12/10/21

LO1

MATH 111 - Number Theory

Look at Set Theory - CSS 120 LO1

11/10/21

$\mathbb{N}$ - Natural Numbers $\{1, 2, 3, 4 \ldots\}$

($\mathbb{Z}^+$) $\mathbb{N}$ - Natural Numbers and zero $\{0, 1, 2, 3 \ldots\}$

Be careful with zero

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

$\mathbb{Q}$ - Rational Numbers $\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$

$\mathbb{R}$ - Real Numbers

↖ All possible real numbers (infinite set)

e.g $\sqrt{2}$, π, e, 1.57

The empty set is written $\varnothing \quad \{\}$

You can enumerate an infinite set with an ellipses

$\mathbb{N} = \{1, 2, 3, \ldots\}$

Preliminaries

$P(x)$ stands for a specified property

$\{x \in A \mid P(x)\}$

$\{\ldots \mid \ldots\}$

Elements — such That — Must Satisfy

LOOK at Ex 1.3.A

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

i) $B = \{n \in \mathbb{Z} : 3n+1 \in A\}$

$B = \{0, 1, 2, 3\}$

ii) $C = \{3n+1 : n \in A\}$

$C = \{4, 7, 10, 13, 16, 19, 22, 25, 28, 31\}$

iii) $D = \{n \in A : 3n+1 \in \mathbb{Z}\}$

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

1.3.B

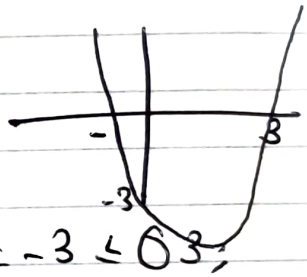
i) $E = \{x \in \mathbb{R} : x^2 - 2x - 3 > 0\}$

Solutions / values when over 0

$(x^2 - 2x - 3)$

$(x+1)(x-3) = -1, 3$

when $x < -1$, $x > 3$



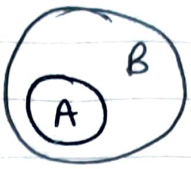
ii) $F = \{x \in \mathbb{N} : x^2 - 2x - 3 \leq 0\}$

$F = \{0, 1, 2, 3\}$

02/11/21

LO2

MATH 111 LO2



Subset ($\subseteq$)

if A is a subset of B if every element of A also lies in B

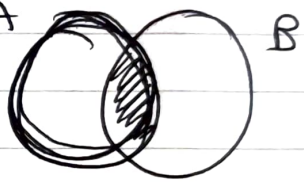
$A \subseteq B$

If $A \subseteq B$ and $B \subseteq A$, $A = B$

Disjoint

If A intersection $B (\cap) = \emptyset$ (empty set) then they are disjoint

Another rule is $(A \cap B) \subseteq A$



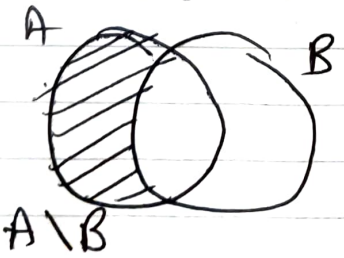
$A \subseteq (A \cup B)$

Set Theoretic Difference ($\setminus$)

$A \setminus B = \{ x \in A \mid x \notin B \}$

When there is none in common

This is the set of elements belonging to A and not B



Logic LO2

The Parity Model

- The universe — variables
- The parity values — the parity switcher
- The parity table — the operations
- Expressions — equivalence of expressio

Universe = $\mathbb{Z}$
Variables = any elements
Parity values = D (odd) E (even)
Parity switcher = 1 - integer

Parity Table

x	$\sim x$
D	E
E	D

There are two operations + (plus) and × (times) which can be used to create expressions from variables

Parity Table of Expressions

x	y	$x+y$
D	D	E
D	E	D
E	D	D
E	E	E

(Almost like XOR)
(If D was 1)

x	y	$x \times y$
D	D	D
D	E	E
E	D	E
E	E	E

(Almost like AND)

~ Acts as a NOT
Use brackets for more complicated expressions + parity tables.

Equivalent expressions are different expressions with the same party table.

Logic Model

Universe — Statement Variable
Truth Value — Negation
Truth table — Conjecture
Compound Statement — Logical Equivalence of Statements

The structure is similar to the parity model with corresponding different terms

Universe - All allowable statements (definitely either true or false statements)

Statement Variables - Letters are used to represent variables

Truth values - T (true), F (false)

The negation - $\neg p$ = not p

Truth tables

p	$\neg p$
T	F
F	T

Logically equivalent statements have the same truth tables, for example this can mean double negations.

Connectives + Compound Statements

Connectives

Symbol	Name	Meaning	Alternate Symbols
&	Conjunction	And	$\wedge, \cap, \times, \cdot$
or	Disjunction	Or	$\vee, \cup, +$
$\Rightarrow$	Implication	Implies	$\rightarrow$
$\Leftarrow$	Reverse Implication	Is Implied by	$\leftarrow$
$\Leftrightarrow$	Bi-Implication	If and only if	$\leftrightarrow$, iff

p	q	p or q
T	T	T
T	F	T
F	T	T
F	F	F

OR

p	q	p & q
T	T	T
T	F	F
F	T	F
F	F	F

AND

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

If p then q (implication)
Analogy of p = studying
q = passing tests
This is called material implication

p	q	$p \Leftarrow q$
T	T	T
T	F	T
F	T	F
F	F	T

This is just the other way around where q implies p.
so TF and FT swap.

p	q	p ⇔ q
T	T	T
T	F	F
F	T	F
F	F	T

Remember both for parity and logic model to write the appropriate number of variable rows using ascending binary

$\neg(p \text{ or } q) \equiv (\neg p) \,\&\, (\neg q)$

Contrapositive statement:

$p \Rightarrow q \equiv (\neg q) \Rightarrow (\neg p)$

This is called the law of contraposition

Negation of Implication:

$\neg(p \Rightarrow q) \equiv p \,\&\, (\neg q)$

14/10/21

LO3

MATH 111 LO3

Quantifiers:

Universal quantifier $\forall$ for all
Existential quantifier $\exists$ there exist

e.g $(\forall n \in \mathbb{N})(n^2 \in \mathbb{N})$
and $(\exists x \in \mathbb{R})(x^2 + 1 = 0)$

$\exists$ can also mean: for some,

You need to be able to use these in writing

e.g There exists a natural number whose square root is greater than five,

$$(\exists n \in \mathbb{N})(\sqrt{n} > 5)$$

If $()$ begins with a quantifier it must be followed by more $()$ with no connective
If $()$ doesn't have a quantifier it must have a connective between $()$

e.g use $\Rightarrow$

e.g $\sqrt{2}$ is a rational number

$$(\exists a \in \mathbb{Z})(\exists b \in \mathbb{N})(\sqrt{2} = a/b)$$

True (~~False~~) For every integer greater than 1 can be written as a product of primes

$(\forall n \in \mathbb{Z} \cap (1, \infty))(\exists m \in \mathbb{N})$
$(\exists p_1, \ldots, p_m \in \mathbb{P})(n = p_1 p_2 \cdots p_m)$

$\mathbb{P}$ for prime set

Be careful with ordering

For negation, one person did not ... $P(x)$

$\neg((\exists x \in A)(P(x)))$
is equivalent to
$(\forall x \in A)(\neg P(x))$

$\forall$ can be considered the negation of $\exists$ when reordering equivalents

14/10/21

LO4

MATH 111 LO4

Mathematical Proofs

□, ■, QED Marks the end of a proof

Direct Proof

- Starts by some assumption

e.g. Verify $x = \sqrt{2+\sqrt{2}}$ satisfies $x^4 - 4x^2 + 2 = 0$

Proof:

Let $x = \sqrt{2+\sqrt{2}}$

$x^2 = (\sqrt{2+\sqrt{2}})^2 = 2 + \sqrt{2}$

$x^4 = (2+\sqrt{2})^2 = 4 + 2 + 4\sqrt{2}$

$x^4 = 6 + 4\sqrt{2}$

Hence

$x^4 - 4x^2 + 2 = (6 + 4\sqrt{2}) - 4(2+\sqrt{2}) + 2$

$= 6 + 4\sqrt{2} - 8 - 4\sqrt{2} + 2$

$= 6 + 2 - 8$

$= 8 - 8$ □

e.g Check $y = 3e^{2x} - 2e^{3x}$ is a solution to

$$\frac{d^2y}{dx^2} - 5\frac{dy}{dx} + 6y = 0$$

Proof:

Let $y = 3e^{2x} - 2e^{3x}$

$dy/dx = 6e^{2x} - 6e^{3x}$

$d^2y/dx^2 = 12e^{2x} - 18e^{3x}$

Hence

$(12e^{2x} - 18e^{3x}) - 5(6e^{2x} - 6e^{3x}) + 6(3e^{2x} - 2e^{3x})$

$= 12e^{2x} - 18e^{3x} - 30e^{2x} + 30e^{3x} + 18e^{2x} - 12e^{3x}$

$= 18e^{2x} - 18e^{2x} - 18e^{3x} + 18e^{3x} = 0$ □

9/10/21

L05

MATH 111 L01

Example 2.4.7

$(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(m = n+1)$ is true

Proof:

