, y \in S$ and $\exists x \in S, \exists y \in S$, as $\exists x, y \in S$

Truth tables

let A, B, C are statements

We can build more complicated statements and use a truth table to decide if they are true/false

A	$\neg A$
T	F
F	T

Definition: We define A and B (written $A \wedge B$) by the following truth table

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

$A \wedge B$ is called the conjunction of A and B

We also define A or B (written $A \vee B$) by the following truth table

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

Note $A \vee B$ is true even if both A and B are true

Exercise: Write down the truth table for $\neg(A \wedge B)$ and $(\neg A) \vee (\neg B)$

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

De Morgan's Law (DML)

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

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

other law

Commutative laws

$A \wedge B \equiv B \wedge A$

$A \vee B \equiv B \vee A$

Associate Laws

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

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

Distributive law

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

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

Example: show that $\neg(\neg A) \wedge (B \vee \neg C)) \equiv (A \vee \neg B) \wedge (A \vee C)$

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

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

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

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

Implication

We will consider statements of the form "If A, then B"

Ex: If you study, then you will pass the exam.

Hypothesis: you study

Conclusion: you pass the exam

* This implication says nothing about what happens when you don't study.

The only way this implication can be false is if you study (hypothesis is true) and you don't pass the exam.

Def": If A and B are statements, we define the statement if A then B (written $A \Rightarrow B$) by the following truth table.

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

Ex: True or false?

1. If $n=2$, then $n^2=4$ (True)
2. $\forall x \in \mathbb{R}$, $x>3 \Rightarrow x^2>9$ (True)
3. $\forall x \in \mathbb{R}$, $x>3 \Rightarrow x^2>16$ (False)

then hypothesis is true, but $x^2=16$ so $x^2>16$, Thus the conclusion is false.

4. If $1=2$, the $\pi+e$ is rational

(True: if the hypothesis is false, the implication is true),

Example: Given statements A and B, write the truth table for $A \Rightarrow B$ $(\neg A) \vee B$

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

Thus, $A \Rightarrow B, (\neg A) \vee B$

We showed that $A \Rightarrow B \equiv (\neg A) \vee B$ hence $(\neg A \Rightarrow B) \equiv A \wedge (\neg B)$

Write down

(a) its negation $\exists n \in \mathbb{Z},\ n=2 \wedge n^2 \neq 4$

(b) the same statement with the implication replaced by

(ii) its converse $n^2=4 \Rightarrow n=2$

(iii) its contrapositive $n^2 \neq 4 \Rightarrow n \neq 2$

Given an implication $A \Rightarrow B$ we define its converse by $B \Rightarrow A$ and we define its contrapositive by $(\neg B) \Rightarrow (\neg A)$

If and only if

Given statement A and B, we define $A \Leftrightarrow B$ (A if and only if B) by

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

Remark: $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

Note: Sometimes we write A iff B instead of $A \Leftrightarrow B$

Ex.

(a) $\forall n \in \mathbb{Z},\ n=2 \Leftrightarrow n^2=4$ FALSE

(b) $\forall n \in \mathbb{Z},\ |n|=2 \Leftrightarrow n^2=4$ TRUE

Proving $\forall$ statements. Chapter 3

Proposition: a statement we will prove

Theorem: Big/important proposition

Lemma: "Helper" proposition

Collary - proposition that follows immediately after a theorem.

§3-1, Proving universally quantified statements

How can prove $\forall x \in S, P(x)$?

Strategy

1. Let $x \in S$, be arbitrary
2. Verify $P(x)$ for this arbitrary x
3. Conclude that since x was arbitrary, $P(x)$ holds $\forall x \in S$

Ex. For all real numbers x, $x^2+9 \geq 6x$

Rough Work:

x - real number $\quad x^2+9 \geq 6x$

$x^2-6x+9 \geq 0$

$(x-3)^2 \geq 0$

Proof: let x be arbitrary real number. since $x-3$ is a real number, $(x-3)^2 \geq 0$

That is, $x^2-6x+9 \geq 0$

by adding $6x$ to both sides, we have $x^2+9 \geq 6x$

Since x was arbitrary, $x^2+9 \geq 6x$ is true for all real number x

1. proof is clearly written
2. uses English words
3. never assumed what would wanted to prove.

Ex: For all real numbers x, y $x^4 + x^2y + y^2 \geq 5x^2y - 3y^2$

Let x, y be arbitrary real numbers, since $x^2 - 2y$ is a real number, $(x^2-2y)^2 \geq 0$

That is, $x^4 - 4x^2y + 4y^2 \geq 0$

by adding $5x^2y$ to each side, $x^4 + x^2y + y^2 \geq 5x^2y - 3y^2$

since x, y was arbitrary, $x^4 + x^2y + y^2 \geq 5x^2y - 3y^2$ is true for all real # x.

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

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

Why can't we assume what we're trying to prove?

Ex. prove $1 = -1$

Proof: starting with $1 = -1$ square both, solves to get $(1)^2 = (-1)^2$ Thus, $1 = 1$ true.

Ex. prove that for all real numbers x and y, $\max\{x, y\} = \frac{x+y+|x-y|}{2}$

Rough work: $x, y \in \mathbb{R}$

Case I: $x \geq y$

$\max\{x, y\} = x$ and $x - y \geq 0$ so $|x-y| = x-y$.

$$\frac{x+y+|x-y|}{2} = \frac{x+y+(x-y)}{2}$$

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

Case II $x < y$

$\max\{x, y\} = y$ and $x - y < 0$, so $|x-y| = y-x$

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

$$= y$$

Proof: let x, y be arbitrary real numbers, we will consider two cases:

Case I: assume $x \geq y$, we then have that $\max\{x, y\} = x$,

Furthermore, since $x - y \geq 0$, we have $|x-y| = x-y$ and hence,

$$\frac{x+y+|x-y|}{2} = \frac{x+y+(x-y)}{2}$$

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

$$= x$$

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

Case II: assume $x < y$, $\max\{x, y\} = y$, Moreover, since $x - y < 0$, we have $|x-y| = -(x-y)$

Hence, $\frac{x+y+|x-y|}{2} = \frac{x+y-(x-y)}{2}$

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

$$= y$$

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

Thus, the equation is true in all cases, and since x and y were arbitrary, it holds for all $x, y \in \mathbb{R}$

* If you decide to use cases, make sure they cover all possible values in the domain

Exercise: Prove that for all real numbers x, $|x-3| + 2|x+2| \geq 5$

Ex: Disprove the following: For all real number x $(x-1)^2 > 0$

To disprove $\forall x \in S, P(x)$ prove its negation $\exists x \in S, \neg P(x)$. In our case, we prove $\exists x \in \mathbb{R}, (x-1)^2 \leq 0$

Proof: $x = 1$ is a real number and $(x-1)^2 = 0^2 = 0$

Thus, $(x-1)^2 \leq 0$

§3.2 Proving Existentially Quantified Statements

To prove $\exists x \in S\ P(x)$, you only need one example of $x \in S$ satisfying $P(x)$

Ex. Prove that there exists an integer k such that

$$\ln(19k+57) = \ln(k^2-15)$$

$$k^2 - 19k - 20 = 0$$

$$(k+1)(k-20) = 0$$

Proof: consider the integer $k = 20$, we have

$$\ln(19k+57) = \ln(19(20)+57)$$

$$= \ln(385)$$

$$\ln(k^2-15) = \ln(20^2-15)$$

$$= \ln(385)$$

$$\ln(385) = \ln(385)$$

Since $\ln(19k+57) = \ln(k^2-15)$, the proof is complete.

Definition:
Let m and n be integers, we say that m divides n and (write $m|n$) if there is an integer k such that $n = mk$

Ex: $7|56$ because $56 = 7 \cdot 8$

$7|(-56)$ because $-56 = 7(-8)$

$56 \nmid 7$ $7 = 56k$ No!!

$2 \nmid 3$

Given $a \in \mathbb{Z}$, $a|0$? Yes! $0 = a \cdot 0$

Given $a \in \mathbb{Z}$, $0|a$? $a = 0 \cdot k$?

If $a \neq 0$, then no!

If $a = 0$, then $a \cdot 0 = 0$, so $0|0$

Ex. Prove that for all integers n, if $12|n$, then $6|n$?

Let n be an integer and assume that $12|n$. There is then an integer k such that $n = 12k$

Thus, $n = 12k$
$= 6(2k)$

Since $2k \in \mathbb{Z}$ and $n = 6(2k)$ we have then $6|n$ as claimed.

Rough $n \in \mathbb{Z}$
Assume $12|n \rightarrow n = 12k$
$= 6(2k)$

proposition [Transitivity of Divisibility (TD)]
For all integers a, b, c if $a|b$ and $b|c$, then $a|c$)
(if $6|12$, and $12|n$, then $6|n$)

Proof: Let a, b, c be integers and assume that $a|b$ and $b|c$. Then there is an integer k such that $b = ak$ and there is an integer m such that $c = bm$

Then $c = bm$
$= (ak)m$
$= a(km)$

Thus, since $km \in \mathbb{Z}$, we have that $a|c$ □

Proposition:
For all integers a, b, c, if $a|b$ or $a|c$, then $a|bc$

2 cases: I $a|b \rightarrow b = ak$ $bc = akc$
II $a|c \rightarrow$

Proof: let a, b, c be integers, we consider 2 cases

Case I: assume that $a|b$, so there is an integer k such that $b = ak$

Thus, $bc = (ak)c$
$= a(kc)$

Since $kc \in \mathbb{Z}$, we have that $a|bc$

The proof of case(in which we assume that $a|c$) proceeds in similar fashion,

Since the result hold for each case, the proof is complete. □

Proposition [Divisibility of Integer of Combination (DIC)]
For all integers a, b, c, if $a \mid b$ and $a \mid c$, then for all integers x and y, $a \mid (bx + cy)$

Proof for DIC

Eg. $a=5$ $b=10$ $c=15$

$5 \mid 10$, $5 \mid 15$ so by DIC, for all x, y, $5 \mid (10x+15y)$

$[10x+15y = 5(2x+3y)]$

Proof: Let a, b, c be integers, and assume that $a \mid b$ and $a \mid c$

Thus, there are integers k, m such that $b = ak$ and $c = am$

To prove the conclusion, let x and y be arbitrary integers. We have

$$bx+cy = ak \cdot x + am \cdot y$$
$$= a(kx+my)$$

Thus, since $kx+my$ is an integer, we have that

$$a \mid bx+cy$$

Since x and y are arbitrary, this works for all $x, y \in \mathbb{Z}$ □

Q: Is the converse of DIC true

What is the converse?

Symbolically, DIC says $\forall a, b, c \in \mathbb{Z}$, $[(a \mid b \wedge a \mid c) \Rightarrow \forall x, y,\ a \mid (bx+cy)]$

Converse:

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

Proof: Let a, b, c be integers, and assume that for all integers x and y, $a \mid (bx+cy)$.

