Logical Methods in Computer Science
Volume 17, Issue 1, 2021, pp. 16:1–16:25
https://lmcs.episciences.org/

Submitted Dec. 16, 2019
Published Feb. 18, 2021

A FORMAL PROOF OF THE IRRATIONALITY OF $\zeta(3)$

ASSIA MAHBOUBI AND THOMAS SIBUT-PINOTE

LS2N UFR Sciences et Techniques, 2 rue de la Houssinière, BP 92208 44322 Nantes Cedex 3 France
e-mail address: Assia.Mahboubi@inria.fr
e-mail address: thomas.sibut-pinote@ens-lyon.org

Abstract. This paper presents a complete formal verification of a proof that the evaluation of the Riemann zeta function at 3 is irrational, using the Coq proof assistant. This result was first presented by Apéry in 1978, and the proof we have formalized essentially follows the path of his original presentation. The crux of this proof is to establish that some sequences satisfy a common recurrence. We formally prove this result by an *a posteriori* verification of calculations performed by computer algebra algorithms in a Maple session. The rest of the proof combines arithmetical ingredients and asymptotic analysis, which we conduct by extending the Mathematical Components libraries.

1. Introduction

In 1978, Apéry proved that $\zeta(3)$, which is the sum $\sum_{i=1}^{\infty} \frac{1}{i^3}$ now known as the *Apéry constant*, is irrational. This result was the first dent in the problem of the irrationality of the evaluation of the Riemann zeta function at *odd* positive integers. As of today, this problem remains a long-standing challenge of number theory. Zudilin [Zud01] showed that at least one of the numbers $\zeta(5)$,$\zeta(7)$,$\zeta(9)$, $\zeta(11)$ must be irrational. Ball and Rivoal [Riv00, BR01] established that there are infinitely many irrational odd zeta values. Fischler, Sprang and Zudilin proved [FSZ19] that there are asymptotically more than any power of $\log(s)$ irrational values of the Riemann zeta function at odd integers between 3 and s. But today $\zeta(3)$ is the only *known* such value to be irrational.

Van der Poorten reports [vdP79] that Apéry's announcement of this result was at first met with wide skepticism. His obscure presentation featured "a sequence of unlikely assertions" without proofs, not the least of which was an enigmatic recurrence (Lemma 3.3) satisfied by two sequences a and b. It took two months of collaboration between Cohen, Lenstra, and Van der Poorten, with the help of Zagier, to obtain a thorough proof of Apéry's theorem:

Theorem 1.1 (Apéry, 1978). *The constant $\zeta(3)$ is irrational.*

Key words and phrases: formal proof, number theory, irrationality, creative telescoping, symbolic computation, Coq, Apéry's recurrences, Riemann zeta function.

This work was supported in part by the project FastRelax ANR-14-CE25-0018-01.

DOI:10.23638/LMCS-17(1:16)2021

In the present paper, we describe a formal proof of this theorem inside the Coq proof assistant [The20], using the Mathematical Components libraries [coq19]. This formalization follows the structure of Apéry's original proof. However, we replace the manual verification of recurrence relations by an automatic discovery of these equations, using symbolic computation. For this purpose, we use Maple packages to perform calculations outside the proof assistant, and we verify a posteriori the resulting claims inside Coq. By combining these verified results with additional formal developments, we obtain a complete formal proof of Theorem 1.1, formalized using the Coq proof assistant without additional axiom. In particular, the proof is entirely constructive, and does *not* rely on the axiomatic definition of real numbers provided in Coq's standard library. A previous paper [CMSPT14] reported on the implementation of the cooperation between a computer algebra system and a proof assistant used in the formalization. The present paper is self-contained: it includes a summary of the latter report, and provides more details about the rest of the formal proof. In particular, it describes the formalization of an upper bound on the asymptotic behavior of $lcm(1, ..., n)$, the least common multiple of the integers from 1 to n, a part of the proof which was missing in the previous report.

The rest of the paper is organized as follows. We first describe the background formal theories used in our development (Section 2). We then outline the proof of Theorem 1.1 (Section 3). We summarize the algorithms used in the Maple session, the data this session produces and the way this data can be used in formal proofs (Section 4). We then describe the proof of the consequences of Apéry's recurrence (Section 5). Finally, we present an elementary proof of the bound on the asymptotic behavior of the sequence $lcm(1, ..., n)$, which is used in this irrationality proof (Section 6), before commenting on related work and concluding (Section 7).

The companion code to the present article can be found in the following repository:
`https://github.com/math-comp/apery`.

2. Preliminaries

This section provides some hints about the representation of the different natures of numbers at stake in this proof in the libraries backing our formal development. It also describes a few extensions we devised for these libraries and sets some notations used throughout this paper. Most of the material presented here is related to the Mathematical Components libraries [coq19, GAA+13].

2.1. Integers.

In Coq, the set $\mathbb{N}$ of natural numbers is usually represented by the type `nat`:

```
Inductive nat := O | S : nat → nat.
```

This type is defined in a prelude library, which is automatically imported by any Coq session. It models the elements of $\mathbb{N}$ using a unary representation: Coq's parser reads the number 2 as the term `S (S O)`. The structural induction principle associated with this inductive type coincides with the usual recurrence scheme on natural numbers. This is convenient for defining elementary functions on natural numbers, like comparison or arithmetical operations, and for developing their associated theory. However, the resulting programs are usually very naive and inefficient implementations, which should only be evaluated for the purpose of small scale computations.

The set $\mathbb{Z}$ of integers can be represented by gluing together two copies of type `nat`, which provides a signed unary representation of integers:

```
Inductive int : Set := Posz of nat | Negz of nat.
```

If the term `n : nat` represents the natural number $n \in \mathbb{N}$, then the term `(Posz n): int` represents the integer $n \in \mathbb{Z}$ and the term `(Negz n): int` represents the integer $-(n+1) \in \mathbb{Z}$. In particular, the constructor `Posz : nat → int` implements the embedding of type `nat` into type `int`, which is invisible on paper because it is just the inclusion $\mathbb{N} \subset \mathbb{Z}$. In order to mimic the mathematical practice, the constant `Posz` is declared as a *coercion*, which means in particular that unless otherwise specified, this function is hidden from the terms displayed by Coq to the user (in the current goal, in answers to search queries, etc).

The Mathematical Components libraries provide formal definitions of a few elementary concepts and results from number theory, defined on the type `nat`. For instance, they provide the theory of Euclidean division, a boolean primality test, the elementary properties of the factorial function, of binomial coefficients, etc. In the rest of the paper, we use the standard mathematical notations $n!$ and $\binom{n}{m}$ for the corresponding formal definition of the factorial and of the binomial coefficients respectively. These libraries also define the p-adic valuation $v_p(n)$ of a number n: if p is a prime number, it is the exponent of p in the prime decomposition of n. However, we had to extend the available basic formal theory with a few extra standard results, like the formula giving the p-adic valuation of factorials:

Lemma 2.1. *For any $n \in \mathbb{N}$ and for any prime number p:*

$$v_p(n!) = \sum_{i=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

Incidentally, the formal version of this formula is a typical example of the slight variations one may introduce in a mathematical statement, in order to come up with a formal sentence which is not only correct and faithful to the original mathematical result, but also a tool which is easy to use in subsequent formal proofs. First, although the fraction in the original statement of Lemma 2.1 may suggest that rational numbers play a role here, $\left\lfloor \frac{n}{m} \right\rfloor$ is in fact exactly the quotient of the Euclidean division of n by m. In the rest of the paper, for $n, m \in \mathbb{N}$ and m non-zero, we thus write $\left\lfloor \frac{n}{m} \right\rfloor$ for the quotient of the Euclidean division of n by m. Perhaps more interestingly, the formal statement of Lemma 2.1 rather corresponds to the following variant:

$$\text{For any prime } p \text{ and any } j, n \in \mathbb{N}, \text{ such that } n < p^{j+1}, v_p(n!) = \sum_{i=1}^{j} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

Adding an extra variable to generalize the upper bound of the sum is a better option because it will ease unification when this formula is applied or used for rewriting. Moreover, we do not really need to introduce logarithms here: indeed, $\lfloor \log_p n \rfloor$ is used to denote the largest power of p smaller than n. For this purpose, we could use the function `trunc_log : nat → nat → nat` provided by the Mathematical Components libraries, which computes the greatest exponent α such that $n^\alpha \leq m$, in other words $\lfloor \log_n m \rfloor$. Better yet, since the summand is zero when the index i exceeds this value, we can simplify the side condition on the extra variable and require only that $n < p^{j+1}$.

The basic theory of binomial coefficients present in the Mathematical Components libraries describes their role in elementary enumerative combinatorics. However, when viewing binomial coefficients as a sequence which is a certain solution of a recurrence system, it becomes natural to extend their domain of definition to integers: we thus developed a small library about these generalized binomial coefficients. We also needed to extend these libraries with properties of multinomial coefficients. For $n, k_1, \ldots, k_l \in \mathbb{N}$, with $k_1 + \cdots + k_l = n$, the coefficient of $x_1^{k_1} \cdots x_l^{k_l}$ in the formal expansion of $(x_1 + \cdots + x_l)^n$ is called a *multinomial coefficient* and denoted $\binom{n}{k_1,\ldots,k_l}$. Its value is $\frac{n!}{k_1!\ldots k_l!}$ or equivalently, $\prod_{i=1}^{l} \binom{k_1+\cdots+k_i}{k_i}$. The latter formula provides for free the fact that multinomial coefficients are non-negative integers and we use it in our formal definition: for `(l : seq nat)` a finite sequence $l_1, \ldots, l_s$ of natural numbers, then `(multinomial l)` is the multinomial coefficient $\binom{l_1+\cdots+l_s}{l_1,\ldots,l_s}$:

```
Definition multinomial (l : seq nat) : nat :=
 \prod_(0 ≤ i < size l) (binomial (\sum_(0 ≤ j < i.+1) l‘_j) l‘_i).
```

From this definition, we prove formally the other characterizations, as well as the generalized Newton formula describing the expansion of $(x_1 + \cdots + x_l)^n$.

2.2. **Rational numbers, algebraic numbers, real numbers.** In the Mathematical Components libraries, rational numbers are represented using a dependent pair. This type construct, also called Σ-type, is specific to dependent type theory: it makes possible to define a type that decorates a data with a proof that a certain property holds on this data. The Mathematical Components libraries also include a construction of the algebraic closure for countable fields, and thus a construction of $\overline{\mathbb{Q}}$, algebraic closure of $\mathbb{Q}$, the field of rational numbers. The corresponding type, named `algC` is equipped with a structure of (partially) ordered, algebraically closed field [GAA+13]. Slightly abusing notation, we denote by $\overline{\mathbb{Q}} \cap \mathbb{R}$ the subset of $\overline{\mathbb{Q}}$ containing elements with a zero imaginary part and we call such elements real algebraic numbers.

Almost all the irrational numbers involved in the present proof are real algebraic numbers, and more precisely, they are of the form $r^{\frac{1}{n}}$ for r a non-negative rational number r and for $n \in \mathbb{N}$. The only place where these numbers play a role is in auxiliary lemmas for the proof of the asymptotic behavior of the sequence $(\ell_n)_{n\in\mathbb{N}}$, where ℓ_n is the least common multiple of integers between 1 and n. They appear in inequalities expressing signs and estimations.

