Proof Pearl: Bounding Least Common Multiples with Triangles

Hing-Lun Chan[1] and Michael Norrish[2]

[1] joseph.chan@anu.edu.au
Australian National University
[2] Michael.Norrish@data61.csiro.au
Canberra Research Lab., NICTA / Data61*;
also, Australian National University

Abstract. We present a proof of the fact that $2^n \leq \mathrm{lcm}\{1 \ldots (n+1)\}$. This result has a standard proof *via* an integral, but our proof is purely number theoretic, requiring little more than list inductions. The proof is based on manipulations of a variant of Leibniz's Harmonic Triangle, itself a relative of Pascal's better-known Triangle.

1 Introduction

The least common multiple of the consecutive natural numbers has a lower bound[1]:

$$2^n \leq \mathrm{lcm}\{1, 2, 3, \ldots, (n+1)\}$$

This result is a minor (though important) part of the proof of the complexity of the "PRIMES is in P" AKS algorithm (see below for more motivational detail). A short proof is given by Nair [5], based on a sum expressed as an integral. That paper ends with these words:

> *It also seems worthwhile to point out that there are different ways to prove the identity implied [...], for example, [...] by using the difference operator.*

Nair's remark indicates the possibility of an elementary proof of the above number-theoretic result. Nair's integral turns out to be an expression of the beta-function, and there is a little-known relationship between the beta-function and Leibniz's harmonic triangle [2]. The harmonic triangle can be described as the difference table of the harmonic sequence: $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots$.

Exploring this connection, we work out an interesting proof of this result that is both clear and elegant. Although the idea has been sketched in various sources (*e.g.*, [4]), we put the necessary pieces together in a coherent argument, and prove it formally in HOL4.

Overview We find that the rows of denominators in Leibniz's harmonic triangle provide a trick to enable an estimation of the lower bound of least common multiple (LCM) of consecutive numbers. The route from this row property to the LCM bound is subtle: we exploit an LCM property of triplets of neighboring elements in the denominator triangle. We shall show how this property gives a wonderful proof of the LCM bound for consecutive numbers in HOL4:

Theorem 1. *Lower bound for LCM of consecutive numbers.*

$\vdash\ 2^n \leq$ list_lcm [1 .. n + 1]

* NICTA is funded by the Australian Government through the Department of Communications and the Australian Research Council through the ICT Centre of Excellence Program.

[1] We use $(n + 1)$ here since we allow $n = 0$.

where list_lcm *is the obvious extension of the binary* lcm *operator to a list of numeric arguments. This satisfies, for example, the following properties:*

$\vdash$ list_lcm (h::t) = lcm h (list_lcm t)
$\vdash$ list_lcm (l_1 ⌢ l_2) = lcm (list_lcm l_1) (list_lcm l_2)
$\vdash$ list_lcm (REVERSE ℓ) = list_lcm ℓ

Motivation This work was initiated as part of our mechanization of the AKS algorithm [1], the first unconditionally deterministic polynomial-time algorithm for primality testing. As part of its initial action, the algorithm searches for a parameter k satisfying a condition dependent on the input number. The major part of AKS algorithm then involves a for-loop whose count depends on the size of k.

In our first paper on the correctness (but not complexity) of the AKS algorithm [3], we proved the existence of such a parameter k on general grounds, but did not give a bound. Now wanting to also show the complexity result for the AKS algorithm, we must provide a tight bound on k. As indicated in the AKS paper [1, Lemma 3.1], the necessary bound can be derived from a lower bound on the LCM of consecutive numbers.

Paper Structure The rest of this paper is devoted to explaining the mechanised proof of this result. We give some background to Pascal's and Leibniz's triangles in Section 2. Section 3 discusses two forms of the Leibniz's triangle: the denominator form and the harmonic form, and proves the important LCM property for our Leibniz triplets. Section 4 shows how paths in the denominator triangle can make use of this LCM property, eventually proving that both the consecutive numbers and a row of the denominator triangle share the same LCM. In Section 5, we use this LCM relationship to give a proof of Theorem 1. We conclude in Section 6.