In particular, with $x=1$, $y=0$ $a \mid b(1)+c(0)$, That is, $a \mid b$

Also, with $x=0$, $y=1$, $a \mid b(0)+c(1)$, That is $a \mid c$ □

Moral: If the hypothesis is of the form $\forall x \in S, P(x)$ and we assume the hypothesis is true, then we can pick "helpful" values from the domain to prove the claim.

Ex. Prove that for all integers, if $3 \nmid (x^2-5x+2)$, then $3 \nmid x$

Sometimes, statements can feel a bit awkward to work. In this case, we can try proving its contrapositive.

[Recall: $A \Rightarrow B \equiv (\neg B) \Rightarrow (\neg A)$]

In this case, the contrapositive is,

"For all integers x, if $3 \mid x$, then $3 \mid (x^2-5x+2)$"

Proof: We will instead prove the contrapositive. Let x be an integer, and assume that $3 \mid x$, Then there is an integer k s.t $x = 3k$,

Hence, $x^2-5x+2 = (3k)^2 - 5(3k) + 2$

$$= 9k^2 - 15k + 2$$
$$= 3(3k^2 - 5k + 7)$$

Thus, since $3k^2-5k+7$ is an integer, $3 \mid x^2-5x+2$ as claimed.

Since the contrapositive holds, so too does the original statement.

Ex. Prove that for $x, y \in \mathbb{R}$, if xy is irrational, then x is irrational or y is irrational.

Prove by contra-positive:

If x, y are rational, then xy is rational.

Let x, y be real, assume both x, y are rational

There they exist integers a, b, c, d where $b \neq 0, d \neq 0$

$$x = \frac{a}{b}, \quad y = \frac{c}{d}$$

Then $x \cdot y = \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$

Since ac and bc are integers and $bd \neq 0$, we have xy is rational.

When proving $A \Rightarrow B$, consider the contrapositive if

1) $\neg B$ is simpler than A

2) A involves negative words (e.g. irrational)

3) The conclusion contains $\forall$

Warm up: Prove that for all $x, y \in \mathbb{R}$, if $x+y<10$, then $x<3$ or $y<7$

Prove by contrapositive

If $x \geq 3$ and $y \geq 7$, then $x+y \geq 10$

Since $x \geq 3$, $y \geq 7$, $x+y \geq 3+7$

$= 10$

$x+y \geq 10$ as claimed.

Let x and y be arbitrary real numbers, We will prove the contrapositive: if $x \geq 3$ and $y \geq 7$ then $x+y \geq 10$

Assume that $x \geq 3$ and $y \geq 7$,

by adding y to both sides of $x \geq 3$, we have $x+y \geq 3+y$

But since $y \geq 7$, $3+y \geq 3+7 \geq 10$.

Thus, $x+y \geq 3+y \geq 10$

Since x, y were arbitrary, this holds for all $x, y \in \mathbb{R}$ □

New proof: Let x and y be real numbers, assume $x+y<10$

and consider the following cases.

Case I:

Assume that $x<3$ in this case ($x<3$) and ($y>7$) is true

so there is nothing to show.

Case II:

Assume that $x<3$ is false, so $x \geq 3$

In this case, since $x+y<10$, $y < 10-x$

$< 10-3=7$

Thus, $(x-3) \vee (y<7)$ is true. Since this holds in all cases, the result is true for all $x, y \in \mathbb{R}$. □

A proof of this form is sometimes called the method of elimination.

Instead of proving $A \Rightarrow B \vee C$, We use $A \wedge (\neg B) \Rightarrow C$

Exercise that $A \Rightarrow B \vee C \equiv A \wedge (\neg B) \Rightarrow C$

Remark: We don't usually write the case where we assume $A \wedge B$ because there's nothing to show.

Exercise: Prove that for all real numbers x, if $x^2-4x+3 \geq 0$ then $x \leq 1$ or $x \geq 3$

Proof by Contradiction:

To prove a statement A, assume $\neg A$, and deduce something absurd.

Thus, $\neg A$ must be false, so A is true.

Ex. Prove that for all integers a, b, c, if $a \mid b$ and $a \mid 5b - 4c$, then $a \mid c$

Proof for the sake of contradiction. that this statement is false,

Then there exist integers a, b, c such that $a \mid b$ and $a \nmid 5b - 4c$, and $a \mid c$

By D1c, since $a \mid b$ and $a \mid c$, $a \mid 5b + c - 4c$ that is a contradiction!

Thus, the statement must be true.

Ex. Prove that $\sqrt{2}$ is irrational.

Proof: Assume that $\sqrt{2}$ is rational, so $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$.

Assume without loss of generality that a and b have no common factor

Since $\sqrt{2} = a/b$, we have $\sqrt{2}\, b = a$

By squaring both sides, $2b^2 = a^2$, Thus a^2 is even and hence so is a (exercise)

So $a = 2k$ for some $k \in \mathbb{Z}$, and since $2b^2 = a^2$, we have $2b^2 = (2k)^2 = 4k^2$

Warm up → use elimination to prove that for all integers x, y if x is even, then $4 \mid (x-y)$ or y is even.

Proof: Let x, y be integers

Assume that x is even, and assume that $4 \mid (x-y)$

There exist integers k, m such that $x = 2k$, and $x - y = 4m$

Thus, $y = x - 4m$

$= 2k - 4m$

$= 2(k - 2m)$

Since $k - 2m \in \mathbb{Z}$, we have that y is even. □

Proving Uniqueness

"prove that there is a unique $x \in S$ satisfying $P(x)$

x is the only thing satisfying $P(x)$

Strategy

To prove that some $x \in S$ is the unique element satisfying $P(x)$

prove $\forall x, y \in S, [P(x) \wedge P(y) \Rightarrow x = y]$

(either directly or by contradiction (assume $x \neq y$))

Ex. Prove that for all integers if $m \mid n$ and $m \neq 0$, then there is a unique integer k such that $n = mk$

Proof: Let m, n be integers, and assume that $m \mid n$ and $m \neq 0$, we will show:

1. There exists $k \in \mathbb{Z}$ such that $n = mk$
2. This is unique

For 1, note that by the definition of $m \mid n$, there does exist $k \in \mathbb{Z}$ such that $n = mk$

For 2, assume that there are $k, y \in \mathbb{Z}$ such that $n = mk$ and $n = mj$.

Thus, $mk = n = mj$, so by dividing by m, $k = j$. k is unique. □

Ex. Prove ~~that for all~~ real numbers x, there is at most one pair of rational number (a, b) such that $x = a + b\sqrt{2}$

Proof: Let x be a real number, suppose for the sake contradiction that there exist different pair of rational numbers (a, b) (c, d) such that $x = a + b\sqrt{2}$ and $x = c + d\sqrt{2}$.

We will assume that $b \neq d$.

We have $a + b\sqrt{2} = c + d\sqrt{2}$

so $a - c = d\sqrt{2} - b\sqrt{2}$

$= \sqrt{2}(d - b)$

Hence, $\sqrt{2} = \frac{a-c}{d-b}$

Since the RHS is rational but $\sqrt{2}$ is not, we have a contradiction.

Therefore, $b = d$.

Since $a + b\sqrt{2} = c + d\sqrt{2}$ we subtract $b\sqrt{2}$ to get $a = c$.

Thus, there is at most one pair rations a, b such that $x = a + b\sqrt{2}$ □

Proving If Statements.

To prove $A \Leftrightarrow B$, we prove $A \Rightarrow B$ and $B \Rightarrow A$

Ex. Prove that for all positive real numbers x and y, $\frac{x+y}{2} = \sqrt{xy}$ iff $x = y$

We will prove

(i) if $\frac{x+y}{2} = \sqrt{xy}$, then $x = y$

(ii) if $x = y$, then $\frac{x+y}{2} = \sqrt{xy}$

For (i), assume $\frac{x+y}{2} = \sqrt{xy}$, we have $x+y = 2\sqrt{xy}$, and by squaring $(x+y)^2 = 4xy$

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

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

Thus, $(x-y)^2 = 0$

so $x - y = 0$, $x = y$

(ii) exercise

Since (i) and (ii) hold, we have that $\frac{x+y}{2} \not\Rightarrow \sqrt{xy} \Leftrightarrow x = y$ □

Chapter 4 - Mathematical Induction.

New notation: Given integers m and n, with $n \geq m$, we define $\sum_{i=m}^{n} x_i = x_m + x_{m+1} + x_{m+2} + \dots + x_n$

$\prod_{i=m}^{n} x_i = x_m \cdot x_{m+1} \cdot x_{m+2} \dots x_n$

Ex. $\sum_{i=-1}^{3} i^2 = (-1)^2 + 0^2 + 1^2 + 2^2 + 3^2$

$= 15$

$\prod_{i=1}^{3} (5-i)! = (5-1)!(5-2)!(5-3)!$

$= 4! \cdot 3! \cdot 2! = 288$

Properties of Sums (PS)

(1) If c is a constant.
Then, $\sum_{i=m}^{n} cx_i = c\sum_{i=m}^{n} x_i$

(2) $\sum_{i=m}^{n} (x_i+y_i) = \sum_{i=m}^{n} x_i + \sum_{i=m}^{n} y_i$

(3) $\sum_{i=m}^{n} x_i = \sum_{i=m+k}^{n+k} x_{i-k}$.

Recurrence Relations

A recurrence relation defines one or more initial values and a formula that allows us to construct new values from old.

Ex. Define $a_1=0$ and $a_n = 3a_{n-1}+5$ for all integers $n \geq 2$

$a_2 = 3a_1+5 = 3(0)+5 = 5$

$a_3 = 3a_2+5 = 3(5)+5 = 20$

Proofs by induction

We want to prove some statement $P(n)$ that depends on $n \in \mathbb{N}$

Principal of Mathematical Induction (POMI)

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

If the following are true:

(1) $P(1)$

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

Then $P(n)$ is true for all $n \in \mathbb{N}$

Ex. Prove that for all $n \in \mathbb{N}$,

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

Proof: For each $n \in \mathbb{N}$, let $P(n)$ be the statement $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$

We will proceed by induction,

Base case: We will verify $P(1)$. That is we will that

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

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

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

Since they are equal $P(1)$ is true!

Inductive Step

Let k be an arbitrary natural number, and assume the inductive hypothesis $P(k)$, that is assume

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

We will show $P(k+1)$:

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

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

Notice that, $\sum_{i=1}^{k+1} i(i+1) = \sum_{i=1}^{k} i(i+1) + (k+1)(k+1)+1)$

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

$$= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \quad \text{(by } P(k)\text{)}$$

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

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

Thus, $P(k+1)$ is true!

Since $P(k) \Rightarrow P(k+1)$, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ by PMI! □

Ex. Prove for all integers $n \geq 4$, $n! > 2^n$

Proof: For each integer $n \geq 4$, let $P(n)$ be the statement $n! > 2^n$

We will proceed by induction.

Base case: We will verify $P(4)$. That is, we prove that $4! > 2^4$

Note: $4! = 24$, $2^4 = 16$

Thus, $4! > 2^4$, so $P(4)$ is true.