It might come as a surprise that we used the type `algC` of algebraic (complex) numbers to cast these quantities, although we do not actually need imaginary complex numbers. But this choice proved convenient due to the fact that the type `algC` features both a definition of n-th roots, and a clever choice of partial order. Indeed, although $\overline{\mathbb{Q}}$ cannot be ordered as a field, it is equipped with a binary relation, denoted $\leq$, which coincides with the real order relation on $\overline{\mathbb{Q}} \cap \mathbb{R}$:

$$\forall x, y \in \overline{\mathbb{Q}},\ x \leq y \Leftrightarrow y - x \in \mathbb{R}_{\geq 0}.$$

In particular, for any $z \in \overline{\mathbb{Q}}$:

$$0 \leq z \Leftrightarrow z \in \mathbb{R}_{\geq 0} \text{ and } z \leq 0 \Leftrightarrow z \in \mathbb{R}_{\leq 0}.$$

Moreover, the type `algC` is equipped with a function `n.-root : algC → algC`, defined for any `(n : nat)`, such that `(n.-root z)` is the n-th (complex) root of `z` with minimal non-negative argument. Crucially, when `(z : algC)` represents a non-negative real number, `(n.-root z)` coincides with the definition of the real n-th root, and thus the following equivalence holds:

```
Lemma rootC_ge0 (n : nat) (z : algC) : n > 0 → (0 ≤ n.-root z) = (0 ≤ z).
```

The shape of Lemma `rootC_ge0` is typical of the style pervasive in the Mathematical Components libraries, where equivalences between decidable statements are stated as boolean equalities. It expresses that for an algebraic number x, that is for $x \in \overline{\mathbb{Q}}$, we have $x^{\frac{1}{n}} \in \mathbb{R}_{\geq 0}$ if and only if $x \in \mathbb{R}_{\geq 0}$.

The one notable place at which we need to resort to a larger subset of the real numbers is the definition of the number $\zeta(3)$, if only because as of today, it is not even known whether $\zeta(3)$ is algebraic or transcendental. This number is actually defined as the limit of the partial sums $\sum_{m=1}^{n} \frac{1}{m^3}$, so we start our formal study by establishing the existence of this limit.

More precisely, we show that this sequence of partial sums is a *Cauchy sequence*, with an explicit modulus of convergence.

Definition 2.2. A *Cauchy sequence* is a sequence $(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ together with a modulus of convergence $m_x : \mathbb{Q} \to \mathbb{N}$ such that if ε is a positive rational number, then any two elements of index greater than $m_x(\varepsilon)$ are separated at most by ε.

Proposition 2.3. *The sequence* $z_n = \sum_{m=1}^{n} \frac{1}{m^3}$ *is a Cauchy sequence.*

Two sequences x and y are *Cauchy equivalent* if x and y are both Cauchy sequences, and if eventually $|x_n - y_n| < \varepsilon$, for any $\varepsilon > 0$. Real numbers could be constructed formally by introducing a quotient type, whose element are the equivalent classes of the latter relation. But this is rather irrelevant for this formalization, which involves explicit sequences and their asymptotic properties, rather than real numbers. For this reason, the formal statements in this formal proof only involve sequences of rational numbers, and a type of Cauchy sequences which pairs such a sequence with a proof that it has the Cauchy property. For instance, for two Cauchy sequences x and y, we write $x < y$ if there is a rational number $\varepsilon > 0$ such that eventually $x_n + \varepsilon \leq y_n$.

We benefited from the formal library about Cauchy sequences developed by Cohen [Coh12]. This library defines Cauchy sequences of elements in a totally ordered field, and introduces a type `(creal F)` of Cauchy sequences over the totally ordered field `F`, given as a parameter. We thus use the instance `(creal rat)`. The infix notation `==`, in the notation scope `CR`, denotes the equivalence of Cauchy sequences, as in the statement `(x == y)%CR`, which states that the two Cauchy sequences `x, y` are equivalent. The library implements a *setoid* of field operations over this type [BCP03, Soz09], so as to facilitate substitutions for equivalents in formulas. In addition, the library provides a tactic called `bigenough`, which eases formal proofs by allowing a dose of laziness. This tactic is specially useful in proofs that a certain property on sequences is eventually true, which involve constructing effective moduli of convergence.

The formal statement corresponding to Theorem 1.1 is thus:

```
Theorem zeta_3_irrational : ~ ∃ (r : rat), (z3 == r%:CR)%CR.
```

where the postfix notation `r%:CR` denotes the Cauchy sequence whose elements are all equal to the rational number `(r : rat)`. The term `z3` is the Cauchy sequence corresponding to the partial sums $(z_n)_{n\in\mathbb{N}}$, that is, the dependent pair of this sequence with a proof of Property 2.3. The formal statement thus expresses that no constant rational sequence can be Cauchy equivalent to $(z_n)_{n\in\mathbb{N}}$. Interestingly, a long-lasting typo has marred the formal statement of theorem `zeta_3_irrational` in the corresponding Coq libraries, until writing the revised version of the present paper. Until then, the (inaccurate) statement was indeed:

```
Theorem incorrect_zeta_3_irrational : ~ ∃ (r : rat), (z3 = r%:CR)%CR.
```

Replacing `==` by `=` changes the statement completely, as it now expresses that there is no constant sequence of rationals equal to `z3`: and this is trivially true. The typo was already present in the version of the code that we made public for our previous report [CMSPT14], and the typo has remained unnoticed since. Yet fortunately, the *proof script* was right, and actually described a correct proof of the stronger statement `zeta_3_irrational`.

2.3. **Notations.** In this section, we provide a few hints on the notations used in the formal statements corresponding to the paper proof, so as to make precise the meaning of the statements we have proved formally. Indeed, this development makes heavy use of the notation facilities offered by the Coq proof assistant, so as to improve the readability of formulas. For instance, notation scopes allow to use the same infix notation for a relation on type `nat`, and in this case `(x < y)` unfolds to `(ltn x y): bool`, or for a relation on type `creal rat`), and in that case `(x < y)` unfolds to `(lt_creal x y): Prop`, the comparison predicate described in Section 2.2. Notation scopes can be made explicit using post-fixed tags: `(x < y)%N` is interpreted in the scope associated with natural numbers, and `(x < y)%CR`, in the scope associated with Cauchy sequences.

Generic notations can also be shared thanks to type-class like mechanisms. The Mathematical Components libraries feature a hierarchy of algebraic structures [GGMR09], which organizes a corpus of theories and notations shared by all the instances of a same structure. This hierarchy implements inheritance and sharing using Coq's mechanisms of coercions and of canonical structures [MT13]. Each structure in the hierarchy is modeled by a dependent record, which packages a type with some operations on this type and with requirements on these operations. In order to equip a given type with a certain structure, one has to endow this type with enough operations and properties, following the signature prescribed by the structure. For example, these structures are all *discrete*, which means that they require a boolean equality test. In turn, all instances of all these structures share the same infix notation `(x == y)` for the latter boolean equality test between `x` and `y`: this notation makes sense for `x,y` in type `nat,int`, `rat`, `alC`, etc. because all these types are instances of the same structure. For instance, although type `rat` is a dependent pair (see Section 2.2), the boolean comparison test only needs to work with the data: by Hedberg's theorem [Hed98], the proof stored in the proof component can be made irrelevant. Note that the situation is different for the type `(creal rat)` of Cauchy sequences. The formal statement of theorem `zeta_3_irrational` (see Section 2.2) uses the same `==` infix symbol, but in a different scope, in which it refers to `Prop`-valued Cauchy equivalence. Indeed, this relation cannot be turned constructively into a boolean predicate, as the comparison of Cauchy sequences is not effective. The type `algC` of algebraic numbers by contrast enjoys the generic version of the notation, as ordered fields only require a partial order relation.

Partial order, but also units of a ring, and inverse operations are examples of operations involved in some structures of the hierarchy, that make sense only on a subset of the elements of the carrier. In the dependent type theory implemented by Coq, it would be possible to use a dependent pair in order to model the source type of such an inverse operation. Instead, as a rule of thumb, the signature of a given structure avoids using rich types as the source types of their operations but rather "curry" the specification. For instance, the source type of the inverse operation in the structure of ring with units is the carrier type itself, but the signature of this structure also has a boolean predicate, which selects the units in this carrier type. The inverse operation has a default behavior outside units and the equations of the theory that involve inverses are typically guarded with invertibility conditions. Hence although the expression `x^-1 * x` is syntactically well-formed for any term `x` of an instance of ring with units, it can be rewritten to `1` only when `x` is known to be invertible.

The readability of formulas also requires dealing in a satisfactory manner with the inclusion of the various collections of numbers at stake, that are represented with distinct types, for instance:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \overline{\mathbb{Q}}.$$

The implementation of the inclusion $\mathbb{N} \subset \mathbb{Z}$ was mentioned in Section 2.1. The canonical embedding of type `int` is available in the generic theory of rings, but unfortunately, it cannot be declared as a coercion, and eluded in formal statements: the type of the corresponding constant would violate the uniform inheritance condition prescribed by Coq's coercion mechanism [The20]. Its formal definition hence comes with a generic postfix notation `_%:~R`, modeled as a reminiscence of the syntax of notation scopes and used to cast an integer as an element of another ring. The latter embedding is pervasive in formulas expressing the recurrence relations involved in this proof. Indeed, these recurrence relations feature polynomial coefficients in their indices and relate the rational elements of their solutions. See for instance Equation 3.2.

2.4. **Computations.** Using the unary representation of integers described in Section 2.1, the command:

```
Compute 100*1000.
```

which asks Coq to evaluate this product, triggers a stack overflow. For the purpose of running computations inside Coq's logic, on integers of a medium size, an alternate data-structure is required, together with less naive implementations of the arithmetical operations. The present formal proof requires this nature of computations at several places, for instance in order to evaluate sequences defined by a recurrence relation at a few particular values. For these computations, we used the binary representation of integers provided by the `ZArith` library included in the standard distribution of Coq, together with the fast reduction mechanism included in Coq's kernel [GL02].

These two ingredients are also used behind the scene by tactics implementing verified decision procedures. For instance, we make extensive use of proof commands dedicated to the normalization of algebraic expressions like the `field` tactic for rational fractions, and the `ring` tactic for polynomials [GM05]. The field tactic generates proof obligations describing sufficient conditions for the simplifications it made. In our case, these conditions in turn are solved using the `lia` decision procedure for linear arithmetics [Bes07].

These tactics work by first converting formulas in the goal into instances of appropriate data structures, suitable for larger scale computation. This pre-processing, hidden to the user, is performed by extra-logical code that is part of the internal implementation of these tactics. The situation is different when a computational step in a proof requires the evaluation of a formula at a given argument, and when both the formula and the argument are described using proof-oriented, inefficient representations. In that case, for instance for evaluating terms in a given sequence, we used the CoqEAL library [CDM13], which provides an infrastructure automating the conversion between different data-structures and algorithms used to model the same mathematical objects, like different representations of integers or different implementations of a matrix product. Note that although the CoqEAL library itself depends on a library for big numbers, which provides direct access in Coq to OCaml's library for arbitrary-precision, arbitrary-size signed integers, the present proof does not need this feature.