HOL4 Notation All statements starting with a turnstile ($\vdash$) are HOL4 theorems, automatically pretty-printed to LaTeX from the relevant theory in the HOL4 development. Generally, our notation allows an appealing combination of quantifiers ($\forall$, $\exists$), logical connectives ($\wedge$ for "and", $\Rightarrow$ for "implies", and $\iff$ for "if and only if"), and λ-expressions for function abstraction. Lists are enclosed in square-brackets `[]`, using infix operators :: for "cons", ⌢ for append, and .. for inclusive-range. Other list operators are: LENGTH, SUM, TAKE, DROP, EVERY, and REVERSE. For a binary relation $\mathcal{R}$, its reflexive and transitive closure is denoted by $\mathcal{R}^*$.

HOL4 Sources Our proof scripts, one for the Binomial Theory and one for the Triangle Theory, can be found at `http://bitbucket.org/jhlchan/hol/src/algebra/lib`.

2 Background

2.1 Pascal's Triangle

Pascal's well-known triangle (see Figure 1) can be constructed as follows:

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

The entries of Pascal's triangle are binomial coefficients $\binom{n}{k}$, with $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Leibniz's triangle (see Section 2.2 below) will be defined using Pascal's triangle, so we include the binomials as a foundation in our HOL4 implementation, proving the above result:

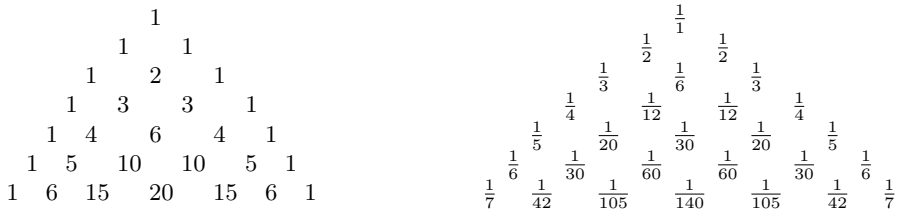

Fig. 1. Pascal's and Leibniz's Triangles

Theorem 2. *Sum of a row in Pascal's Triangle.*

$\vdash$ SUM ($\mathcal{P}_{\text{row}}$ n) = 2^n

We use $(\mathcal{P}_{\text{row}} \;\; n)$ to represent the n-th row of the Pascal's triangle, counting from 0.

2.2 Leibniz's Harmonic Triangle

Leibniz's harmonic triangle (second in Figure 1) can be similarly constructed:

- Each boundary entry: $\dfrac{1}{(n+1)}$ for the n-th row, with n starts from 0.
- Each inside entry: sum of two immediate children.

With the boundary entries forming the harmonic sequence, this Leibniz's triangle is closely related to Pascal's triangle. Denoting the harmonic triangle entries by $\begin{bmatrix} n \\ k \end{bmatrix}$, then it is not hard to show (*e.g.*, [2]) from the construction rules that:

- $\begin{bmatrix} n \\ k \end{bmatrix} = \dfrac{1}{(n+1)\binom{n}{k}}$
- $\displaystyle\sum_{k=0}^{n} \binom{n}{k} \begin{bmatrix} n \\ k \end{bmatrix} = 1$

Therefore all entries of the harmonic triangle are unit fractions. So, we choose to work with Leibniz's "Denominator Triangle", allowing us to avoid the rational numbers.

3 Leibniz's Denominator Triangle and Its Triplets

The elements of the denominator triangle can be defined in HOL4 *via* the binomial coefficients:

Definition 1. *Denominator form of Leibniz's triangle.*

$\vdash$ $\mathcal{L}$ n k = (n + 1) $\times$ $\binom{n}{k}$

The first few rows of the denominator triangle are shown (Table 1) in a vertical-horizontal format. Evidently from Definition 1, the left vertical boundary consists of consecutive numbers:

$\vdash$ $\mathcal{L}$ n 0 = n + 1

and the n-th horizontal row is just a multiple of the n-th row in Pascal's triangle by a factor $(n+1)$.

