From Weierstraß to Dedekind via Jacobi: Formalising Foundations of Modular Forms

Manuel Eberl
University of Innsbruck, Austria

Wenda Li
University of Edinburgh, United Kingdom

Lawrence C. Paulson
University of Cambridge, United Kingdom

Abstract

We present an Isabelle/HOL formalisation of the foundations of analytic number theory related to modular forms. We begin by refactoring and extending the existing library on elliptic functions, adding the theorem that every elliptic function can be written in terms of the Weierstraß elliptic function $\wp$ and the addition theorem for $\wp$, which links complex lattices to elliptic curves. Next, we develop an extensive library on the Jacobi theta functions, including well-known results such as the Jacobi triple product, the Pentagonal Number Theorem, and the Rogers–Ramanujan identities. Finally, we apply this library to the study of the Dedekind η function and 'forbidden' Eisenstein series G_2. In all of this, we aim for short and clean proofs, building a library of reusable lemmas.

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Isabelle/HOL, elliptic functions, Eisenstein series, modular forms, theta functions, number theory, complex analysis, formalisation of mathematics

Digital Object Identifier 10.4230/LIPIcs.ITP.2026.23

Supplementary Material *Other*: `10.5281/zenodo.20359735`

Acknowledgements We would like to thank Alexey Ustinov for explaining how to prove an auxiliary lemma required for deriving the inversion formula for η from that for ϑ_{xy}, and George Andrews for clarifying an issue related to uniform convergence in the context of the Rogers–Ramanujan identities. Our thanks also go to Kristina Magnussen, who commented on a draft of this article, and to the anonymous reviewers.

1 Introduction

Modular forms are integral to modern number theory: for one, they play a key role in Wiles's celebrated proof of Fermat's Last Theorem. While we did not formalise the concept of modular forms themselves, we have created solid foundations for such work by formalising a mature library of closely related concepts: elliptic functions, Eisenstein series, Jacobi theta functions, and Dedekind's η function. These are, among other things, important building blocks to construct modular forms.

This article has three goals: first, to show how to do complex analysis in Isabelle/HOL elegantly; second, to demonstrate the most painless way (that we are aware of) to obtain the results we present, which may help others developing similar libraries in other systems; third, to highlight technical obstacles that we encountered and how we resolved them.

We aim for short proofs and attempt to tackle each big theorem modularly by developing a stack of reusable material of general interest, rather than by attacking the problem head-on with a large monolithic proof. As a striking example of the success of this approach, we were able to cut a 1,300-line proof (following Siegel [27]) that consisted mostly of computations and contour integrals with no reuse value down to a mere 90 lines.

Of course, this reduction does not come for free: the new proof builds on thousands of lines of new library material on the q-Pochhammer symbol and Jacobi theta functions. The difference, however, is that the new proof is short and readable, and those thousands of lines of new material are not specific to this one proof but 'general purpose'. In fact, we *first* built the theta function library and then noticed that it could be used to replace Siegel's proof.

Most of the material discussed is spread over two entries in the *Archive of Formal Proofs*: one on complex lattices and elliptic functions [19] and one on theta functions [17]. Some of the material is also found in other, smaller entries, which we will reference in the places where the material in them is discussed.

1.1 Related Work

The mathematics involved in our topic is advanced and few systems even have the necessary prerequisites (most importantly a library on complex analysis). There are only three such systems that we are aware of: HOL Light was the first [22, 23], with a formalisation of the Prime Number Theorem. Isabelle/HOL had its complex analysis library ported from HOL Light by Paulson and extended significantly by Li and Eberl [29]. As of recently, Lean's Mathlib also contains significant complex analysis [30].

Earlier work by us (namely by Eberl [10] in 2019 and Eberl et al. [20] in 2024) included a formalisation of a substantial amount of analytic number theory in Isabelle/HOL. The latter publication (a short paper describing work in progress) follows Apostol's textbook [3] and covers an extensive list of topics: elliptic functions, Eisenstein series, modular forms and their valence formula, Klein's j invariant, and Dedekind's η function. This article has a narrower focus: we refactor the material on elliptic functions and η, and in the process develop an extensive and mature library on the Jacobi theta function. We are planning to eventually refactor the remaining material as well and integrate it with the one presented here.

We would like to stress that the work presented here also contains much material that was not present in the earlier formalisation. The most notable examples are: everything on the Jacobi theta functions and the forbidden Eisenstein series G_2, the Pentagonal Number Theorem, the Rogers–Ramanujan identities, the fact that all elliptic functions can be written in terms of the Weierstraß $\wp$ function, and the addition theorem for $\wp$.

There is also related formalisation work in Lean, but most of it is not published. We are aware of unpublished work by Birkbeck [7], formalising results on Eisenstein series and modular forms. There is also an article by Loeffler and Stoll [26] focusing on L-functions and in the process also defining the Jacobi theta function. The development is much less comprehensive than ours, but it does include the Jacobi Inversion Formula, which is a notable non-trivial result. The Lean formalisation uses Poisson summation to derive this formula, whereas we use contour integration. This plays to each system's strengths: Isabelle does not have a library of Poisson summation and Fourier analysis, whereas Lean's Mathlib only has rudimentary support for contour integration so far.

1.2 Notation

In this article, τ will always refer to a parameter in the complex upper half plane (i.e. $\mathrm{Im}(\tau) > 0$). The variable z will be an arbitrary complex number. The variables q and w will often denote 'q-parameters' of the form $q = \exp(i\pi\tau)$ or sometimes $q = \exp(2i\pi\tau)$.

The multiplicity of zeros and poles is always taken into account: when we say that the number of poles of a function is 2 then it either has two simple poles or one double pole. Sums over poles and/or zeros are implicitly weighted with their *signed* multiplicity (cf. Section 2.4).

For a complex number z, the square root $\sqrt{z}$ will always denote the principal branch, where $\text{Arg}(\sqrt{z}) \in (-\frac{\pi}{2}, \frac{\pi}{2}]$ (which is also the convention used in Isabelle's `csqrt` operator).

The material presented in this article is dense and we do not have the space to explain it in detail, so we will only show the most interesting results in sufficient detail to be understandable, using standard mathematical notation for the most part. Isabelle notation is only shown when it adds something to the presentation.

2 Preliminary Material

During our work, we frequently found that Isabelle's complex analysis library had gaps or was difficult to use, e.g. certain simple things were hard to express. In this section, we talk about how we extended or modified the library to capture particular notions from complex analysis idiomatically. All these changes are now distributed with `Isabelle-2025-2`.

2.1 Analyticity, Meromorphicity, Formal Power Series

If a complex function $f(z)$ is differentiable on an open set A, it is in fact *analytic* at every point $z_0 \in A$, i.e. it can be expanded into a power series $f(z) = \sum_{n\geq 0} a_n(z - z_0)^n$ within some non-empty disc around z_0. Thus, the notions of holomorphicity and analyticity coincide.

The Isabelle/HOL definitions *f holomorphic_on A* and *f analytic_on A* were inherited from HOL Light. On open sets, they coincide. On a non-open set, however, *holomorphic_on* only requires f to be differentiable *within* A at every point in A, whereas *analytic_on* requires it to be differentiable on some open superset of A, or, equivalently, that f can be locally expanded into a power series at every point in A. It is worth noting that in mathematics, the term 'holomorphic function' is usually only used when the domain is open, making the Isabelle/HOL notion somewhat nonstandard when applied to non-open domains.

Isabelle/HOL has had a decent library for *formal* power series for a long time [8], and it was easy to connect these formal series to complex functions via a predicate *has_fps_expansion*:

$$f \text{ has\_fps\_expansion } F \longleftrightarrow$$
$$\text{fps\_conv\_radius } F > 0 \wedge \text{eventually } (\lambda z.\ \text{eval\_fps } F\ z = f\ z)\ (\text{nhds } 0)$$

The functions *eventually* and *nhds* are taken from Isabelle's filter library [24].

Proving that a particular function has a particular FPS expansion is usually mostly automatic using the extensible set of introduction rules *fps_expansion_intros*.

One advantage of the behaviour of *analytic_on* on non-open sets is that one can write e.g. *f analytic_on* $\{z\}$ to mean that f is holomorphic in some open neighbourhood of z. It also holds that f is analytic on a set A iff f is analytic at every point in A. We use this frequently as a convenient way to prove analyticity of functions defined by limits or series.