3. Outline of the proof

There exists several other proofs of Apéry's theorem. Notably, Beukers [Beu79] published an elegant proof, based on integrals of pseudo-Lengendre polynomials, shortly after Apéry's announcement. According to Fischler's survey [Fis04], all these proofs share a common structure. They rely on the asymptotic behavior of the sequence ℓ_n, the least common multiple of integers between 1 and n, and they proceed by exhibiting two sequences of rational numbers a_n and b_n, which have the following properties:

(1) For a sufficiently large n:

$$a_n \in \mathbb{Z} \quad \text{ and } 2\ell_n^3 b_n \in \mathbb{Z};$$

(2) The sequence $\delta_n = a_n\zeta(3) - b_n$ is such that:

$$\limsup_{n\to\infty} |2\delta_n|^{\frac{1}{n}} \leq (\sqrt{2}-1)^4;$$

(3) For an infinite number of values n, $\delta_n \neq 0$.

Altogether, these properties entail the irrationality of $\zeta(3)$. Indeed, if we suppose that there exists $p, q \in \mathbb{Z}$ such that $\zeta(3) = \frac{p}{q}$, then $2q\ell_n^3\delta_n$ is an integer when n is large enough. One variant of the Prime Number theorem states that $\ell_n = e^{n\,(1+o(1))}$ and since $(\sqrt{2}-1)^4 e^3 < 1$, the sequence $2q\ell_n^3\delta_n$ has a zero limit, which contradicts the third property. Actually, the Prime Number theorem can be replaced by a weaker estimation of the asymptotic behavior of ℓ_n, that can be obtained by more elementary means.

Lemma 3.1. *Let ℓ_n be the least common multiple of integers $1, \ldots, n$, then*

$$\ell_n = O(3^n).$$

Since we still have $(\sqrt{2}-1)^4 3^3 < 1$, this observation [Han72, Fen05] is enough to conclude. Section 6 discusses the formal proof of Lemma 3.1, an ingredient which was missing at the time of writing the previous report on this work [CMSPT14].

In our formal proof, we consider the pair of sequences proposed by Apéry in his proof [Apé79, vdP79]:

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \qquad b_n = a_n z_n + \sum_{k=1}^{n}\sum_{m=1}^{k} \frac{(-1)^{m+1}\binom{n}{k}^2\binom{n+k}{k}^2}{2m^3\binom{n}{m}\binom{n+m}{m}} \tag{3.1}$$

where z_n denotes $\sum_{m=1}^{n} \frac{1}{m^3}$, as already used in Proposition 2.3.

By definition, a_n is a positive integer for any $n \in \mathbb{N}$. The integrality of $2\ell_n^3 b_n$ is not as straightforward, but rather easy to see as well: each summand in the double sum defining b_n has a denominator that divides $2\ell_n^3$. Indeed, after a suitable re-organization in the expression of the summand, using standard properties of binomial coefficients, this follows easily from the following slightly less standard property:

Lemma 3.2. *For any integers i, j, n such that $1 \leq j \leq i \leq n$, $j\binom{i}{j}$ divides ℓ_n.*

Proof. For i, j, n such that $1 \leq j \leq i \leq n$, the proof goes by showing that for any prime p, the p-adic valuation of $j\binom{i}{j}$ is at most that of ℓ_n. Let us fix a prime number p. Let $t_p(i)$ be the largest integer e such that $p^e \leq i$. By definition, and since $i \leq n$, we thus have $p^{t_p(i)}|\ell_n$ and so $t_p(i) \leq v_p(\ell_n)$. Hence it suffices to prove that $v_p(\binom{i}{j}) \leq t_p(i) - v_p(j)$. Using Lemma 2.1, and because $j \leq i < p^{t_p(i)+1}$, we have:

$$v_p(\binom{i}{j}) = \sum_{k=1}^{t_p(i)} \left\lfloor \frac{i}{p^k} \right\rfloor - (\sum_{k=1}^{t_p(i)} \left\lfloor \frac{j}{p^k} \right\rfloor + \sum_{k=1}^{t_p(i)} \left\lfloor \frac{(i-j)}{p^k} \right\rfloor)$$

Remember that for $a, b \in \mathbb{N}$, $\left\lfloor \frac{a}{b} \right\rfloor$ is just a modulo b. Now for $1 \leq k \leq v_p(j)$, and because $p^k|j$, we have $\left\lfloor \frac{i}{p^k} \right\rfloor = \left\lfloor \frac{j}{p^k} \right\rfloor + \left\lfloor \frac{(i-j)}{p^k} \right\rfloor$, and thus:

$$\begin{aligned} v_p(\binom{i}{j}) &= \sum_{k=v_p(j)+1}^{t_p(i)} \left\lfloor \frac{i}{p^k} \right\rfloor - (\sum_{k=v_p(j)+1}^{t_p(i)} \left\lfloor \frac{j}{p^k} \right\rfloor + \sum_{k=v_p(j)+1}^{t_p(i)} \left\lfloor \frac{(i-j)}{p^k} \right\rfloor) \\ &= \sum_{k=1}^{t_p(i)-v_p(j)} \left\lfloor \frac{i}{p^{v_p(j)+k}} \right\rfloor - (\sum_{k=1}^{t_p(i)-v_p(j)} \left\lfloor \frac{j}{p^{v_p(j)+k}} \right\rfloor + \sum_{k=1}^{t_p(i)-v_p(j)} \left\lfloor \frac{(i-j)}{p^{v_p(j)+k}} \right\rfloor) \end{aligned}$$

Now for any $1 \leq k \leq t_p(i) - v_p(j)$, we have:

$$\left\lfloor \frac{i}{p^{v_p(j)+k}} \right\rfloor \leq \left\lfloor \frac{j}{p^{v_p(j)+k}} \right\rfloor + \left\lfloor \frac{(i-j)}{p^{v_p(j)+k}} \right\rfloor + 1$$

Summing both sides for k from 1 to $t_p(i) - v_p(j)$ and using the previous identity for $v_p(\binom{i}{j})$ eventually proves that $v_p(\binom{i}{j}) \leq t_p(i) - v_p(j)$, which concludes the proof. □

The rest of the proof is a study of the sequence $\delta_n = a_n\zeta(3) - b_n$. It not difficult to see that δ_n tends to zero, from the formulas defining the sequences a and b, but we also need to prove that it does so fast enough to compensate for ℓ_n^3, while being positive. In his original proof, Apéry derived the latter facts by combining the definitions of the sequences a and b with the study of a mysterious recurrence relation. Indeed, he made the surprising claim that Lemma 3.3 holds:

Lemma 3.3. *For $n \geq 0$, the sequences $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ satisfy the* same *second-order recurrence:*

$$(n+2)^3 y_{n+2} - (17n^2 + 51n + 39)(2n+3)y_{n+1} + (n+1)^3 y_n = 0. \tag{3.2}$$

Equation 3.2 is a typical example of a linear recurrence equation with polynomial coefficients and standard techniques [Sal03, vdP79] can be used to study the asymptotic behavior of its solutions. Using this recurrence and the initial conditions satisfied by a and b, one can thus obtain the two last properties of our criterion, and conclude with the irrationality of $\zeta(3)$. For the purpose of our formal proof, we devised an elementary version of this asymptotic study, mostly based on variations on the presentation of van der Poorten [vdP79]. We detail this part of the proof in Section 5.

Using only Equation 3.2, even with sufficiently many initial conditions, it would not be easy to obtain the first property of our criterion, about the integrality of a_n and b_n for a large enough n. In fact, it would also be difficult to prove that the sequence δ tends to zero:

we would only know that it has a finite limit, and how fast the convergence is. By contrast, it is fairly easy to obtain these facts from the explicit closed forms given in Formula 3.1.

The proof of Lemma 3.3 was by far the most difficult part in Apéry's original exposition. In his report [vdP79], van der Poorten describes how he, with other colleagues, devoted significant efforts to this verification after having attended the talk in which Apéry exposed his result for the first time. Actually, the proof of Lemma 3.3 boils down to a routine calculation using the two auxiliary sequences $U_{n,k}$ and $V_{n,k}$, themselves defined in terms of $\lambda_{n,k} = \binom{n}{k}^2\binom{n+k}{k}^2$ (with $\lambda_{n,k} = 0$ if $k < 0$ or $k > n$):

$$\begin{aligned} U_{n,k} &= 4(2n+1)(k(2k+1)-(2n+1)^2)\lambda_{n,k}, \\ V_{n,k} &= U_{n,k}\left(\sum_{m=1}^{n}\frac{1}{m^3} + \sum_{m=1}^{k}\frac{(-1)^{m-1}}{2m^3\binom{n}{m}\binom{n+m}{m}}\right) + \frac{5(2n+1)k(-1)^{k-1}}{n(n+1)}\binom{n}{k}\binom{n+k}{k} \end{aligned}$$

The key idea is to compute telescoping sums for U and V. For instance, we have:

$$U_{n,k} - U_{n,k-1} = (n+1)^3\lambda_{n+1,k} - (34n^3+51n^2+27n+5)\lambda_{n,k} + n^3\lambda_{n-1,k} \tag{3.3}$$

Summing Equation 3.3 on k shows that the sequence a satisfies the recurrence relation of Lemma 3.3. A similar calculation proves the analogue for b, using telescoping sums of the sequence V.

Not only is the statement of Formula 3.2 difficult to discover: even when this recurrence is given, finding the suitable auxiliary sequences U and V by hand is a difficult task. Moreover, there is no other known way of proving Lemma 3.3 than by exhibiting this nature of certificates. Fortunately, the sequences a and b belong in fact to a class of objects well known in the fields of combinatorics and of computer-algebra. Following seminal work of Zeilberger's [Zei90], algorithms have been designed and implemented in computer-algebra systems, which are able to obtain linear recurrences for these sequences. For instance the Maple package Mgfun (distributed as part of the Algolib [alg13] library) implements these algorithms, among others. Basing on this implementation, Salvy wrote a Maple worksheet [Sal03] that follows Apéry's original method but interlaces Maple calculations with human-written parts. In particular, this worksheet illustrates how parts of this proof, including the discovery of Apéry's mysterious recurrence, can be performed by symbolic computations. Our formal proof of Lemma 3.3 follows an approach similar to the one of Salvy. It is based on calculations performed using the Algolib library, and certified a posteriori. This part of the formal proof is discussed in Section 4.1.

4. Algorithms, Recurrences and Formal Proofs

This section quotes and summarizes an earlier publication [CMSPT14]*, describing a joint work with Chyzak and Tassi.*

Lemma 3.3 is the bottleneck in Apéry's proof. Both sums a_n and b_n in there are instances of *parameterized summation*: they follow the pattern $F_n = \sum_{k=\alpha(n)}^{\beta(n)} f_{n,k}$ in which the summand $f_{n,k}$, potentially the bounds, and thus the sum, depend on a parameter n. This makes it appealing to resort to the algorithmic paradigm of *creative telescoping*, which was developed for this situation in computer algebra.