Within this vertical-horizontal format, we identify L-shaped "Leibniz triplets" rooted at row n and column k, with the top of the triplet being α_{nk}, and its two child entries as β_{nk} and γ_{nk} on the next row. In other words, we can define the constituents of the triplets:

row $n \setminus$ column k	$k=0$,	$k=1$,	$k=2$,	$k=3$,	$k=4$,	$k=5$,	$k=6, \cdots$
row $n=0$	1						
row $n=1$	2	2					
row $n=2$	3	6	3				
row $n=3$	4	12	12	4			
row $n=4$	5	20	30	20	5		
row $n=5$	6	30	60	60	30	6	
row $n=6$	7	42	105	140	105	42	7

Table 1. Leibniz's Denominator Triangle. A typical triplet is marked.

$$\vdash \alpha_{nk} = \mathcal{L}\ n\ k$$

$$\vdash \beta_{nk} = \mathcal{L}\ (n+1)\ k \qquad \vdash \gamma_{nk} = \mathcal{L}\ (n+1)\ (k+1)$$

	Denominator Triangle	Harmonic Triangle
	$\cdots$	$\cdots$
row $\cdots$	$\cdots\cdots\ \cdots$	$\cdots$
row n	$\cdots\ \alpha_{nk}\ \cdots$	$\cdots\ \frac{1}{\alpha_{nk}}\ \cdots$
row $(n+1)$	$\cdots\ \beta_{nk}\ \gamma_{nk}\ \cdots$	$\cdots\ \frac{1}{\beta_{nk}}\ \cdots\ \frac{1}{\gamma_{nk}}\ \cdots$
row $\cdots$	$\cdots\cdots\ \cdots\ \cdots\cdots$	$\cdots\cdots\ \cdots\ \cdots\ \cdots$

Table 2. The Leibniz triplet

Note that the values α_{nk}, β_{nk} and γ_{nk} occur as denominators in Leibniz's original harmonic triangle, corresponding to the situation that entry $\frac{1}{\alpha_{nk}}$ has immediate children $\frac{1}{\beta_{nk}}$ and $\frac{1}{\gamma_{nk}}$. By the construction rule of harmonic triangle, we should have:

$$\frac{1}{\alpha_{nk}} = \frac{1}{\beta_{nk}} + \frac{1}{\gamma_{nk}}, \quad \text{or} \quad \frac{1}{\gamma_{nk}} = \frac{1}{\alpha_{nk}} - \frac{1}{\beta_{nk}}$$

which, upon clearing fractions, becomes:

$$\alpha_{nk} \times \beta_{nk} = \gamma_{nk} \times (\beta_{nk} - \alpha_{nk})$$

Indeed, it is straightforward to show that our definition of $\mathcal{L}\ n\ k$ satisfies this property:

Theorem 3. *Property of a Leibniz triple in Denominator Triangle.*

$$\vdash \alpha_{nk} \times \beta_{nk} = \gamma_{nk} \times (\beta_{nk} - \alpha_{nk})$$

This identity for a Leibniz triplet is useful for computing the entry γ_{nk} from previously calculated entries α_{nk} and β_{nk}. It is also the key to the next important property of the triplet.

3.1 LCM Exchange

A Leibniz triplet has an important property related to least common multiple:

Theorem 4. *In a Leibniz triplet (as above), the pairs* $\{\beta_{nk}, \alpha_{nk}\}$ *and* $\{\beta_{nk}, \gamma_{nk}\}$ *have the same least common multiple.*

$\vdash$ lcm β_{nk} α_{nk} = lcm β_{nk} γ_{nk}

Proof. Let $a = \alpha_{nk}$, $b = \beta_{nk}$, $c = \gamma_{nk}$.

lcm b c	
$= bc \div \mathsf{gcd}(b, c)$	by definition
$= bca \div (a \times \mathsf{gcd}(b, c))$	introduce a factor above and below division
$= bac \div \mathsf{gcd}(ab, ca)$	by common factor, commutativity
$= bac \div \mathsf{gcd}(c(b-a), ca)$	by Leibniz triplet property, Theorem 3
$= bac \div (c \times \mathsf{gcd}(b-a, a))$	by extracting common factor
$= ba \div \mathsf{gcd}(b, a)$	apply GCD subtraction and cancel factor c
= lcm b a	by definition.

□

4 Paths Through Triangles

Our theorem requires us to capture the notion of the least common multiple of a list of elements (a path within the Denominator Triangle). We formalize paths as lists of numbers, without requiring the path to be connected within the triangle. However, the paths we work with will be connected and include:

- ($\mathcal{L}_{\mathrm{col}}$ n): the list `[1 .. n + 1]`, which happens to be the first $n + 1$ elements of the leftmost column of the Denominator Triangle;
- ($\mathcal{L}_{\mathrm{up}}$ n): the reverse of $\mathcal{L}_{\mathrm{col}}$ n, or the leftmost column of the triangle reading up; and
- ($\mathcal{L}_{\mathrm{row}}$ n): the n-th row of the Denominator Triangle, reading from the left.