The notion of *meromorphicity* is weaker: it does not require f to be differentiable at *every* point in A, but f may also have *non-essential singularities* (i.e. poles or removable singularities), as long as the singularities have no accumulation point. Meromorphic functions are exactly those functions that can be written as the quotient of two holomorphic functions. Functions meromorphic on some open set A are alternatively classified as those functions that can be locally expanded into a Laurent series $f(z) = \sum_{n\geq n_0} a_n(z - z_0)^n$ around any $z_0 \in A$ (where n_0 may be negative).

It was initially unclear how to best formalise meromorphicity in the most easy-to-use way in Isabelle/HOL. In the end, the most elegant definition turned out to be the one using the

Laurent series classification:

$$f \text{ meromorphic\_on } A \longleftrightarrow (\forall z{\in}A.\ \exists F.\ (\lambda w.\ f\ (z+w)) \text{ has\_laurent\_expansion } F)$$

where the predicate *has_laurent_expansion* connects a complex function to the formal Laurent series library by Sylvestre [28], analogously to *has_fps_expansion*.

The connection to Laurent series is tremendously useful. It allowed us to simplify many concepts that were originally defined awkwardly in the library, such as residues or *zorder* (the signed multiplicity of a pole or zero). It also makes it easier to study the behaviour of a concrete function at a given point, e.g. computing residues or proving that it has a zero or pole of a certain multiplicity. A further advantage is that 'our' meromorphicity naturally behaves analogously to *analytic_on* when applied to a non-open set: in this case, it is equivalent to saying that there is an open superset on which the function is meromorphic.

2.2 Removable Singularities

Another complication, however, is that of removable singularities. If we let $f(z) = g(z) = z$, the quotient of f and g is the constant function $h(z) = 1$. But in fact $f(z)/g(z)$ has a singularity at $z = 0$, and we only get equality to h if we recognise that this is a *removable singularity* and remove it. Doing this in a theorem prover is not automatic and takes work. In the total logic of Isabelle/HOL, $0/0$ is defined as 0, so f/g is *not* in fact equal to h.

We introduced some tools to solve this problem. First, we introduced the notion of a 'nicely meromorphic function', which is a function that is meromorphic, has no removable singularities, and returns 0 at its poles (as an arbitrary convention). Second, we defined the *remove_sings* operator, which takes a function and returns a version of that function with all removable singularities removed and all poles mapped to 0. Of course, this does not *eliminate* the need to reason about removable singularities: we still sometimes have two versions of the same theorem, a nice one for nicely meromorphic functions and an uglier one for the rest. However, these tools made the issue much easier to handle.

Lastly, we introduced the notion of *sparseness*: a set of points X is sparse in another set A if every point in A has an open neighbourhood that contains no limit points of X:

$$\text{X sparse\_in A} \longleftrightarrow (\forall x{\in}A.\ \exists B.\ x \in B \wedge \text{open } B \wedge (\forall y{\in}B.\ \neg y \text{ islimpt } X))$$

In the case where A itself is open, this simply means that all limit points of X lie outside A.

We then noticed that for any given A, the set of sets whose *complements* are sparse in A form a filter, which we call the *cosparseness* filter relative to A. This allows us to use the extensive filter library and write e.g. *eventually* P (*cosparse* A) to say that a property P holds on a set A except for some points that have no accumulation point in A. The connection to the above notion of removable singularities is immediately apparent.

We use this notion sufficiently often that we introduced the notation $\forall_{\approx} x{\in}A.\ P\ x$ for it (and we omit the $\in A$ part when $A = UNIV$). We often use this to state that two functions are equal up to removable singularities by writing $\forall_{\approx} z.\ f(z) = g(z)$.

2.3 Zeros

Another surprisingly tricky notion is that of a *zero*. On the face of it, a zero of a function f is simply a point z_0 where $f(z_0) = 0$, and the multiplicity of the zero is the least number n such that $(z - z_0)^{-n} f(z)$ tends to a non-zero value for $z \to z_0$. However, if f is the constant zero function (or, more generally, identically zero in a neighbourhood of z_0), the multiplicity

of the zero is not well-defined. Many theorems break down in this special case. Removable singularities complicate things even further: if f has a removable singularity at z_0, then it is possible for f to 'morally' have a zero at z_0 but still $f(z_0) \neq 0$, or the other way round.

We introduced the following definition in order to capture the notion of a zero robustly even in the presence of removable singularities and to exclude the case of 'identically zero':

isolated_zero $f\ z \longleftrightarrow f \mathrel{-z\to} 0 \wedge$ eventually $(\lambda x.\ f\ x \neq 0)$ (at z)

2.4 Multiplicity of Zeros and Poles

Zeros and poles of meromorphic functions have a *multiplicity*. To make the treatment more uniform, these two concepts are unified into the signed multiplicity *zorder* $f\ z$ in Isabelle, which is defined as the unique integer n such that $\lim_{z\to z_0}(z-z_0)^{-n} f(z) \neq 0$.

For zeros, this gives us the multiplicity of the zero; for poles, it gives us minus the multiplicity; otherwise it gives us 0. An equivalent definition is that *zorder* $f\ z$ is the *subdegree* (the exponent of the leading term) of the Laurent series expansion of f at z. This is usually the most convenient view when proving things about *zorder* or establishing that a particular function has a particular *zorder* at some point.

One complication is again that *zorder* is ill-defined for functions that are locally identically zero. Even if one were to define it to be, say ∞, in such cases, the resulting definition would not obey many of its usual laws. This means that when working with *zorder*, one often needs to prove tedious side conditions about things not being identically zero.

However, for meromorphic functions, local zeroness is equivalent to the function being identically zero on its entire domain if the domain is connected (which it often is). Especially in contexts where the domain is fixed (e.g. modular forms or elliptic functions) one can set up a proof context (e.g. using Isabelle's *locale* system [4]) to easily show that a given function is not locally zero by showing that it has a pole or a non-zero value somewhere.

Orthogonally to this, we suspect that some of our proofs where we manipulate sums over zeros and poles could benefit from having a *multiset* of zeros (and similarly for poles), or a *free abelian group* of both, rather than explicitly dealing with multiplicities.

2.5 Auxiliary Libraries

Beyond these improvements to the complex analysis library, our work relies heavily on several specialised auxiliary libraries that we developed.

- a library on Lambert series, i.e. series of the form $\sum_{n\geq 1} a_n\, q^n/(1-q^n)$ [13]
- a formalisation of the polylogarithm function $\mathrm{Li}_s(z) = \sum_{k\geq 1} k^{-s} z^k$ [14]
- a proof of the partial fraction decomposition of the cotangent function using Herglotz's trick: $\pi \cot(\pi z) = z^{-1} + \sum_{n\geq 1}[(z+n)^{-1} + (z-n)^{-1}]$ [12]
- a library on q-analogues of various combinatorial symbols, most importantly the infinite q-Pochhammer symbol $(a;q)_\infty = \prod_{k\geq 0}(1-aq^k)$, the Euler function $\varphi(q) = \prod_{k\geq 1}(1-q^k)$, and two q-series representations for $(a;q)_\infty$ due to Euler [15]
- a library on Dedekind sums, including their reciprocity law and efficient computation [21]

Some of these were developed specifically for this project, some of them independently.

With these foundations in place, let us now move on to our first main formalisation goal.

3 Complex Lattices and Elliptic Functions

In this first section, we will take a look at elliptic functions. These are particular meromorphic functions related to *lattices* in the complex plane. We first define what a lattice is.

▶ **Definition 1** (Complex lattice). *A complex lattice is the $\mathbb{Z}$-span of two complex numbers ω_1, ω_2 (the generators) which must not be $\mathbb{R}$-multiples of one another.*

Since ω_1, ω_2 are $\mathbb{R}$-linearly independent, any $z \in \mathbb{C}$ can be written in the form $z = a\omega_1 + b\omega_2$. We refer to a, b as the ω_1 and ω_2 coordinates of z. We have $z \in \Lambda \leftrightarrow a, b \in \mathbb{Z}$.

The lattice induces an equivalence relation $z_1 \sim_\Lambda z_2 \longleftrightarrow (z_1 - z_2) \in \Lambda$, i.e. we identify any two complex numbers that differ by a lattice point.