Inductive step: Let k be an arbitrary integer with $k \geq 4$, and assume the inductive hypothesis $P(k)$:

That is, assume $k! > 2^k$

We will verify $P(k+1)$: $(k+1)! > 2^{k+1}$

We have $(k+1)! = k!(k+1) > 2^k(k+1)$ (by $P(k)$)

$> 2^k(5)$ (as $k \geq 4$)

$> 2^k \cdot 2$

$= 2^{k+1}$

Thus, $P(k+1)$ holds.

Since $P(k) \Rightarrow P(k+1)$, $P(n)$ holds for all integers $n \geq 4$. □

New Notation

Given $n \in \mathbb{N}$, we define $n! = \prod_{i=1}^{n} i$ and $0! = 1$

Given non-negative integers m, n with $m \le n$, we define $\binom{n}{m} = \frac{n!}{m!(n-m)!}$

("n choose m")

We call $\binom{n}{m}$ a binomial coefficient

eg. $\binom{n}{0} = \frac{n!}{0!(n-0)!} = 1$

$\binom{n}{1} = \frac{n!}{1!(n-1)!} = n$

$\binom{n}{n} = \frac{n!}{n!(n-n)!} = 1$

Pascal's Identity (PI)

For all positive integers m, n with $m < n$, we have,

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

Proof: In the book. □

n \ m	0	1	2	3	4	...
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
⋮	⋮					

The Binomial Theorem.

For all real number x and all integers $n \ge 0$, $(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$

(eg. $(1+x)^3 = \binom{3}{0}x^0 + \binom{3}{1}x^1 + \binom{3}{2}x^2 + \binom{3}{3}x^3$

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

Proof: Let $x \in \mathbb{R}$ be arbitrary and for each integer $n \ge 0$, let $P(n)$ be the statement:

$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$ We proceed by induction.

Base Case: We check $P(0)$:

$P(0)$: $(1+x)^0 = \sum_{i=0}^{0} \binom{0}{i} x^i$

We have $(1+x)^0 = 1$ and $\sum_{i=0}^{0} \binom{0}{i} x^i = \binom{0}{0} x^0 = 1$

Thus, P(0) holds.

Inductive Step:

Let k be an integer with $k \geq 0$, and assume the inductive hypothesis

P(k): $(1+x)^k = \sum_{i=0}^{k} \binom{k}{i} x^i$

We will prove P(k+1):

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

We have, $(1+x)^{k+1} = (1+x)^k (1+x)$

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

$= \sum_{i=0}^{k} \binom{k}{i} x^i + \sum_{i=0}^{k} \binom{k}{i} x^{i+1}$

$= \sum_{i=0}^{k} \binom{k}{i} x^i + \sum_{i=0}^{k+1} \binom{k}{i-1} x^i$

$= \binom{k}{0} x^0 + \sum_{i=1}^{k} \binom{k}{i} x^i + \sum_{i=1}^{k} \binom{k}{i-1} x^i + \binom{k}{k} x^{k+1}$

$= \binom{k}{0} x^0 + \sum_{i=1}^{k} \left(\binom{k}{i} + \binom{k}{i-1} \right) x^i + \binom{k}{k} x^{k+1}$

$= \binom{k+1}{0} x^0 + \sum_{i=1}^{k} \binom{k+1}{i} x^i + \binom{k+1}{k+1} x^{k+1}$

$= \sum_{i=0}^{k+1} \binom{k+1}{i} x^i$

Thus, P(k+1) is true. Since P(k) ⇒ P(k+1), by PoMI, P(n) holds for all $n \geq 0$. □

Corollary (Binomial Theorem V2 (BT2))

For all $a, b \in \mathbb{R}$, and all non-negative integers n, $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$

Proof: Let $a, b \in \mathbb{R}$, let n be a non-negative integer

Exercise: Prove this is true when $a = 0$.

Instead, assume $a \neq 0$

Then,

$(a+b)^n = \left(a\left(1+\frac{b}{a}\right)\right)^n$

$= a^n \left(1+\frac{b}{a}\right)^n$

$= a^n \sum_{i=0}^{n} \binom{n}{i} \left(\frac{b}{a}\right)^i$

$= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$ □

Exercises

1. Evaluate $\sum_{i=0}^{n} \binom{n}{i}$

2. Find the coefficient of x^9 in $\left(x - \frac{1}{x^2}\right)^{12}$

1. $\sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^i$

$= (1+1)^n = 2^n$

Warm up: Find the coefficient of x^9 in $(x-\frac{1}{x^2})^{12}$

Solution: $(x-\frac{1}{x^2})^{12} = (x+(\frac{-1}{x^2}))^{12}$

$$= \sum_{i=0}^{12} \binom{12}{i} x^{12-i} \left(\frac{-1}{x^2}\right)^i$$

$$= \sum_{i=0}^{12} \binom{12}{i} (-1)^i \frac{x^{12-i}}{x^{2i}}$$

$$= \sum_{i=0}^{12} \binom{12}{i} (-1)^i x^{12-3i}$$

If $12-3i=9$, then $3i=3$, so $i=1$

The coefficient of x^9 is $\binom{12}{1}(-1)^9 = -12$

Ex. consider a sequence defined by $a_1=4$, $a_2=68$, and $a_n = 2a_{n-1} + 15a_{n-2}$ for all integers $n \geq 3$.

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

Proof: For each $n \in \mathbb{N}$, let $P(n)$ be the statement that $a_n = 2(-3)^n + 10 \cdot 5^{n-1}$

We proceed by induction.

Base Case. We verify $P(1)$

Since $2 \cdot (-3)^1 + 10 \cdot 5^{n-1}$

$= 2(-3) + 10 \cdot 1$

$= -6 + 10$

$= 4$ and $a_1 = 4$ by definition

$P(1)$ is true.

Inductive step

Let $k \in \mathbb{N}$ be arbitrary and assume the inductive hypothesis

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

We verify $P(k+1)$: $a_{k+1} = 2(-3)^{k+1} + 10 \cdot 5^k$

$a_{k+1} = 2a_k + 15a_{k-1}$

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

Pause

Remarks:

1. To prove something about $a_{n+1} = 2a_k + 15a_{k-1}$ We need to assume something about a_k AND a_{k-1}
2. The recursive definition $a_{k+1} = 2a_k + 15a_{k-1}$ only applies when $k+1 \geq 3$ i.e. when $k \geq 2$) so a_2 is not covered in the inductive step.

Fix:

1. Assume not just $P(k)$ but $P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ in the inductive step.
2. Check $P(2)$ as a second base case!

Principal of Strong Induction (POSI)

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

If the following are true:

1. $P(1)$
2. For all $k \in \mathbb{N}$, $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \Rightarrow P(k+1)$ then $P(n)$ is true for all $n \in \mathbb{N}$

Let's return to our example.

Base Case (new):

We verify $P(1)$ and $P(2)$ when $n=1$

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

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

$= 18 + 50 = 68$

Since $a_1 = 4$, and $a_2 = 68$, $P(1)$ and $P(2)$ are true.

Inductive hypothesis (new)

Let $k \geq 2$ be arbitrary, and assume the inductive hypothesis: $P(1) \wedge P(2) \wedge P(3) \wedge \cdots \wedge P(k)$

We verify $P(k+1)$: $a_{k+1} = 2(-3)^{k+1} + 10 \cdot 5^k$.

We have $a_{k+1} = 2a_k + 15a_{k-1}$

$= 2[2(-3)^k + 10 \cdot 5^{k-1}] + 15[2(-3)^{k-1} + 10 \cdot 5^{k-2}]$ by $P(k)$ & $P(k-1)$

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

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

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

Thus, $P(k+1)$ holds.

Since $P(1) \wedge P(2) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$

$P(n)$ is true for all $n \in \mathbb{N}$ by POSI. □

Ex. Consider a sequence defined by $a_1 = 3, a_2 = 5$ and $a_n = 3a_{n-1} + 2a_{n-2}$ for all integers $n \geq 3$. Prove that $a_n < 4^n$ for all $n \in \mathbb{N}$

Proof: For each $n \in \mathbb{N}$, let $P(n)$ be the statement that $a_n < 4^n$. We proceed by strong induction.

Base Cases: Verify $P(1)$, $P(2)$

$a_1 = 3 < 4$

$a_2 = 5 < 4^2$ Thus, $P(1)$, $P(2)$ are true.

Inductive Step:

Let k be an arbitrary integer with $k \geq 2$ and assume the inductive hypothesis.

$P(1) \wedge P(2) \wedge \cdots \wedge P(k)$

That is, assume that $a_j < 4^j$ for all integers j with $1 \leq j \leq k$

We verify $P(k+1)$:

$a_{k+1} < 4^{k+1}$

$a_{k+1} = 3a_k + 2a_{k-1}$

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

$= (3)(4)\, 4^{k-1} + 2(4^{k-1})$

$= 14(4^{k-1})$

$< 16 \cdot (4^{k-1})$

$= 4^2 \cdot 4^{k-1}$

$= 4^{k+1}$

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

Since $[P(1) \wedge P(2) \wedge P(3) \wedge \cdots \wedge P(k)] \Rightarrow P(k+1)$

$P(n)$ is true for all $n \in \mathbb{N}$ by PoSI. □

Ex. Prove that every positive integer n can be written as a sum of distinct, non-negative power of 2.
($n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_k}$ where all of the powers are different, and $i_j \geq 0$ for all j.)
eg. $9 = 2^3 + 2^0$ In binary $9 = 1001$ ($2^3\ 2^2\ 2^1\ 2^0$)
Proof:
For each $n \in \mathbb{N}$, let $P(n)$ be the statement, that n is a sum of distinct non-negative powers of 2.
Base Case:
When $n=1$, we have $n = 2^0$. thus $P(1)$ holds.
Inductive step
Let $k \in \mathbb{N}$ be arbitrary, assume $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$
We prove $P(k+1)$
Case I: Assume $k+1$ is odd
Then k is even, $k < k+1$, $P(k)$ implies that k is a sum of distinct non-neg. powers of 2
Since k is even, 2^0 is not part of this sum. By adding 2^0. we get a sum that works for $k+1$
Case II: Assume $k+1$ is even
Then $\frac{k+1}{2}$ is an integer and $\frac{k+1}{2} < k+1$, so by $P(\frac{k+1}{2})$ we get a sum that works for $\frac{k+1}{2}$
By multiplying by 2, we get a sum that works for $k+1$. Thus $P(k+1)$ holds.
- conclusion □.

Sets.
Whenever we talk about sets there is a "big" universal set that we have in mind.
This set is called the universe of discourse, and it contains all objects of interest.