$(n \in \mathbb{N}) \Rightarrow (\exists m \in \mathbb{N})(m = n+1)$

Let $n \in \mathbb{N}$ be given

Define $m = n+1$, which is a natural number □

$(\exists m \in \mathbb{N})(\forall n \in \mathbb{N})(m = n+1)$ is false

Proof:

To prove a statement is false we must prove it's negation is true

$(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})(m \neq n+1)$ Negation

We prove this:

$(m \in \mathbb{N}) \Rightarrow (\exists n \in \mathbb{N})(m \neq n+1)$ equivalent

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

Define $n = m \in \mathbb{N}$:

Then $n+1 \neq m$ □

Therefore order matters

Direct Proof:

x	y	x+y
D	D	E

x	y	x·y
D	D	D

Proof:

Let $x = 2m+1$, $y = 2n+1$ $\quad m, n \in \mathbb{Z}$

$x+y = (2m+1) + (2n+1)$

$= 2m + 2n + 2$

$= 2(m+n+1)$ $\quad \therefore$ Even

($m+n+1 \in \mathbb{Z}$)

$x \cdot y = (2m+1)(2n+1)$

$= 4mn + 2m + 2n + 1$

$= 2(2mn + m + n) + 1$ $\quad =$ Odd

($2mn + m + n \in \mathbb{Z}$) $\quad \square$

$(\forall x \in A)(P(x)) \equiv (x \in A) \Rightarrow (P(x))$

Logically Equivalent

3.2.B

$m^2 + n + mn^2$ is always even

m	n	$m^2 = m$ in parity	$n^2 = n$ in parity	$= m+n+mn$
D	D			
D	E			
E	D			
E	E			

$m+n$	$m+n+mn$
E	
D	
D	
E	

m	n	$m+n$	mn	$(m+n)+mn$
D	D	E	D	D
D	E	D	E	D
E	D	D	E	D
E	E	E	E	E

$m \neq n + mn \quad = mn + mn = 2(mn)$

Case 1: m and n both odd

mn = odd , $m+n$ = even

m and $n \in \mathbb{Z}$ Therefore $2(mn)$ = even

3.2.10 Look at 3.2.10

↓

if and only if means bi-implication connective (2 proofs)

Proof by Contraposition

$p \Rightarrow q \equiv (\neg q) \Rightarrow (\neg p)$

Example 3.3.1

Let x be real If $x^2 < 9$ then $x < 3$

$\neg(x < 3) \Rightarrow \neg(x^2 < 9)$

$(x \geq 3) \Rightarrow (x^2 \geq 9)$ True

Therefore by law of contraposition this is true

19/10/21

L06

MATH 111 L02

Proof by Contraposition

$p \Rightarrow q \equiv (\neg q) \Rightarrow (\neg p)$

3.3.3 Let n = integer. n is even if and only if n^2 is even

$(n^2$ is even$) \Rightarrow (n$ is even$)$

By contraposition

$\neg(n$ is even$) \Rightarrow \neg(n^2$ is even$)$

$(n$ is odd$) \Rightarrow (n^2$ is odd$)$

Let $n = 2m+1$

$(2m+1)^2 = 4m^2 + 4m + 1$

$= 2(2m^2 + 2m) + 1$ ∴ Odd □

$2m^2 + 2m \in \mathbb{Z}$

* Try 3.3.4 , 3.3.5 , 3.3.A

Proof by Contradiction

$\neg(p \Rightarrow q) \equiv p \text{ and } (\neg q)$

$p \Rightarrow q \equiv \neg(p \text{ and } (\neg q))$

3.4.1 There is a rational number which is greater than every natural number

$(\exists r \in \mathbb{Q})(\forall n \in \mathbb{N})(r > n)$

Claim: False, so negation true

$(\forall r \in \mathbb{Q}) \neg((\forall n \in \mathbb{N})(r > n))$

$\underbrace{(r \in \mathbb{Q})}_{p} \Rightarrow \underbrace{\neg((\forall n \in \mathbb{N})(r > n))}_{q}$

Proof by contradiction

$p \Rightarrow q \equiv p \text{ and } (\neg q)$

Assume p and $(\neg q)$

$(r \in \mathbb{Q})$ and $(\forall n \in \mathbb{N})(r > n)$

Observe: $r > 1$, so $r = \frac{k}{m}$ for some $k, m \in \mathbb{N}$ with $k > m$

Define $n = k + 1$. Then $n = k + 1 > k \geq \frac{k}{m} = r$

This contradicts that $r > n$ □

3.4.2 The most famous proof by contradiction

$\sqrt{2}$ is irrational

$x = \sqrt{2}$ $x^2 = 2$

$((x \in (0, \infty) \text{ and } (x^2 = 2)) \Rightarrow (x \notin \mathbb{Q})$

$(x \in (0, \infty) \text{ and } (x^2 = 2) \text{ and } \neg(x \notin \mathbb{Q}))$

$(x \in (0, \infty) \text{ and } (x^2 = 2) \text{ and } (x \in \mathbb{Q}))$

$(x \in (0, \infty)$ and $(x^2 = 2)$ and $(x \in \mathbb{Q})$
Then write $x = a/b$ where $a, b \in \mathbb{N}$
Assume a and b have no common factors (Simplified)

$$2 = (\sqrt{2})^2 = x^2 = (a/b)^2 = \frac{a^2}{b^2}$$

$2 = a^2/b^2$ $a^2 = 2b^2$

Therefore a^2 is even, a is even

$\therefore a = 2c$ where $c \in \mathbb{N}$

$(2c)^2 = 4c^2 = 2b^2$

$b^2 = 2c^2$ Therefore b^2 is even. b is even

This is a contradiction as it shows a common factor of 2 when there should be no common factors

□

Proof by Counterexample

Just need to display one instance that disproves a statement

Terminology

Theorem - Important result that has been proved
Proposition - Less important result - proved
Lemma - stepping stone in further proof
Corollary - Consequence of another result - proved
Conjecture - Not yet proved
Counterexample - Example shows conjecture false

* How to Self-Explain proof Lara Alcock

Number Theory –

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

a divides b if there exists $q \in \mathbb{Z}$ such that $b = qa$

$a \mid b$ = a divides b (a is a factor / divisor of b)

$a \nmid b$ = a doesn't divide b

(+/-) signs are irelevant to questions of divisibility

If either $a = 0$ or $b = 0$ or both then $\mathbb{Z}$ has no zero divisors

4.1.6 (i)

If $a \mid b$ and $b \mid c$ then $a \mid c$

Proof:

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

Then: $b = aq$ and $c = br$ for some $q, r \in \mathbb{Z}$

$c = br = (aq)r = a(qr)$

so $a \mid c$ □

21/10/21

LO7

MATH 111 L03

* Self-Explain Lara Alcock

Recall $a, b \in \mathbb{Z}$ $a|b$ a is a factor of b if $b = qa$ for some $q \in \mathbb{Z}$

Don't confuse
- \ Set-Theory difference
- | is a factor of or divides
- / division, fractions e.g 2/3

4.1.6 (ii) If $a|b$ then $ac|bc$

Proof: (Direct) Suppose $b = qa$ for some $q \in \mathbb{Z}$

Then $bc = (qa)c = q(ac)$ so $ac|bc$. □

$|x|$ = Absolute value (modulus)

4.1.6 (iii) $a|1$ if and only if $a = \pm 1$

Bi-implication (prove $\Rightarrow$, $\Leftarrow$)

$\Rightarrow$ Suppose $a|1$, so $1 = aq$ for some $q \in \mathbb{Z}$. Then $1 = |1| = |aq| = |a| \cdot |q|$

Note: $|a|, |q| \in \mathbb{N}$, and $1 = 1 \cdot 1$ is the only factorisation of 1 as a product of two natural numbers.

Hence: $|a| = 1$, $|q| = 1$, $a = \pm 1$

$\Leftarrow$ Suppose $a = \pm 1$ then $1 = a \cdot a$ so $a|1$

□

Bi-implication

4.1.6 (iv) $a|b$ and $b|a$ if and only if $b = \pm a$

Proof:

$\Rightarrow$ Suppose $a|b$ and $b|a$, say $b = qa$ and $a = rb$, $q, r \in \mathbb{Z}$

$a = rb = r(qa) = rq(a)$ so $(rq) = 1$

and $r, q \in \mathbb{Z}$

$0 = (rq)a - a$

$= (rq - 1)a = 0$

Hence either $a = 0$ or $rq - 1$ is 0

If $a = 0$, then $b = 0$ so $a = b$

Otherwise $rq = 1 \therefore q | 1$ so $q = \pm 1$ by (iii)

Then $b = qa$ $\quad b = (\pm 1)a$

$b = \pm a$

$\Leftarrow$ Suppose $\underline{b = a}$ or $\underline{b = -a}$

clearly $a|b$, $b|a$ because $a = 1 \cdot b$, $b = 1 \cdot a$

$b = (-1)a$ so $a|b$ Also $a = (-1)b$ so $b|a$

Proved for both cases □

Theorem Division with Remainder

Theorem 4.18

4.1.9

Theorem 4.18 Division with Remainder

Proof: Given $a \in \mathbb{Z}$ and $d \in \mathbb{N}$ there exist unique $q, r \in \mathbb{Z}$ such that $a = qd + r$ and $0 \leq r < d$

"Existence": Define *
$S = \{n \in \mathbb{Z} : dn \leq a\}$

I want to define q to be the max of set S

I must check:

- $S \neq \emptyset$ (because $-|a| \in S$ because $-|a| \in \mathbb{Z}$ and $d \cdot (-|a|) = -d \cdot |a|$ (≥ 1)
  so $-d \cdot |a| \leq 1$
  $-|a| \leq a$)
- S is bounded above $S \subseteq (-\infty, |a|]$, that is, $(n \in S) \Rightarrow (n \leq |a|)$

Proof by contraposition:
Suppose $n > |a|$, then $dn \geq n > |a| \geq a$ ($d \geq 1$)

* $dn > a$ so $n \notin S$

Define $r = a - qd \in \mathbb{Z}$ Then $a = qd + r$ by definition. Moreover, $q \in S$, so $dq \leq a$, so $0 \leq a - dq = r$.
Also $q+1 \notin S$ because q is the max of S
so $d(q+1) > a$
so $dq + d > a$
so $d > a - dq$
so $d > r$
In conclusion, $0 \leq r < d$.