4.1. **Recurrences as a data structure for sequences.** A fruitful idea from the realm of computer algebra is to represent sequences not explicitly, such as the univariate $(n!)_n$ or the bivariate $(\binom{n}{k})_{n,k}$, but by a system of linear recurrences of which they are solutions such as $\{u_{n+1} = (n+1)u_n\}$ or $\{u_{n+1,k} = \frac{n+1}{n+1-k}u_{n,k}, u_{n,k+1} = \frac{n-k}{k+1}u_{n,k}\}$, accompanied with sufficient initial conditions. Sequences which can be represented in such a way are called *∂-finite*. The finiteness property of their definition makes algorithmic most operations under which the class of ∂-finite sequences is stable.

In the specific bivariate case which interests us, let S_n be the shift operator in n mapping a sequence $(u_{n,k})_{n,k}$ to $(u_{n+1,k})_{n,k}$ and similarly, let S_k map $(u_{n,k})_{n,k}$ to $(u_{n,k+1})_{n,k}$. Linear recurrences canceling a sequence f can be seen as elements of a non-commutative ring of polynomials with coefficients in $\mathbb{Q}(n,k)$, and with the two indeterminates S_n and S_k, with the action $(P \cdot f)_{n,k} = \sum_{(i,j)\in I} p_{i,j}(n,k) f_{n+i,k+j}$, where subscripts denote evaluation. For example for $f_{n,k} = \binom{n}{k}$, the previous recurrences once rewritten as equalities to zero can be represented as $P \cdot f = 0$ for $P = S_n - \frac{n+1}{n+1-k}$ and $P = S_k - \frac{n-k}{k+1}$, respectively.

Computer algebra gives us algorithms to produce canceling operators for operations such as the addition or product of two ∂-finite sequences, using for both its inputs and output a Gröbner basis as a canonical way to represent the set of their canceling operators, which gives some uniqueness guarantees.

The case of summing a sequence $(f_{n,k})$ into a parameterized sum $F_n = \sum_{k=0}^{n} f_{n,k}$ is more involved: it follows the method of *creative telescoping* [Zei91], in two stages. First, an *algorithmic* step determines pairs (P, Q) satisfying

$$P \cdot f = (S_k - 1)Q \cdot f \tag{4.1}$$

with $P \in \mathbb{Q}(n)[S_n]$ and $Q \in \mathcal{A}$. To continue with our example $f_{n,k} = \binom{n}{k}$, we could choose $P = S_n - 2$ and $Q = S_n - 1$. Second, a *systematic* but not fully algorithmic step follows: summing (4.1) for k between 0 and $n + \deg P$ yields

$$(P \cdot F)_n = (Q \cdot f)_{k=n+\deg P+1} - (Q \cdot f)_{k=0}. \tag{4.2}$$

Continuing with our binomial example, summing (4.1) for k from 0 to $n+1$ (and taking special values into account) yields $\sum_{k=0}^{n+1}\binom{n+1}{k} - 2\sum_{k=0}^{n}\binom{n}{k} = 0$, a special form of (4.2) with right-hand side canceling to zero. This tells us that the sequence $(\sum_{k=0}^{n}\binom{n}{k})_{n\in\mathbb{N}}$ is a solution of the same recurrence $P = S_n - 2$ as $(2^n)_{n\in\mathbb{N}}$: a simple check of initial values gives us the identity $\forall n \in \mathbb{N}, 2^n = \sum_{k=0}^{n}\binom{n}{k}$. The formula (4.2) in fact assumes several hypotheses that hold not so often in practice; this will be formalized by Equation (4.3) below.

4.2. **Apéry's sequences are ∂-finite constructions.** The sequences a and b in (3.1) are ∂-finite: they have been announced to be solutions of (3.2). But more precisely, they can be viewed as constructed from "atomic" sequences by operations under which the class of ∂-finite sequences is stable. This is summarized in Table 1.

In this table, Gröbner bases are systems of recurrence operators: at each line in the table, the sequence given in explicit form is a solution of the system of recurrences described by the operators in the Gröbner basis column. Note that in fact none of these results rely on the *specific* sequences in the explicit form: at each step, a new Gröbner basis is obtained from known ones, the ones that are cited in the input column. The table can also be read bottom-up for the purpose of verification: the Gröbner basis obtained at a given step can be verified using *only* the Gröbner bases obtained at some previous steps, all the way down to C and D. These operators describe a more general class of (germs of) sequences than

step	explicit form	GB	operation	input(s)
1	$c_{n,k} = \binom{n}{k}^2\binom{n+k}{k}^2$	C	direct	
2	$a_n = \sum_{k=1}^{n} c_{n,k}$	A	creative telescoping	C
3	$d_{n,m} = \frac{(-1)^{m+1}}{2m^3\binom{n}{m}\binom{n+m}{m}}$	D	direct	
4	$s_{n,k} = \sum_{m=1}^{k} d_{n,m}$	S	creative telescoping	D
5	$z_n = \sum_{m=1}^{n} \frac{1}{m^3}$	Z	direct	
6	$u_{n,k} = z_n + s_{n,k}$	U	addition	Z and S
7	$v_{n,k} = c_{n,k}u_{n,k}$	V	product	C and U
8	$b_n = \sum_{k=1}^{n} v_{n,k}$	B	creative telescoping	V

Table 1: Construction of a_n and b_n: At each step, the Gröbner basis named in column GB, which annihilates the sequence given in explicit form, is obtained by the corresponding operation *on ideals*, with input(s) given on the last column.

just the explicit sequences used in this table, thus initial conditions are needed to describe a precise sequence.

4.3. **Provisos and sound creative telescoping.** We illustrate the process of verifying candidate new recurrences using known ones on the example of Pascal's triangle rule. One can "almost prove" Pascal's triangle rule using only the following recurrences, satisfied by binomial coefficients:

$$u_{n+1,k} = \frac{n+1}{n+1-k}u_{n,k} \quad \text{and} \quad u_{n,k+1} = \frac{n-k}{k+1}u_{n,k}.$$

Indeed, we have:

$$\binom{n+1}{k+1} - \binom{n}{k+1} - \binom{n}{k} = \left(\frac{n+1}{n-k}\frac{n-k}{k+1} - \frac{n-k}{k+1} - 1\right)\binom{n}{k} = 0 \times \binom{n}{k} = 0,$$

but this requires $k \neq -1$ and $k \neq n$. Therefore, this does not prove Pascal's rule for all n and k. The phenomenon is general: computer algebra is unable to take denominators into account. This incomplete modeling of sequences by algebraic objects may cast doubt on these computer-algebra proofs, in particular when it comes to the output of creative-telescoping algorithms.

By contrast, in our formal proofs, we augmented the recurrences with provisos that restrict their applicability. In this setting, we validate a candidate identity like the Pascal triangle rule by a normalization modulo the elements of a Gröbner basis plus a verification that this normalization only involves legal instances of the recurrences. In the case of creative telescoping, Eq. (4.1) takes the form:

$$(n,k) \notin \Delta \Rightarrow (P \cdot f_{\_,k})_n = (Q \cdot f)_{n,k+1} - (Q \cdot f)_{n,k}, \tag{4.3}$$

where $\Delta \subset \mathbb{Z}^2$ guards the relation and where $f_{\_,j}$ denotes the univariate sequence obtained by specializing the second argument of f to j. Thus our formal analogue of Eq. (4.2) takes this restriction into account and has the shape

$$\begin{aligned}(P\cdot F)_n = \Big((Q\cdot f)_{n,n+\beta+1} - (Q\cdot f)_{n,\alpha}\Big) + \sum_{i=1}^{r}\sum_{j=1}^{i} p_i(n)\, f_{n+i,n+\beta+j} \\ + \sum_{\alpha\le k\le n+\beta\ \wedge\ (n,k)\in\Delta} (P\cdot f_{\_,k})_n - (Q\cdot f)_{n,k+1} + (Q\cdot f)_{n,k},\end{aligned} \tag{4.4}$$

for F the sequence with general term $F_n = \sum_{k=\alpha}^{n+\beta} f_{n,k}$ and where $P = \sum_{i=0}^{r} p_i(n) S_n^i$.

The last term of the right-hand side, which we will call the singular part, witnesses the possible partial domain of validity of relation (4.3). Thus the operator P is a valid recurrence for the sequence F if the right-hand side of Eq. (4.4) normalizes to zero, at least outside of an algebraic locus that will guard the recurrence.

4.4. **Generated Operators, hand-written provisos, and formal proofs.** For each step in Table 1, we make use of the data computed by the Maple session in a systematic way, using pretty-printing code to express this data in Coq. As mentioned in Section 4.3, we manually annotate each operator produced by the computer-algebra program with provisos and turn it this way into a conditional recurrence predicate on sequences. In our formal proof, each step in Table 1 consists in proving that some conditional recurrences on a composed sequence can be proved from some conditional recurrences known for the arguments of the operation.

These steps are far from automatic, mainly because the singular part yields terms which have to be reduced manually through trial-and-error using a Gröbner basis of annihilators for f, but also because we have to show that some rational-function coefficients of the remaining instances of f are zero. This is done through a combination of the `field` and `lia` proof commands, helped by some factoring of denominators pre-obtained in Maple.

4.5. **Composing closures and reducing the order of B.** In order to complete the formal proof of Lemma 3.3, we verify formally that each sequence involved in the construction of a_n and b_n is a solution of the corresponding Gröbner system of annotated recurrence, starting from c_n, d_n, and z_n all the way to the the final conclusions. This proves that a_n is a solution of the recurrence (3.2) but only provides a recurrence of order four for b_n. We then prove that b also satisfies the recurrence (3.2) using four evaluations b_0, b_1, b_2, b_3.

5. Consequences of Apéry's recurrence

In this section, we detail the elementary proofs of the properties obtained as corollaries of Lemma 3.3. We recall, from Section 3, that these properties describe the asymptotic behavior of the sequence $\delta_n = a_n\zeta(3) - b_n$, with:

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2\binom{n+k}{k}^2, \qquad b_n = a_n z_n + \sum_{k=1}^{n}\sum_{m=1}^{k} \frac{(-1)^{m+1}\binom{n}{k}^2\binom{n+k}{k}^2}{2m^3\binom{n}{m}\binom{n+m}{m}} \tag{5.1}$$

Throughout the section, we use the vocabulary and notations of Cauchy sequences numbers, as introduced in Section 2.2. For instance, we have:

Lemma 5.1. *For any ε, eventually $|z_n - \frac{b_n}{a_n}| < \varepsilon$.*

Proof. Easy from the definition of z, a and b. □

Corollary 5.2. *The sequence* $(\frac{b_n}{a_n})_{n\in\mathbb{N}}$ *is a Cauchy sequence, which is Cauchy equivalent to* $(z_n)_{n\in\mathbb{N}}$.