Set Builder Notation.
2. Ingredients
1). Universe $\mathcal{U}$
2. Some condition for membership $P(x)$

Ex. $\{n \in \mathbb{N} : n \mid 3\}$
universe, Pred, such that
$= \{1, 3\}$

The book calls set of the form $\{x \in \mathcal{U} : P(x)\}$ (Type I)

Ex. $\{2k : k \in \mathbb{Z}\}$
"form" of an element, universe. (Type II)

Ex: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$
form, universe (Type II), pred

Sometimes people use "|" instead of ":"
In this course we always use :

(i) All multiples of 7
$\{7k : k \in \mathbb{Z}\}$

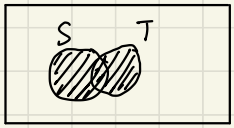
(ii) All odd perfect squares
$\{(2k+1)^2 : k \in \mathbb{Z}\}$

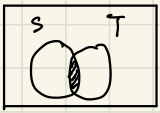
Set operations.

Let S, T be set in some universe $\mathcal{U}$ we define

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

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





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

$B = \{2k+1 : k \in \mathbb{Z}\}$

$A \cup B = \mathbb{Z}$

$A \cap B = \emptyset$

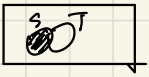
We say that S, T are disjoint if $S \cap T = \emptyset$

$S \cup S = S$ $S \cup \emptyset = S$

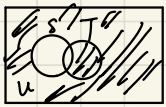
$S \cap S = S$ $S \cap \emptyset = \emptyset$

We define

$S - T = \{x : (x \in S) \wedge \neg(x \in T)\}$ ("difference of S and T")



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



(Other people sometimes write $S - T$ as $S \setminus T$, and write S^c instead of $\overline{S}$. We will not.)

If S is a finite set, we define the cardinality of S to be the number of elements in S. It is denoted by $|S|$.

Exercise:

$\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

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

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

Find $|A - B|$

$= 2$

Subsets

We say that S is the subset of T, and we write $S \subseteq T$ if every element of S is also an element of T

We say that S is a proper subset of T if $S \subseteq T$ and there is at least one element of T that is not in S.

In this case we write $S \subsetneq T$

CAUTION

(other people may write $S \subset T$ to mean that, S is a subset (or proper subset) of T. (But we don't)

Don't confuse $S \subsetneq T$ with $S \not\subseteq T$ (which means "S is not a subset of T.")

Remark:

We write $S \supseteq T$ to mean that $T \subseteq S$ (here we say that S is a superset of T)

Similarly, we define $S \supsetneq T$ and $S \not\supseteq T$

Note: Given sets S, T to prove that $S \subseteq T$

We prove $\forall x \in U \cdot (x \in S) \Rightarrow (x \in T)$

Ex: Let $A = \{n \in \mathbb{Z} : 4 \mid (n-3)\}$ $B = \{2k+1 : k \in \mathbb{Z}\}$

Prove (i) $A \subseteq B$

(ii) $A \subsetneq B$

(i) Let $n \in \mathbb{Z}$ be arbitrary.

Assume that $n \in A$, so $4 \mid (n-3)$

Thus, $n-3 = 4m$ for some m in $\mathbb{Z}$

$$n = 4m+3$$
$$= 2(2m+1)+1$$

Since $2m+1 \in \mathbb{Z}$, we have that $n \in B$

Since n was arbitrary, $A \subseteq B$

(ii) Consider $1 = 2(0)+1$

We have that $1 \in B$

We claim that $1 \notin A$.

Suppose for sake of contradiction that $1 \in A$

So $4 \mid (1-3)$, that is $4 \mid -2$ (false!)

This is a contradiction. So $1 \notin A$. We can conclude that $A \subsetneq B$

Warm up:

Let S, T be sets in a universe. prove that if $S \cup T \subseteq S \cap T$, then $S \subseteq T$

Assume $S \cup T \subseteq S \cap T$, $S \not\subseteq T$

let $x \in S$, $x \notin T$

$x \in S \cup T$

$x \notin S \cap T$

but $S \cup T \subseteq S \cap T$ means every $x \subseteq S \cup T$

also belongs to $S \cap T$, which is a contradiction!

Thus, $S \subseteq T$

Exercise: Let A, B, C be sets. Prove that if $A \subseteq B \cap C$, then $(A \cap B) - C = \emptyset$

Definition: Let S and T be sets in a universe $\mathcal{U}$ we say that S and T are equal if $S \subseteq T$ and $T \subseteq S$.

To prove that $S = T$, prove $\forall x \in \mathcal{U}, (x \in S) \Leftrightarrow (x \in T)$

Ex. Let A, B be sets in a Universe $\mathcal{U}$, prove that $A - \bar{B} = A \cap B$

proof: We will check

(i) $A - \bar{B} \subseteq A \cap B$ and

(ii) $A \cap B \subseteq A - \bar{B}$

For (i) let $x \in \mathcal{U}$ and assume that $x \in A - \bar{B}$. Then $x \in A$ and $x \in \bar{B}$

Since $x \notin \bar{B}$, $x \in B$. Therefore, $x \in A$ and $x \in B$. So $x \in A \cap B$ This proves (i)

For (ii) let $x \in \mathcal{U}$ and assume that $x \in A \cap B$, then $x \in A$ and $x \in B$

Since $x \in B$, $x \notin \bar{B}$. Since $x \in A$ and $x \notin \bar{B}$, $x \in A - B$. This proves (ii)

Since (i) and (ii) are true.

$A - \bar{B} = A \cap B$

Chapter 6 - GCDs

We will start by furthering our results on integer divisibility

Proposition [Bounds by Divisibility (BBD)]

For all integers a and b, if $b|a$ and $a \neq 0$, the $b \leq |a|$

Proof: Let $a, b \in \mathbb{Z}$ and assume that $b|a$ and $a \neq 0$, then there is an integer q such that $a = bq$.

Note that since $a \neq 0$, $q \neq 0$, we have $|a| = |bq| = |b||q|$

Since $q \neq 0$, $|q| \geq 1$ (as $q \in \mathbb{Z}$)

Therefore, $|a| = |b||q| \geq |b| \cdot 1$

$= |b|$

Finally, since $b \leq |b|$, we have $b \leq |b| \leq |a|$, so $b \leq |a|$. □

Division Algorithm (DA)

For all integers a and positive integers b, there exists unique integers q and r such that

$a = bq + r$ and $a \leq r < b$

(q = quotient, r = remainder)

Ex. $\underbrace{7143}_{a} = \underbrace{11}_{b} \cdot \underbrace{649}_{q} + \underbrace{4}_{r}$

$\underbrace{-7143}_{a} = 11(-650) + \underbrace{7}_{r}$

$a = 11(-650) + r$

Proof: Let $a, b \in \mathbb{Z}$ with $b > 0$. We will assume that q, r exist. and prove they're unique.

Assume that q_1, q_2, r_1, r_2 are integers such that $a = bq_1 + r_1$, $a = bq_2 + r_2$ and $0 \leq r_1, r_2 < b$

We have $bq_1 + r_1 = bq_2 + r_2$

So $b(q_1 - q_2) = r_2 - r_1$

Note that since $0 \leq r_1 < b$, we have $-b < -r_1 \leq 0$. Also $0 \leq r_2 < b$, adding these inequalities

$-b < r_2 - r_1 < b$

Thus, $-b < b(q_1 - q_2) < b$

Dividing by b we get $-1 < q_1 - q_2 < 1$

Since $q_1 - q_2 \in \mathbb{Z}$

$q_1 - q_2 = 0$ so $q_1 = q_2$

Finally, $r_2 - r_1 = b(q_1 - q_2) = b(0) = 0$

Thus, $r_1 = r_2$ □

Warm-up:

Given a and b, find $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \le r < b$

(i) $a = 30$ $b = 18$

(ii) $a = 384$ $b = 171$

Solution:

(i) $30 = 18 \cdot 1 + 12$

(ii) $384 = 172 \cdot 2 + 72$

Definition: Let a and b be integers, not both 0. An integer $d > 0$ is called the greatest common divisor of a and b if (i) $d \mid a$ and $d \mid b$

(ii) for all integers c, if $c \mid a$ and $c \mid b$, then $c \le d$

In this case we write $d = \gcd(a, b)$

We also define $\gcd(0, 0) = 0$

Ex. With $a = 30$, $b = 18$, we have $\gcd(30, 18) = 6$

Ex. With $a = 384$ and $b = 171$, $\gcd(384, 171) = ???$

One way to find $\gcd(384, 171)$ would be write out all divisors of 384, and all divisors of 171.

But... that is really lame. It is even worse for $\gcd(17402, 7032)$

Properties: Let $a \in \mathbb{Z} \to \gcd(a, a) = \gcd(a, -a) = |a|$

$\gcd(a, 1) = \gcd(a, -1) = 1$

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

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

Ex. Let a, b be integers. Prove that

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

Proof: If $a = b = 0$, then $\gcd(a, b) = \gcd(0, 0) = 0$

Also, $\gcd(3a + b, a) = \gcd(0, 0)$

$= 0$

Suppose now that at least one of a or b is not 0.

Let $d = \gcd(a, b)$

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

We will show

(i) $d \mid (3a + b)$ and $d \mid a$

(ii) For all $c \in \mathbb{Z}$, if $c = 3a + b$ and $c \mid a$, then $c \le d$

For (ii) Since $d = \gcd(a, b)$, $d \mid a$ and $d \mid b$. In particular, $d \mid a$.

Also, by Dic, d divides $3a+b$. This proves (i)

(iii). Let $c \in \mathbb{Z}$ and assume that $c \mid (3a+b)$ and $c \mid a$

Then, by Dic, $c \mid [(3a+b) + (-3)a]$

Thus, $c \mid b$

Since $c \mid a$ and $c \mid b$, $c \leq \gcd(c, d) = d$

Thus, (iii) holds.

Therefore, by the definition of gcd, $d = \gcd(3a+b, a)$ □

Theorem. [GCD with Remainder (GCDwR)]

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

In other words, $\gcd(bq+r, b) = \gcd(b, r)$

↳ we can remove multiples of b from the first position.

Proof: Let $a, b, r \in \mathbb{Z}$ and assume that $a = bq + r$, for some $q \in \mathbb{Z}$

If $a - b = 0$, then $r = a - bq = 0 - 0 \cdot q = 0$, hence $\gcd(a, b) = \gcd(0, 0) = 0$

and $\gcd(b, r) = \gcd(0, 0) = 0$

Assume now that at least one of a or b is not 0.

Let $d = \gcd(a, b)$, we will prove that $d = \gcd(b, r)$ by showing

(i) $d \mid b$ and $d \mid r$

(ii) For all $c \in \mathbb{Z}$, if $c \mid b$ and $c \mid r$, then $c \leq d$.