Given some $z \in \mathbb{C}$, the parallelogram with corners $z, z + \omega_1, z + \omega_2, z + \omega_1 + \omega_2$ is called the period parallelogram *at z. To achieve a perfect tiling of the complex plane by period parallelograms, we only consider the two edges $[z, z + \omega_1)$ and $[z, z + \omega_2)$ to belong to the parallelogram by convention. The parallelogram at $z = 0$ is called the* fundamental parallelogram *and holds the canonical representatives for every point in $\mathbb{C}$.*

Two lattices Λ_1, Λ_2 are said to be homothetic *if there exists an $\alpha \in \mathbb{C} \setminus \{0\}$ such that $\Lambda_1 = \alpha\Lambda_2$, i.e. if one can be transformed into the other by rotation and scaling. By applying homothetic transformations and possibly swapping the generators, any lattice can be transformed into one with the generators 1 and τ with $\operatorname{Im}(\tau) > 0$. This is the standard form of the lattice, which simplifies things since we only have one parameter instead of two.*

Given a complex lattice Λ, elliptic functions are now simply 'nice' functions $\mathbb{C}/\Lambda \to \mathbb{C}$, where $\mathbb{C}/\Lambda$ denotes the equivalence classes of our relation $\sim_\Lambda$. Geometrically, $\mathbb{C}/\Lambda$ is a *complex torus*, i.e. a parallelogram where each pair of opposite sides has been glued together. However, a more convenient view in Isabelle/HOL (also assumed in Apostol's book [3]) is to *not* make the quotient explicit but rather talk about lattice-periodic functions.

▶ **Definition 2** (Elliptic function). *Given a complex lattice Λ, an* elliptic function *is a meromorphic function f that is periodic w.r.t. the lattice, i.e. $z_1 \sim_\Lambda z_2 \Longrightarrow f(z_1) = f(z_2)$.*

In Isabelle, we capture this notion in a locale called *elliptic_function*. For convenience, we also introduce a locale called *nicely_elliptic_function* that additionally requires nice meromorphicity. This makes some results less awkward to state. Any non-nicely elliptic function can easily be converted to a nicely elliptic function using our *remove_sings* operator.

Various closure properties are immediately apparent: any constant function is elliptic, and usual operators that preserve meromorphicity also preserve ellipticity (in particular all the standard arithmetic operations and the derivative). In Isabelle, we collect these rules in a dynamic theorem collection called *elliptic_function_intros*, which makes it easy to prove that a particular composite function is elliptic when its components are elliptic.

Next, we define the following important characteristic of an elliptic function:

▶ **Definition 3.** *The order of an elliptic function is the number of its poles in any period parallelogram.*

Since the closure of a period parallelogram is compact, the order is always finite. For a nicely elliptic function, it is moreover easy to see that the order is 0 iff it is constant (due to Liouville's theorem). For a non-nicely elliptic function, this is not true due to the possibility of removable singularities. In this case, the order is 0 iff the function is constant except for a *sparse* set of points (cf. Section 2.2).

The first non-trivial thing we now prove is an alternative view on the order using zeros instead of poles. The proof is conceptually simple but must address a common problem in complex-analytical proofs that is often handwaved in informal presentations (e.g. Apostol [3] completely ignores it), namely the possible presence of singularities on the integration contour.

▶ **Theorem 4.** *The number of zeros of an elliptic function $f \neq 0$ (i.e. not identically zero) in any period parallelogram is equal to its order.*

Proof. Assume for now that the border of the period parallelogram has no zeros or poles on it. The number of zeros minus the number of poles is then given by the *Argument Principle*, i.e. it is equal to $\frac{1}{2i\pi}\oint f'(w)/f(w)\,\mathrm{d}w$, where the integration proceeds counter-clockwise along the border of the parallelogram. Due to the periodicity of f, the integrals along opposite sides of the parallelogram cancel and we get 0.

It remains to get rid of the assumption that there are no zeros or poles on the border of the parallelogram. Due to the periodicity of f, it is enough to find one such parallelogram. Since the number of zeros and poles is countable, the number of coordinates a, b that can appear as the ω_1 or ω_2 coordinate of a zero or pole is countable. So there are uncountably many a, b left such that $a\omega_1 + y\omega_2$ and $x\omega_1 + b\omega_2$ are not a zero or pole for any $x, y \in \mathbb{R}$. We simply pick a parallelogram whose top-left corner is any such $a\omega_1 + b\omega_2$.[1] ◀

Some related facts can be proven similarly:

▶ **Theorem 5.** *Let f be an elliptic function.*

1. *If $f \neq 0$, its zeros and poles in a period parallelogram sum to a lattice point.*
2. *The residues of f in a period parallelogram sum to 0.*

Caution: Recall that, by convention, zeros and poles are weighted by their multiplicity here.

Proof. Analogous to Theorem 4, using the Argument Principle with weight $h(w) = w$ (i.e. $\oint f'(w)/f(w)w\,\mathrm{d}w$) and the Residue Theorem, respectively. ◀

▶ **Corollary 6.** *There is no elliptic function of order 1.*

Proof. If an elliptic function had order 1, it would have one simple zero z_1 and one simple pole z_2. However, we then also know that $z_1 - z_2$ is a lattice point, i.e. $z_1 \sim_\Lambda z_2$. But this is impossible, since z_1 would then have to be both a zero and a pole. ◀

▶ **Corollary 7.** *Every non-constant elliptic function of positive order is surjective.*

Proof. If $f(z)$ is an elliptic function of order $m > 0$ then for any $c \in \mathbb{C}$, the function $g(z) = f(z) - c$ is also an elliptic function of order m (since the number of poles does not change). Thus g has $m \geq 1$ zeros in every period parallelogram. ◀

So far, we have not seen a single non-constant elliptic function. We will therefore now look at the prototypical example: the *Weierstraß elliptic function*.

3.1 The Weierstraß $\wp$ Function

▶ **Definition 8.** *The Weierstraß elliptic function and its derivative are defined as follows:*

$$\wp(z) = z^{-2} + \sum\nolimits_{\omega\in\Lambda\setminus\{0\}} \left[(z-\omega)^{-2} - \omega^{-2}\right] \qquad \wp'(z) = -2\sum\nolimits_{\omega\in\Lambda}(z-\omega)^{-3}$$

It takes some tedious but straightforward work (following Apostol) to show that these two sums converge uniformly on compact subsets of $\mathbb{C}\setminus\Lambda$ and that $\wp'$ is indeed the derivative of $\wp$. It is then easy to see that $\wp'$ is elliptic with a triple pole at every lattice point (and therefore order 3). It follows that $\wp$ has a double pole at every lattice point and order 2, since $\wp'$ is its derivative. It is also obvious that $\wp'$ is an odd function and $\wp$ is an even function.

[1] In Isabelle, we prove a more generic 'wlog' rule that allows us to prove a property involving a period parallelogram while assuming that no points from some fixed set A lie on the border. The preconditions are that A is sparse and that the property is stable under translation. We reuse this rule several times.

Lattice periodicity together with the oddness of $\wp'$ implies that $\wp'(\omega/2) = 0$ for any $\omega \in \Lambda$, i.e. every half-lattice point is a zero of $\wp'$. Since there are three half-lattice points in every period parallelogram (namely the analogues of $\omega_1/2$, $\omega_2/2$, and $(\omega_1 + \omega_2)/2$) and $\wp'$ has order 3, these are the only zeros of $\wp'$ and they must be simple zeros.

We can also derive the following 'quasi-injectivity' result for $\wp$:

▶ **Theorem 9** (Quasi-injectivity of $\wp$). $\wp(z_1) = \wp(z_2) \longleftrightarrow z_1 \sim_\Lambda \pm z_2$

Proof. We split the fundamental parallelogram into two halves that are images of one another under negation (we omit the slightly messy details). For every $c \in \mathbb{C}$, the function $f(z) = \wp(z) - c$ has exactly one zero in each half and is therefore injective on each half. The result follows. This takes about 120 lines, not counting library facts about even elliptic functions and 'half-parallelograms'. ◀

Lastly, we show that $\wp$ really is the *prototypical* elliptic function: all others can be constructed from it. Our proof follows Lang [25].

▶ **Proposition 10.** *Every even elliptic function can be written as a rational function of $\wp(z)$.*

Proof. For any $w \in \mathbb{C}$ define $g_w(z) = \wp(z) - \wp(w)$. Then g_w is elliptic with order two. If $2w \notin \Lambda$, the two (simple) zeros of g_w must be $\pm w$. If $2w \in \Lambda$, we have $g_w(w) = 0$ and $g_w'(w) = \wp'(w) = 0$, i.e. a double zero at w.