"Uniqueness"

Suppose $a = q_1 d + r_1$ and $a = q_2 d + r_2$ where $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < d$

Need to show: $r_1 = r_2$ and $q_1 = q_2$

LO4...

We may suppose $r_1 \geq r_2$

I show:

- $r_1 - r_2 \in \{0, 1, \ldots d-1\}$
- $d \mid r_1 - r_2$

Once this is shown $r_1 - r_2 = 0$

$r_1 - r_2 \in \mathbb{Z}$ and $r_1 \geq r_2$, so $r_1 - r_2 \geq 0$

Also $r_1 - r_2 \leq r_1$ because $r_2 \geq 0$

$r_1 \leq d-1$. $r_1 - r_2 \leq d-1$ so $r_1 - r_2 = 0$

Second bullet point:

$r_1 - r_2 = (a - q_1 d) - (a - q_2 d)$

$r_1 - r_2 = a - q_1 d - a + q_2 d$

$r_1 - r_2 = (q_2 - q_1) d$

$\therefore d \mid r_1 - r_2$ ($q_2 - q_1 \in \mathbb{Z}$)

So $r_1 - r_2$ must be equal to 0

Hence $r_1 = r_2$

$(q_2 - q_1) d = 0$ and $d \neq 0$

so $(q_2 - q_1) = 0$

so $q_1 = q_2$

$q_1 = q_2$

$r_1 = r_2$ □

21/10/21

LO8

MATH 111 LO4 (Bezout, Eudidean)

A common factor is a factor that divides both a and b
The set of common factors of a and b is the intersection of the sets of factors of a and b

If a and b are both not-zero the set of common factors is non-empty and bounded above (by $|a|$ if $a \neq 0$). This largest element is named the highest common factor

hcf(18, 30) = highest common factor of 18 and 30.
hcf(18, 30) = 6

Rules
- hcf(0, 0) = undefined
- hcf(a, b) = hcf(-a, b) signs don't matter
- hcf(a, b) = hcf(b, a) order doesn't matter
- if $b|a$ hcf(a, b) = $|b|$.

Lemma 4.2.6

Let $a, b \in \mathbb{Z} \setminus \{0\}$ $d \in \mathbb{N}$ is a common factor of a and b. If every other factor is also a factor of d then d is the hcf.

An (integral) linear combination of two integers a and b is an integer c
$c = ra + sb$ for some $r, s \in \mathbb{Z}$

eg $114 = 3(18) + 2(30)$
114 is integral linear combination of 18 and 30

r and s will never be the same (unique) as then the linear combination must be factors.

Example 4.2.10

Suppose $n = ra + sb$

$= ra + ba - ab + sb$

$= (r+b)a + (s-a)b$.

$t \in \mathbb{Z}$ $u \in \mathbb{Z}$

$= ta + ub$

$114 = 3(18) + 2(30)$

$114 = (3+30)18 + (2-18)30$

$114 = (33)18 + (-16)30$

shows there are many linear combinations

Lemma 4.2.11

Let $a, b, c \in \mathbb{Z}$ and suppose c is a common factor of a and b. c is then a factor of every integral linear combination

Proof:

$a = qc$, $b = rc$ for $q, r \in \mathbb{Z}$

Let $n \in \mathbb{Z}$ be an l.l.c of a, b, say $n = sa + tb$, where $s, t \in \mathbb{Z}$

Then $n = sa + tb = s(qc) + t(rc)$

$= (sq + tr)c$. Then c is a factor of n

$\in \mathbb{Z}$. □

Corollary 4.2.13 Let $a, b \in \mathbb{Z} \setminus \{0\}$ and $d \in \mathbb{N}$ is a common factor of a and b which is also a l.l.c of a and b then $d = hcf(a, b)$

Bézout's Theorem. (4.2.15).

Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then hcf (a,b) is the smallest natural number which is an integral linear combination of a and b.

Proof: Let S be the set of natural numbers which are l.l.c of a and b.

$$S = \{n \in \mathbb{N} : (\exists r, s \in \mathbb{Z})(n = ra + sb)\}$$

S is non-empty as $|a| = \pm 1 \cdot a + 0 \cdot b$ so it has a smallest element d

$d = \min S$

$\therefore d = ra + sb$ for some $r, s \in \mathbb{Z}$

Use Theorem 4.1.8 to see $d \mid a$:

$a = qd + t$ with $q, t \in \mathbb{Z}$ and $0 \leq t < d$

Then $t = a - qd$

$= a - q(ra + sb)$

$= a - qra - qsb$

$= (1 - qr)a - (qs)b$

$\in \mathbb{Z}$ $\in \mathbb{Z}$

$\therefore t$ is an l.l.c of a and b and if $t > 0$ then $t \in S$

However $0 \leq t < d$ and d min S so $t \notin S$

so $t = 0$, $a = qd$

and $d \mid a$

A similar argument also shows $d \mid b$

and so d is a common factor of a and b.

Corollary 4.2.13 shows therefore that $d = \text{hcf}(a,b)$

The Euclidean Algorithm (4.3)

A purpose of calculating hcf and writing hcf as an i.l.c

4.3.1 If $a, b, q, r \in \mathbb{Z}$ with $b \neq 0$ and $a = qb + r$ then $hcf(a,b) = hcf(b,r)$

e.g $38 = 4(8) + 6$
$hcf(38,8) = hcf(8,6) = 2$

Proof: Let $d \in \mathbb{Z}$ be a factor of b
$d \mid a$ if and only if $d \mid r$. Lemma 4.2.11
If $d \mid a$ then $d \mid r = a - qb$ and if $d \mid r$ then $d \mid a = qb + r$
Because $a = qb + r$ and $r = a - qb$ is the integral linear combination so d is a common factor of a and b and so $hcf(a,b) = hcf(b,r)$

Example 4.3.3
Find $hcf(115, 25)$
$115 = 4(25) + 15$
$25 = 1(15) + 10$
$15 = 1(10) + 5$
$10 = 2(5) + 0$
so $hcf(115, 25) = 5$
Terminates when remainder 0, inversely

$5 = 15 - 10$
$= 15 - (25 - 15)$
$= 2 \cdot 15 - 25$
$= 2(115 - 4 \cdot 25) - 25$
$= 2 \cdot 115 + (-9)25$

Example Find hcf (49, 237) as an i.l.c

$237 = 4(49) + (41)$
$49 = 1(41) + (8)$
$41 = 5(8) + (1)$
$8 = 8(1) + 0$
so hcf (237, 49) = 1

$1 = 41 - 5(8)$ $\quad 8 = 49 - 41$
$1 = 41 - 5(49 - 41)$
$= 41(6) - 5(49) \quad 41 = 237 - 4(49)$
$= 6(237 - 4(49)) - 5(49)$
$= 6(237) - 24(49) - 5(49)$
$1 = 6(237) - 29(49)$

Example Find hcf (117, 48) as an i.l.c

$117 = 2(48) + (21)$
$48 = 2(21) + (6)$
$21 = 3(6) + (3)$
$6 = 2(3)$
so hcf (117, 48) = 3

$3 = 21 - 3(6) \quad 6 = 48 - 2(21)$
$= 21 - 3(48 - 2(21))$
$= 7(21) - 3(48) \quad 21 = 117 - 2(48)$
$7(117 - 2(48)) - 3(48)$
$3 = 7(117) - 17(48)$

26/10/21

L09

MATH 111 L09

Euclidean Algorithm formula

$a = q_1 b + r_1 \quad (0 < r_1 < |b|)$

$b = q_2 r_1 + r_2 \quad (0 < r_2 < r_1)$

$r_1 = q_3 r_2 + r_3 \quad (0 < r_3 < r_2)$

...