For (i), since $d = \gcd(a, b)$, $d \mid a$ and $d \mid b$. Since $r = a + (-q)b$, we have that $d \mid r$ by Dic

Thus, $d \mid b$ and $d \mid r$

For (ii), let $c \in \mathbb{Z}$ and assume that $c \mid b$ and $c \mid r$

By Dic. c divides a. That is, $c \mid a$. Since $c \mid a$ and $c \mid b$, $c \leq \gcd(a, b) = d$

Ex. Let a, b be integers. Prove that $\gcd(3a+b, a) = \gcd(a, b)$

Proof: $\gcd(3a+b, a)$ — multiples of a

$= \gcd(b, a)$ (which is the 2nd argument)

$= \gcd(a, b)$ (by GCD WR)

□

Ex: prove that for all $a \in \mathbb{Z}$, $\gcd(15a+3, 5a+1) = 1$

Proof: Let $a \in \mathbb{Z}$

Since $15a+3 = 3(5a+1) + a$

We have that $\gcd(15a+3, 5a+1)$

$= \gcd(a, 5a+1)$ by GCD WR

Also, we can remove $5a$ from the second argument. By GCD WR,

so $\gcd(a, 5a+1) = \gcd(a, 1)$

$= 1$

Thus, $\gcd(15a+3, 5a+1) = \gcd(a, 1) = 1$ □

Note: We can also use GCD WR to compute gcd of particular integers.

Ex. Compute $\gcd(384, 171)$

Solution: Since $\overset{a}{384} = \overset{b}{171} \cdot \overset{q}{2} + \overset{r}{42}$ (by DA)

We have that $\gcd(384, 171) = \gcd(171, 42)$ (by GCD WR)

Also, $\overset{a}{171} = \overset{b}{42} \cdot \overset{q}{4} + \overset{r}{3}$ so $\gcd(171, 42) = \gcd(42, 3)$

Finally, $42 = 3 \cdot 14 + 0$

by GCD WR, $\gcd(42, 3) = \gcd(3, 0) = 3$

Thus, $\gcd(384, 171) = \gcd(3, 0) = 3$

Euclidean Algorithm (EA)

Let a, b be integers with $0 < b \le a$, we want $\gcd(a, b)$

① Use DA to write $a = bq + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < b$

② If $r = 0$, then stop. We have $\gcd(a, b) = \gcd(b, r)$

$= \gcd(b, 0)$

$= b$

③ If $r \neq 0$, replace (a, b) with (b, r) and return to ①

Ex. Compute gcd (1002, 954)

By EA

$1002 = 954 \cdot 1 + 48$

$954 = 48 \cdot 19 + 42$

$48 = 42 \cdot 1 + 6$

$42 = 6 \cdot 7 + 0$

$\gcd(1002, 954)$

$= \gcd(954, 48)$

$= \gcd(48, 42)$

$= \gcd(42, 6)$

$= \gcd(6, 0) = 6$

Note: gcd (a, b) is the last non-zero remainder in EA

Q: What if we want gcd (a, b) when the condition $0 < b \le a$ is not satisfied?

(i) if $a < 0$ or $b < 0$, compute gcd (|a|, |b|) instead (same as gcd (a, b))

(ii) if $a < b$, replace (a, b) with (b, a)

(iii) if $b = 0$, then gcd (a, b) = gcd (a, 0) = |a|

if $a = 0$, then gcd (a, b) = gcd (0, b) = |b|

Bezout's Lemma.

Let's revisit our computation of gcd (354, 171)

We had $354 = 171 \cdot 2 + 42$ Equivalently, $354 - 171 \cdot 2 = 42$

$171 = 42 \cdot 4 + 3$ $171 - 42 \cdot 4 = 3$

$42 = 3 \cdot 14 + 0$ $42 - 3 \cdot 14 = 0$

Note: $3 = 171 - 42 \cdot 4$

$= 171 - [354 - 171 \cdot 2] \cdot 4$

$= 354 \cdot (-4) + 171 \cdot 9$

Thus, we have written gcd (354, 171) as an integer combination of 354 and 171

Bezout's Lemma

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

Warm-up

Find integers s and t such that $2550s + 1750t = d$ where $d = \gcd(2550, 1750)$

We have $2550 = (1)(1750) + 800$ $\quad 800 = 2550 - 1750(1)$

$1750 = (2)(800) + 150$ $\quad 150 = 1750 - (800)(2)$

$800 = (5)(150) + 50$ $\quad 50 = 800 - (150)(5)$

Using back substitution

$50 = 800 - 150 \cdot 5$

$= 800 - [1750 - 800 \cdot 2]5$

$= 1750(-5) + 800(11)$

$= 1750(-5) + [2550 - 1750](11)$

$= 2550(11) + 1750(-16)$

Here's an application of (BL):

Proposition: [Common Division Divides GCD] (CDD GCD)

For all integers a, b, c

if $c|a$, $c|b$, then $c \mid \gcd(a, b)$

Proof: Let $a, b, c \in \mathbb{Z}$, and assume that $c|a$ and $c|b$

By BL, there are integers s, t such that $as + bt = \gcd(a, b)$

Thus, by DIC, we have that c divides $as + bt = \gcd(a, b)$

Note: $\gcd(a, b)$ is NOT the only integer of the form $as + bt$ for some $s, t \in \mathbb{Z}$. For example, with $a = 2550$, $b = 1750$,

$2550(22) + 1750(-32) = 100$

$2550(-55) + 1750(80) = -250$

Theorem, [GCD Characterization Theorem (GCDCT)]

For all, $a, b \in \mathbb{Z}$, and all non-negative $d \in \mathbb{Z}$, if,

(i) $d|a$ and $d|b$, and

(ii) there are integers s and t such that $d = as + bt$

then $d = \gcd(a, b)$

Proof: Let $a, b, d \in \mathbb{Z}$ with $d \geq 0$ and assume that

(i) $d|a$ and $d|b$ and

(ii) there are integers s, t such that $d = as + bt$

Case I: Suppose that $a = b = 0$ We have $d = as + bt = 0 + 0 = 0$

Since $d = 0 = \gcd(0, 0) = \gcd(a, b)$

Case I is completed

Case II: Suppose that not both a and b are zero. We will show that $d = \gcd(a,b)$ by proving:

- $d > 0$
- $d \mid a$ and $d \mid b$, and
- for all $c \in \mathbb{Z}$ if $c \mid a$ and $c \mid b$, then $c \leq d$

Note that we have assumed that $d \mid a$ and $d \mid b$ and not both a and b are 0, then, since $d \geq 0$, we have that $d > 0$.

Finally, let $c \in \mathbb{Z}$ and suppose that $c \mid a$ and $c \mid b$. Note that $d = as + bt$

so by DIC, c divides $as + bt = d$

Hence, by Bounds by Divisibility (BBD) $c \leq |d|$

Since $d > 0$, we have $c \leq d$. By definition of gcd, $d = \gcd(a,b)$. □

Remarks:

1. Suppose you have integers a, b, d with $d \geq 0$ and you claim that $d = \gcd(a,b)$

To convince me, you only to show that,

- $d \mid a$ and $d \mid b$. and
- $d = as + bt$ for some $s, t \in \mathbb{Z}$

Ex: Consider $a = 2550$, $b = 1750$, $d = 50$

We have that $2550 = 50(51)$

$1750 = 50(35)$

$2550(11) + 1750(-16) = 50$

Sometimes we call s and t a certificate of correctness that $d = \gcd(a,b)$

2. The converse of GCD OT is also true!

i.e. if $d = \gcd(a,b)$ then

(i) $d \mid a$ and $d \mid b$ (by definition)

(ii) there exist integers s, t such that $as + bt = d$ (by BL)

Ex: Prove that for all $n \in \mathbb{Z}$, $\gcd(n, n+1) = 1$

Proof: Let $n \in \mathbb{Z}$, note that $1 \mid n$ and $1 \mid (n+1)$.

Also, $1 = (n+1) + (-1)n$ so we are done GCD OT. □

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

Solution: $1 \mid n$ and $1 \mid n+1$ Also, $1 = n(-1) + (n+1)(1)$

Thus, by GCD CT. $1 = \gcd(n, n+1)$ □

Proposition: [Division by GCD CDB GCD]

For all integers a, b, not both 0, we have $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, where $d = \gcd(a, b)$

Eg: With $a = 14$, $b = 21$, we have $d = \gcd(a, b) = 7$

and $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \gcd(2, 3)$

$= 1$

Proof: Let $a, b \in \mathbb{Z}$, not both 0. Set $d = \gcd(a, b)$

First note that $1 \mid \frac{a}{d}$ and $1 \mid \frac{b}{d}$

Since $d = \gcd(a, b)$ Bezout's Lemma implies that $d = as + bt$ for some $s, t \in \mathbb{Z}$

Dividing by d, $\left(\frac{a}{d}\right)s + \left(\frac{b}{d}\right)t = 1$ □.

Ex. Prove that for all $a, b, c \in \mathbb{Z}$, if $\gcd(a, b, c) = 1$ then $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$

Proof: Let $a, b, c \in \mathbb{Z}$, assume that $\gcd(ab, c) = 1$

We will prove that $\gcd(a, c) = 1$

Note that $1 \mid a$ and $1 \mid c$

By Bezout's Lemma, $(ab)s + ct = 1$ for some $s, t \in \mathbb{Z}$

So $a(bs) + ct = 1$

By GCD CT $\gcd(a, c) = 1$

A similar argument can be made for $\gcd(b, c)$. □

Q: Is the converse true? i.e. if $\gcd(a, c) = 1$ and, $\gcd(b, c) = 1$ do we have $\gcd(ab, c) = 1$?)

A: Yes!

Proof: Let $a, b \in \mathbb{Z}$ and assume that $\gcd(a, c) = \gcd(b, c)$

By (BL), there are integers s, t, p, q such that $as + ct = 1$ and $bp + cq = 1$

We then have, $1 = 1 \cdot 1$

$= (as + ct)(bp + cq)$

$= asbp + ctbp + ascq + ctcq$

$= ab(sp) + c(asq + tbq + tcq)$

Thus, since $1 \mid ab$ and $1 \mid c$, we have $1 = \gcd(a, b, c)$ by GCD CT □.

Extended Euclidean Algorithm (EEA)

EA: Find the gcd of integers a, b

Back sub: Work backward to find $s, t \in \mathbb{Z}$ such that $\gcd(a,b) = as + bt$

EEA: Combine these two processes!