We also use the operators TAKE and DROP to extract prefixes and suffixes of our paths.

Then, due to the possibility of LCM exchange within a Leibniz triplet (Theorem 4), we can prove the following:

Theorem 5. *In the Denominator Triangle, pick an entry at the left boundary. This is the intersection of a vertical column and a horizontal row. The least common multiple of the vertical column equals that of the horizontal row.*

$\vdash$ list_lcm ($\mathcal{L}_{\mathrm{col}}$ n) = list_lcm ($\mathcal{L}_{\mathrm{row}}$ n)

The proof is done *via* a kind of zig-zag transformation, see Figure 2. In the Denominator Triangle, we represent the entries for LCM consideration as a path of black circles, and indicate the Leibniz triplets by marking with small gray dots. Recall that, by Theorem 4, the vertical pair of a Leibniz triplet can be swapped with its horizontal pair without affecting the least common multiple.

It takes a little effort to formalize such a transformation. We use the following approach in HOL4.

4.1 Zig-zag Paths

If a path happens to have a vertical pair, we can match the vertical pair with a Leibniz triplet and swap with its horizontal pair to form another path, its zig-zag equivalent, which keeps the list LCM of the path.

Definition 2. *Zig-zag paths are those transformable by a Leibniz triplet.*

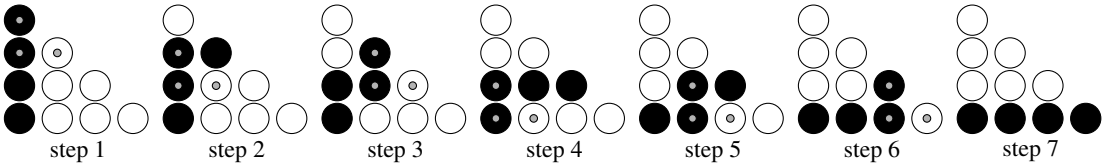

Fig. 2. Transformation of a path from vertical to horizontal in the Denominator Triangle, stepping from left to right. The path is indicated by entries with black circles. The 3 gray-dotted circles in L-shape indicate the Leibniz triplet, which allows LCM exchange. Each step preserves the overall LCM of the path.

$$\vdash\ p_1 \rightsquigarrow p_2 \iff \exists n\ k\ x\ y.\ p_1 = x \frown [\beta_{nk};\ \alpha_{nk}] \frown y \wedge p_2 = x \frown [\beta_{nk};\ \gamma_{nk}] \frown y$$

Basic properties of zig-zag paths are:

Theorem 6. *Zig-zag path properties.*

$\vdash\ p_1 \rightsquigarrow p_2 \Rightarrow \forall x.\ [x] \frown p_1 \rightsquigarrow [x] \frown p_2$	zig-zag a congruence wrt (::)
$\vdash\ p_1 \rightsquigarrow p_2 \Rightarrow \mathsf{list\_lcm}\ p_1 = \mathsf{list\_lcm}\ p_2$	preserving LCM by exchange *via* triplet

4.2 Wriggle Paths

A path can *wriggle* to another path if there are zig-zag paths in between to facilitate the transformation. Thus, wriggling is the reflexive and transitive closure of zig-zagging, giving the following:

Theorem 7. *Wriggle path properties.*

$\vdash\ p_1 \rightsquigarrow^* p_2 \Rightarrow \forall x.\ [x] \frown p_1 \rightsquigarrow^* [x] \frown p_2$	wriggle a congruence wrt (::)
$\vdash p_1 \rightsquigarrow^* p_2 \Rightarrow \mathsf{list\_lcm}\ p_1 = \mathsf{list\_lcm}\ p_2$	preserves LCM

4.3 Wriggling Inductions

We use wriggle paths to establish a key step[2]:

Theorem 8. *In the Denominator Triangle, a left boundary entry with the entire row above it can wriggle to its own row.*

$$\vdash\ [\mathcal{L}\ (n+1)\ 0] \frown \mathcal{L}_{\mathrm{row}}\ n \rightsquigarrow^*\ \mathcal{L}_{\mathrm{row}}\ (n+1)$$

