Least Common Multiples and Triangles based on ITP 2016: Proof Pearl

Hing Lun Chan and Michael Norrish

College of Engineering and Computer Science Australian National University

August 2016, Nancy, France.

Play with numbers

How to play with numbers

Given the numbers: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. What can you do with them?

• add them: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 =Add[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 55

- add them: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 =Add[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 55
- multiply them: $1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 =$ Multiply[1,2,3,4,5,6,7,8,9,10] = 3628800

- add them: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 =Add[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 55
- multiply them: $1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 =$ Multiply[1,2,3,4,5,6,7,8,9,10] = 3628800
- combine by GCD: GCD[1,2,3,4,5,6,7,8,9,10] = 1

- add them: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 =Add[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 55
- multiply them: $1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 =$ Multiply[1,2,3,4,5,6,7,8,9,10] = 3628800
- combine by GCD: GCD[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 1
- combine by LCM: LCM[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 2520

Given the numbers: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. What can you do with them?

- add them: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 =Add[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 55
- multiply them: $1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 =$ Multiply[1,2,3,4,5,6,7,8,9,10] = 3628800
- combine by GCD: GCD[1,2,3,4,5,6,7,8,9,10] = 1
- combine by LCM: LCM[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 2520

Theorem

$$\vdash \texttt{GCD}[1,2,3,\ldots,\textit{n}] = 1$$

True, but not interesting. ©

Math is about patterns.

• Add
$$[1, 2, 3, ..., n] = n(n + 1)/2$$
, or
 $n^2/2 \le \text{Add}[1, 2, 3, ..., n] \le (n + 1)^2/2$
known from antiquity.

- Add[1, 2, 3, ..., n] = n(n+1)/2, or $n^2/2 \le \text{Add}[1, 2, 3, ..., n] \le (n+1)^2/2$ known from antiquity.
- $\sqrt{2\pi}\sqrt{n}(n/e)^n \leq \text{Multiply}[1,2,3,\ldots,n] \leq e\sqrt{n}(n/e)^n$ known as Stirling's approximation.

- Add[1, 2, 3, ..., n] = n(n+1)/2, or $n^2/2 \le \text{Add}[1, 2, 3, ..., n] \le (n+1)^2/2$ known from antiquity.
- $\sqrt{2\pi}\sqrt{n}(n/e)^n \leq \text{Multiply}[1,2,3,\ldots,n] \leq e\sqrt{n}(n/e)^n$ known as Stirling's approximation.
- GCD[1, 2, 3, ..., n] = 1

- Add[1, 2, 3, ..., n] = n(n+1)/2, or $n^2/2 \le \text{Add}[1, 2, 3, ..., n] \le (n+1)^2/2$ known from antiquity.
- $\sqrt{2\pi} \sqrt{n} (n/e)^n \leq \text{Multiply}[1, 2, 3, ..., n] \leq e \sqrt{n} (n/e)^n$ known as Stirling's approximation.
- GCD[1,2,3,...,*n*] = 1
- $2^n/2 \leq \text{LCM}[1, 2, 3, \dots, n] \leq 4^n$ useful for my PhD work.

Math is about patterns. ... Beauty is in the eye of the beholder.

- Add[1, 2, 3, ..., n] = n(n + 1)/2, or $n^2/2 \le \text{Add}[1, 2, 3, ..., n] \le (n + 1)^2/2$ known from antiquity.
- $\sqrt{2\pi} \sqrt{n} (n/e)^n \leq \text{Multiply}[1, 2, 3, ..., n] \leq e \sqrt{n} (n/e)^n$ known as Stirling's approximation.
- GCD[1,2,3,...,*n*] = 1
- $2^n/2 \leq \text{LCM}[1, 2, 3, \dots, n] \leq 4^n$ useful for my PhD work.

Theorem

$$\vdash 2^n \leq \texttt{LCM}[1,2,3,\ldots,(n+1)]$$

True, and interesting! ©

LCM of a List

LCM [1, 2] LCM [1, 2, 3] LCM [1, 2, 3, 4] LCM [1, 2, 3, 4, 5] LCM [1, 2, 3, 4, 5, 6]

LCM
$$[1, 2] = 2$$

LCM $[1, 2, 3] = 6$
LCM $[1, 2, 3, 4] = 12$
LCM $[1, 2, 3, 4, 5] = 60$
LCM $[1, 2, 3, 4, 5, 6] = 60$

LCM [1, 2] = 2LCM [1, 2, 3] = 6LCM [1, 2, 3, 4] = 12LCM [1, 2, 3, 4, 5] = 60LCM [1, 2, 3, 4, 5, 6] = 60

Note that the LCM is a multiple of each element, or each element is less than the overall LCM.