To describe EEA, we need to define the floor function

Def^n: Given a real number x, we define the floor of x $\lfloor x \rfloor$ to be the biggest integer less than or equal to x.

eg $\lfloor \frac{5}{2} \rfloor = 5$

$\lfloor 2 \rfloor = 2$

$\lfloor -\frac{3}{2} \rfloor = -2$

In EA, we compute $a = b\lfloor \frac{a}{b} \rfloor + r_1$ $(i=1)$

$b = r_1\lfloor \frac{b}{r_1} \rfloor + r_2$ $(i=2)$

$r_1 = r_2\lfloor \frac{r_1}{r_2} \rfloor + r_3$ $(i=3)$

In general, $q_i = \lfloor \frac{r_{i-2}}{r_{i-1}} \rfloor$

$r_i = r_{i-2} - q_i r_{i-1}$

We record these computations in a table with columns. $\boxed{x_i \; y_i}$ r_i q_i

At each stage, we will have $ax_i + by_i = r_i$

Extended Euclidean Algorithm (EEA)

Input: Integers a, b with $0 < b \leq a$

Initialize

x_i	y_i	r_i	q_i
1	0	a	0
0	1	b	0

Repeat: $q_i = \lfloor \frac{r_{i-2}}{r_{i-1}} \rfloor$

$\text{Row}_i = \text{Row}_{i-2} - q_i \text{Row}_{i-1}$

Stop: When $r_i = 0$

Output: Let $n = i-1$

$\gcd(a,b) = r_n$

$ax_n + by_n = r_n = \gcd(a,b)$

Ex: Find $s, t \in \mathbb{Z}$ such that $2550s + 1750t = \gcd(2550, 1750)$

Solution: Let $a = 2550$, $b = 1750$

x	y	r_i	q_i
1	0	2550	0
0	1	1750	0
1	−1	800	1
−2	3	150	2
11	−16	50	5
−35	51	0	3

$q_2 = \lfloor \frac{r_1}{r_2} \rfloor = \lfloor \frac{2550}{1750} \rfloor = 1$

$\text{Row}_3 = \text{Row}_1 - 1\,\text{Row}_2$

$\gcd(2550, 1750) = 50$

and $2550(11) + 1750(-16) = 50$

Ex: Find $s, t \in \mathbb{Z}$ such that $3540s + 351t = \gcd(3540, 351)$

Solution: Let $a = 3540$, $b = 351$

x	y	r_i	q_i
1	0	3540	0
0	1	351	0
1	−10	30	10
−11	111	21	11
12	−121	9	1
−35	353	3	2
		0	3

$\gcd(3540, 351) = 3$

$3540(-35) + 351(353) = 3$

Coprimeness

Definition: We say that integers a, b are coprime (or negatively prime) if $\gcd(a,b)=1$

e.g. $16, 19$ are coprime

$16, 18$ are Not coprime.

Theorem [Coprimeness characterization theorem (CCOT)]

For all integers a, b, we have that $\gcd(a,b)=1$ if and only if $1=as+bt$ for some $s,t \in \mathbb{Z}$

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

First suppose that $\gcd(a,b)=1$. By Bezout's Lemma, $1=as+bt$ for some $s,t \in \mathbb{Z}$

Now assume that $1=as+bt$ for some $s,t \in \mathbb{Z}$ Since $1|a$, $1|b$, we have $1=\gcd(a,b)$ by GCD of 1 □

Proposition [Coprimeness and Divisibility] (CAD)

For all integers a, b, c, if $c|ab$ and $\gcd(a,c)=1$ then $c|b$.

Proposition [Coprimeness and Divisibility] (CAD)

For all integers a, b, c, if $c \mid ab$ and $\gcd(a, c) = 1$ then $c \mid b$.

Proof: Let $a, b, c \in \mathbb{Z}$ and assume that $c \mid ab$ and $\gcd(a, c) = 1$

Since $c \mid ab$, there exists $k \in \mathbb{Z}$ such that $ab = ck$. Also by CUT, there are integers s, t such that $as + ct = 1$

By multiplying by b, $abs + bct = b$

$$c(ks) + bct = b$$

Thus, $c(ks + bt) = b$

so $c \mid b$ □

Definition: An integer $p > 1$ is said to be prime if its only positive divisors are 1 and p.

If $p \in \mathbb{Z}$, $p > 1$ and p is not prime we say that p is composite

Q: Is 1 a prime number?

A: According to our definition, 1 is neither prime nor composite.

Theorem: [Prime Factorization (PF)]

Every integer $n > 1$, can be written as a product of primes.

eg $35 = 5 \cdot 7$

$100 = 4 \cdot 25$

$= 2^2 \cdot 5^2$

$17 = 17$

Proof: For each integer $n > 1$, let $P(n)$ be the statement, that n can be written as a product of primes.

We will proceed by induction.

Base case: When $n = 2$, we have that 2 is the product of one prime,

hence, $P(2)$ is true.

Inductive Step: let k be an integer with $k \geq 2$ and assume the inductive hypothesis:

$P(2) \wedge P(3) \wedge \dots \wedge P(k)$

That is, assume that for all $y \in \mathbb{Z}$ with $2 \leq j < k$, j can be written as a product of prime

We will prove $P(k+1)$,

If $k+1$ is prime, $P(k+1)$ is true

Assume now $k+1$ is composite,

Then there exists integer a, b such that $k+1 = ab$ and $1 < a < k+1$, $1 < b < k+1$

By P(a) and P(b), a and b can be written as products of primes. Thus, $k+1 = ab$ is also a product of primes.
Since $P(2) \wedge P(3) \wedge \ldots \wedge P(k) \Rightarrow P(k+1)$ the result holds by P.O.I.

Theorem: [Euclid Theorem (ET)] There are infinitely many primes.
Proof: Assume for contradiction that there are only finitely many primes:
$p_1, p_2, p_3, \ldots p_k$
Consider the integer $N = p_1 p_2 \ldots p_k + 1$
Note that $N > 1$
by P.F., N can be written as a product of primes $p_1, p_2 \ldots p_k$
Thus, there is some prime p_i that divides N
Note that p_i also divides $p_1, p_2 \ldots p_k$
Thus, by D.I.C., p_i divides $N - p_1 p_2 p_3 \ldots p_k = 1$
This is a contradiction (as no prime divides 1)
Thus, there must exist infinitely many primes.

Lemma [Euclid's Lemma (EL)]
For all integers a, b and all primes p, if $p \mid ab$ then $p \mid a$ or $p \mid b$

Euclid's Lemma (EL)

For all integers a and b, and prime numbers p, if $p \mid ab$, then $p \mid a$ or $p \mid b$

Proof: Let $a, b \in \mathbb{Z}$ and let p be an arbitrary prime number.

Prove by elimination: We will prove "if $p \mid ab$ and $p \nmid a$, then $p \mid b$

So assume that $p \mid ab$ and $p \nmid a$

Since p is a prime number, 1 and p are the only positive divisor of p.

Thus, $\gcd(p, a) = 1$. However, $\gcd(p, a) \neq p$ since $p \nmid a$

So we conclude that $\gcd(p, a) = 1$ Since $\gcd(p, a) = 1$ and $p \mid ab$, $p \mid b$ by CAD.

Exercise: Prove the following generalization: For all prime P and all $n \in \mathbb{N}$, and all integers $a_1, a_2, a_3 \ldots a_n$.

If $p \mid a_1 \cdot a_2 \cdot \cdots a_n$, then $p \mid a_i$ for some i.

Unique Factorization Theorem (UFT)

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

e.g. $100 = 2 \cdot 2 \cdot 5 \cdot 5$

Proof: For each integer $n \geq 2$, let $P(n)$ be the statement that n can be written as a product of primes uniquely apart from reordering the primes. We proceed by induction

Base case: When $n = 2$, n is a single prime, so $P(2)$ is true

Inductive step: Let $k \in \mathbb{Z}$ with $k \geq 2$ and assume $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$ We will prove $P(k+1)$

Case 1: if $P(k+1)$ is prime, then $P(k+1)$ is true

Case 2: Assume $k+1$ is composite.

By PF, $k+1$ can be written as a product of prime.

To show this can be done uniquely, suppose that $k+1 = p_1 \cdot p_2 \cdot p_3 \cdots p_j = q_1 \cdot q_2 \cdot q_3 \cdots q_l$ p_1 divides $q_1 q_2 q_3 \cdots q_l$

By the generalization of EL, p divides one of the q's

By reordering if necessary, assume that $p_1 \mid q_2$ Since p_1 and q_2 are primes, $p_1 = q_1$.

By dividing $p_1 p_2 \cdots p_j$ and $q_1 q_2 q_3 \cdots q_l$ by $p_1 = q_1$, we have $p_2 \cdots p_j = q_2 \cdots q_l$ call this product m

Note that $2 \leq m \leq k$

By P(m), we have that m can be written uniquely as a product of primes up to reordering.

Since $m = p_2 \cdots p_j = q_2 \cdots q_l$ we have that $j = l$ and $p_2 \cdots p_j$ is the same after re-ordering.

Therefore, since $p_2 = q_i$, we have that the primes $p_1, p_2 \cdots p_j$ and $q_1, q_2 \cdots q_l$ are the same.

This proves $P(k+1)$

Remark: UFT has important applications to divisibility.

E.g. What are positive integers of 12?

Solution: 1, 2, 3, 4, 6, 12

Note that: $12 = 2^2 \cdot 3$

$1 = 2^0 3^0$ $\quad$ $4 = 2^2 3^0$

$2 = 2^1 3^0$ $\quad$ $6 = 2^1 3^1$

$3 = 2^0 3^1$ $\quad$ $12 = 2^2 3^1$

(Divisors From Prime Factorization (DFPF))

Let n and c be positive integers, and let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

be a way to express n as a product of the distinct primes $p_1, p_2, \ldots, p_k$, where some or all of the exponents may be zero. The integer c is a positive divisor of n if and only if c can be represented as a product

$$c = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \text{ where } 0 \leq \beta_i \leq \alpha_i \text{ for } i = 1, 2, \ldots, k.$$

Ex. How many positive multiples of 35 divide 1750?

Solution: Note that $1750 = 2^1 \cdot 5^3 \cdot 7^1$

Thus, a positive integer d divides 1750 if and only if $d = 2^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3}$ with $0 \le \alpha_1 \le 1$, $0 \le \alpha_2 \le 2$, $0 \le \alpha_3 \le 1$ by DFPF

To make d a multiple of 35, include at least one 5 and at least one 7

So we really have $0 \le \alpha_1 \le 1$

$1 \le \alpha_2 \le 3$

and $\alpha_3 = 1$

We have 2 choices for α_1, 3 choices for α_2, 1 choice for α_3

Total: $2 \cdot 3 \cdot 1 = 6$ positive integers

Ex: Prove that for all positive integers a, b, $a|b$ if and only if $a^3|b^3$

Proof: Let $a, b \in \mathbb{N}$, assume first that $a|b$

By definition, $b = am$ for some $m \in \mathbb{Z}$

Thus, $b^3 = (am)^3 = a^3 m^3$, so $a^3 | b^3$

Now assume that $a^3 | b^3$. Let $p_1, p_2, \dots p_k$ be primes such that

$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$

$b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_k^{\beta_k}$ where α_i, β_i are non-negative integers. (exponents can be 0)

$a^3 = p_1^{3\alpha_1} p_2^{3\alpha_2} p_3^{3\alpha_3} \dots p_k^{3\alpha_k}$

$b^3 = p_1^{3\beta_1} p_2^{3\beta_2} p_3^{3\beta_3} \dots p_k^{3\beta_k}$

Since $a^3 | b^3$, DFPF says that $3\alpha_i \le 3\beta_i$ for all i. Thus, $\alpha_i \le \beta_i$ for all i.

Thus, by DFPF, $a|b$. □

Theorem [GCD from prime Factorization (GCD PF)]

Let a, b be positive integers, and let $a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_k^{\beta_k}$ be ways to express a, b as products of distinct primes $p_1 p_2 \dots p_k$ with α_i, β_i non-negative integers. Then, $\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} p_3^{\min(\alpha_3,\beta_3)} \dots p_k^{\min(\alpha_k,\beta_k)}$

Ex. $2550 = 2 \cdot 3 \cdot 5^2 \cdot 17$

$1750 = 2 \cdot 5^3 \cdot 7$

So $\gcd(2550, 1750) = 2 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 17^0 = 50$

Chapter 7: Linear Diophantine Equations

Ex: Mario has forgotten how to run, but he can jump forward or backward. 150 m away sits a Goomba. If Mario can make long jumps of 24m and short jumps of 9m, is there a sequence of jump he can make to land on the Goomba?