The formal statement corresponding to Lemma 5.1 is:

```
Lemma z3seq_b_over_a_asympt : {asympt e : n / |z3seq n - b_over_a_seq n| < e}.
```

where `b_over_a_seq n` represents $\frac{b_n}{a_n}$. The notation `{asympt e : i / P}`, used in this formal statement, comes from the external library for Cauchy sequences [Coh12]. In the expression `{asympt e : i / P}`, `asympt` is a keyword, and both `e` and `i` are names for variables bound in the term `P`. This expression unfolds to the term `(asympt1 (fun e i => P))`, a dependent pair that ensures the existence of an explicit witness that property `P` asymptotically holds:

```
Definition asympt1 R (P : R → nat → Prop) :=
  {m : R → nat | ∀ (eps : R) (i : nat), 0 < eps → m eps ≤ i → P eps i}.
```

The formalization of Corollary 5.2 then comes in three steps: first the proof that $(\frac{b_n}{a_n})_{n\in\mathbb{N}}$ is a Cauchy sequence, as formalized by the `creal_aiom` predicate:

```
Corollary creal_b_over_a_seq : creal_axiom b_over_a_seq.
```

This formal proof is a one-liner, because the corresponding general argument, a sequence that is asymptotically close to a Cauchy sequence will itself satisfy the Cauchy property, is already present in the library. Then, the latter proof is used to forge an inhabitant of the type of rational Cauchy sequences, which just amounts to pairing the sequence `b_over_a_seq : nat → rat` with the latter proof:

```
Definition b_over_a : {creal rat} := CReal creal_b_over_a_seq.
```

Now we can state the proof of equivalence between the two Cauchy sequences, i.e., between the two corresponding terms of type `{creal rat}`:

```
Fact z3_eq_b_over_a : (z3 == b_over_a)%CR.
```

The proof of the latter fact is again a one-liner, with no additional mathematical content added to lemma `creal_b_over_a_seq`, but it provides access to automation based on setoid rewriting facilities

The MATHEMATICAL COMPONENTS libraries do not cover any topic of analysis, and even the most basic definitions of transcendental functions like the exponential or the logarithm are not available. However, it is possible to obtain the required properties of the sequence δ by very elementary means, and almost all these elementary proofs can be inferred from a careful reading and a combination of Salvy's proof [Sal03] and of van der Poorten's description [vdP79].

Following van der Poorten, we introduce an auxiliary sequence $(w_n) \in \mathbb{Q}^n$, defined as:

$$w_n = \begin{vmatrix} b_{n+1} & a_{n+1} \\ b_n & a_n \end{vmatrix} = b_{n+1}a_n - a_{n+1}b_n.$$

The sequence w is called a *Casoratian*: as a and b are solutions of a same linear recurrence relation (3.2) of order 2, this can be seen as a discrete analogue of the Wronskian for linear differential systems. For example, w satisfies a recurrence relation of order 1, which provides a closed form for w:

Lemma 5.3. *For* $n \geq 2$, $w_n = \frac{6}{(n+1)^3}$.

Proof. Since a and b satisfy the recurrence relation 3.1, w satisfies the relation:

$$\forall k \in \mathbb{N}, (k+2)^3 w_{k+1} - (k+1)^3 w_k = 0.$$

The result follows from the computation of w_0. $\square$

From this formula, we can obtain the positivity of the sequence δ, and an evaluation of its asymptotic behavior in terms of the sequence a.

Corollary 5.4. *For any $n \in \mathbb{N}$ such that $2 \leq n$, $0 < \zeta(3) - \frac{b_n}{a_n}$.*

The formal statement corresponding to Corollary 5.4 is the following:

```
Lemma lt0_z3_minus_b_over_a (n : nat) : 2 ≤ n → (0%:CR < z3 - (b_over_a_seq n)%:CR)%CR.
```

Note the postfix `CR` tag which enforces that inside the corresponding parentheses, notations are interpreted in the scope associated with Cauchy sequences: in particular, the order relation (on Cauchy sequences) is the one described in Section 2.2.

Term `(b_over_a_seq n : rat)` is the rational number $\frac{a_n}{b_n}$, which is casted as a Cauchy real, the corresponding constant sequence, using the postfix `%:CR`, so as to be subtracted to the Cauchy sequence `z3`. This proof in particular benefits from setoid rewriting using equivalences like `z3_eq_b_over_a`, the formal counterpart of Corollary 5.2.

Proof. Since $\zeta(3)$ is Cauchy equivalent to $(\frac{b_n}{a_n})_{n\in\mathbb{N}}$, it is sufficient to show that for any $k < l$, we have $0 < \frac{b_l}{a_l} - \frac{b_k}{a_k}$. Thus it is sufficient to observe that for any k, we have $0 < \frac{b_{k+1}}{a_{k+1}} - \frac{b_k}{a_k}$, which follows from Lemma 5.3. $\square$

Corollary 5.5. $\zeta(3) - \frac{b_n}{a_n} = \mathcal{O}(\frac{1}{a_n^2})$.

Proof. Since $\zeta(3) = \frac{b}{a}$, it is sufficient to show that there exists a constant K, such that for any $k < l$, $\frac{b_l}{a_l} - \frac{b_k}{a_k} \leq \frac{K}{a_k^2}$. But since a is an increasing sequence, Lemma 5.3 proves that for any $k < l$, $\frac{b_l}{a_l} - \frac{b_k}{a_k} \leq \sum_{i=k}^{l-1} \frac{w_i}{a_i a_{i+1}} \leq \sum_{i=k}^{l-1} \frac{6}{(i+1)^3 a_k^2} \leq \frac{K}{a_k^2}$, for any K greater than $6 \cdot \zeta(3)$. $\square$

The last remaining step of the proof is to show that the sequence a grows fast enough. The elementary version of Lemma 5.6 is based on a suggestion by F. Chyzak.

Lemma 5.6. $33^n = \mathcal{O}(a_n)$.

Proof. Consider the auxiliary sequence $\rho_n = \frac{a_{n+1}}{a_n}$. Since ρ_{51} is greater than 33, we only need to show that the sequence ρ is increasing. For the sake of readability, we denote μ_n and ν_n the fractions coefficients of the recurrence satisfied by a, obtained from Equation 3.2 after division by its leading coefficient. Thus a satisfies the recurrence relation:

$$a_{n+2} - \mu_n a_{n+1} + \nu_n = 0.$$

For $n \in \mathbb{N}$, we also introduce the function $h_n(x) = \mu_n + \frac{\nu_n}{x}$, so that $\rho_{n+1} = h_n(\rho_n)$. The polynomial $P_n(x) = x^2 - \mu_n x + \nu_n$ has two distinct roots $x'_n < x_n$, and the formula describing the roots of polynomials of degree 2 show that $0 < x'_n < 1 < x_n$ and that the sequence x_n is increasing. But since $h_n(x) - x = -\frac{P_n(x)}{x}$, for $1 < x < x_n$, we have $h_n(x) > x$. A direct recurrence shows that for any $n \geq 2$, $\rho_n \in [1, x_n]$, which concludes the proof. $\square$

In the formal proof of Lemma 5.6, the computation of ρ_{51} was made possible by using the CoqEAL library, as already mentioned in Section 2.4. This proof also requires a few symbolic computations that are a bit tedious to perform by hand: in these cases, we used Maple as an oracle to massage algebraic expressions, before formally proving the correctness of the simplification. This was especially useful to study the roots x'_n and x_n of P_n.

We can now conclude with the limit of the sequence $\ell_n^3\delta_n$, under the assumption that $\ell_n = \mathcal{O}(3^n)$.

Corollary 5.7. $\lim\limits_{n\to\infty}(\ell_n^3\delta_n) = 0$.

Proof. Immediate, since $\delta_n = \mathcal{O}(\frac{1}{a_n})$ by Corollary 5.5, and $\ell_n^3 = \mathcal{O}((3^3)^n)$, and $3^3 < 33$. □

In the next Section, we describe the proof of the last remaining assumption, about the asymptotic behavior of ℓ_n.

6. Asymptotics of $lcm(1, ..., n)$

For any integer $1 \leq n$, let ℓ_n denote the least common multiple $lcm(1, ..., n)$ of the integers no greater than n. By convention, we set $\ell_0 = 1$. The asymptotic behavior of the sequence (ℓ_n) is a classical corollary of the Prime Number Theorem. A sufficient estimation for the present proof can actually but obtained as a direct consequence, using an elementary remark about the p-adic valuations of ℓ_n.

Remark 6.1. For any prime number p, the integer $p^{v_p(\ell_n)}$ is the highest power of p not exceeding n, so that:

$$v_p(\ell_n) = \left\lfloor \log_p(n) \right\rfloor .$$

Proof. Noticing that $v_p(lcm(a, b)) = \max(v_p(a), v_p(b))$, we see by induction on n that $v_p(\ell_n) = \max\limits_{i=1}^{n} v_p(i)$. Recall from Section 2.1 that $\lfloor \log_p(n) \rfloor$ is a notation for the greatest integer α such that $p^\alpha \leq n$. Since $\alpha = v_p(p^\alpha)$, we have $\alpha \leq v_p(\ell_n)$. Now suppose that $v_p(\ell_n) = v_p(i)$ for some $i \in \{1, \ldots, n\}$. Then $i = p^{v_p(i)}q$ with $gcd(p, q) = 1$ so that $p^{v_p(\ell_n)} = p^{v_p(i)} \leq i \leq n$ and thus $v_p(\ell_n) \leq \alpha$. This proves that $v_p(\ell_n) = \alpha$. □

By Remark 6.1, ℓ_n can hence be written as $\prod_{p\leq n} p^{\lfloor \log_p(n) \rfloor}$ and therefore:

$$\ln(\ell_n) = \sum_{p\leq n} \ln(p^{\lfloor \log_p(n) \rfloor}) \leq \sum_{p\leq n} \ln(n).$$

If $\pi(n)$ is the number of prime numbers no greater than n, we hence have:

$$\ln(\ell_n) \leq \pi(n) \ln(n).$$

The Prime Number theorem states that $\pi(n) \sim \frac{n}{\ln(n)}$; we can thus conclude that:

$$\ell_n = \mathcal{O}(e^n).$$

Note that this estimation is in fact rather precise, as in fact:

$$\ell_n \sim e^{n\,(1+o(1))}.$$

J. Avigad and his co-authors provided the first machine-checked proof of the Prime Number theorem [ADGR07], which was considered at the time as a formalization *tour de force*. Their formalization is based on a proof attributed to A. Selberg and P. Erdös.

Although the standard proofs of this theorem use tools from complex analysis like contour integrals, their choice was guided by the corpus of formalized mathematics available for the Isabelle proof assistant, or the limits thereof. Although less direct, the proof by A. Selberg and P. Erdös is indeed more elementary and avoids complex analysis completely.

6.1. **Statement, Notations and Outline.** In order to prove Corollary 5.7 in Section 5, we only need to resort to Lemma 3.1, i.e., to the fact that:

$$\ell_n = \mathcal{O}(3^n).$$

This part of the proof was left as an assumption in our previous report [CMSPT14]. This weaker description of the asymptotic behavior of (ℓ_n) was in fact known before the first proofs of the Prime Number theorem but our formal proof is a variation on an elementary proof proposed by Hanson [Han72].

The idea of the proof is to replace the study of ℓ_n by that of another sequence $C(n)$. The latter is defined as a multinomial coefficient depending on elements of a fast-growing sequence α. The fact that $\prod_{i=1}^n \alpha_i^{1/\alpha_i} < 3$ independently of n then allows to show that $C(n) = \mathcal{O}(3^n)$.