Note that the LCM is a multiple of each element, or each element is less than the overall LCM.

Note that the LCM is a multiple of each element, or each element is less than the overall LCM.

Theorem

 \vdash LCM [1 .. n + 1] $\geq 2^{n}$

Note that the LCM is a multiple of each element, or each element is less than the overall LCM.

Theorem

 \vdash LCM [1 .. n + 1] $\geq 2^{n}$

How to prove this interesting result?

Note that the LCM is a multiple of each element, or each element is less than the overall LCM.

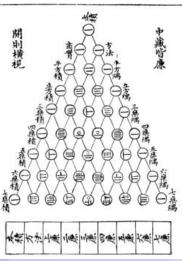
Theorem

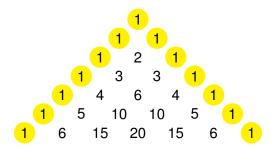
 \vdash LCM [1 .. n + 1] $\geq 2^{n}$

How to prove this interesting result? ... use Triangles! $\ensuremath{\Xi}$

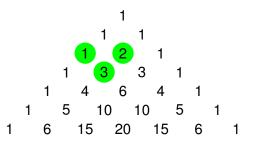
Yang Hui's Triangle



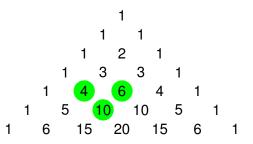




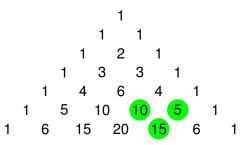
• Each boundary entry: always 1.



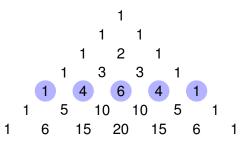
- Each boundary entry: always 1.
- Each inside entry: sum of two immediate parents.



- Each boundary entry: always 1.
- Each inside entry: sum of two immediate parents.



- Each boundary entry: always 1.
- Each inside entry: sum of two immediate parents.



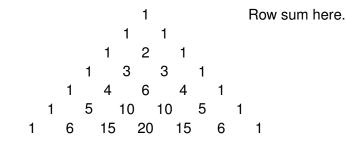
- Each boundary entry: always 1.
- Each inside entry: sum of two immediate parents.

Sum of the *n*-th row:

$$\sum_{k=0}^{n} \binom{n}{k} = (1+1)^{n} = 2^{n}$$

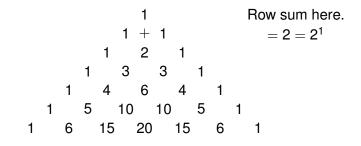
Meaning of:

$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n$$



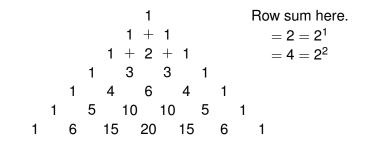
Meaning of:

$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n$$



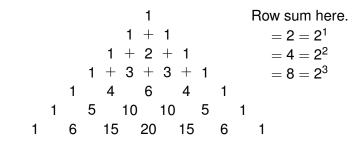
Meaning of:

$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n$$



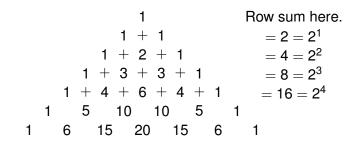
Meaning of:

$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n$$



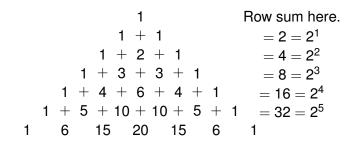
Meaning of:

$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n$$



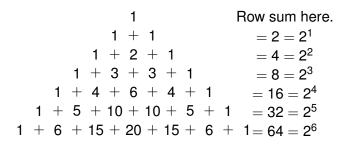
Meaning of:

$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n$$



Meaning of:

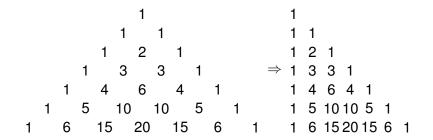
$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n$$



Meaning of:

$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n$$

Triangle Pattern



From symmetrical form to vertical-horizontal form.