Solution: Let x be the number of short jump. y = # of short jumps.

We want x, y such that $24x + 9y = 150$

We require x, y to be integers.

Method 1: Inspection

We have $24(-1) + 9(-2) = 150$

Method 2: Use EEA

x_i	y_i	r_i	q_i
1	0	24	0
0	1	9	0
1	−2	6	2
1	−2	3	1
−1	3	3	1
—	—	0	2

We have $24(-1) + 9(2) = 3$

Multiplying by 50:

$24(-50) + 9(100) = 150$

So we can make 50 long jumps back wards are 100 short jumps forward.

Modification: What if instead the Goomba sits 100 away.

If a solution (x_0, y_0) exists, then $24x_0 + 9y_0 = 100$

Since $3 | 24$, and $3 | 9$, 3 divides left-hand side by DIC

$3 \nmid 100$ by DIC. Since $3 \nmid 100$, no solution can exist.

Ex. Find the complete set of solutions to the LDE $42x - 18y = 72$.

Solution: We start by finding a particular solution via EEA

x_i	y_i	r_i	q_i
1	0	42	0
0	1	18	0
1	−2	6	2
–	–	0	3

use positive numbers in EEA

We have $\gcd(42, -18) = \gcd(42, 18) = 6$

Since $6 \mid 72$, a solution exists.

We have $42(1) + 18(-2) = 6$, so $42(1) - 18(2) = 6$

multiplying by 12, $42(12) - 18(24) = 72$

Thus, $x_0 = 12$ $y_0 = 24$

$a = 42$ $b = -18$ $d = \gcd(42, -18) = 6$

Complete solution:

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

$= \{(x,y): x = 12 - 3n,\ y = 24 - 7n,\ n \in \mathbb{Z}\}$

Ex. Find all solutions to the LDE $24x + 9y = 150$

Recall: $(x_0, y_0) = (-50, 150)$ is a particular solution.

$x_0 = -50$ $y_0 = 150$ $a = 24$, $b = 9$ $\gcd(a,b) = 3$

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

$\{(x,y): x = -50 + 3n$ $y = 150 - 8n,\ n \in \mathbb{Z}\}$

Modification: Mario is not willing to jump backward. Can he still reach the Goomba 150m away? Find all possible ways.

Solution: We require $x \geq 0$ and $y \geq 0$,

Since $(x,y) = (-50 + 3n, 150 - 8n)$ for some $n \in \mathbb{Z}$

we have $x \geq 0 \Rightarrow -50 + 3n \geq 0$

$\Rightarrow 3n \geq 50$

$\Rightarrow n \geq \frac{50}{3} \approx 16.6$

$\Rightarrow n \geq 17$ (as $n \in \mathbb{Z}$)

$y \geq 0 \Rightarrow 150 - 8n \geq 0$

$\Rightarrow 150 \geq 8n$

$\Rightarrow n \leq \frac{150}{8} = 18.75$

$\Rightarrow n \leq 18$

Thus, $17 \leq n \leq 18$, so $n = 17$ or $n = 18$

when $n = 17$ $(x,y) = (-50 + 3n, 150 - 8n) = (1, 14)$

when $n = 18$ $(x,y) = (4, 6)$

Chapter 8 - Congruence and Modular Arithmetic

Remark: In many divisibility problems we are most interested in remainders.

Ex. Find gcd(2500, 1750) (look for the remainder in EEA!)

Ex. Is $5^{9} + 62^{2000} - 14$ divisible by 7? i.e. Is the remainder 0 after dividing by 7.

Idea: Group together numbers with the same remainder after division by m?

Ex. With $m=3$

Remainder 0

$0, 3, 6, 9 \ldots; -3, -6, -9$

Remainder 1

$1, 4, 7 \ldots; -2, -5, -8$

$3(-1)+1$

Remainder 2

$2, 5, 8 \ldots, -1, -4, -7$

Two integers a, b are said to be congruent module m if they have the same remainder division by m.

Definition: Given $m \in \mathbb{N}$, we say that integers a, b are congruent modulo m if $m \mid (a-b)$

Ex. Decide whether each of the pairs are congruent modulo m.

(a) $a=22$ $b=10$ $m=3$

(b) $a=10$ $b=22$ $m=3$

(c) $a=10$ $b=-10$ $m=3$

(d) $a=10$ $b=-10$ $m=4$

Proposition For all $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, if $a_1 \equiv b_1 \pmod m$, and $a_2 \equiv b_2 \pmod m$ then

(i) $a_1 + a_2 \equiv b_1 + b_2 \pmod m$

(ii) $a_1 - a_2 \equiv b_1 - b_2 \pmod m$

(iii) $a_1 a_2 \equiv b_1 b_2 \pmod m$

Proof: Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and assume that $a_1 \equiv b_1 \pmod m$ and $a_2 \equiv b_2 \pmod m$

By definition, $m \mid (a_1 - b_1)$ and $m \mid (a_2 - b_2)$

By (i), m divides $(a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$

so $(a_1 + a_2) \equiv (b_1 + b_2) \pmod m$

(ii) Exercise

(iii) By (i), m divides $(a_1 - b_1)a_2 + (a_2 - b_2)b_1$

$= a_1 a_2 - b_1 b_2$

so $a_1 a_2 \equiv b_1 b_2 \pmod m$ □

Remark: This prop says that if $a \equiv b \pmod m$, then for many $c \in \mathbb{Z}$. Since $c \equiv c \pmod m$.

We have $a + c \equiv b + c \pmod m$

$a - c \equiv b - c \pmod m$

$ac \equiv bc \pmod m$

Proposition 3 **(Congruence Add and Multiply (CAM))**

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

1. $a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \pmod m$,
2. $a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod m$.

Ex. Is $5^9+62^{2000}-14$ divisible by 7

We want to know if $5^9+62^{2000}-14 \equiv 0 \pmod 7$

Solution:

Note $14=0 \pmod 7$

Thus, $5^9+62^{2000}-14 \equiv 5^9+62^{2000}-0$

$\equiv 5^9+62^{2000} \pmod 7$

Note $62=-1 \pmod 7$

So by CP, $62^{2000} \equiv (-1)^{2000} \pmod 7$

Since $(-1)^{2000}=1$, we have $62^{2000}=1 \pmod 7$

By CAM:

$5^9+62^{2000}=5^9+1 \pmod 7$

Note $5=-2 \pmod 7$

By CP: $5^9 \equiv (-2)^9 \pmod 7$

So $5^9 \equiv (-1)^9 2^9$

$\equiv (-1)(2^3)^3$

$\equiv (-1)(8)^3$

$8 \equiv 1 \pmod 7$

$\equiv -1 \cdot 1^3$

$\equiv -1 \pmod 7$

So $5^9+62^{2000}-14$

$=-1+1+0$

$=0 \pmod 7$

So yes! $7 \mid (5^9+62^{2000}-14)$

Remark: In general, it is NOT true that if $ac=bc \pmod m$ then $a \equiv b \pmod m$

Ex: $70 \equiv 40 \pmod 6$

but when we divide by 2; $35 \not\equiv 20 \pmod 6$

Proposition [Congruence Divide (CD)]

Proposition 5 **(Congruence Divide (CD))**

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

Proof: Let a, b and c be arbitrary integers, and assume that $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$. Since $ac \equiv bc \pmod{m}$, we obtain $m \mid (ac - bc)$ by the definition of congruence, so $m \mid c(a-b)$. Since $\gcd(c, m) = 1$, we can apply the proposition Coprimeness and Divisibility, which gives $m \mid (a-b)$. Hence, by the definition of congruence we conclude that $a \equiv b \pmod{m}$. □

(Congruent Iff Same Remainder (CISR))

For all integers a and b, $a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m.

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

By DA, we can write $a = mq_1 + r_1$, $b = mq_2 + r_2$ for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \le r_1, r_2 < m$

Assume first that $a \equiv b \pmod{m}$, so $m \mid (a-b)$. Hence $a - b = mk$ for some $k \in \mathbb{Z}$

Thus, $mk = a - b$

$= [mq_1 + r_1] - [mq_2 + r_2]$

$= m(q_1 - q_2) + (r_1 - r_2)$

So, $m(k - q_1 + q_2) = r_1 - r_2$

Thus, $r_1 - r_2$ is a multiple of m but $-m < r_1 - r_2 < m$

So $r_1 - r_2 = m$ hence, $r_1 = r_2$

Assume now that $r_1 = r_2$, we have $a - b = [mq_1 + r_1] - [mq_2 + r_2]$

$= m(q_1 - q_2)$

Thus, $m \mid (a-b)$. so $a \equiv b \pmod{m}$

□

Corollary [Congruent to Remainder (CTR)]

For all $a, b \in \mathbb{Z}$, with $a \le b < m$, $a \equiv b \pmod{m}$

iff b is the remainder of a after division by m.

Ex. Find the remainder when $7^{100(999)} - 6^{83}$ is divided by 4

Solution: Note that $4 \mid 1000$

So $999 \equiv (-1) \pmod 4$ $\quad 999 - (-1)$

Also $77^{100} \equiv 1^{100}$

$\equiv 1 \pmod 4$

Finally, $6^{83} \equiv 2^{83}$ (as $6 \equiv 2 \pmod 4$)

$\equiv \underbrace{6 \cdot 2}_{\equiv 4}{}^{41} \cdot 2$

$\equiv 0^{41} \cdot 2$

$\equiv 0$

By CAM and CP, $77^{100(999)} - 6^{83}$

$\equiv (1)(-1) - 0$

$\equiv -1 \equiv 3 \pmod 4$

Thus, remainder $= 3$

Ex. Find the last digit (the units digit) of $5^{32} 3^{10} + 9^{22}$

Solution: We find the remainder after division by 10

We have $9 \equiv (-1) \pmod{10}$

So by CP, $9^{22} \equiv (-1)^{22} \equiv 1 \pmod{10}$

Also, $3^{10} \equiv (3^2)^5 \equiv (-1)^5 \equiv -1 \pmod{10}$

Finally, $5^{32} \equiv (5^2)^{16}$

$\equiv 25^{16}$ — By CAM and CP, we have $5^{32} 3^{10} + 9^{22}$

$\equiv (5^2)^8$ $\equiv 5(-1) + 1$

$\equiv (5^2)^4$ $\equiv -5 + 1$

$\equiv 5^4$ $\equiv -4$

$\equiv 625$ $\equiv 6 \pmod{10}$ — units digit: 6

Divisibility Tests

We can derive quick tests for divisibility using our understanding of congruence.

Proposition [Divisibility by 3]

A non-negative integer a is divisible by 3 iff the sum of its digit is divisible by 3.