$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \quad (0 < r_{n-1} < r_{n-2})$

$r_{n-2} = q_n r_{n-1} + 0$

4.4 Bézout's Theorem Applications

Chcf(a,b) is the smallest natural number which is an i.l.c.f a and b)

Proposition 4.4.1 $(a, b \in \mathbb{Z} \setminus \{0\})$ and $d \in \mathbb{N}$ has a common factor of a and b.

a) d is the highest common factor of a and b

b) d is an i.l.c.f a and b

c) every common factor is a factor of d

Bézout's theorem proves a) implies b), Lemma 4.2.11 makes b) imply c) c) implies a by Lemma 4.2.6

a) => b)

⇑ ⇙ Proved

c)

Definition 4.4.2

Co-prime means no common factors other than ± 1

Euclid's Lemma

If a and b are co-prime then hcf(a,b) = 1
1 is an i.l.c ∴ since there are no ℕ smaller than 1 this is true by (Bézout's)

Theorem 4.4.6

Let $a, b, p \in \mathbb{Z} \setminus \{0\}$ and suppose $p \mid ab$ and a and p are co-prime then $p \mid b$

Proof:

Since $p \mid ab$, $ab = pq$ for $q \in \mathbb{Z}$

Since hcf $(a,p) = 1$ $\quad 1 = ra + sp$ for $r, s \in \mathbb{Z}$

Then $b = b \cdot 1 = b(ra + sp)$

$= bra + bsp$

$= (ab)r + bsp$ (remember $ab = pq$)

$= (pq)r + bsp$

$= p(qr + bs)$

$\mathbb{Z}$ ∴ $p \mid b$ □

4.4.8 Let $a, b \in \mathbb{Z} \setminus \{0\}$ i.l.c of a and b are precisely multiples of hcf(a,b)

e.g hcf(18, 30) = 6

$6 = 2a - b \quad 24 = 4(6) = 4(2a - b)$

Proof:

Let $d = \text{hcf}(a,b)$ and $n \in \mathbb{Z}$

$(\exists r, s \in \mathbb{Z})(n = ra + sb) \iff (d \mid n)$

$\Rightarrow$ suppose $n = ra + sb$, $d \mid a$ and $d \mid b$

Lemma 4.2.11 implies $d \mid n$

$\Leftarrow$ suppose $d \mid n$ say $n = md$ for some $m \in \mathbb{Z}$

by 4.2.15 $d = ua + vb$ for $u, v \in \mathbb{Z}$

∴

$n = md = (mu)a + (mv)b = ra + sb$ □

Exercise 4.4.A

(using 4.4.8 result)

$-28, -24, 276, 284$ i.l.c of 36 and 48?

$\text{hcf}(36, 48)$

$48 = 1(36) + 12$

$36 = 3(12) + 0$

$\text{hcf} = 12$

$-24, 276$ are multiples of 12 and therefore can be written as i.l.c of 36 and 48.

Proposition 4.4.10 $\text{hcf}(ca, cb) = c \cdot \text{hcf}(a, b)$

e.g. $\text{hcf}(12, 20) = 4$

$\text{hcf}(120, 200) = 10(4) = 40$

Proof:

set $d = \text{hcf}(a, b)$, since $d \mid a$, $cd \mid ca$ and $d \mid b$ so $cd \mid cb$

so cd is a common factor of ca and cb.

Use Bézout's to write as i.l.c

write $d = ra + sb$ for $r, s \in \mathbb{Z}$

$cd = cra + csb$

$= r(ca) + s(cb)$

cd is an i.l.c of ca and cb

$\therefore cd = \text{hcf}(ca, cb)$ and i.l.c of ca and cb (by Prop 4.4.1)

Corollary 4.4.12 Let $a, b \in \mathbb{Z} \setminus \{0\}$ $d = \text{hcf}(a, b)$ $a = d\alpha$ $b = d\beta$ $\alpha, \beta \in \mathbb{Z}$ then α and β are co-prime.

Proof: $\text{hcf}(a, b) = \text{hcf}(d\alpha, d\beta)$

$d = d\,\text{hcf}(\alpha, \beta)$

$\text{hcf}(\alpha, \beta) = 1$ ∎

4.5 Lowest common multiples

4.5.1 $a, b \in \mathbb{Z} \setminus \{0\}$ c is a common multiple of a and b if it is a multiple of a and b
$a|c$ and $a|b$

The set of positive multiples a and b must not $= \emptyset$

4.5.3 The smallest set of common multiples of a and b $= \text{lcm}(a,b)$

If A is the set of multiples of a and B is the set of multiples of b then $\text{lcm}(a,b)$
$= (A \cap B \cap \mathbb{N})$

Theorem 4.5.5 Let $a, b \in \mathbb{N}$

$$\text{lcm}(a,b) = \frac{ab}{\text{hcf}(a,b)}$$

Proof: Let $d = \text{hcf}(a,b)$ $a = d\alpha$ $b = d\beta$, $\alpha, \beta \in \mathbb{N}$
Corollary 4.4.12, Theorem 4.2.7.5 imply
$r, s \in \mathbb{Z}$ such that ab/d is the $\text{lcm}(a,b)$

$r\alpha + s\beta = 1$

$$\frac{ab}{d} = \frac{d\alpha b}{d} = \alpha b \qquad \frac{ab}{d} = \frac{ad\beta}{d} = a\beta$$

so therefore ab/d is a common multiple of a and b.

Suppose c is a common multiple of a and b.

$c = ap$, bq $\quad p, q \in \mathbb{Z}$

$c = c \cdot 1 = c(r\alpha + s\beta) = cr\alpha + cs\beta = (bq)r\alpha +$

$(bq)r\alpha + (ap)s\beta = (qr)(ab) + (ps)(a\beta)$

$= (qr)\left(\frac{ab}{d}\right) + (ps)\left(\frac{ab}{d}\right) = (qr + ps)\left(\frac{ab}{d}\right)$

$(qr + ps) \in \mathbb{Z}$

ab/d is a factor of c

Since c is positive $ab/d \leq c$ so ab/d is the smallest positive common multiple of a and b. This statement is also true when c is a negative common multiple

Therefore

$$lcm(a,b) = \frac{ab}{hcf(a,b)}$$

26/10/21

L10

MATH 111 Prime Numbers (4.6) L10

p is prime if the only natural numbers that divide p are 1 and p itself. Otherwise, p is composite
* 1 is neither prime nor composite ($0, \pm 1$)

Sieve of Eratosthenes - Grid of first 100 and cross out composites.

Reminder [Euclid's Lemma (Let $a, b, p \in \mathbb{Z} \setminus \{0\}$ suppose $p \mid ab$ and $hcf(a,p) = 1$ Then $p \mid b$. (Proved in L09)]

4.6.2 Let $p \in \{2, 3, 4 \ldots\}$ Then p is prime, when $a, b \in \mathbb{N}$ and $p \mid ab$ then $p \mid a$ or $p \mid b$.
$(\forall a, b \in \mathbb{N})\,((p \mid ab) \Rightarrow ((p \mid a) \text{ or } (p \mid b)))$

Proof:
If $p \mid a$ then true so assume $p \nmid a$. Suppose p is prime so $p \nmid a$. Then $hcf(a,p) \neq p$ so $hcf(a,p) \mid p$ and p is prime so $hcf(a,p) = 1$.
Euclid's Lemma means $p \mid b$ and so this is true.
$\Leftarrow$ contraposition $(s \Rightarrow t)$ Negate $(t \Rightarrow s)$ $(\neg s \Rightarrow \neg t)$
Suppose p is composite then $p = ab$ for $a, b \in \{2, 3, 4, \ldots, p-1\}$
$\therefore p \mid ab$ but $p \nmid a$ or $p \nmid b$ because a and b are smaller than b. So this is not true $\square$

4.6.3 then goes on to show this works for products of more than 2 factors.

Fundamental Theorem of Arithmetic

- All natural number ≥ 2 can be expressed as a product of prime factors

4.6.4

$P(n)$: "n can be written as a product of primes"
Existence

$Q(n)$: "there is only one way of writing n as a product of primes, upto the order of the factors."
"Uniqueness"

Proof:

Proof by Induction

True for $n=2$ so $P(2)$ and $Q(2)$ are satisfied as it is both true and unique

Induction Step:

Let $n \geq 2$ and assume $P(k)$ and $Q(k)$ are true for each k. If $n+1$ is prime, then $P(n+1)$ and $Q(n+1)$ are true for the same reasons as before.

"Existence" $P(n+1)$, since $n+1$ is composite $n+1 = ab$ $ab \in \{2, 3, \dots, n^3\}$, by the induction hypothesis $p(a)$ and $p(b)$ are true.

$\therefore$ $n+1$ can be written as a product of primes as a and b can be written as products of primes.

$n+1 = ab = p_1 p_2 \dots p_r \cdot q_1 q_2 \dots q_r$

so $P(n+1)$ is true

Q(n+1) suppose

$n+1 = p_1 p_2 \cdots p_r \cdot q_1 q_2 \cdots q_s$

$n+1 = q_1 q_2 \cdots q_s$

$n+1 = p_1 p_2 \cdots p_r$

where $r, s \in \mathbb{N}$ $p_1 p_2 \cdots$ are primes and equivalent to $q_1 q_2 \cdots$

$r, s \geq 2$ because $n+1$ is composite

p_1 dindes $n+1$ so 4.6.3 implies $p_1 \mid q_j$ for some j.

prime

therefore $p_1 = q_j$

$p_2 p_3 \cdots p_r = m = q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_s$

(call p but p_1) (call q but q_j)

$m \neq 1$ because $r \geq 2$ so Q(m) is true so $m \in \{2, 3, 4 \ldots n\}$

Therefore the two prime factorisations are the same so therefore as $r = s$ then it means there are the same number of elements and they must be equal.