Hing Lun Chan & Michael Norrish (ANU)

Bounding LCM with Triangles

ITP 2016 8 / 16

Leibniz's Denominator Triangle

1 1 1 2 1 1 3 3 1 1 4 6 4 1 1 5 1010 5 1 1 6 152015 6 1

Leibniz's Denominator Triangle

$$\Leftarrow \times 1 \quad 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \\ 1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\ 1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1$$

1

Leibniz's Denominator Triangle

1 2 2 $\begin{array}{c} \Leftarrow \times 1 & 1 \\ \Leftarrow \times 2 & 1 & 1 \\ & 1 & 2 & 1 \\ & 1 & 3 & 3 & 1 \\ & 1 & 4 & 6 & 4 & 1 \\ & 1 & 5 & 10 & 10 & 5 & 1 \\ & 1 & 6 & 15 & 20 & 15 & 6 & 1 \end{array}$

Leibniz's Denominator Triangle



Leibniz's Denominator Triangle



1 6 15 20 15 6 1

Leibniz's Denominator Triangle

1					$\Leftarrow \times 1$	1	
2	2				⇐ × 2	1	1
3	6	3			⇐×3	1	2 1
4	12	12	4		$\Leftarrow \times 4$	1	3 3 1
5	20	30	20	5	$\Leftarrow \times 5$	1	4 6 4 1
						1	5 10 10 5 1

1 6 15 20 15 6 1

Leibniz's Denominator Triangle

1						$\Leftarrow \times 1 1$
2	2					⇐×2 1 1
3	6	3				$\Leftarrow imes 3$ 1 2 1
4	12	12	4			$\Leftarrow \times 4$ 1 3 3 1
5	20	30	20	5		$\Leftarrow \times 5$ 1 4 6 4 1
6	30	60	60	30	6	$\Leftarrow \times 6$ 1 5 10 10 5 1
						1 6 15 20 15 6 1

Leibniz's Denominator Triangle

1						$\Leftarrow \times 1 1$
2	2					$\Leftarrow \times 2$ 1 1
3	6	3				$\Leftarrow imes 3$ 1 2 1
4	12	12	4			$\Leftarrow \times 4$ 1 3 3 1
5	20	30	20	5		$\Leftarrow \times 5$ 1 4 6 4 1
6	30	60	60	30	6	$\Leftarrow \times 6$ 1 5 10 10 5 1
7	42	105	140	105	42	$7 \iff \times 7 \ 1 \ 6 \ 15 \ 20 \ 15 \ 6 \ 1$

Leibniz's Denominator Triangle

1						$\Leftarrow \times 1 1$
2	2					⇐×2 1 1
3	6	3				\Leftarrow \times 3 1 2 1
4	12	12	4			$\Leftarrow \times 4$ 1 3 3 1
5	20	30	20	5		$\Leftarrow \times 5$ 1 4 6 4 1
6	30	60	60	30	6	$\Leftarrow \times 6$ 1 5 10 10 5 1
7	42	105	140	105	42	$7 \iff \times 7$ 1 6 15 20 15 6 1

Multiplying each row by the number of elements of that row, the result is Leibniz's Triangle, in denominator form.

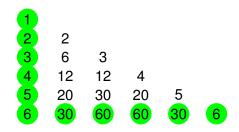
Hing Lun Chan & Michael Norrish (ANU)

Consecutive LCM

1					
2	2				
3	6	3			
4	12	12	4		
5	20	30	20	5	
6	30	60	60	30	6

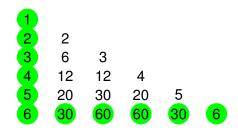
How does this triangle relate to our goal?

Consecutive LCM



How does this triangle relate to our goal? We shall show this: LCM (vertical column) = LCM (horizontal row).

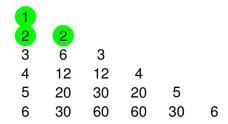
Consecutive LCM



How does this triangle relate to our goal? We shall show this: LCM (vertical column) = LCM (horizontal row).

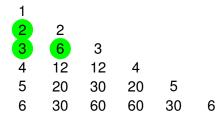
This is LCM exchange for big-L, and LCM (horizontal row) is easier to estimate.

Triplets in Triangle



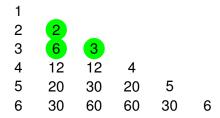
Building blocks of Leibniz's triangle: the small-Ls, called triplets.

Triplets in Triangle



Building blocks of Leibniz's triangle: the small-Ls, called triplets.