Now let $f(z)$ be elliptic and even and Z the set of its zeros and poles in a 'half parallelogram' minus any lattice points. For any $w \in Z$ let a_w be the signed multiplicity of the zero or pole w (i.e. *zorder f w*), unless $2w \in \Lambda$, in which case let it be half that (this is possible; the multiplicity must be even since f is even).

Now define $h(z) = \prod_{w \in Z} g_w(z)^{a_w}$. Then $f(z)/h(z)$ has no poles or zeros except possibly at the lattice points. If it had a zero there, it would have to have a pole elsewhere (which it does not), and vice versa. Therefore it has neither and must be constant. ◀

▶ **Theorem 11.** *Every elliptic function $f(z)$ can be written in the form $f(z) = g(\wp(z)) + \wp'(z)h(\wp(z))$, where g and h are rational functions.*

Proof. It is easy to see that $\frac{1}{2}(f(z) + f(-z))$ and $\frac{1}{2}(f(z) - f(-z))/\wp'(z)$ are even elliptic functions and can therefore be written as rational combinations of $\wp(z)$. ◀

4 Eisenstein Series

The Eisenstein series G_k are a sequence of numbers attached to a lattice. They are modular forms that are closely connected to elliptic functions. They are given by infinite sums similar to the ones we saw for $\wp$ and $\wp'$, and they are related to the coefficients of the Laurent series expansion of the $\wp$ function.

▶ **Definition 12** (Eisenstein series). *For a lattice Λ and $k \geq 3$, the Eisenstein series G_k is given by the absolutely convergent series $\sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-k}$. However, the definition can be generalised to also allow $k = 2$, and this is the definition that we use in Isabelle: let ω_1 and ω_2 be the generators of Λ. Then:*

$$G_k = 2\omega_1^{-k}\zeta(k) + \sum_{n \in \mathbb{Z} \setminus \{0\}} \sum_{m \in \mathbb{Z}} (m\omega_1 + n\omega_2)^{-k} \tag{1}$$

Here, $\zeta(s) = \sum_{n \geq 1} n^{-s}$ is the Riemann zeta function. For $k \geq 3$, this definition is equivalent to the absolutely convergent series that we considered initially.

It is clear that $G_k = 0$ for odd k, so only the G_k with even k are interesting. Another thing we can immediately see from the $\sum_{\omega\in\Lambda\setminus\{0\}}$ definition is that for $k \geq 3$, G_k is independent from the generators ω_1 and ω_2; it only depends on the lattice itself. To make the dependency on the lattice clear, one may write $G_k(\Lambda)$. Since the general case can be reduced to the case of a lattice generated by 1 and τ, one usually considers $G_k(\tau)$, i.e. one may treat G_k as a function in one complex variable.

Next, we show that $G_k(\tau)$ is a *modular form* for $k \geq 3$. A full discussion of what this means would be out of scope for this article; we refer the reader to introductory textbooks (e.g. by Apostol [3] or by Diamond and Shurman [9]). The short version is that a modular form is a function on the complex upper half plane that satisfies certain symmetries with respect to *unimodular transformations* of the form $z \mapsto \frac{az+b}{cz+d}$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

▶ **Theorem 13.** *$G_k(\tau)$ is a modular form of weight k for $k \geq 3$.*

Proof. For a function f to be a modular form of integer weight k, we must verify that it is holomorphic on the complex upper half plane (which in our case follows easily from the uniform convergence of the sum), that $f(\tau + 1) = f(\tau)$ and $f(-1/\tau) = \tau^k f(\tau)$ (since these two transformations generate the group of unimodular transformations), and that f is 'holomorphic at the cusp', i.e. it has a Fourier expansion without negative powers.

Since the generator pair $(1, \tau+1)$ generates the same lattice as $(1, \tau)$, we have $G_k(\tau+1) = G_k(\tau)$. Moreover, if the pair $(1, -1/\tau)$ generates a lattice Λ then $(1, \tau)$ generates the scaled lattice $\tau\Lambda$. Thus we clearly have $G_k(-1/\tau) = \tau^k G_k(\tau)$.

The only thing missing now is the Fourier expansion of $G_k(\tau)$. For odd k, this is trivial (since $G_k = 0$ for any lattice). We will derive the Fourier expansion for even k next. ◀

▶ **Theorem 14** (Fourier expansion of G_k)**.** *For $k \geq 2$ even, we have*

$$G_k(\tau) \;=\; 2\zeta(k) + 2c\sum\nolimits_{n\geq 1} n^{k-1}\, q^n/(1-q^n) \;=\; 2\zeta(k) + 2c\sum\nolimits_{n\geq 1} \sigma_{k-1}(n)\, q^n$$

where $q = \exp(2i\pi\tau)$ and $c = (2i\pi)^k/(k-1)!$ and $\sigma_s(n) = \sum_{d|n} d^s$ is the divisor function.

Proof. The starting point is Equation (1) with $\omega_1 = 1$ and $\omega_2 = \tau$.

To evaluate the inner sum, we first derive a closed form for the related sum $\sum_{m\in\mathbb{Z}}(z+m)^{-k}$:

$$\begin{aligned}\sum\nolimits_{m\in\mathbb{Z}}(z+m)^{-k} &\overset{(*)}{=} \frac{1}{(k-1)!}\left[\psi^{(k-1)}(1+z) + \psi^{(k-1)}(1-z)\right] + z^{-k}\\ &\overset{(**)}{=} c\,\mathrm{Li}_{1-k}(e^{2i\pi z})\end{aligned} \tag{2}$$

Here, $\psi^{(n)}(z)$ is the Polygamma function and $\mathrm{Li}_s(z)$ the Polylogarithm.

Step $(*)$ is straightforward, using the definition of ψ as a series. It takes about 85 lines, mostly due to side conditions involving summability. Step $(**)$ is done by taking the $(k-1)$-th derivative of the well-known partial fraction decomposition for the cotangent, $\pi\cot(\pi z) = z^{-1} + \sum_{n\geq 1}[(z+n)^{-1} + (z-n)^{-1}]$. This takes about 110 lines.

Now, applying (2) with $z = n\tau$ to (1) and noting $\exp(2i\pi n\tau) = q^n$, we obtain:

$$\begin{aligned}\sum\nolimits_{n\in\mathbb{Z}\setminus\{0\}}\sum\nolimits_{m\in\mathbb{Z}}(m+n\tau)^{-k} &= 2\sum\nolimits_{n\geq 1}\sum\nolimits_{m\in\mathbb{Z}}(m+n\tau)^{-k}\\ &\overset{(2)}{=} 2\sum\nolimits_{n\geq 1} c\,\mathrm{Li}_{1-k}(q^n) \overset{(***)}{=} 2c\sum\nolimits_{n\geq 1} n^{k-1}q^n/(1-q^n)\end{aligned}$$

The last step $(***)$ and the equivalence to the second form given in the theorem statement are identities from our Lambert series library, so the derivation only takes about 60 lines. ◀

Overall, this proof is essentially the same as Apostol's [3]. However, our version benefits from having libraries on the Polygamma and Polylogarithm function (which Apostol uses ad-hoc as infinite series without naming them).

Next, we will explore the aforementioned connection of G_k to the Laurent series expansion of $\wp$, which is easily proven by computing the k-th derivative of $\wp(z)$ and plugging in $z = 0$:

▶ **Proposition 15.** *The Laurent series expansion of $\wp$ around its double pole at the origin is:* $\wp(z) = z^{-2} + \sum_{k\geq 1}(k+1)\,G_{k+2}\,z^k$

With this, we can now show another important result about $\wp$:

▶ **Theorem 16.** *$\wp$ is a solution of both of the following ordinary differential equations:*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6 \qquad \wp''(z) = 6\wp(z)^2 - 30G_4$$

Proof. To show the first ODE, define $f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z)$. This is again an elliptic function, and the only place where a pole could be is $z = 0$. By computing the Laurent series expansion of f at $z = 0$, we find that all the poles cancel and the first non-zero term is the constant term, which is $-140G_6$. Since an elliptic function with no poles must be constant, we have $f(z) = -140G_6$ for all z, which concludes the proof.

This proof has about 100 lines in Isabelle and it illustrates nicely how easy it is to switch between the analytic world of complex functions and the algebraic world of formal Laurent series. The computation of the first few terms of the Laurent series expansion can be done automatically by Isabelle's simplifier in about 2 seconds after some setup. There is potential to automate this further by computing Laurent series expansions of meromorphic functions automatically, similarly to the powerful `real_asymp` method for real-valued functions [11].