6.2. **Proof.** Define the sequence $(\alpha_n)_{n\in\mathbb{N}}$ by $\alpha_0 = 2$, and $\alpha_{n+1} = \alpha_1\alpha_2\cdots\alpha_n + 1$ for $n \geq 1$. By an induction on n, this is equivalent to $\alpha_{n+1} = \alpha_n^2 - \alpha_n + 1$. For $n, k \in \mathbb{N}$, let

$$C(n,k) = \frac{n!}{\lfloor n/\alpha_1\rfloor!\lfloor n/\alpha_2\rfloor!\cdots\lfloor n/\alpha_k\rfloor!}.$$

As soon as $\alpha_k \geq n$, $C(n,k)$ is independent of k and we denote $C(n) = C(n,k)$ for all such k. Hanson directly defines $C(n)$ as a limit, but we found this to be inconvenient to manipulate in the proof. Moreover, most inequalities stated on $C(n)$ actually hold for $C(n,k)$ with little or no more hypotheses. The following technical lemma will be useful in the study of this sequence.

Lemma 6.2. *For $k \in \mathbb{N}$,*

$$\sum_{i=1}^{k}\frac{1}{\alpha_i} = \frac{\alpha_{k+1}-2}{\alpha_{k+1}-1} < 1 \text{ and thus for } x \in \mathbb{Q} \text{ with } x \geq 1, \lfloor x\rfloor > \sum_{i=1}^{k}\left\lfloor\frac{x}{\alpha_i}\right\rfloor.$$

Proof. The proof is done by induction and relies on the fact that if $a \in \mathbb{Q}$ and $m \in \mathbb{N}^+$, we have $\left\lfloor\frac{a}{m}\right\rfloor = \left\lfloor\frac{\lfloor a\rfloor}{m}\right\rfloor$. ☐

Notice that by Lemma 6.2, $\sum\limits_{i=0}^{k}\left\lfloor\frac{n}{\alpha_i}\right\rfloor < n$ and thus:

$$C(n,k) = \binom{\sum_{i=0}^{k}\left\lfloor\frac{n}{\alpha_i}\right\rfloor}{\lfloor n/\alpha_1\rfloor, \lfloor n/\alpha_2\rfloor, \ldots, \lfloor n/\alpha_k\rfloor}\frac{n!}{\left(\sum_{i=0}^{k}\left\lfloor\frac{n}{\alpha_i}\right\rfloor\right)!}.$$

In particular, $C(n,k) \in \mathbb{N}$. The goal is now to show that $\ell_n \leq C(n) < K\cdot 3^n$ for some K.

In the following, for $n, k, p \in \mathbb{N}$ and p prime, we denote $\beta_p(n,k)$ for $v_p(C(n,k))$.

Lemma 6.3. *For all $n, k \in \mathbb{N}$, with $1 \le n$ and p prime, $\beta_p(n,k) \ge \lfloor \log_p(n) \rfloor = v_p(\ell_n)$. Therefore $C(n,k) \ge \ell_n$ for all n.*

Proof. The proof uses Lemma 2.1.

$$\begin{aligned}
\beta_p(n,k) &= v_p(n!) - \sum_{i=1}^{k} v_p(\lfloor n/\alpha_i \rfloor !) \\
&= \sum_{i=1}^{\lfloor \log_p(n) \rfloor} \lfloor n/p^i \rfloor - \sum_{i=1}^{k} \sum_{j=1}^{\lfloor \log_p(\lfloor \frac{n}{\alpha_i} \rfloor) \rfloor} \left\lfloor \frac{n}{\alpha_i p^j} \right\rfloor \\
&= \sum_{i=1}^{\lfloor \log_p(n) \rfloor} \left(\lfloor n/p^i \rfloor - \sum_{j=1}^{k} \left\lfloor \frac{\lfloor \frac{n}{p^i} \rfloor}{\alpha_j} \right\rfloor \right) \\
&\ge \sum_{i=1}^{\lfloor \log_p(n) \rfloor} 1 \text{ (because } \sum \frac{1}{\alpha_i} < 1 \text{ by Lemma 6.2).}
\end{aligned}$$

Since $\ell_n = \prod_{p \le n} p^{\lfloor \log_p(n) \rfloor}$ from Remark 6.1, we get $\ell_n \le C(n,k) = \prod_{p \le n} p^{\beta_p(n,k)}$. □

Lemma 6.4. *For $i \ge 1$ and $n \ge \alpha_i$,*

$$\frac{\left(\frac{n}{\alpha_i}\right)^{\frac{n}{\alpha_i}}}{\left\lfloor \frac{n}{\alpha_i} \right\rfloor^{\lfloor \frac{n}{\alpha_i} \rfloor}} < \left(\frac{10\, n}{\alpha_i} \right)^{\frac{\alpha_i - 1}{\alpha_i}}.$$

Proof. If $n = \alpha_i$, we have $1 < \sqrt{10} \le 10^{\frac{\alpha_i - 1}{\alpha_i}}$, hence the result. Otherwise $n > \alpha_i$: let us write $n = b\alpha_i + r$, with $0 \le r < \alpha_i$ the Euclidean division of n by α_i. We have:

$$\frac{n - \alpha_i + 1}{\alpha_i} = b - 1 + \frac{r+1}{\alpha_i} \le b.$$

Since $b = \left\lfloor \frac{n}{\alpha_i} \right\rfloor$, it follows that $\frac{n - \alpha_i + 1}{\alpha_i} \le \left\lfloor \frac{n}{\alpha_i} \right\rfloor$. Now for $\frac{1}{2} \le x$, the function x^x is increasing, thus since $\frac{1}{2} \le \frac{1}{\alpha_i} \le \frac{n-\alpha_i+1}{\alpha_i}$, we deduce that $\left(\frac{n-\alpha_i+1}{\alpha_i}\right)^{\frac{n-\alpha_i+1}{\alpha_i}} \le \left\lfloor \frac{n}{\alpha_i} \right\rfloor^{\lfloor \frac{n}{\alpha_i} \rfloor}$, and we hence have:

$$\frac{\left(\frac{n}{\alpha_i}\right)^{\frac{n}{\alpha_i}}}{\left\lfloor \frac{n}{\alpha_i} \right\rfloor^{\lfloor \frac{n}{\alpha_i} \rfloor}} \le \frac{\left(\frac{n}{\alpha_i}\right)^{\frac{n}{\alpha_i}}}{\left(\frac{n-\alpha_i+1}{\alpha_i}\right)^{\frac{n-\alpha_i+1}{\alpha_i}}} = \left(1 + \frac{\alpha_i - 1}{n - \alpha_i + 1}\right)^{\frac{n-\alpha_i+1}{\alpha_i - 1} \frac{\alpha_i - 1}{\alpha_i}} \left(\frac{n}{\alpha_i}\right)^{\frac{\alpha_i - 1}{\alpha_i}}.$$

The first operand in the last expression is of the shape $\left(\left(1 + \frac{1}{x}\right)^x\right)^{\frac{\alpha_i - 1}{\alpha_i}}$, where x is a positive rational. We showed using only elementary properties of rational numbers, like the binomial formula or the summation formula for geometric progressions, that for any such positive rational number x, $\left(1 + \frac{1}{x}\right)^x < 10$, hence the result. Note that we only needed that there exist a constant $K > 0$ such that $\left(1 + \frac{1}{x}\right)^x < K$. □

Of course, using elementary real analysis allows for the tighter bound e, which was used in Hanson's paper, but this bound is irrelevant for the final result. We can now establish the following bound on $C(n,k)$:

Lemma 6.5. *For $k \geq 1$ and $n \geq 2$,*

$$C(n,k) < \frac{n^n}{\left\lfloor \frac{n}{\alpha_1} \right\rfloor^{\left\lfloor \frac{n}{\alpha_1} \right\rfloor} \cdots \left\lfloor \frac{n}{\alpha_k} \right\rfloor^{\left\lfloor \frac{n}{\alpha_k} \right\rfloor}}.$$

Proof. First observe that if $m = m_1 + \cdots + m_k$ where m and the m_i are (not all zero) non-negative integers, we have because of the multinomial theorem:

$$(m_1 + \cdots + m_k)^m \geq \binom{m}{m_1, \ldots, m_k} m_1^{m_1} \cdots m_k^{m_k}. \tag{6.1}$$

Let $k \geq 1$, and define:

$$t = \sum_{i=1}^{k} \left\lfloor \frac{n}{\alpha_i} \right\rfloor.$$

Then $t < n$ by Lemma 6.2. We have:

$$C(n,k) = n \cdot (n-1) \cdots (t+1) \binom{t}{\lfloor n/\alpha_1 \rfloor, \lfloor n/\alpha_2 \rfloor, \ldots, \lfloor n/\alpha_k \rfloor}. \tag{6.2}$$

Because of equation (6.1), we know that

$$\binom{t}{\lfloor n/\alpha_1 \rfloor, \lfloor n/\alpha_2 \rfloor, \ldots, \lfloor n/\alpha_k \rfloor} \leq \frac{t^t}{\lfloor n/\alpha_1 \rfloor^{\lfloor n/\alpha_1 \rfloor} \lfloor n/\alpha_2 \rfloor^{\lfloor n/\alpha_2 \rfloor} \cdots \lfloor n/\alpha_k \rfloor^{\lfloor n/\alpha_k \rfloor}}. \tag{6.3}$$

From equations (6.2) and (6.3) we deduce that

$$C(n,k) < \frac{n^n}{\lfloor n/\alpha_1 \rfloor^{\lfloor n/\alpha_1 \rfloor} \lfloor n/\alpha_2 \rfloor^{\lfloor n/\alpha_2 \rfloor} \cdots \lfloor n/\alpha_k \rfloor^{\lfloor n/\alpha_k \rfloor}}. \qquad \square$$

Lemma 6.6. *Let $k \geq 3$, $n \in \mathbb{N}$. If $\alpha_k \leq n$ then*

$$k < \lfloor \log_2 \lfloor \log_2 n \rfloor \rfloor + 2.$$

Proof. First observe by a simple induction that for all $k \geq 3$, $\alpha_k > 2^{2^{k-2}} + 1$ so that $k - 2 < \lfloor \log_2 (\lfloor \log_2 \alpha_k \rfloor) \rfloor \leq \lfloor \log_2 (\lfloor \log_2 n \rfloor) \rfloor$. $\square$

Lemma 6.7. *Let $k \geq 1$, $n \in \mathbb{N}$. If $\alpha_k \leq n$,*

$$C(n,k) < \frac{n^n \left(\frac{10\,n}{\alpha_1}\right)^{\frac{\alpha_1 - 1}{\alpha_1}} \left(\frac{10\,n}{\alpha_2}\right)^{\frac{\alpha_2 - 1}{\alpha_2}} \cdots \left(\frac{10\,n}{\alpha_k}\right)^{\frac{\alpha_k - 1}{\alpha_k}}}{\left(\frac{10\,n}{\alpha_1}\right)^{\frac{10\,n}{\alpha_1}} \left(\frac{10\,n}{\alpha_1}\right)^{\frac{10\,n}{\alpha_1}} \cdots \left(\frac{10\,n}{\alpha_k}\right)^{\frac{10\,n}{\alpha_k}}}.$$

Proof. The result is straightforward by combining Lemmas 6.4 and 6.5. $\square$

Lemma 6.8. *Let $w_k = \prod_{i=1}^{k} \alpha_i^{\frac{1}{\alpha_i}}$, $k \geq 1$. Then w_k is increasing and there exists $w \in \mathbb{R}$, with*

$$w < 2.98,$$

such that $w_k < w$.