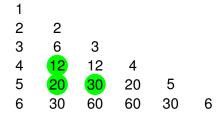
Triplets in Triangle



Building blocks of Leibniz's triangle: the small-Ls, called triplets.

• Each triplet has a vertical pair and a horizontal pair.

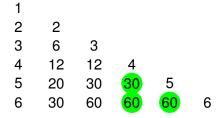
Triplets in Triangle



Building blocks of Leibniz's triangle: the small-Ls, called triplets.

- Each triplet has a vertical pair and a horizontal pair.
- We will show: LCM (vertical pair) = LCM (horizontal pair)

Triplets in Triangle



Building blocks of Leibniz's triangle: the small-Ls, called triplets.

- Each triplet has a vertical pair and a horizontal pair.
- We will show: LCM (vertical pair) = LCM (horizontal pair)

This is LCM exchange for small-L.

LCM and Triangle

Leibniz Triplet Property

Leibniz Triplet Property



For a Leibniz triplet $\{a, b, c\}$, ab = c(b - a).

Hing Lun Chan & Michael Norrish (ANU)

Bounding LCM with Triangles

Leibniz Triplet Property

Theorem (LCM Exchange)

For a Leibniz triplet $\{a, b, c\}$, lcm b c = lcm b a.



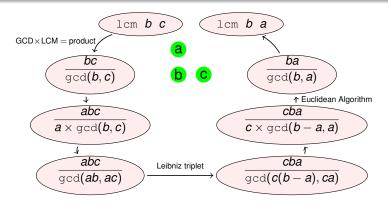
For a Leibniz triplet $\{a, b, c\}$, ab = c(b - a).

Hing Lun Chan & Michael Norrish (ANU)

Leibniz Triplet Property

Theorem (LCM Exchange)

For a Leibniz triplet $\{a, b, c\}$, lcm b c = lcm b a.

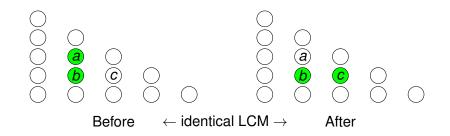


For a Leibniz triplet $\{a, b, c\}$, ab = c(b - a).

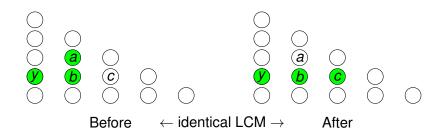
Hing Lun Chan & Michael Norrish (ANU)

Bounding LCM with Triangles

Zig-zag Paths

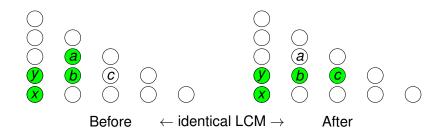


Zig-zag Paths



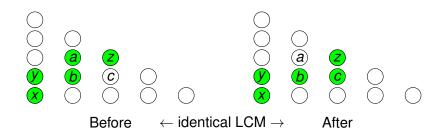
• Arms of a Leibniz triplet extend to paths, keeping overall LCM.

Zig-zag Paths



• Arms of a Leibniz triplet extend to paths, keeping overall LCM.

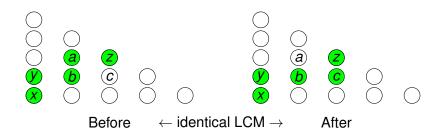
Zig-zag Paths



• Arms of a Leibniz triplet extend to paths, keeping overall LCM.

• A path can zig-zag to another by a suitable Leibniz triplet.

Zig-zag Paths



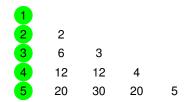
• Arms of a Leibniz triplet extend to paths, keeping overall LCM.

• A path can zig-zag to another by a suitable Leibniz triplet.

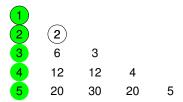
By Leibniz triplet property,

 Theorem
 $\vdash p_1 \rightsquigarrow p_2 \Rightarrow LCM p_1 = LCM p_2$

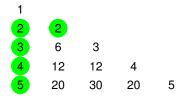
 Hing Lun Chan & Michael Norrish (ANU)
 Bounding LCM with Triangles
 ITP 2016 13/16