To derive the second ODE from the first, we simply take the derivative of both sides and then cancel $2\wp'(z)$. This could lead to problems in the cases where $\wp'(z) = 0$, necessitating an analytic continuation to extend the identity to these points. However, we chose a different, easier route: from the 'analytic' version of the first ODE, one can also easily derive a 'formal' version on the Laurent series of $\wp(z)$ and derive the formal version of the second ODE from it purely on the algebraic level of formal Laurent series, where the issue of zeros does not arise. One can then simply convert this to an 'analytic' ODE again. ◀

▶ **Corollary 17.** *Every G_k for $k \geq 4$ can be expressed as a rational polynomial in G_4 and G_6. This polynomial can be computed efficiently using a memoisation-based recursive algorithm.*

Proof. The second ODE we derived for $\wp$ gives us the $(k+2)$-th coefficient of the Laurent series expansion of $\wp(z)$ in terms of the k-th coefficient of $\wp(z)^2$, which can easily be computed knowing only the coefficients of $\wp(z)$ up to k. We omit the details. ◀

As an example, we have $G_8 = \frac{3}{7}G_4^2$ and $G_{12} = \frac{18}{143}G_4^3 + \frac{25}{143}G_6^2$. By looking at the coefficient of the q^n term of the Fourier expansions of both sides, one obtains profound convolution identities for the divisor function, e.g. for $G_8 = \frac{3}{7}G_4^2$:

▶ **Theorem 18.** $\sigma_7(n) = \sigma_3(n) + 120\sum_{k=1}^{n-1}\sigma_3(k)\,\sigma_3(n-k)$

The ODE for $\wp$ also allows us to study the values of $\wp$ at the half-periods and to develop the modular discriminant Δ, another important modular form.

▶ **Theorem 19.** *Define the polynomial $P(x) = 4x^3 - 60G_4x - 140G_6$. Let e_1, e_2, e_3 be the values of $\wp$ at the half-lattice points $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, and $\frac{1}{2}(\omega_1+\omega_2)$, respectively. Then:*

1. *The values e_1, e_2, e_3 are all distinct from one another and they are the roots of $P(x)$.*

2. *The discriminant of* $P(x)$ *is* $\Delta = (60G_4)^3 - 27(140G_6)^2$ *and it is non-zero.*

Proof. 1. That the e_i are roots of $P(x)$ is clear, since we just showed that $P(\wp(z)) = \wp'(z)^2$ and $\wp'(z) = 0$ for any half-lattice point z. Now suppose two of them were identical. That is, $\wp$ assumes the same value at two non-equivalent half-lattice points z_1, z_2. Then the function $f(z) = \wp(z) - \wp(z_1)$ would be elliptic of order 2 (just like $\wp$) with zeros at z_1 and z_2. Because z_1 and z_2 are half-lattice points, we would have $f'(z_1) = f'(z_2) = \wp'(z_1) = 0$, so the zeros have multiplicity at least 2. But then the order of $f(z)$ would be at least 4.
2. Since the e_i are the roots of $P(x)$, we have $\Delta = (4(e_1 - e_2)(e_1 - e_3)(e_2 - e_3))^2$. This immediately shows that $\Delta \neq 0$, since the e_i are distinct. We can verify that $\Delta = (60G_4)^3 - 27(140G_6)^2$ by writing $P(x) = 4(x - e_1)(x - e_2)(x - e_3)$ and doing some algebra (fully automatic in Isabelle via the *algebra* method, using Gröbner bases).

◀

The first proof has about 130 lines in Isabelle and is tedious due to the usual problems dealing with side conditions and counting zeros. The second one is quite short with 30 lines.

▶ **Theorem 20** (Addition and duplication theorems for $\wp$)**.** *Let* $u_1, u_2 \notin \Lambda$ *and* $u_1 \nsim_\Lambda \pm u_2$. *Let also* $2u \notin \Lambda$. *Then:*

$$\wp(u_1 + u_2) = -\wp(u_1) - \wp(u_2) + \frac{1}{4}\left[\frac{\wp'(u_1) - \wp'(u_2)}{\wp(u_1) - \wp(u_2)}\right]^2 \qquad \wp(2u) = -2\wp(u) + \frac{1}{4}\left[\frac{\wp''(u)}{\wp'(u)}\right]^2$$

Proof. Our proofs follow the presentation by Lang [25].

The duplication theorem is easily proven (in about 30 lines) from the addition theorem by a straightforward limiting argument, letting $u_1 \to u_2$ and using L'Hospital's rule.

To prove the addition theorem, we first assume w.l.o.g. that u_1 and u_2 are in the fundamental parallelogram and 'in general position', i.e. that $u_1 + 2u_2 \notin \Lambda$ and $2u_1 + u_2 \notin \Lambda$. Let a, b be such that $(u_1, \wp(u_1))$ and $(u_2, \wp(u_2))$ both lie on the line $ax + b = y$. Concretely, $a = (\wp'(u_1) - \wp'(u_2))/(\wp(u_1) - \wp(u_2))$ and $b = \wp'(u_1) - a\wp(u_1)$. Our first goal is now to show that $(\wp(u_1 + u_2), \wp'(u_1 + u_2))$ also lies on that line.

To that end, we define $f(z) = \wp'(z) - (a\wp(z) + b)$. By examining the Laurent series expansion of $f(z)$ at $z = 0$, we find that it has a triple pole at $z = 0$ and therefore order 3.

Due to the 'general position' assumption, u_1 and u_2 are simple zeros of f. Let u_3 be its third zero. Since the zeros and poles of f sum to a lattice point, we have $u_3 \sim_\Lambda -(u_1 + u_2)$. We define the polynomials $P(x) = 4x^3 - 60G_4x - 140G_6 - (ax + b)^2$ and $Q(x) = 4(x - \wp(u_1))(x - \wp(u_2))(x - \wp(u_3))$. Clearly, P and Q have the same roots, namely $\wp(u_1)$, $\wp(u_2)$, $\wp(u_3)$. Since the leading coefficients also match, we have $P = Q$.

Now $-a^2 = -4(\wp(u_1) + \wp(u_2) + \wp(u_3))$, since the coefficient of x^2 in $P(x)$ and $Q(x)$ has to be the same. Solving for $\wp(u_3) = \wp(u_1 + u_2)$ concludes the proof. All of this takes about 280 lines, mostly due to the difficulty of dealing with *zorder*.

It remains to get rid of the 'general position' assumption. This is done by keeping u_1 fixed and viewing $\wp(u_1 + u_2)$ as a function of u_2. We can then simply use analytic continuation to extend the result to the isolated 'non-general' values of u_2 as well. This takes another 50 lines of 'boilerplate' proofs. ◀

Note that this proof also gives us the similar addition and duplication theorems for $\wp'$ basically for free, since $\wp'(u_3) = a\wp(u_3) + b$.

▶ Remark 21. Theorems 16 and 19 along with our other results show that $(\wp(z), \wp'(z))$ is a parametrisation of the elliptic curve $y^2 = 4x^3 - 60G_4x - 140G_6$ in Weierstraß normal form in the projective complex space $\mathbb{CP}^2$ (if we additionally map lattice points to the 'point at

infinity'). In fact, this map is a group isomorphism between the additive abelian group $\mathbb{C}/\Lambda$ and the elliptic curve (with the usual addition operation on elliptic curves).

This means that every complex lattice is isomorphic to an elliptic curve.[2] From this we can also see why addition on elliptic curves is defined the way it is and why it 'works': it is the result of taking the natural addition operation on $\mathbb{C}/\Lambda$ and transferring it to the elliptic curve via the above isomorphism and using the addition theorems for $\wp$ and $\wp'$.

Next, we will look at an important tool linking the elliptic world and the modular world.

5 The Jacobi Theta Functions

The Jacobi theta functions are a family of closely related functions of two complex variables. They satisfy various interesting properties – most importantly, they behave somewhat like a modular form in their second parameter and 'quasi-elliptically' in their first. They have applications in various fields, from number theory to physics.

Unfortunately, the conventions for the functions themselves and their notations are very inconsistent in the literature. We will focus mostly on the 'main' Jacobi theta function, which we will denote as ϑ_{00}. The others can easily be derived from it.