Proof: Let a be a non-negative integer.

We can write $a = d_0 + d_1 \cdot 10 + d_2 \cdot 10^2 + \dots + d_k 10^k$.

Thus, $a_0 = a_0 + \underbrace{10 a_1}_{10 \equiv 1 \pmod 3} + \cdots + 10^k a_k$

$\equiv a_0 + a_1 + \cdots + a_k \pmod 3$

Since a and the sum of its digits are congruent mod 3, we have that $a \equiv 0 \pmod 3$ iff $a_0 + a_1 + \cdots + a_k \equiv 0 \pmod 3$

Now that we have studied the basic algebra surrounding congruence (+, −, ·, ÷?) it's time to start solving equations

Ex: Find integers x such that $4x \equiv 5 \pmod 8$

Solution: The solution are the integers x such that $8 \mid (4x-5)$

That is, $4x-5 = 8k$ for some $k \in \mathbb{Z}$

Equivalently, $4x+8y=5$ for some $y \in \mathbb{Z}$, this is an LDE!

Since $\gcd(4,8)=4$ and $4 \nmid 5$, LDET1 says there are no solutions thus $4x \equiv 5 \pmod 8$ has no solution.

Ex. Consider the congruence $5x \equiv 3 \pmod 7$

(a) Does this equation have solution?

Solution: We can write this as an LDE. $5x+7y=3$

Since $\gcd(5,7) \mid 3$, solution exist by LDET1.

(b) Find all solutions to $5x \equiv 3 \pmod 7$

Solution: We find the complete solution to the LDE

A particular solution is $(x,y) = (-2,1)$

By LDET2, the complete solution is $\{(x,y): x = -2+7n,\ y = 1-5n,\ n \in \mathbb{Z}\}$

Thus, $x = -2+7n$, $n \in \mathbb{Z}$ so $x \equiv 2 \pmod 7$

Alternatively,

Every $x \in \mathbb{Z}$ is congruent to some $x_0 \in \{0,1,2,3,4,5,6\}$

If $x \equiv x_0 \pmod 7$ and $5x_0 \equiv 3 \pmod 7$ then $5x \equiv 5x_0 \equiv 3 \pmod 7$

So we can check all values $x_0 \in \{0,1,2,3,4,5,6\}$

Ex. Solve $2x \equiv 4 \pmod 6$

Solution:

Method 1: check $x_0 \in \{0,1,2,3,4,5\}$

$2(0) = 0 \pmod 6$ ✗

$2(1) = 2$ ✗

$2(2) = 4$ ✓

$2(3) = 0$ ✗

$2(4) = 2$ ✗

$2(5) = 4$ ✗

So $x \equiv 2 \pmod 6$ or $x \equiv 5 \pmod 6$

Method 2: Consider the LDE $2x+6y=4$, solution exist as $\gcd(2,6) \mid 4$

Particular solution: $(x,y)=(2,0)$

Complete solution: $\{(x,y): x=2+3n, y=0-n, n\in\mathbb{Z}\}$

So $x=2+3n, n\in\mathbb{Z}$

Hence $x\equiv 2 \pmod 3$

Linear Congruence Theorem (LCT)

Let $a,c\in\mathbb{Z}$ with $a\neq 0$. The congruence $ax\equiv c \pmod m$ has a solution iff $d\mid c$ where $d=\gcd(a,m)$. Moreover, if x_0 is a particular solution, then the complete solution is $x\equiv x_0 \pmod{\left(\frac{m}{d}\right)}$

Equivalently:

$\{x\in\mathbb{Z}: x=x_0, x\equiv x_0+\frac{m}{d}, x\equiv x_0+2\left(\frac{m}{d}\right) \cdots x\equiv x_0+(d-1)\left(\frac{m}{d}\right)\}$ (modulus m)

Proof: Proving the first part will be left as an exercise.

Suppose that $x=x_0$ is a particular solution, so $ax_0\equiv c \pmod m$ or equivalently,

$ax_0+my_0=c$ for some $y\in\mathbb{Z}$

By LDE T2, the complete solution 2 is

$\{x\in\mathbb{Z}: x=x_0+\left(\frac{m}{d}\right)n, n\in\mathbb{Z}\}$

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

Alternatively,

$x=\ldots x_0, x_0+\frac{m}{d}$

$x_0+2\left(\frac{m}{d}\right)\ldots$

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

$x_0+d\left(\frac{m}{d}\right)$

Hence, $x\equiv x_0+j\left(\frac{m}{d}\right) \pmod m$ where $0\le j\le d-1$ □

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

Solution: Since $\gcd(9,15)=3$, $3\mid 6$, solution exists.

Looking at $9x+15y=6$

Warm up / Recall

(a) Which is $\mathbb{Z}_5$?

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

(b) In $\mathbb{Z}_5$, what is 3?

$[3] = \{x \in \mathbb{Z}, x \equiv 3 \bmod 5\}$

(c) In $\mathbb{Z}_5$, what is $[2][1] - [6]$?

$= [2][2] - [1] = [3]$

(d) In $\mathbb{Z}_5$, what is $[3]^{-1}$?

$([3][x] = [1])$ $[3]^{-1} = [2]$

(e) In $\mathbb{Z}_6$, what is $[3]^{-1}$?

$([3][x] = [1] \Leftrightarrow 3x \equiv 1 \bmod 6)$

No solutions since $\gcd(3, 6) \neq 1$

(Modular Arithmetic Theorem (MAT))

For all integers a and c, with a non-zero, the equation

$$[a][x] = [c]$$

in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$, where $d = \gcd(a, m)$. Moreover, when $d \mid c$, there are d solutions, given by

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

where $[x] = [x_0]$ is one particular solution.

Proof: From the proposition Congruence Add and Multiply,

$$[a][x_0] = [c],$$

in $\mathbb{Z}_m$, if and only if

$$ax_0 \equiv c \pmod{m}.$$

Hence the solutions to the equation $[a][x] = [c]$ in $\mathbb{Z}_m$ can be determined precisely from the solutions to the congruence relation $ax \equiv c \pmod{m}$. The result now follows directly from the Linear Congruence Theorem. □

REMARK

By comparing the proofs of the Linear Congruence Theorem and Modular Arithmetic Theorem, we see that to find solutions to the equation $[a][x] = [c]$ in $\mathbb{Z}_m$, we should consider the corresponding linear Diophantine equation $ax + my = c$.

Ex. Solve $[8][x] - [1] = [1]$ in $\mathbb{Z}_5$

Solution:

$[8][x] - [1] = [1]$

$[8][x] = [2]$

$\Rightarrow [3][x] = [2]$ in $\mathbb{Z}_5$

Since $\gcd(3,5) = 1$ and $1 | 2$, we have $d = 1$ solution.

$[x] = [4]$ is a particular solution and hence the only solution.

Ex. Solve $[2][x] + [5] = [3]$ in $\mathbb{Z}_6$.

$[2][x] + [5] = [3] \Leftrightarrow [2][x] = [4]$

$\gcd(2,4) = 2, \quad 2 | 6$

Since $d = \gcd(2,6) = 2$ and $2 | 4$, solution exist (in fact, there are $d = 2$ solutions $[x_0] = [x]$ is a particular solution.

Other solution: $[x] = [x_0 + \frac{m}{2}]$

$= [2 + \frac{6}{2}] = [5]$

An alternate approach to our first example.

Recall that $[3]^{-1} = [2]$ in $\mathbb{Z}_5$, so by multiplying both sides of $[3][x] = [2]$ by $[3]^{-1} = [2]$, we get $[3]^{-1}[3][x] = [3]^{-1}[2]$

$\Rightarrow [x] = [2][2] = [4]$

Moral: If we know $[a]^{-1}$, we can easily solve $[a][x] = [c]$

Warning: DO NOT multiply $[a][x] = [c]$ by something that doesn't have an inverse.

Ex. $[3][x] = [4]$ in $\mathbb{Z}_6$ (no solution as $\gcd(3,6) \nmid 4$) But if we multiply by $[2]$:

$[2][3][x] = [2][4] \Rightarrow [0][x] \Rightarrow [0]$ in $\mathbb{Z}_6$

(3 solutions, as $d = \gcd(3,6) = 3$ and $3 | 0$

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

Let a be an integer with $1 \leq a \leq m-1$. The element $[a]$ in $\mathbb{Z}_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$. Moreover, when $\gcd(a, m) = 1$, the multiplicative inverse is unique.

Consider the situation for multiplicative inverses when m is a prime, say $m = p$. Then in the above corollary Inverses in $\mathbb{Z}_m$, the condition $\gcd(a, p) = 1$ is true for all a not divisible by p. We record the result in this case separately, below.

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

For all prime numbers p and non-zero elements $[a]$ in $\mathbb{Z}_p$, the multiplicative inverse $[a]^{-1}$ exists and is unique.

Fermat's Little Theorem (FLT)

For all integers a and all primes p, if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$

Ex. $2^6 \equiv 1 \pmod{7}$

$6^6 \equiv 1 \pmod{7}$

$100^6 \equiv 1 \pmod{7}$

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

Solution: Since 11 is prime, and $11 \nmid 7$, FLT says that $7^{10} \equiv 1 \pmod{11}$

We have $7^{92} \equiv (7^{10})^9 \cdot 7^2$

$\equiv 1^9 \cdot 7^2$

$\equiv 49$

$\equiv 5 \pmod{11}$

Ex: Let $r, s, p, a \in \mathbb{Z}$ and assume p is prime. Prove that if $p \nmid a$ and $r \equiv s \pmod{p-1}$ then $a^r \equiv a^s \pmod{p}$

Proof: Assume $p \nmid a$ and that $r \equiv s \pmod{p-1}$

Ex: Let $r, s, p, a \in \mathbb{Z}$ and assume p is prime. Prove that if $p \nmid a$ and $r \equiv s \pmod{p-1}$ then $a^r \equiv a^s \pmod{p}$

Proof: Assume $p \nmid a$ and that $r \equiv s \pmod{p-1}$

$p-1 \mid r-s$

let $r-s = k(p-1)$ for some $k \in \mathbb{Z}$

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

$a^{k\cdot(p-1)} \equiv 1 \pmod{p}$

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

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

Corollary

For all primes p and all $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$

Ex. Find all integers x such that
$17x^{22}+x^{6}+x^{5}-x \equiv 3 \pmod{15}$

Ex. Solve $\begin{cases} x \equiv 3 \pmod{13} \\ x \equiv 2 \pmod{12} \end{cases}$

$13 \mid x-3$

$x = 13k+3$ $\qquad x = 12k+2$

$n = pq$

$\phi(n) = (p-1)(q-1)$

$1 < e < \phi(n)$ $\gcd(e, \phi(n)) = 1$

$ed \equiv 1 \pmod{\phi(n)}$ $1 < d < \phi(n)$

public key (e, n)

private key (d, n)

(a) $n = 143$

$\phi(n) = 120$

$103d \equiv 1 \pmod{120}$

$(103, 143)$

$(7, 143)$

30