Proof. The sequence w_k is increasing because $\alpha_i^{\frac{1}{\alpha_i}} > 1$ (because $\alpha_i > 1$). Since $\alpha_i^2 > \alpha_{i+1} > (\alpha_i - 1)^2$, one can see that for $i \geq 3$, $\alpha_{i+1}^{\frac{1}{\alpha_{i+1}}} < \sqrt{\alpha_i^{\frac{1}{\alpha_i}}}$, so that for all $k \geq 1$ and $l \geq 0$,

$$w_{k+l} \leq \prod_{i=1}^{k} \alpha_i^{\frac{1}{\alpha_i}} \cdot \alpha_{k+1}^{\frac{1}{\alpha_{k+1}} \sum_{i=0}^{l} \frac{1}{2^i}} \leq w_k \cdot \alpha_{k+1}^{\frac{2}{\alpha_{k+1}}}.$$

We establish by an elementary external computation verified in Coq that $\alpha_1^{\frac{1}{\alpha_1}} < \frac{283}{200}$, $\alpha_2^{\frac{1}{\alpha_2}} < \frac{1443}{1000}$, $\alpha_3^{\frac{1}{\alpha_3}} < \frac{1321}{1000}$, $\alpha_4^{\frac{1}{\alpha_4}} < \frac{273}{250}$ and $\alpha_5^{\frac{1}{\alpha_5}} < \frac{201}{200}$. From the bound above with $k = 4$ we get $w < w_4 \cdot \alpha_5^{\frac{2}{\alpha_5}} \leq \frac{5949909309448377}{2 \cdot 10^{15}} < 2.98$. □

Remark 6.9. For $k \geq 1$, we have

$$\frac{\alpha_1 - 1}{\alpha_1} + \frac{\alpha_2 - 1}{\alpha_2} + \cdots + \frac{\alpha_k - 1}{\alpha_k} = k - 1 + \frac{1}{\alpha_{k+1} - 1}.$$

Proof. It is a direct consequence of Lemma 6.2. □

Note that the statement of Remark 6.9 actually corrects a typo in the original paper.

Theorem 6.10. *If* $\alpha_k \leq n < \alpha_{k+1}$,

$$C(n, k) = C(n) < (10\, n)^{k - \frac{1}{2}} w^{n+1}.$$

Proof. From Lemma 6.7, recall that we have

$$\begin{aligned} C(n,k) &< \frac{n^n \left(\frac{10\, n}{\alpha_1}\right)^{\frac{\alpha_1 - 1}{\alpha_1}} \left(\frac{10\, n}{\alpha_2}\right)^{\frac{\alpha_2 - 1}{\alpha_2}} \cdots \left(\frac{10\, n}{\alpha_k}\right)^{\frac{\alpha_k - 1}{\alpha_k}}}{\left(\frac{n}{\alpha_1}\right)^{\frac{n}{\alpha_1}} \left(\frac{n}{\alpha_2}\right)^{\frac{n}{\alpha_2}} \cdots \left(\frac{n}{\alpha_k}\right)^{\frac{n}{\alpha_k}}} \\ &= \frac{n^n (10\, n)^{\left(\sum\limits_{i=1}^{k} \frac{\alpha_i - 1}{\alpha_i}\right)} \left(\prod_{i=1}^{k} \alpha_i^{\frac{1}{\alpha_i}}\right)^n}{n^{n \sum_{i=1}^{k} \frac{1}{\alpha_i}} \prod_{i=1}^{k} \alpha_i^{\frac{\alpha_i - 1}{\alpha_i}}}. \end{aligned}$$

It can be seen using Lemma 6.2 that:

$$n^{n\left(1 - \sum_{i=1}^{k} \frac{1}{\alpha_i}\right)} \leq n.$$

Thus

$$\begin{aligned} C(n,k) &< n \frac{(10\, n)^{k - 1 + \frac{1}{\alpha_{k+1} - 1}} w_k^n}{\prod_{i=1}^{k} \alpha_i^{\frac{\alpha_i - 1}{\alpha_i}}} \text{ (by Remark 6.9)} \\ &\leq n \frac{(10\, n)^{k - 1 + \frac{1}{\alpha_{k+1} - 1}} w^n}{\prod_{i=1}^{k} \alpha_i^{\frac{\alpha_i - 1}{\alpha_i}}} \text{ because } w_k \leq w. \end{aligned}$$

Since $n < \alpha_{k+1} = 1 + \prod_{i=1}^{k} \alpha_i$, $n \leq \prod_{i=1}^{k} \alpha_i$, and we have

$$\prod_{i=1}^{k} \alpha_i^{\frac{\alpha_i - 1}{\alpha_i}} = \frac{\prod\limits_{i=1}^{k} \alpha_i}{w_k} \geq \frac{n}{w_k}.$$

Thus

$$\begin{aligned} C(n,k) &< (10\,n)^{k-1+\frac{1}{\alpha_{k+1}-1}} w^n w_k \\ &\leq (10\,n)^{k-\frac{1}{2}} w^{n+1} \text{ as } \alpha_{k+1} \geq 3 \text{ and } w_k \leq w. \end{aligned}$$ □

We can now prove Lemma 3.1:

Proof. We have:

$$\ell_n/3^n \leq C(n,k)/3^n = (10\,n)^{k-\frac{1}{2}} \left(\frac{w}{3}\right)^{n+1}.$$

Remembering that $k < \lfloor \log_2 \lfloor \log_2 n \rfloor \rfloor + 2$ and $w < 3$, it is elementary to show that the quantity on the right is eventually decreasing to 0 and therefore bounded, which proves the result. We once again make use of the fact that $\left(1 + \frac{1}{x}\right)^x$ is bounded in the course of this elementary proof. □

7. Conclusion

We are not aware of a comprehensive, reference, formal proof library on the topic of number theory, in any guise. The most comprehensive work in this direction is probably the Isabelle/HOL library on analytic number theory contributed by Eberl [Ebe19b], which covers a substantial part of an introductory textbook by Apostol [Apo76]. This library is based on an extensive corpus in complex analysis initially formalized by Harrison in the HOL-Light prover, and later ported to the Isabelle/HOL prover by Paulson and Li. Formal proofs also exists of a few emblematic results. The elementary fact that $\sqrt{2}$ is irrational was used as an example problem in a comparative study of the styles of various theorem provers [Wie06], including Coq. The Prime Number theorem was proved formally for the first time by Avigad *et al.* [ADGR07], using the Isabelle/HOL prover and later by Harrison [Har09] with the HOL-Light prover. Shortly after the submission of the first version of the present paper, Eberl verified [Ebe19a] Beuker's proof of Apéry's theorem [Beu79], using the Isabelle/HOL prover, and relying on the Prime Number theorem to derive the asymptotic properties of ℓ_n. Bingham was the first to formalize a proof that e is transcendental [Bin11], with the HOL-Light prover. Later, Bernard *et al.* formally proved the transcendence of both π and e in Coq [BBRS15].

Some of the ingredients needed in the present proof are however not specific to number theory. For instance, we here use a very basic, but sufficient, infrastructure to represent asymptotic behaviors. But "big Oh", also called Bachman-Landau, notations have been discussed more extensively by Avigad *et al.* [ADGR07] in the context of their formal proof of the Prime Number Theorem, and by Boldo *et al.* [BCF+10], for the asymptotic behavior of real-valued continuous functions. Affeldt *et al.* designed a sophisticated infrastructure for equational reasoning in Coq with Bachman-Landau notation [ACR18], which relies on a non-constructive choice operator. Another example of such a secondary topic is the theory of multinomial coefficients, which is also relevant to combinatorics, and which is also defined by Hivert in his Coq library Coq-Combi [Hiv]. However, up to our knowledge this library does not feature a proof of the generalized Newton identity.

Harrison [Har15] presented a way to produce rigorous proofs from certificates produced by Wilf-Zeilberger certificates, by seeing sequences as limits of complex functions. His method applies to the sequence a, and can in principle prove that it satisfies the recurrence equation (3.2). However, this method does not allow for a proof that b satisfies the recurrence relation (3.2), because the summand is itself a sum but not a hypergeometric one. Up to our knowledge, there is no known way today to justify the output of the efficient algorithms of creative telescoping used here without handling a trace of provisos.

The idea to use computer algebra software (CAS) as an oracle outputting a certificate to be checked by a theorem prover, dubbed a *skeptic's* approach, was first introduced by Harrison and Théry [HT98]. It is based on the observation that CAS are very efficient albeit not always correct, while theorem provers are sound but slow. This technique thus takes the best of both worlds to produce reliable proofs requiring large scale computations. In the case of Coq, this viewpoint is especially fruitful since the kernel of the proof assistant includes efficient evaluation mechanisms for the functional programs written inside the logic [GL02]. Notable successes based on this idea include the use of Pocklington certificates to check primality inside Coq [GTW06] or external computations of commutative Gröbner bases, with applications for instance in geometry [Pot10]. Delahaye and Mayero proposed [DM05] to use CAS to help experimenting with algebraic expressions inside a proof assistant, before deciding what to prove and how to prove it. Unfortunately, their tool was not usable in our case, where algebraic expressions are made with operations that come from a hierarchy of structures.

Organizing the cooperation of a CAS and a proof assistant sheds light on their respective differences and drawbacks. The initial motivation of this work was to study the algorithms used for the automatic discovery and proof of recurrences. Our hope was to be able to craft an automated tool providing formal proofs of recurrences, by using the output of these algorithms, in a skeptical way. This plan did not work and Section 4 illustrates the impact of confusing the rational fractions manipulated by symbolic computations with their evaluations, which should be guarded by conditions on the denominators. On the other hand, proof assistants are not yet equipped to manipulate the large expressions imported during the cooperation, even those which are of a small to moderate size for the standards of computer algebra systems. For instance, we have highlighted in our previous report [CMSPT14] the necessity to combine two distinct natures of data-structures in our libraries: one devoted to formal proofs, which may use computation inside the logic to ease bureaucratic steps, and one devoted to larger scale computations, which provides a fine-grained control on the complexity of operations. The later was crucial for the computations involved in the normalization of ring expressions during the a posteriori verification of computer-algebra produced recurrences. But it was also instrumental in our proof of Lemma 5.6.

Incidentally, our initial formal proof of Lemma 6.8 also involved this nature of calculations, with rather larger numbers[1]. Indeed, the proof requires bounding the five first values of sequence α_n^{1/a_n} and the straightforward strategy involves intermediate computations with integers with about 4160 decimal digits. Following a suggestion by one of the anonymous referees, we now use a less naive formula to bound α_5. This dramatically reduces the size of the numbers involved, to the price of some additional manual bureaucracy in the proof script, mostly for evaluating binomial coefficients without an appropriate support at the level of libraries.

The Coq proof assistant is not equipped with a code generation feature akin to what is offered, for instance, in the Isabelle/HOL prover [HN18]. In principle, it is possible to plug in Isabelle/HOL formal developments the result of computations executed by external, generated programs that are verified down to machine code. In the present formal proofs,

[1]For the current standards of proof assistants.

computation are instead carried *inside* the logic, using the Calculus of Inductive constructions as a programming language. Such an approach is possible in Coq because its proof-checker includes an efficient mechanism for evaluating these functional programs [GL02]. Automating the correctness proofs of the program transformations required for the sake of efficiency is on-going research. In the present work, we have used the CoqEAL library [CDM13], which is itself based on a plugin for parametricity proofs [KL12]. The variant proposed by Tabareau *et al.* [TTS18] might eventually help improving the extensibility of the refinement framework, which is a key issue.