Proof. We prove a more general result by induction, with the step case given by the following lemma:

$$\begin{aligned}\vdash\ & k \le n \Rightarrow \\ & \mathsf{TAKE}\ (k+1)\ (\mathcal{L}_{\mathrm{row}}\ (n+1)) \frown \mathsf{DROP}\ k\ (\mathcal{L}_{\mathrm{row}}\ n) \rightsquigarrow \\ & \mathsf{TAKE}\ (k+2)\ (\mathcal{L}_{\mathrm{row}}\ (n+1)) \frown \mathsf{DROP}\ (k+1)\ (\mathcal{L}_{\mathrm{row}}\ n)\end{aligned}$$

In other words: in the Denominator Triangle, the two partial rows $\mathsf{TAKE}\ (k+1)\ (\mathcal{L}_{\mathrm{row}}\ (n+1))$ and $\mathsf{DROP}\ k\ (\mathcal{L}_{\mathrm{row}}\ n)$ can zig-zag to a longer prefix of the lower row, with the upper row becoming one entry shorter. This is because there is a Leibniz triplet at the zig-zag point (see, for example, Step 5 of Figure 2), making the zig-zag condition possible. The subsequent induction is on the length of the upper partial row. □

With this key step, we can prove the whole transformation illustrated in Figure 2.

[2] This is illustrated in Figure 2 from the middle (step 4) to the last (step 7).

Theorem 9. *In the Denominator Triangle, pick any boundary entry. Its upward vertical path wriggles to its horizontal path.*

$\vdash \ \mathcal{L}_{\mathrm{up}} \ n \rightsquigarrow^* \ \mathcal{L}_{\mathrm{row}} \ n$

Proof. By induction on n. For the basis $n = 0$, both $(\mathcal{L}_{\mathrm{up}} \ 0)$ and $(\mathcal{L}_{\mathrm{row}} \ 0)$ are $[1]$, hence they wriggle trivially. For the induction step, note that the head of $(\mathcal{L}_{\mathrm{up}} \ (n + 1))$ is $(\mathcal{L} \ (n + 1) \ 0)$. Then:

$$
\begin{array}{rll}
& \mathcal{L}_{\mathrm{up}} \ (n + 1) & \\
= & [\mathcal{L} \ (n + 1) \ 0] \frown \mathcal{L}_{\mathrm{up}} \ n & \text{by taking apart head and tail} \\
\rightsquigarrow^* & [\mathcal{L} \ (n + 1) \ 0] \frown \mathcal{L}_{\mathrm{row}} \ n & \text{by induction hypothesis and tail wriggle (Theorem 7)} \\
\rightsquigarrow^* & \mathcal{L}_{\mathrm{row}} \ (n + 1) & \text{by key step of wriggling (Theorem 8).}
\end{array}
$$

□

Now we can formally prove the LCM transform of Theorem 5.

$\vdash$ list_lcm $(\mathcal{L}_{\mathrm{col}} \ n)$ = list_lcm $(\mathcal{L}_{\mathrm{row}} \ n)$

Proof. Applying path wriggling of Theorem 9 in the last step,

$$
\begin{array}{rll}
& \text{list\_lcm} \ (\mathcal{L}_{\mathrm{col}} \ n) & \\
= & \text{list\_lcm} \ (\mathcal{L}_{\mathrm{up}} \ n) & \text{by reverse paths keeping LCM} \\
= & \text{list\_lcm} \ (\mathcal{L}_{\mathrm{row}} \ n) & \text{by wriggle paths keeping LCM (Theorem 7).}
\end{array}
$$

□

5 LCM Lower Bound

Using the equality of least common multiples in Theorem 5, here is the proof of Theorem 1:

$\vdash 2^n \leq$ list_lcm $[1 \ .. \ n + 1]$

Proof. Recall from Section 3 that the left boundary of Denominator Triangle are consecutive numbers, thus $(\mathcal{L}_{\mathrm{col}} \ n) = [1 \ .. \ n + 1]$. Also, $(\mathcal{L}_{\mathrm{row}} \ n)$ is just a multiple of $(\mathcal{P}_{\mathrm{row}} \ n)$ by a factor $(n + 1)$. Therefore,

$$
\begin{array}{rll}
& \text{list\_lcm} \ [1 \ .. \ n + 1] & \\
= & \text{list\_lcm} \ (\mathcal{L}_{\mathrm{col}} \ n) & \text{by above} \\
= & \text{list\_lcm} \ (\mathcal{L}_{\mathrm{row}} \ n) & \text{by LCM transform (Theorem 5)} \\
= & (n + 1) \times \text{list\_lcm} \ (\mathcal{P}_{\mathrm{row}} \ n) & \text{by LCM common factor} \\
= & \text{LENGTH} \ (\mathcal{P}_{\mathrm{row}} \ n) \times \text{list\_lcm} \ (\mathcal{P}_{\mathrm{row}} \ n) & \text{by length of horizontal row} \\
\geq & \text{SUM} \ (\mathcal{P}_{\mathrm{row}} \ n) & \text{by unrolling, see Theorem 10 below} \\
= & 2^n & \text{by binomial sum (Theorem 2).}
\end{array}
$$

□

This proof uses the technique of unrolling, the principle of which can be illustrated for the case $n = 4$ of the Denominator Triangle:

- $\mathcal{L}_{\mathrm{col}} \ 4 = [1; \ 2; \ 3; \ 4; \ 5]$
- $\mathcal{L}_{\mathrm{row}} \ 4 = [5; \ 20; \ 30; \ 20; \ 5]$

Using the fact that list LCM cannot be smaller than any of its members, the unrolling goes like this:

$$
\begin{array}{lll}
& \mathsf{list\_lcm}\ [1;\ 2;\ 3;\ 4;\ 5] & \\
= & \mathsf{list\_lcm}\ [5;\ 20;\ 30;\ 20;\ 5] & \text{by path transform, Theorem } 5 \\
= & 5 \times \mathsf{list\_lcm}\ [1;\ 4;\ 6;\ 4;\ 1] & \text{note } 5 = \mathsf{LENGTH}\ [1;\ 4;\ 6;\ 4;\ 1] \\
= & \quad \mathsf{list\_lcm}\ [1;\ 4;\ 6;\ 4;\ 1] & \text{by unrolling multiplication} \\
& + \mathsf{list\_lcm}\ [1;\ 4;\ 6;\ 4;\ 1] & \\
& + \mathsf{list\_lcm}\ [1;\ 4;\ 6;\ 4;\ 1] & \\
& + \mathsf{list\_lcm}\ [1;\ 4;\ 6;\ 4;\ 1] & \\
& + \mathsf{list\_lcm}\ [1;\ 4;\ 6;\ 4;\ 1] & \\
\geq & 1 + 4 + 6 + 4 + 1 & \text{by picking diagonal elements} \\
= & (1 + 1)^4 & \text{by binomial expansion} \\
= & 2^4 & \text{by arithmetic.}
\end{array}
$$

Our unrolling theorem has the following formal statement in HOL4:

Theorem 10. *The least common multiple of a list of positive numbers at least equals its average.*

$$\vdash \mathsf{EVERY}\ (\lambda k.\ 0 < k)\ \ell \Rightarrow \mathsf{SUM}\ \ell \leq \mathsf{LENGTH}\ \ell \times \mathsf{list\_lcm}\ \ell$$

6 Conclusion

We have proved a lower bound for the least common multiple of consecutive numbers, using an interesting application of Leibniz's Triangle in denominator form. Using elementary reasoning over natural numbers and lists, we have not just mechanized what we believe to be a cute proof, but now have a result that will be useful in our ongoing work on the mechanization of the AKS algorithm.

References

1. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, September 2004.
2. Ayoub B. Ayoub. The Harmonic Triangle and the Beta Function. *Mathematics Magazine*, 60(4):223–225, October 1987.
3. Hing-Lun Chan and Michael Norrish. Mechanisation of AKS Algorithm: Part 1—the Main Theorem. In Christian Urban and Xingyuan Zhang, editors, *Interactive Theorem Proving*, number 9236 in LNCS, pages 117–136. Springer, August 2015.
4. Grigory M. Answer to: Is there a Direct Proof of this LCM identity?, August 2010. Question 1442 on Math Stack Exchange: `http://math.stackexchange.com/questions/1442/`.
5. M. Nair. On Chebyshev-type Inequalities for Primes. *American Mathematical Monthly*, 89(2):126–129, February 1982.