Q(n+1) satisfied □

Fermat's prime conjecture 4.6.7

P(n): " $2^{2^n} + 1$ is prime"

True for $n = 1, 2, 3, 4$ Fermat conjectured it was true for all n.

However, Euler disproved this using P(5)

28/10/21

L11

MATH 111 L011

"Existence" **Theorem 4.7.1** There are infinitely many prime numbers.

Proof by contradiction: Assume only finite amount

$p_1, p_2 \dots p_n$. $n \in \mathbb{N}$

$N = p_1 p_2 \dots p_n + 1 \in \{2,3,4,\dots\}$

4.6.4 shows this must be written as a product of primes. Call this p_j $j \in \{1,2,\dots n\}$

$N = p_j \cdot q$, $q \in \mathbb{N}$

$N = (p_j \cdot r) + 1$ when $r = p_1 p_2 \dots p_{j-1} \cdot p_{j+1} \cdot p_n$

$p_j q = N = (p_j \cdot r) + 1$

$1 = p_j q - p_j r$

$1 = p_j(q - r)$ $\therefore p_j = \pm 1$ however this contradicts p_j is prime $\square$

$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ where $p_1 < p_2 < \dots p_r$ (product of primes formula)

remember $p^0 = 1$

Proposition 4.7.3 $m \mid n$ if

$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ and $m = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r}$

where $b_j \in \{0, 1, \dots a_j\}$ for $j \in \{1, 2, \dots r\}$

When you have a number expressed as a product of prime factors e.g.

$1400 = 2^3 \times 5 \times 5 \times 7 = 2^3 \times 5^2 \times 7$

Number of factors $= (3+1) \times (2+1) \times (1+1)$

$= 24$ factors

Proof of this:

$\Rightarrow$ Suppose $m \in \mathbb{N}$ $m|n$ where $n = qm$

$q \in \mathbb{N}$ since the prime factors of qm = qm = prime factors of q + prime factors of m. $= p_1 p_2 \cdots p_r$.

$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ and $q = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$ when $b_1, \ldots b_r$ and $c_1 \ldots c_r$ are $\mathbb{N}$ or 0

$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = n = qm$

$= p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} p_1^{c_1} p_2^{c_2} \cdots$

$= p_1^{b_1+c_1} p_2^{b_2+c_2} \cdots p_r^{b_r+c_r}$

Using uniqueness of prime factorisation $\therefore$ $a_j = b_j + c_j$ for each j and $b \ldots$ $c \ldots$ are non-negative and because $a_j = b_j + c_j$ then $b_j \leq a_j$

If $(b_1, b_2, b_r) \neq (c_1, c_2, c_r)$ then $p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} \neq p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$

4.7.11 (using 4.7.9 Lemma)

Let $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ $n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$

$\text{hcf}(m,n) = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$

$\text{lcm}(m,n) = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$

where $c_i = \min\{a_j, b_j\}$ and $d_j = \{\max\{a_j, b_j\}$ for each $j \in \{1, 2, \ldots r\}$

[min and max means largest / smallest powers.]

e.g $m = 240$ $n = 108$

$m = 2^4 \cdot 3 \cdot 5$ $n = 2^2 \cdot 3^3$

so $\text{hcf}(m,n) = 2^2 \cdot 3$ (12)

$\text{lcm}(m,n) = 2^4 \cdot 3^3 \cdot 5$ (2160)

4.7.11 Proof

If factor k of m has the form $k = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where $0 \le e_j \le a_j$ for each $j \in \{1, 2, \cdots r\}$. For k|m k must be a factor of n. so $0 \le e_j \le b_j$ as well.

common factors of m and n

$k = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ with $0 \le e_j \le a_j$ and $0 \le e_j \le b_j$

so largest value of $e_j = \min\{a_j, b_j\}$

so hcf $= \min\{a_j, b_j\}$

$$\text{lcf}(m,n) = \frac{m,n}{\text{hcf}(m,n)} = \frac{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \; p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}}{p_1^{e_1} p_2^{e_2} \cdots p_r^{c_r}}$$

$= p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$ by collecting like powers

$= p_1^{a_1+b_1-c_1} \; p_2^{a_2+b_2-c_2} \cdots p_r^{a_r+b_r-c_r}$

Then $d_j = a_j + b_j - c_j$

$= a_j + b_j - \min\{a_j, b_j\}$

$\text{lcf}(m,n) = \max\{a_j, b_j\}$

28/10/21

L12

MATH 111 L12 Congruences

Given $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$ a is congruent to b modulo m if $m \mid a-b$ in this case:

$m \mid a-b$ $[a \equiv b \bmod m;]$ (m is named the modulus)

congruence — not the same as the other modulus !!

e.g $7 \equiv 2 \bmod 5$
$7-2 =$ multiple of 5

e.g $-10 \equiv 8 \bmod 6$
$-10-8 = -18 =$ multiple of 6

e.g $28 \equiv 13 \bmod 5$
$15 = 5(3)$
$28 = 3(5)+13$ Other ways of expression.
$28 = 5(5)+3$

5.1.14 $a \equiv b \bmod m \iff m \mid a-b$ (*)

If $a \equiv b \bmod m$ then $a-b = qm$
$a = qm+b$

Suppose $a = qm+b$ Let remainder of b/m be r
$r \in \{0, 1, \ldots m-1\}$ and $b = sm+r$

$a = qm+b = qm+sm+r$
$= (q+s)m + r$ ∴ remainder $a/m = r$

If a and b have remainder r
$a = qm+r$ $b = sm+r$
$a-b = (qm+r)-(sm+r)$
$= (q-s)m$ so m divides $a-b$ (*)
$\in \mathbb{Z}$

Numbers congruent to $a \bmod m$

$\ldots\ a-2m,\ a-m,\ a,\ a+m,\ a+2m\ \ldots$

If remainder $a/m = r$

$a \equiv r \bmod m$

Lemma 5.1.17

Suppose $a \equiv b \bmod m$

then $b \equiv a \bmod m$

because if m divides $a-b$ it divides $-(a-b)$ ie $b-a$

Lemma 5.1.19

Suppose $a \equiv b \bmod m$ $b \equiv c \bmod m$ The $a \equiv c \bmod m$

because $(a+c)-(b+c) = a-b$

↓

$m \mid a-b$ and $m \mid b-c$

so $m \mid (a-b)+(b-c)$

$m \mid a-c$

Linear Congruences (5.2)

This involves an unknown x

eg $x \equiv c \bmod n$, $x+a \equiv b \bmod m$ or $ax \equiv b \bmod m$

5.2.1

e.g $4x \equiv 3 \bmod 10$ has no solutions $4x$ = even, 3 = odd

$6x \equiv 9 \bmod 15$ has $x = 4$ and $x = 9$

as $6(4) - 9 = 15$ and $6(9) - 9 = 45$

since $4 \not\equiv 9 \bmod 15$ the solution cannot be of the form $x \equiv c \bmod 15$.

Theorem 5.2.2 The congruence $ax = b \bmod m$ has solutions if and only if $hcf(a, m) \mid b$

Proof: Let $d = hcf(a,m)$

$\Rightarrow$ Suppose congruence has solutions

$ax \equiv b \bmod m$

$ax = qm + b$ so $b = ax - qm$

since $d \mid a$ and $d \mid m$ then $d \mid b$

$\Leftarrow$ Suppose that $d \mid b$ say $b = td$ for $t \in \mathbb{Z}$.

By Bézouts Theorem $d = ra + sm$ $r, s \in \mathbb{Z}$

so $b = td = t(ra + sm) = tra + tsm$

= multiple of a + multiple of m.

$\bmod m$; $= a(tr)$

so a solution is $x = tr$. □

Lemma 5.2.5 If a and m are co-prime $hcf(a,m) = 1$ then $ax \equiv b \bmod m$ is given by $x \equiv br \bmod m$

↓

Theorem 5.2.6 Similar to Euclid's Lemma

Proof:

$m \mid ab - ac = m \mid a(b-c)$

as a and m are co-prime $m \mid b - c$

* 5.2.6 and proof ...

5.2.8 $ad = bd \bmod nd$ if and only if $a = b \bmod n$

Proof: $ad = bd \bmod nd$ means $ad - bd = q(nd)$

$a \equiv b \bmod n = a - b = qn$ so equivalent. □

* ex 5.2.A

2/11/2021

L13

MATH 111 L13

$ax \equiv b \bmod m$
$x \equiv c \bmod n$ } Last Lecture

Chinese Remainder Theorem (Simultaneous Congruence)

e.g $x \equiv 7 \bmod 10$ $\quad x \equiv 9 \bmod 13$
$x \equiv a \bmod m$ $\quad x \equiv b \bmod n$

Consider the case where m and n are co-prime
$\therefore rm + sn = 1$
$arm + asn = a$
$asn \equiv a \bmod m$ } because $asn - a = (ar)m$, $ar \in \mathbb{Z}$

On the other hand
$rm + sn = 1$
$brm + bsn = b$
$brm \equiv b \bmod n$ } because $brm - b = (-bs)n$, $-bs \in \mathbb{Z}$

Therefore $x = asn$ is a solution and $x = brm$ is the other solution.
$c = asn + brm$ ← This solves both $a \bmod m$ and $b \bmod n$
c is called a particular simultaneous solution using a, m, b, n, r, s

Lemma $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{Z}$ and $c \in \mathbb{Z}$ is a particular simultaneous solution to $x \equiv a \bmod m$, $x \equiv b \bmod n$.