Due to their periodicity, the Jacobi theta functions can either be written in the form $\vartheta(z;\tau)$ in terms of two complex parameters $z \in \mathbb{C}$ and τ with $\operatorname{Im}(\tau) > 0$, or as $\vartheta(w,q)$ in terms of the nomes $w = \exp(i\pi z)$ and $q = \exp(i\pi\tau)$. The latter form is sometimes referred to as the *q-expansion* or the *Fourier expansion*.

Both forms have their advantages, so we want to have both. We start by defining everything in terms of the nomes and then derive the other versions from it, since that direction is easier as one does not have to deal with branch cuts.

We first introduce Ramanujan's theta function [6]. We mostly use it as a stepping stone to the more well-known Jacobi theta function.

▶ **Definition 22.** *For $a, b \in \mathbb{C}$ with $|ab| < 1$, the Ramanujan theta function (denoted as simply $f(a,b)$) is defined as $f(a,b) = \sum_{n\in\mathbb{Z}} a^{n(n+1)/2} b^{n(n-1)/2}$.*

Its basic properties are easily established: it is commutative (via the substitution $n \mapsto -n$) and converges uniformly on compact subsets of its domain, making it holomorphic.[3]

We also formalise a number of basic identities from Ramanujan's Notebook [6], such as $f(1,a) = 2f(a,a^3)$ and $f(a,b) = af(a^2b, 1/a)$.

▶ **Definition 23** (Auxiliary Jacobi theta function)**.** *We define another Jacobi-style theta function as $\vartheta(w,q) = f(qw, q/w) = \sum_{n\in\mathbb{Z}} w^n q^{n^2}$ for $|q| < 1$ and $w \neq 0$. We call this function* jacobi_theta_nome *in Isabelle.*

From the properties of the Ramanujan theta function, we immediately derive the identity $\vartheta(q^2w, q) = \vartheta(w,q)/(wq)$, which will give us the quasiperiodicity identity for the 'normal' Jacobi theta function.

[2] The opposite direction also holds but is not included in our formalisation since it requires significant results about Klein's j invariant; it is however already part of our previous formalisation [20].

[3] Note that there is currently no way in Isabelle/HOL to explicitly state that a function is simultaneously holomorphic in two arguments, but for practical purposes it is sufficient to prove that $f(g(z), h(z))$ is holomorphic in z whenever g and h are.

▶ **Definition 24** (Jacobi theta function and auxiliary theta functions). *The 'usual' Jacobi theta function is written as $\vartheta_{00}(w, q)$ when in terms of the nome and as $\vartheta_{00}(z;\tau)$ in terms of the complex plane. It is defined as follows:*

$$\vartheta_{00}(w,q) = \vartheta(w^2, q) \qquad \vartheta_{00}(z;\tau) = \vartheta(\exp(2i\pi z), \exp(i\pi\tau))$$

Three more auxiliary functions ϑ_{10}, ϑ_{01}, and ϑ_{11} are also defined:

$$\vartheta_{01}(z;\tau) = \vartheta_{00}(z + \tfrac{1}{2};\tau)$$
$$\vartheta_{10}(z;\tau) = \exp(i\pi(z + \tfrac{1}{4}\tau))\,\vartheta_{00}(z + \tfrac{1}{2}\tau;\tau)$$
$$\vartheta_{11}(z;\tau) = \exp(i\pi(z + \tfrac{1}{4}\tau + \tfrac{1}{2}))\,\vartheta_{00}(z + \tfrac{1}{2}\tau + \tfrac{1}{2};\tau)$$

These are shifted versions of ϑ_{00} that are sometimes convenient to have.

We prove various important properties of these functions, in particular some for the *theta nullwert* functions $\vartheta_{xy}(1, q)$ (e.g. their relationship to counting the number of ways to write an integer as a sum of squares). For reasons of space, we omit these here.

One important property of the Jacobi theta functions is that they are quasi-elliptic in their first parameter and act somewhat like a modular form in their second parameter:

▶ **Theorem 25** (Quasi-elliptic and quasi-modular properties of Jacobi theta functions).

$$\vartheta_{00}(z+1;\tau) = \vartheta_{00}(z;\tau) \qquad \vartheta_{00}(z+\tau;\tau) = \vartheta_{00}(z;\tau)/\exp(i\pi(2z+\tau))$$
$$\vartheta_{00}(z;\tau+1) = \vartheta_{00}(z+1/2;\tau) \qquad \vartheta_{00}(z;-1/\tau) = \sqrt{-i\tau}\exp(i\pi\tau z^2)\,\vartheta_{00}(\tau z;\tau)$$

Similar identities hold for the other ϑ_{xy}.

The first three are either obvious consequences of the definition or of similar properties of $\vartheta(w, q)$ and $f(a, b)$. The last identity – sometimes referred to as the *Jacobi Inversion Formula* – is somewhat more difficult to derive, but will lead to easy proofs of similar identities for other functions, as we will see later.

The usual way to derive it is via the Poisson summation formula. Since Isabelle/HOL does not have a library of Fourier transforms yet, we instead chose a different path that is arguably also fairly elegant. Before we do this, however, we will first go through a few other interesting properties of the Jacobi theta functions that will help us.

5.1 The Jacobi Triple Product

The Jacobi triple product is a fundamental theorem that gives an alternative, 'multiplicative' view on the Jacobi theta function.

▶ **Theorem 26** (Jacobi triple product). $\vartheta(w, q) = (q^2;q^2)_\infty\,(-qw;q^2)_\infty\,(-q/w;q^2)_\infty$
A more explicit version is: $\sum_{n\in\mathbb{Z}} w^n q^{n^2} = \prod_{m\geq 1}(1-q^{2m})(1+q^{2m-1}w)(1+q^{2m-1}/w)$
Or, equivalently, in terms of Ramanujan's theta: $f(a, b) = (-a;ab)_\infty\,(-b;ab)_\infty\,(ab;ab)_\infty$

Our proof of Theorem 26 (first version) follows the particularly succinct one-page proof given by Andrews [2]. He uses two beautiful identities due to Euler, which are similar in spirit to the Jacobi triple product in the sense that they express an infinite product as a series:

▶ **Lemma 27** (Euler's q-series identities).

$$(a;q)_\infty = \sum\nolimits_{n\geq 0} \frac{q^{n(n-1)/2}\,a^n}{(q-1)\cdots(q^n-1)} \qquad \frac{1}{(a;q)_\infty} = \sum\nolimits_{n\geq 0} \frac{a^n}{(1-q)\cdots(1-q^n)}$$

Proof. Our formalisation follows the elegant proofs given by Bellman [5].

Let $f(x) = (x;q)_\infty$. Then f satisfies the functional equation $f(x) = (1-x)\,f(qx)$. We expand f into a power series $f(x) = \sum_{n\geq 0} a_n x^n$ at $x = 0$. Clearly we have $a_0 = 1$, and with the functional equation we obtain the recurrence $(q^{n+1}-1)a_{n+1} = q^n a_n$. The solution of this recurrence is $a_n = q^{n(n-1)/2}/[(q-1)(q^2-1)\cdots(q^n-1)]$.

The proof of the second identity is analogous with $f(x) = 1/(x;q)_\infty$.

The proofs of both identities take about 200 lines together, and they again illustrate the process of switching between analytic functions and formal power series in Isabelle/HOL. ◀

Proof of the Jacobi Triple Product (Theorem 26). We will only sketch the major steps of the proof and refer to Andrews [2] for the full version. Briefly:

- Assume w.l.o.g. that w and q are real and $0 < q < \frac{1}{4}$ and $\frac{1}{2} < w < 1$.[4]
- Use the first identity of Lemma 27 twice to express the product of two of the q-Pochhammer symbols in the theorem statement as a double sum.
- Prove absolute convergence of the double sum, change the order of summation, shift indices, and apply the second identity once. The remaining sum is the definition of ϑ.
- Use analytic continuation once in w and then in q to lift the theorem to the full domain.

The proof is about 340 lines long, including about 140 for the absolute convergence of the double sum and 80 for the analytic continuation in the end. In contrast, Andrews does not mention the issue of absolute convergence or give any details on the analytic continuation (which is common in paper proofs, and probably sensible).