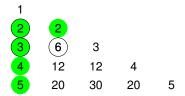
Wriggle Paths



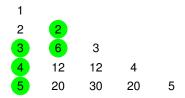
Wriggle Paths

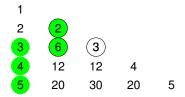


Wriggle Paths

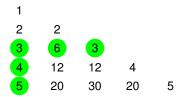


Wriggle Paths

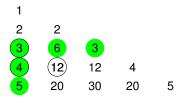




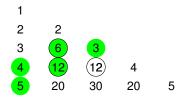
- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



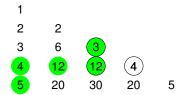
- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



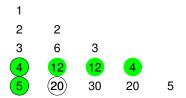
- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



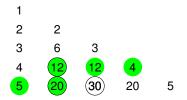
- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



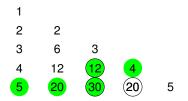
- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



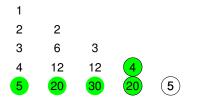
- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



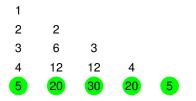
- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.



- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.

Wriggle Paths



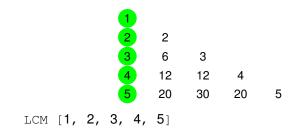
- Transform a path by successive zig-zags keeps overall LCM.
- A path can wriggle to another by successive zig-zags.

By Leibniz triplet property,

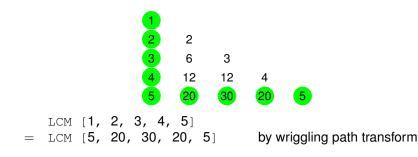
Theorem

 $\vdash \boldsymbol{\rho}_1 \rightsquigarrow^* \boldsymbol{\rho}_2 \Rightarrow LCM \, \boldsymbol{\rho}_1 = LCM \, \boldsymbol{\rho}_2$

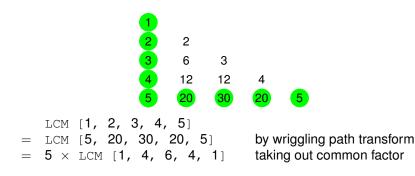
Proof Idea



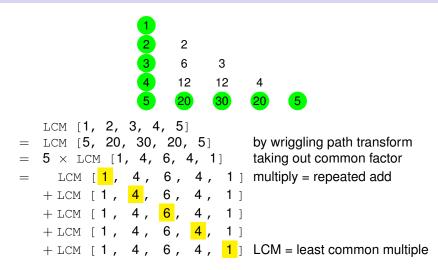
Proof Idea



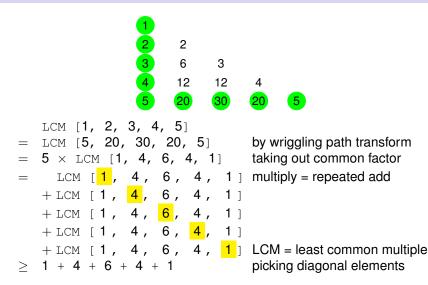
Proof Idea



Proof Idea

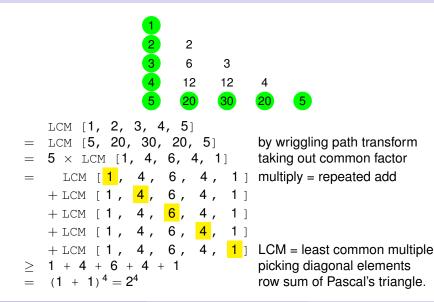


Proof Idea



Proof Idea

Proof Idea for $2^n \leq LCM[1, \ldots, (n+1)]$



Hing Lun Chan & Michael Norrish (ANU)

Summary

• ITP 2016 (Interactive Theorem Proving) https://itp2016.inria.fr Click "Program" to find the original slides.

Summary

• ITP 2016 (Interactive Theorem Proving) https://itp2016.inria.fr Click "Program" to find the original slides.

Paper

https://bitbucket.org/jhlchan/hol/downloads/ lcmTheorem.pdf

Summary

- ITP 2016 (Interactive Theorem Proving) https://itp2016.inria.fr Click "Program" to find the original slides.
- Paper

https://bitbucket.org/jhlchan/hol/downloads/ lcmTheorem.pdf

 What have you learnt? Leibniz's denominator triangle has LCM exchange.

Summary

- ITP 2016 (Interactive Theorem Proving) https://itp2016.inria.fr Click "Program" to find the original slides.
- Paper

https://bitbucket.org/jhlchan/hol/downloads/ lcmTheorem.pdf

- What have you learnt? Leibniz's denominator triangle has LCM exchange.
- Google: LCM chan hing lun