Then any integer x is a solution to the pair if and only if $x \equiv c \bmod \text{lcm}(m, n)$

Proof of lemma

$\Rightarrow$ Suppose $x \equiv a \bmod m$ and $x \equiv b \bmod n$

Then $x \equiv a \equiv c \bmod m$

and $x \equiv b \equiv c \bmod n$

so $m \mid x-c$ and $n \mid x-c$

so $x-c$ is a common multiple of m and n

Hence, by 4.5.5, $x-c$ is a multiple of $\text{lcm}(m,n)$ so,

$x \equiv c \bmod \text{lcm}(m,n)$

$\Leftarrow$ Suppose $x \equiv c \bmod \text{lcm}(m,n)$

so that $\text{lcm}(m,n) \mid x-c$

Since $m \mid \text{lcm}(m,n)$ we have $m \mid x-c$

so $x \equiv c \bmod m$,

Since $c \equiv a \bmod m$, $x \equiv a \bmod m$

Since $n \mid \text{lcm}(m,n)$ we have $n \mid x-c$

so $x \equiv c \bmod n$

Since $c \equiv b \bmod n$, $x \equiv b \bmod n$ □

Theorem 5.3.2 Let $a, b \in \mathbb{Z}$ Let $m, n \in \mathbb{N}$ be co-prime $rm + sn = 1$, $r, s \in \mathbb{Z}$ Then $x \equiv a \bmod m$ and $x \equiv b \bmod n$ if and only if $x \equiv asn + brm \bmod mn$

Example 5.3.3 :

$x \equiv 2 \bmod 8 \quad x \equiv 5 \bmod 9$

since $\text{hcf}(8,9) = 1$ C.R.T applies

$a = 2, b = 5, m = 8, n = 9$

$8r + 9s = 1$ so take $r = -1 \quad s = 1$

$asn + brm = 2(1)(9) + 5(-1)(8) = -22 + 72$

$= 50 \bmod 72$

and then check this fits both ...

Without being co-prime:

5.3.5 $x \equiv a \bmod m \quad x \equiv b \bmod n$
can be solved if and only if $hcf(m,n) \mid a-b$

Proof:
Set $d = hcf(m,n)$
$\Rightarrow$ Suppose they can be solved simultaneously
$x \equiv a \bmod m \quad x \equiv b \bmod n$
$x - a = pm \quad x - b = qn \quad p, q \in \mathbb{Z}$
$a = x - pm \quad b = x - qn$
$a - b = qn - pm \quad d = hcf(m,n)$
so $d \mid qn - pm$
so $d \mid a - b$
$\Leftarrow$ Suppose $d \mid a-b$, $a - b = dq \quad q \in \mathbb{Z}$
by Bezout's $d = rm + sn \quad r, s \in \mathbb{Z}$
Define $c = a - qrm$
so $c \equiv a \bmod m$
and $c \equiv b \bmod n$ because
$c - b = a - qrm - b \quad (a - b = dq)$
$c - b = dq - qrm$
$c - b = q(d - rm) \quad (d = rm + sn)$
$c - b = qsn$ so
$c \equiv b \bmod n$

By this proof and lemma
then if $hcf(m,n) \mid a-b$ then
$x \equiv a \bmod m \quad x \equiv b \bmod n$
$x \equiv a - qrm \bmod lcm(m,n)$
where $q = \frac{a-b}{hcf(m,n)} \in \mathbb{Z}$ and r is $s \in \mathbb{Z}$
satisfy $rm + sn = hcf(m,n)$

$c \equiv a \bmod n$ $\quad$ $c = b \bmod n$

$\Updownarrow$ $\quad$ $\Uparrow$

if $c = a + kn$ $\quad$ if $c - b = a + kn - b$

$(\exists k \in \mathbb{Z})$

so

$c - b = kn + dq$ from earlier proof

$= kn + (rn + sn)q$

$= (k + rq)n + qsn$

$\equiv (k + rq)n \bmod n$

↳ let $k = -rq$

$c - b \equiv \bmod n$

$c = b \bmod n$

2/11/2021

L14

MATH 111 L14

Relations 6.1

6.1.1 Let S be a non-empty set. A relation on S is a statement concerning pairs of elements of S which may be true for some pairs and false for others. (SCC 120)

$\sim$ is related to.
e.g in ≤ 1 only $0 \sim 1$ for example

Reflexivity -
A relation $\sim$ on a set S is reflexive if $a \sim a$ for each $a \in S$.

Symmetry -
A relation $\sim$ on a set S is symmetrical if whenever $a \sim b$, $b \sim a$, a and $b \in S$

Transitivity -
A relation $\sim$ on a set S is transitive if whenever $a \sim b$, $b \sim c$ then $a \sim c$, a and b and $c \in S$.

Examples

S	meaning of $a \sim b$	reflexive	symmetric	transitive
$\mathbb{Z}$	$a+b > 7$	×	✓	×
$\mathbb{Z}$	$a \mid b$	✓	×	✓
$\mathbb{Z}$	$a \equiv b \bmod 5$	✓	✓	✓
$\mathbb{R}$	$\lvert a-b \rvert \leq 1$	✓	✓	×
$\mathbb{R}$	$a \leq b$	✓	×	✓

* Exercise 6.1.A

4/11/2024

L15

MATH 111 L15

Relations Recap:

$a, b \in S$: $a \sim b$ = a relation b
$a \not\sim b$ = a not related to b.

Reflexive if $(\forall a \in S)(a \sim a)$
Symmetric if $(\forall a, b \in S)((a \sim b) \Rightarrow (b \sim a))$
Transitive if $(\forall a, b, c \in S)((a \sim b) \text{ and } (b \sim c)) \Rightarrow (a \sim c))$

Equivalence relation if all three properties hold.
Equivalence class. For all $a \in S$ the set $\hat{a} = \{b \in S : b \sim a\}$ is the equivalence class of a.

e.g $a \sim b$ if $a \equiv b \bmod 5$ is an equivalence relation on $\mathbb{Z}$.
$\hat{3} = \{b \in \mathbb{Z} : b \equiv 3 \bmod 5\}$ ← This can also be a congruence class
$= \{\ldots -7, -2, 3, 8, 13, 18 \ldots\}$
You would observe $3 \cap 1 = \emptyset$

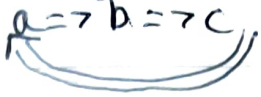
Proposition:

Let $\sim$ be an equivalence relation on a set S.
(i) For $a \in S$ we have $a \in \hat{a}$
Pf: This is true because $a \sim a$ by reflexivity
(ii) For $a, b \in S$ the following three conditions are equivalent:

6.2.3

a) $b \in \hat{a}$
b) $\hat{a} \cap \hat{b} \neq \emptyset$
c) $\hat{a} = \hat{b}$

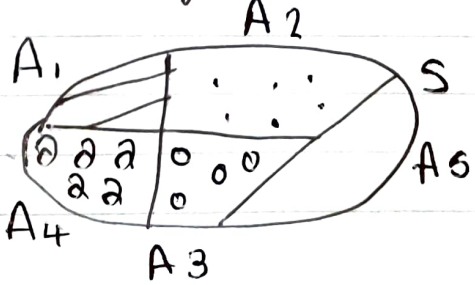
Proof by implications



Proof: (a) => (b):
suppose $b \in \hat{a}$. By (i) $b \in \hat{b}$
so $\hat{a} \cap \hat{b} \neq \emptyset$ because it contains b
(b) => (c):
suppose $\hat{a} \cap \hat{b} \neq \emptyset$ and take $c \in \hat{a} \cap \hat{b}$
so $c \in \hat{a}$, so $c \sim a$, and $c \in \hat{b}$ so $c \sim b$.
We want to prove $\hat{a} = \hat{b}$.
First $\hat{a} \subseteq \hat{b}$. Take $d \in \hat{a}$, so $d \sim a$.
By symmetry $c \sim a$ implies $a \sim c$
By transitivity, $d \sim a$, $a \sim c$ then $d \sim c$
By transitivity, $d \sim c$, $c \sim b$ then $d \sim b$
Hence $d \in \hat{b}$
Second $\hat{b} \subseteq \hat{a}$. swap a and b in $\hat{a} \subseteq \hat{b}$ argument.
Therefore $\hat{a} = \hat{b}$ so proved (b) => (c)
(c) => (a):
suppose $\hat{a} = \hat{b}$. By (c) $b \in \hat{b}$ so $b \in \hat{a}$.

6.2.4
Let $\sim$ be an eq rel on a non empty set S.
Then each element of S belongs to a unique equivalence class!
e.g $\hat{3}$ and $\hat{-2}$ from before are the same set yet have different equivalence classes

6.2.5 A partition of a set S is a collection of non-empty subsets of S such that each element of S belongs to exactly one of the subsets.



e.g partitions of S

Equivalence classes can be seen as partitions

e.g from partition diagram
Define relation $\sim$ on S by $a \sim b$ if $a, b \in A_i$ for some $i \in \{1, 2, 3, 4, 5\}$

6.2.6 -
Any element belonging to a given equivalence class is called a representative of that class

6.2.7 example of congruence classes

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

4/11/2021

L16

MATH 111 L16

$\mathbb{Z}_5 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}\}$ Notation for congruence ....