The version for the Ramanujan theta function follows easily in principle but requires some care due to branch cuts. We first prove it for positive reals (which avoids the branch cuts) and then again derive the full version using analytic continuation twice. ◀

The Jacobi Triple Product has several interesting corollaries:

- Since the right-hand side vanishes iff one of its factors vanishes, one can immediately see that the zeros of $\vartheta_{00}(z;\tau)$ are exactly at the points of the form $z = m + \frac{1}{2} + (n+\frac{1}{2})\tau$, i.e. at the half-lattice points of the lattice generated by 1 and τ.[5]
- Letting $a = -q$ and $b = -q^2$ we get the Pentagonal Number Theorem [18], namely $\varphi(q) = f(-q,-q^2) = \sum_{k\in\mathbb{Z}} (-1)^k q^{k(3k-1)/2}$. In other words, we get the power series expansion of $\varphi(q)$ in terms of the *generalised pentagonal numbers*. This is significant because $1/\varphi(q)$ is the generating function of the *partition function* $p(n)$: the number of ways to write n as a sum of positive integers.

  From this power series for $\varphi(q)$, we derive the upper bound $p(n) \leq \pi e^{\pi\sqrt{2/3n}}/\sqrt{6(n-1)}$ in about 110 lines (following Apostol [3]) and an efficient algorithm to compute $p(n)$ by computing the reciprocal of this (very sparse) power series in the naïve way.[6]
- With some work, following Andrews and Eriksson [1], we derive the Rogers–Ramanujan identities from the Jacobi triple product [16]. We omit the details.

---

[4] Our conditions on w and q are stronger than Andrews's, but we were not able to prove absolute convergence with his bounds. Anyway, we obtain the same conclusion after the analytic continuation.

[5] One can also see from this that they are *simple* zeros, but this is tedious in Isabelle due to the problems with *zorder* mentioned in Section 2.4. We will obtain this fact more easily in our proof of Lemma 29.

[6] We formalised an imperative algorithm based on this which takes $O(n^2)$ bit operations to compute $p(n)$, which is known to have $\Theta(n^{3/2})$ bits.

5.2 Additional Properties

▶ **Theorem 28** (Heat equation). *The Jacobi theta function $\vartheta_{00}(z;\tau)$ is a solution to the following partial differential equation (also known as the one-dimensional heat equation):*

$$\frac{\partial^2}{\partial z^2}\,\vartheta_{00}(z;\tau) = 4i\pi\,\frac{\partial}{\partial \tau}\,\vartheta_{00}(z;\tau)$$

For illustration, the theorem statement looks as follows in Isabelle:

```
(deriv ^^ 2) (λz. jacobi_theta_00 z t) z = 4 * pi * i * deriv (λt. jacobi_theta_00 z t) t
```

Proof. This proof is mathematically trivial, but it is worth examining how to do it in a theorem prover anyway, since it involves the somewhat delicate interchange of an infinite sum and a derivative operator, whose subtleties are typically ignored in informal proofs.

We use the definition of ϑ_{00} in terms of the Ramanujan theta function, which is defined as an infinite sum that we proved converges uniformly on compact subsets of its domain. We therefore first pick a compact neighbourhood of (z,τ) and show that $\vartheta_{00}(z;\tau)$ is given in that neighbourhood by the uniformly convergent sum $\vartheta_{00}(z;\tau) = \sum_{n\in\mathbb{Z}} \exp(i\pi(n^2\tau + 2nz))$. Since derivatives commute with uniformly convergent sums, it then only remains to pull the derivative operators into the sums, apply them to the summands, and do the arithmetic.

All of this takes about 130 lines in Isabelle, about half of which is dedicated to establishing the uniformly convergent sum. ◀

▶ **Lemma 29** (Uniqueness of the Jacobi theta function). *Let us call any entire function $g(z)$ that satisfies the same quasi-elliptic identities as $\vartheta_{00}(z;\tau)$ for a fixed τ (namely $g(z+1) = g(z)$ and $g(z+\tau) = g(z)/\exp(i\pi(2z+\tau))$)* thetalike.

Then any thetalike function is a constant multiple of $\vartheta_{00}(z;\tau)$.

Proof. We first show that any thetalike function $g(z)$ that is not identically zero has exactly the same zeros as $\vartheta_{00}(z;\tau)$. Consider the lattice generated by 1 and τ. Our proof now mirrors what we did earlier in Theorems 4 and 5: we apply the Argument Principle to $g(z)$ along a period parallelogram with weight 1, using the same strategy as before to avoid singularities. We find that the integral evaluates to 1, so $g(z)$ has exactly one simple zero in the period parallelogram. We then apply the Argument Principle with weight z and find that the integral evaluates to $\frac{1}{2}(\tau+1)$ plus a lattice point. Therefore, the zeros are located exactly at the half-lattice points $\frac{1}{2}(\tau+1)+\Lambda$, exactly where the zeros of $\vartheta_{00}(z;\tau)$ are.[7]

To show that any thetalike function $g(z)$ is a constant multiple of ϑ_{00}, define $h(z) = \vartheta_{00}(0;\tau)g(z) - g(0)\vartheta_{00}(z;\tau)$ and note that it is thetalike and vanishes at the origin. Since the origin is *not* a half-lattice point, this means that h must be identically zero. Thus $g(z) = c\vartheta_{00}(z;\tau)$ with $c := g(0)/\vartheta_{00}(0;\tau)$. ◀

5.3 Proving the Inversion Formula

Using these components, we can now obtain a very simple proof of the inversion formula.

Proof of the Jacobi Inversion Formula (cf. Theorem 25). Recall that we want to prove $\vartheta_{00}(z;-1/\tau) = \sqrt{-i\tau}\,\exp(i\pi\tau z^2)\,\vartheta_{00}(\tau z;\tau)$.

[7] Since ϑ_{00} is clearly thetalike, we also obtain that the zeros of ϑ_{00} are simple as a byproduct.

For any fixed τ, the function $z \mapsto \exp(i\pi\tau z^2)\,\vartheta_{00}(\tau z;\tau)$ satisfies the assumptions of Lemma 29 (with τ instantiated with $-1/\tau$), so there must be a $c(\tau)$ such that:

$$\exp(i\pi\tau z^2)\,\vartheta_{00}(\tau z;\tau) = c(\tau)\,\vartheta_{00}(z;-1/\tau) \tag{3}$$

Applying $\partial_\tau|_{z=0}$ to (3) gives us $\partial_\tau\vartheta_{00}(0;\tau) = c'(\tau)\,\vartheta_{00}(0;-1/\tau) + \tau^{-2}\,c(\tau)\,\partial_\tau\vartheta_{00}(0;-1/\tau)$.

Applying $\partial_z^2|_{z=0}$ to (3), applying Theorem 28 (the heat equation), and cancelling $4i\pi\tau^2$ gives us $\partial_\tau\vartheta_{00}(0;\tau) + \vartheta_{00}(0;\tau)/(2\tau) = \tau^{-2}\,c(\tau)\,\partial_\tau\vartheta_{00}(0;-1/\tau)$.

Subtracting these last two equations gives us $\vartheta_{00}(0;\tau)/(2\tau) = -c'(\tau)\,\vartheta_{00}(0;-1/\tau)$, and using (3) again we obtain the separable ODE $-c'(\tau) = c(\tau)/(2\tau)$, which can easily be shown to have the general solution $c(\tau) = C/\sqrt{\tau}$. We check that $c(i) = 1$, so $C = \sqrt{i}$ and $c(\tau) = 1/\sqrt{-i\tau}$.

All of this takes about 180 lines. ◀

5.4 Applications of the Inversion Formula

In this section, we will look at two useful applications of the inversion formula in the context of modular forms, namely to Dedekind's η function and the 'forbidden' Eisenstein series G_2.

5.4.1 Dedekind's η Function

The η function is interesting because it is – according to a reasonable generalisation of the notion of modular forms to half-integer values – a modular form of weight $\frac{1}{2}$ and closely related to the modular discriminant $\Delta(\tau)$ that we saw earlier. Through the closely related Euler function $\varphi(q)$, it is also important in the study of the partition function $p(n)$ (particularly in the derivation of Rademacher's convergent sum for $p(n)$).