The interfaces of proof assistants are also notoriously less advanced than those of modern computer algebra. For instance, reasoning by transitivity on long chains of equalities/inequalities is often cumbersome in Coq, because of the limited support for selecting terms in an expression and for reasoning by transitivity. The Lean theorem prover [dMKA+15] features a `calc` environment for proofs on transitive relations which might be used as a first step in this direction.

On several occasions in this work, we wrote more elementary versions of the proofs than what we had found in the texts we were formalizing. We partly agree with Avigad *et al.* [ADGR07] when they write that this can be both frustrating and enjoyable: on one hand, it can illustrate the lack of mathematical libraries for theorems which mathematicians would find simple, such as elementary analysis for studying the asymptotics of sequences as in Section 5. Ten years later, "the need for elementary workarounds" is still present, despite his fear that it would "gradually fade, and with it, alas, one good reason for investing time in such exercises"[ADGR07]. On the other hand, this need gives an opportunity to better understand the minimal scope of mathematical theories used in a proof, with the help of a computer. For instance, it was not clear to us at first that we could manage to completely avoid the need to define transcendental functions, or to avoid defining the constant e, base of the natural logarithm, to formalize Hanson's paper [Han72]. This minimality however comes at the price of arguably more pedestrian calculations.

Acknowledgment

We wish to thank the anonymous reviewers, Alin Bostan, Frédéric Chyzak, Georges Gonthier, Marc Mezzarobba, and Bruno Salvy for their comments and suggestions. We also thank Cyril Cohen, Pierre Roux and Enrico Tassi for their help, in particular with the libraries this work depends on.

References

[ACR18] Reynald Affeldt, Cyril Cohen, and Damien Rouhling. Formalization techniques for asymptotic reasoning in classical analysis. *J. Formalized Reasoning*, 11(1):43–76, 2018.

[ADGR07] Jeremy Avigad, Kevin Donnelly, David Gray, and Paul Raff. A formally verified proof of the prime number theorem. *ACM Trans. Comput. Logic*, 9(1), December 2007.

[alg13] Algolib. `http://algo.inria.fr/libraries/`, 2013. Version 17.0. For Maple 17.

[Apé79] Roger Apéry. Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque*, 61, 1979. Société Mathématique de France.

[Apo76] Tom M. Apostol. *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics. Springer, 1976.

[BBRS15] Sophie Bernard, Yves Bertot, Laurence Rideau, and Pierre-Yves Strub. Formal proofs of transcendence for e and π as an application of multivariate and symmetric polynomials. *CoRR*, abs/1512.02791, 2015.

[BCF+10] Sylvie Boldo, François Clément, Jean-Christophe Filliâtre, Micaela Mayero, Guillaume Melquiond, and Pierre Weis. Formal proof of a wave equation resolution scheme: the method error. *CoRR*, abs/1005.0824, 2010.

[BCP03] Gilles Barthe, Venanzio Capretta, and Olivier Pons. Setoids in type theory. *J. Funct. Program.*, 13(2):261–293, 2003.

[Bes07] Frédéric Besson. Fast reflexive arithmetic tactics the linear case and beyond. In *TYPES'06*, LNCS, pages 48–62, Berlin, Heidelberg, 2007. Springer-Verlag.

[Beu79] F. Beukers. A note on the irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.*, 11(3):268–272, 1979.

[Bin11] Jesse Bingham. Formalizing a proof that e is transcendental. *Journal of Formalized Reasoning*, 4(1):71–84, 2011.

[BR01] Keith Ball and Tanguy Rivoal. Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs. *Invent. Math.*, 146(1):193–207, 2001.

[CDM13] Cyril Cohen, Maxime Dénès, and Anders Mörtberg. Refinements for Free! In *Certified Programs and Proofs*, pages 147 – 162, Melbourne, Australia, December 2013.

[CMSPT14] Frédéric Chyzak, Assia Mahboubi, Thomas Sibut-Pinote, and Enrico Tassi. A Computer-Algebra-Based Formal Proof of the Irrationality of $\zeta(3)$. In *ITP - 5th International Conference on Interactive Theorem Proving*, Vienna, Austria, 2014.

[Coh12] Cyril Cohen. Construction of real algebraic numbers in Coq. In *ITP*, volume 7406 of *LNCS*. Springer, August 2012.

[coq19] Mathematical Components Libraries. `http://math-comp.github.io/math-comp/`, 2019.

[DM05] David Delahaye and Micaela Mayero. Dealing with algebraic expressions over a field in Coq using Maple. *J. Symb. Comput.*, 39(5):569–592, May 2005.

[dMKA+15] Leonardo de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer. *The Lean Theorem Prover (System Description)*, pages 378–388. Springer International Publishing, Cham, 2015.

[Ebe19a] Manuel Eberl. The irrationality of $\zeta(3)$. *Archive of Formal Proofs*, December 2019. `http://isa-afp.org/entries/Zeta_3_Irrational.html`, Formal proof development.

[Ebe19b] Manuel Eberl. Nine chapters of analytic number theory in isabelle/hol. In John Harrison, John O'Leary, and Andrew Tolmach, editors, *10th International Conference on Interactive Theorem Proving, ITP 2019, September 9-12, 2019, Portland, OR, USA*, volume 141 of *LIPIcs*, pages 16:1–16:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[Fen05] Bei-ye Feng. A simple elementary proof for the inequality $d_n < 3^n$. *Acta Math. Appl. Sin. Engl. Ser.*, 21(3):455–458, 2005.

[Fis04] Stéphane Fischler. Irrationalité de valeurs de zêta (d'après Apéry, Rivoal, ...). In *Séminaire Bourbaki. Volume 2002/2003. Exposés 909–923*, pages 27–62, ex. Paris: Société Mathématique de France, 2004.

[FSZ19] Stéphane Fischler, Johannes Sprang, and Wadim Zudilin. Many odd zeta values are irrational. *Compositio Mathematica*, 155(5):938–952, 2019.

[GAA+13] Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O'Connor, Sidi Ould Biha, Ioana Pasca, Laurence Rideau, Alexey Solovyev, Enrico Tassi, and Laurent Théry. A Machine-Checked Proof of the Odd Order Theorem. In Sandrine Blazy, Christine Paulin, and David Pichardie, editors, *ITP 2013, 4th Conference on Interactive Theorem Proving*, volume 7998 of *LNCS*, pages 163–179, Rennes, France, July 2013. Springer.

[GGMR09] François Garillot, Georges Gonthier, Assia Mahboubi, and Laurence Rideau. Packaging Mathematical Structures. working paper or preprint, March 2009.

[GL02] Benjamin Grégoire and Xavier Leroy. A compiled implementation of strong reduction. In *Proceedings of the Seventh ACM SIGPLAN International Conference on Functional Programming*, ICFP '02, pages 235–246, New York, NY, USA, 2002. ACM.

[GM05] Benjamin Grégoire and Assia Mahboubi. Proving equalities in a commutative ring done right in Coq. In *TPHOLs 2005*, volume 3603 of *LNCS*, pages 98–113, Oxford, United Kingdom, August 2005. Springer.

[GTW06] Benjamin Grégoire, Laurent Théry, and Benjamin Werner. *A Computational Approach to Pocklington Certificates in Type Theory*, pages 97–113. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[Han72] Denis Hanson. On the product of the primes. *Canad. Math. Bull.*, 15:33–37, 1972.

[Har09] John Harrison. Formalizing an analytic proof of the Prime Number Theorem. *Journal of Automated Reasoning*, 43:243–261, 2009.

[Har15] John Harrison. Formal proofs of hypergeometric sums (dedicated to the memory of andrzej trybulec). *Journal of Automated Reasoning*, 55:223–243, 2015.

[Hed98] Michael Hedberg. A coherence theorem for Martin-Löf's type theory. *Journal of Functional Programming*, 8(4):413–436, July 1998.

[Hiv] Florent Hivert. Coq-combi. `https://github.com/hivert/Coq-Combi`.

[HN18] Lars Hupel and Tobias Nipkow. A verified compiler from isabelle/hol to cakeml. In Amal Ahmed, editor, *Programming Languages and Systems - 27th European Symposium on Programming, ESOP 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings*, volume 10801 of *Lecture Notes in Computer Science*, pages 999–1026. Springer, 2018.

[HT98] John Harrison and L. Théry. A skeptic's approach to combining HOL and Maple. *J. Automat. Reason.*, 21(3):279–294, 1998.

[KL12] Chantal Keller and Marc Lasson. Parametricity in an impredicative sort. In Patrick Cégielski and Arnaud Durand, editors, *Computer Science Logic (CSL'12) - 26th International Workshop/21st Annual Conference of the EACSL, CSL 2012, September 3-6, 2012, Fontainebleau, France*, volume 16 of *LIPIcs*, pages 381–395. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2012.

[MT13] Assia Mahboubi and Enrico Tassi. Canonical Structures for the working Coq user. In Sandrine Blazy, Christine Paulin, and David Pichardie, editors, *ITP 2013, 4th Conference on Interactive Theorem Proving*, volume 7998 of *LNCS*, pages 19–34, Rennes, France, July 2013. Springer.

[Pot10] Loïc Pottier. Connecting Gröbner Bases Programs with Coq to do Proofs in Algebra, Geometry and Arithmetics. *CoRR*, abs/1007.3615, 2010.

[Riv00] Tanguy Rivoal. La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs. *C. R. Acad. Sci. Paris Sér. I Math.*, 331(4):267–270, 2000.

[Sal03] Bruno Salvy. An Algolib-aided version of Apéry's proof of the irrationality of $\zeta(3)$. `http://algo.inria.fr/libraries/autocomb/Apery2-html/apery.html`, 2003.

[Soz09] Matthieu Sozeau. A new look at generalized rewriting in type theory. *J. Formalized Reasoning*, 2(1):41–62, 2009.

[The20] The Coq Development Team. The Coq Proof Assistant, version 8.11.0, January 2020.

[TTS18] Nicolas Tabareau, Éric Tanter, and Matthieu Sozeau. Equivalences for free: univalent parametricity for effective transport. *PACMPL*, 2(ICFP):92:1–92:29, 2018.

[vdP79] Alfred van der Poorten. A proof that Euler missed: Apéry's proof of the irrationality of $\zeta(3)$. *Math. Intelligencer*, 1(4):195–203, 1979. An informal report.

[Wie06] Freek Wiedijk. *The Seventeen Provers of the World: Foreword by Dana S. Scott (Lecture Notes in Computer Science / Lecture Notes in Artificial Intelligence)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[Zei90] Doron Zeilberger. A holonomic systems approach to special functions identities. *J. Comput. Appl. Math.*, 32(3):321–368, 1990.

[Zei91] Doron Zeilberger. The method of creative telescoping. *J. Symbolic Comput.*, 11(3):195–204, 1991.

[Zud01] V. V. Zudilin. One of the numbers $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ is irrational. *Uspekhi Mat. Nauk*, 56(4(340)):149–150, 2001.