Interesting paragraph at end of notes for L15 about equivalence classes

Given $m \in \mathbb{N}$ we write $\mathbb{Z}_m$ for the set of congruence classes mod m.
eg $\mathbb{Z}_m = \{\hat{0}, \hat{1} \dots \widehat{m-1}\}$

Define $\hat{1} + \hat{2}$ in $\mathbb{Z}_5$

$\hat{1} = \{\dots, -9, -4, 1, 6, 11, \dots\}$

$\hat{2} = \{\dots, -8, -3, 2, 7, 12, \dots\}$

This is more difficult than it seems.

* **Lemma 6.3.2**

$\hat{a} = \hat{c}$, $\hat{b} = \hat{d}$

$\widehat{a+b} = \widehat{c+d}$

Therefore $\hat{a} + \hat{b} = \widehat{a+b}$

$\hat{a} \cdot \hat{b} = \widehat{ab}$

$-\hat{b} = \widehat{-b}$

$\hat{a} + \hat{b} = \hat{b} + \hat{a}$

$\mathbb{Z}_5$ addition and multiplication tables

+	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{4}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{4}$	$\hat{4}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$

·	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{1}$	$\hat{3}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{1}$	$\hat{4}$	$\hat{2}$
$\hat{4}$	$\hat{0}$	$\hat{4}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

For example in $\mathbb{Z}_4$ $\hat{2} \cdot \hat{2} = \hat{0}$. Therefore $\hat{2}$ is a zero divisor in $\mathbb{Z}_4$

In general $\hat{n}$ is a zero divisor in $\mathbb{Z}_m$ if $\hat{n} \cdot \hat{k} = \hat{0}$ for some $k \in \{1, 2, 3 \dots m-1\}$

6.3.5 All squares are congruent to 0 or 1 mod 4 0 mod 4 or 1 mod 4

Proof:

if $n \equiv 0 \bmod 4$ $n^2 = 0 \cdot 0 = 0 \bmod 4$

if $n = 1 \bmod 4$ $n^2 = 1 \cdot 1 = 1 \bmod 4$

if $n = 2 \bmod 4$ $n^2 = 2 \cdot 2 = 4 \bmod 4 = 0 \bmod 4$

if $n = 3 \bmod 4$ $n^2 = 3 \cdot 3 = 9 \bmod 4 = 1 \bmod 4$

6.3.7 if $n \in \mathbb{N} \equiv 3 \bmod 4$ Then n cannot be expressed as the sum of two squares

This is proved in 6.3.8

6.3.9

if $a \equiv b \bmod m$

then $a^n \equiv b^n \bmod m$ for any $n \in \mathbb{N}$

e.g find $2^{27} \bmod 15$ without $x \to 10$

(means find $x \in \{0, 1, 2, \dots, 14\}$)

(means find remainder of $2^{27} / 15$).

$2^2 = 4$ $2^3 = 8$ $2^4 = 16$ $16 = 1 \bmod 15$

$2^{27} = 2^{(4 \cdot 6)+3} = (2^4)^6 \cdot 2^3 = (1)^6 \cdot 8 = 8 \bmod 15$

Remainder $= 8$

mod 15 remainder value

$x^{odd} = x$ in this rule when negative.

6.3.12

$5 \mid (8^{4n+2} + 4^{2n})$

$8 \equiv 3 \bmod 5$

$8^2 = 3^2 = 9 = 4 \bmod 5$

$8^{4n+2} = 8^{2(2n+1)} \equiv (-1)^{2n+1} = -1 \bmod 5$

$4^2 = 16 = 1 \bmod 5$

$4^{2n} = (4^2)^n = 1^n = 1 \bmod 5$

$8^{4n+2} + 4^{2n} = 0 \bmod 5$

Therefore no remainder when divided by 5 so it is divisible

9/11/2021

L17

MATH 111 L17

6.4 Constructing Number Systems

If we have 2 sets A and B. We call the set of all ordered pairs, the cartesian product is denoted as $A \times B$

$A \times B = \{(a,b) : a \in A, b \in B\}$

If $A = B$ you may also write it as A^2

Natural Numbers:

Define a relation $\sim$ on $\mathbb{N}^2$ by $(a,b) \sim (c,d)$ if $a+d = b+c$:

R: $(a,b) \sim (a,b) \iff a+b = b+a$ which is true ← reflexivity proof

Symmetry: $(a,b) \sim (c,d)$, so that $a+d = b+c$

Then $(c,d) \sim (a,b)$ because $c+b = d+a$

Transitivity: Suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then $a+d = b+c$ and $c+f = d+e$.

We want to show $(a,b) \sim (e,f)$ $(a+f = b+e)$

Find $(a+d)+f = (b+c)+f = b+(c+f)$

$= b+(d+e)$ cancel d

$(a+f) = (b+e)$ is then transitive

This can then be shown as an equivalence relation

$\widehat{(a,b)} = \{(c,d) \in \mathbb{N}^2 : (a,b) \sim (c,d)\}$

$= \{(c,d) \in \mathbb{N}^2 : a+d = b+c\}$

For $a \in \mathbb{N}$ $\widehat{(a+1,1)} = \{(c,d) \in \mathbb{N}^2 : a+1+d = 1+c\}$

$= \{(c,d) \in \mathbb{N}^2 : a+d = c\}$

$= \{(a+d,d) \in \mathbb{N}^2 : d \in \mathbb{N}\}$

$\widehat{(a,b)} + \widehat{(c,d)} = \widehat{(a+c, b+d)}$

$\widehat{(a,b)} \cdot \widehat{(c,d)} = \widehat{(a-b)(c-d)} = \widehat{(ac+bd, ad+bc)}$

$-\widehat{(a,b)} = \widehat{(b,a)}$ Therefore $\widehat{(a,b)} - \widehat{(c,d)}$

$= \widehat{(a,b)} + (-\widehat{(c,d)})$

Rational Numbers -

$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ $\quad a/b = c/d \iff ad = bc$

On $\mathbb{Z} \times \mathbb{Z}^*$ define a relation $\sim$

$(a,b) \sim (c,d)$ if $ad = bc$, $a, c \in \mathbb{Z}$, $b, d \in \mathbb{Z}^*$

Reflexivity: $(a,b) \sim (a,b) \iff ab = ba$ which is true so it is reflexive

Symmetry: Suppose $(a,b) \sim (c,d)$. Then $ad = bc$ so $(c,d) \sim (a,b)$: $cb = da$. Therefore this is true and symmetric.

Transitivity: Suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ where $a, c, e \in \mathbb{Z}$ $b, d, f \in \mathbb{Z}^*$

Then $ad = bc$ and $cf = de$. We want $(a,b) \sim (e,f)$

$af = be$

$(ad)f = (bc)f$

$= b(cf) = b(de)$, so $af = be$

because $d \neq 0$

General rule:

$xy = xz$ where $x, y, z \in \mathbb{Z}$ and $x \neq 0$. Then $y = z$.

Equivalence Relation

$\widehat{(a,b)} = \{(c,d) \in \mathbb{Z} \times \mathbb{Z}^* : ad = bc\}$

Working

$(a\hat{,}b) + (c\hat{,}d) = (ad+bc\hat{,}bd)$ $\left[\frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd}\right]$

$(a\hat{,}b) \cdot (c\hat{,}d) = (ac\hat{,}bd)$ $\left[\frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd}\right]$

$-(a\hat{,}b) = (-a\hat{,}b)$ so $(a\hat{,}b) - (c\hat{,}d) =$
$(a\hat{,}b) + (-(c\hat{,}d))$

$(a\hat{,}b)^{-1} = (b\hat{,}a)$ for $a,b \in \mathbb{Z}^*$

Now we have division:

$\frac{(a\hat{,}b)}{(c\hat{,}d)} = (a\hat{,}b) \cdot (c\hat{,}d)^{-1}$

Real Numbers and Complex number systems can then further be created.

9/11/2021

L18

MATH 111 L18

7.1 Polynomial Arithmetic

A (real) polynomial in the indeterminate X is an expression:
$a_0 + a_1X + a_2X^2 + \dots a_nX^n$
where $n \in \mathbb{N}$ and $a_0, a_1 \dots a_n$ are called coefficients of polynomials.

These polynomials may be represented by $f(x)$ or $g(x)$
The zero polynomial is written as 0.

7.1.14

If $f(x) = a_0 + a_1X + \dots a_nX^n$ if $a_n \neq 0$ then n is the degree of $f(x)$, $\deg f(x)$ and a_nX^n is it's highest term.
The zero polynomial has no degree or highest term.

Constant polynomial - Only a_0
Linear polynomial - $a_0 + a_1X$
Quadratic polynomial - $a_0 + a_1X + a_2X^2$
etc.

Polynomials over $\mathbb{Z}$ = Integral polynomials
over $\mathbb{Q}$ = Rational polynomials
over $\mathbb{C}$ = Complex polynomials.

Polynomials are not thought of as functions.
Therefore use a X and call it indeterminate

e.g $f: \mathbb{Z}_2 \to \mathbb{Z}_2$

$f(\hat{0}) = \hat{0}$ $\quad$ $f(\hat{1}) = \hat{1}$

$g(\hat{0}) = \hat{0}^2 = \hat{0}$ $\quad$ $g(\hat{1}) = \hat{1}^2 = \hat{1}$

Therefore if polynomials are taken as functions. Then this doesn't work

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

$f(x) = q(x)g(x) + r(x)$ Dividing

$q(x)$ ← quotient, $r(x)$ ← remainder, $g(x)$ ← Divisor

e.g $3x+2 \;\overline{)\; 6x^3+7x^2+4x-1}$

$2x^2 + x + 2/3$

$6x^3 + 4x^2$

$3x^2 + 4x - 1$

$3x^2 + 2x$

$2x - 1$

$2x + 4/3$

$-7/3$

$\frac{6x^3}{3x} = 2x^2$

$\frac{3x^2}{3x} = x$

$\frac{2x}{3x} = 2/3$

$q(x) = 2x^2 + x + 2/3$

$g(x) = 3x+2$

$r(x) = -7/3$

Lemma 7.1.19

$f(x)$, $g(x)$ polynomials non-zero. $\deg f(x) \geq \deg g(x)$

$f(x) = a_0 + a_1 X \dots + a_m X^m$ $\quad$ $g(x) = b_0 + b_1 X \dots + b_n X^n$

$h(X) = \frac{a_m}{b_n} X^{m-n}$ Then either

* $f(x) = h(x)g(x)$
* $\deg(f(x) - h(x)g(x)) < \deg f(x)$

Proof of 7.1.19

$$h(x)g(x) = \frac{a_m}{b_n} x^{m-n}(b_n x^n + b_{n-1}x^{n-1} + \dots b_1 x + b_0)$$
$$= a_m x^m + \frac{a_m b_{n-1}}{b_n} x^{m-1} + \frac{a_m b_{n-2}}{b_n} x^{m-2} \dots + \frac{a_m b_0}{b_n} x$$

so

$$f(x) - h(x)g(x)$$
$$= -\left(a_m x^m + \frac{a_m b_{n-1}}{b_n} x^{n-1} + \dots + \frac{a_m b_0}{b_n} x^{m-n}\right)$$
$$= \left(a_{m-1} - \frac{a_m b_{n-1}}{b_n}\right) x^{m-1} + \dots$$

Therefore either $f(x) - h(x)g(x) = 0$ if all coefficients vanish or the polynomial has deg (1) at $m-1$.

Division of Polynomials

Theorem 7.1.10

$$f(x) = q(x)g(x) + r(x)$$

* either $r(x) = 0$
* or $\deg r(x) < \deg g(x)$

Proof:

"Existence"

Suppose $g(x) \mid f(x)$ then $f(x) = q(x)g(x)$ for some polynomial $q(x)$. This also covers $f(x) = 0$ and $g(x)$ deg (0)

Hence $f(x) \neq 0$ so $m = \deg f(x)$ $n = \deg g(x)$

This can then be proved by generalised induction on m.

$(m=0)$ step $q(x) = 0$ $r(x) = f(x)$ is true

$(m > 1)$:

$$f_0(x) = q_0(x)g(x) + r_0(x) \quad \text{either } r_0(x) = 0 \text{ or } \deg r_0(x) < n$$

If $m < n$ then $q(x) = 0$ $r(x) = f(x)$
otherwise choose $h(x)$ Lemma 7.1.9
and define $f_0(x) = f(x) - h(x)g(x)$
either 1) $f_0(x) = 0$ or 2) $\deg f_0(x) < m$

If 1) $q(x) = h(x)$ and $r(x) = 0$

If 2) Induction hypothesis implies polynomials $q_0(x)$ and $r_0(x)$ satisfying 7.0.3

$$\begin{aligned} f(x) &= f_0(x) + h(x)g(x) \\ &= q_0(x)g(x) + r_0(x) + h(x)g(x) \\ &= (q_0(x) + h(x))g(x) + r_0(x) \end{aligned}$$

Hence
$$f(x) = q(x)g(x) + r(x)$$

If $q(x) = q_0(x) + h(x)$
and $r(x) = r_0(x)$

So this holds by induction.

"Uniqueness"
$q(x)$ and $r(x)$ unique
suppose
$f(x) = q_j(x)g(x) + r_j(x)$
either $r_j(x) = 0$ or $\deg r_j(x) < \deg g(x)$
$j = 1, 2$.
$r_j(x) = f(x) - q_j(x)g(x)$
$r_1(x) - r_2(x) = (f(x) - q_1(x)g(x)) - (f(x) - q_2(x)g(x))$
$= q_2(x)g(x) - q_1(x)g(x)$
Prove by contradiction $r_1(x) \neq r_2(x)$

$$\deg(r_1(x) - r_2(x)) =$$
$$\deg(q_2(x) - q_1(x)) + \deg g(x) \geq \deg g(x) = n$$

On the other hand
$\deg(r_1(x) - r_2(x)) < \deg g(x)$
This is then impossible for both statements to be true. $\therefore$ $r_1(x) = r_2(x)$
Therefore $q_1(x) = q_2(x)$

□

L19

MATH 111 L19

7.2 Hcf and Euclidean revisited

There are only finite possible factors of a number. However there are infinite factors of a polynomial.

if $d(x)$ is a factor of $f(x)$ so that:

$f(x) = d(x)q(x)$

then:

$f(x) = r d(x) \cdot \frac{1}{r} q(x)$ for some non-zero $r \in \mathbb{R}$

$\deg d(x) \leq \deg f(x)$ so there are infinite factors as above

$1/r$ and r have infinite possibilities or $d(x)$ and $q(x)$ could then have infinite possibilities.

Approaches to Develop a theory

$p(x) \sim q(x)$ if $p(x) = rq(x)$ for some $r \in \mathbb{R} \setminus \{0\}$

Alternatively choose a monic polynomial (leading term 1)

Remember there will be no highest factor because of the infinite issue.

7.2.1

given $f(x)$ and $g(x)$ a polynomial $d(x)$ is the $\text{hcf}(f(x), g(x))$ if

* $d(x)$ is a common factor of $f(x)$ and $g(x)$
* any other common factor of $f(x)$ and $g(x)$ is also a factor of $d(x)$

(Makes no claim for uniqueness)

if $c(x)$ and $d(x)$ are both hcfs then $c(x) | d(x)$
so that $d(x) = q(x)c(x)$ and
$\deg c(x) + \deg q(x) \geq \deg c(x)$
on the other hand $d(x) | c(x)$ so $\deg c(x) = \deg d(x)$

7.2.2 A polynomial linear combination of two polynomials can also be formed.

e.g Let $f(x) = x^2 + x - 6 \quad g(x) = x^3 - 5x + 2$

$(x^2+1)f(x) - (x+1)g(x) = (x^2+1)(x^2+x+6) - (x+1)(x^3+5x+2)$

form $d(x) = h(x)f(x) + k(x)g(x)$

$= 4x - 8$ = plc of $f(x)$ and $g(x)$
having chose $h(x) = x^2 + 1$ $k(x) = -x - 1$

Lemma 7.2.4 $4x - 8 = (x^2+1)f(x) - (x+1)g(x)$

7.2.5 $x - 2 = (\frac{1}{4}x^2 + \frac{1}{4})f(x) - (\frac{1}{4}x + \frac{1}{4})g(x)$

Therefore $f(2) = 2^2 + 2 = 0 \quad g(2) = 2^3 - 10 + 2 = 0$
so $x - 2$ is the highest common factor as it is a plc and a common factor of $f(x)$ and $g(x)$

7.2.7

7.2.8 e.g

$f(x) = 6x^3 + 20x^2 + 7x - 12$

$g(x) = 6x^5 + 8x^4 - 27x^3 - 4x^2 + 35x - 15$

$\deg f(x) < \deg g(x)$ so

$$
\begin{array}{r|l}
6x^3 + 20x^2 + 7x - 12 & x^2 - 2x + 1 \\
\hline
 & 6x^5 + 8x^4 - 27x^3 - 4x^2 + 35x - 15 \\
 & \underline{6x^5 + 20x^4 + 7x^3 - 12x^2} \\
 & \quad -12x^4 - 34x^3 + 8x^2 + 35x \\
 & \quad \underline{-12x^4 - 40x^3 - 14x^2 + 24x} \\
 & \quad\quad 6x^3 + 22x^2 + 11x - 15 \\
 & \quad\quad \underline{6x^3 + 20x^2 + 7x - 12} \\
 & \quad\quad\quad 2x^2 + 4x - 3
\end{array}
$$

$g(x) = (x^2 - 2x + 1) f(x) + 2x^2 + 4x - 3$

Now divide $f(x)$ by $r(x)$

$$
\begin{array}{r|l}
2x^2 + 4x - 3 & 3x + 4 \\
\hline
 & 6x^3 + 20x^2 + 7x - 12 \\
 & \underline{6x^3 + 12x^2 - 9x} \\
 & \quad 8x^2 + 16x - 12 \\
 & \quad \underline{8x^2 + 16x - 12} \\
 & \quad\quad 0
\end{array}
$$

Last non-zero remainder = hcf so

hcf $= 2x^2 + 4x - 3$

to rewrite as plc

$2x^2 + 4x - 3 = g(x) - (x^2 - 2x + 1) f(x)$

7.2.9

e.g