▶ **Definition 30** (Dedekind's η function). $\eta(\tau) = \exp(i\pi\tau/12)\,\varphi(\exp(2i\pi\tau))$

Using the Jacobi triple product and some simple identities for the q-Pochhammer symbol from the library, it is easy to relate $\eta(\tau)$ to the Jacobi theta functions, e.g.:

$$\eta(\tau) = \exp(i\pi\tau/12)\,\vartheta_{01}(-\tau/2;3\tau) \qquad\qquad \vartheta_{01}(0;\tau) = \eta(\tau/2)^2/\eta(\tau)$$

It is also easy to see from the definition of $\eta(\tau)$ that $\eta(\tau+1) = \exp(i\pi/12)\,\eta(\tau)$, similarly to what we saw for $G_k(\tau)$. Just like the G_k and the ϑ_{xy}, it also satisfies an inversion identity:

▶ **Theorem 31.** $\eta(-1/\tau) = \sqrt{-i\tau}\,\eta(\tau)$

Or, the more general modular transformation formula: $\eta(\gamma(\tau)) = \varepsilon(\gamma)\sqrt{c\tau+d}\,\eta(\tau)$ where $\gamma(z) = (az+b)/(cz+d)$ is a modular transformation and $\varepsilon(\gamma)$ is a root of unity depending on a, b, c, d (we omit the definition of ε here).

Proving this key identity takes up almost an entire chapter in Apostol [3]. Our previous formalisation [20] instead followed Siegel's considerably more concise contour-integration proof. It had over 1,300 lines of fairly 'monolithic' proofs, consisting mostly of intricate calculations and contour integrals of no reuse value. Our new proof, on the other hand, has a mere 90 lines (while building on a much larger stack of reusable library material):

Proof. With a tedious but short and straightforward computation (about 70 lines) involving the Jacobi triple product and manipulations of q-Pochhammer symbols using standard identities, one can check that $\vartheta_{10}(1/6;\tau/3) = \sqrt{3}\exp(i\pi\tau/12)\,\vartheta_{01}(-\tau/2;3\tau)$. Using this together with our identities relating η to ϑ_{xy} and the Jacobi Inversion Formula, one obtains the inversion formula for $\eta(-1/\tau)$ in another 20 lines.

The general transformation formula follows by an induction on γ, noting that the modular group is generated by the maps $z \mapsto z+1$ and $z \mapsto -1/z$. ◀

5.4.2 The Forbidden Eisenstein Series G_2

We previously noted that some of the results for the Eisenstein series G_k only hold for $k \geq 3$, since the lattice sum fails to converge for $k \leq 2$. This is true in particular for the simple inversion identity $G_k(-1/\tau) = \tau^k G_k(\tau)$, which makes G_k a modular form for $k \geq 3$.

However, the 'forbidden' Eisenstein series G_2 is still of interest. It is not a modular form, but it does satisfy the following quasi-modular identity:

▶ **Theorem 32.** $G_2(-1/\tau) = \tau^2 G_2(\tau) - 2i\pi\tau$

A more general version for arbitrary modular transformations similar to the one for η can easily be derived from this as well.

Deriving this identity typically takes up several pages of intricate and technical reasoning in textbooks or lectures on modular forms. We, however, obtain it almost for free from the inversion identity for η and the following connection between G_2 and η:

▶ **Proposition 33.** $\eta'(\tau)/\eta(\tau) = i/(4\pi)\, G_2(\tau)$

That is, G_2 is – up to a constant factor – the logarithmic derivative of η.

Proof. The logarithmic derivative of Euler's function φ is given by the Lambert series $\varphi'(q)/\varphi(q) = \sum_{k\geq 1} kq^{k-1}/(q^k - 1)$, as can easily be seen from its definition. Plugging this into the definition of $\eta(\tau)$ and comparing with the Fourier expansion of $G_2(\tau)$ (Theorem 14) proves the identity (in three lemmas of about 25 lines each). ◀

The proof of the inversion identity for G_2 is then obtained simply by taking the logarithmic derivative of the inversion identity for η (about 40 lines in Isabelle).

6 Conclusion

It is well known that with sufficient effort, practically any piece of mathematics can be formalised. Here, we have striven to not only 'get to the finish line', but to keep proofs short and elegant while building a whole array of reusable libraries. Elegant proofs are a reward in and of themselves, but we also believe that this approach will make extending and maintaining our proof development easier.

Notably, our formalisation of Jacobi theta functions was originally created for no particular purpose but rather out of curiosity. It was merely by coincidence that we then discovered that it could improve the existing formalisation of Dedekind's η function, reducing one particularly messy proof from 1,300 lines down to 90. The situation for the libraries on Lambert series and on q-analogues of combinatorial operators is similar. We conclude that building libraries of formal mathematics, even without a clear purpose, can pay unexpected dividends.

All in all, our formalisation comprises about 21,000 lines excluding comments and blank lines, plus 5,000 lines of supporting libraries (e.g. Lambert series, the polylogarithm).

Some aspects of the work could be done better. We currently formalise sets of zeros and poles, and separately keep their orders; multisets of zeros and poles, or a free abelian group of both, might be less painful. A better Isabelle/HOL library of infinite products is necessary to handle some further topics such as the Weierstraß σ function. But even now, we have a fairly comprehensive library of elliptic functions and theta functions, ready to serve as a foundation for further work in analytic number theory.

Note: No generative AI tools were used in the production of this proof development.

References

1. G. E. Andrews and K. Eriksson. *Integer Partitions*. Cambridge University Press, 2004.
2. George E. Andrews. A simple proof of Jacobi's triple product identity. *Proceedings of the American Mathematical Society*, 16(2):333–334, April 1965. doi:10.1090/s0002-9939-1965-0171725-x.
3. Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Graduate Texts in Mathematics. Springer New York, 1990. doi:10.1007/978-1-4612-0999-7.
4. Clemens Ballarin. Locales: A module system for mathematical theories. *Journal of Automated Reasoning*, 52(2):123–153, April 2013. doi:10.1007/s10817-013-9284-7.
5. Richard Bellman. *A Brief Introduction to Theta Functions*. Holt, Rinehart and Winston, New York, 1961.
6. Bruce C. Berndt. *Ramanujan's Notebooks*. Springer New York, 1991. doi:10.1007/978-1-4612-0965-2.
7. Chris Birkbeck. Formalising modular forms, eisenstein series and the statement of the modularity conjecture. Preprint, available at https://cdbirkbeck.wixsite.com/website/research, 2023.
8. Amine Chaieb. Formal power series. *Journal of Automated Reasoning*, 47(3):291–318, August 2010. doi:10.1007/s10817-010-9195-9.
9. Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer New York, 2005. doi:10.1007/978-0-387-27226-9.
10. 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)*, volume 141 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:19, Dagstuhl, Germany, 2019. Leibniz International Proceedings in Informatics.
11. Manuel Eberl. Verified real asymptotics in Isabelle/HOL. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '19, New York, NY, USA, 2019. ACM. doi:10.1145/3326229.3326240.
12. Manuel Eberl. A proof from THE BOOK: The partial fraction expansion of the cotangent. *Archive of Formal Proofs*, March 2022. https://isa-afp.org/entries/Cotangent_PFD_Formula.html, Formal proof development.
13. Manuel Eberl. Lambert series. *Archive of Formal Proofs*, November 2023. https://isa-afp.org/entries/Lambert_Series.html, Formal proof development.
14. Manuel Eberl. The polylogarithm function. *Archive of Formal Proofs*, November 2023. https://isa-afp.org/entries/Polylog.html, Formal proof development.
15. Manuel Eberl. Combinatorial q-analogues. *Archive of Formal Proofs*, December 2024. https://isa-afp.org/entries/Combinatorial_Q_Analogues.html, Formal proof development.
16. Manuel Eberl. The Rogers–Ramanujan identities. *Archive of Formal Proofs*, December 2024. https://isa-afp.org/entries/Rogers_Ramanujan.html, Formal proof development.
17. Manuel Eberl. Theta functions. *Archive of Formal Proofs*, December 2024. https://isa-afp.org/entries/Theta_Functions.html, Formal proof development.
18. Manuel Eberl. The partition function and the pentagonal number theorem. *Archive of Formal Proofs*, April 2025. https://isa-afp.org/entries/Pentagonal_Number_Theorem.html, Formal proof development.
19. Manuel Eberl, Anthony Bordg, Wenda Li, and Lawrence C. Paulson. Complex lattices, elliptic functions, and the modular group. *Archive of Formal Proofs*, May 2025. https://isa-afp.org/entries/Elliptic_Functions.html, Formal proof development.
20. Manuel Eberl, Anthony Bordg, Lawrence C. Paulson, and Wenda Li. Formalising half of a graduate textbook on number theory. In Yves Bertot, Temur Kutsia, and Michael Norrish, editors, *15th International Conference on Interactive Theorem Proving (ITP 2024)*, pages 40:1–40:7, Dagstuhl, Germany, 2024. Leibniz International Proceedings in Informatics. doi:10.4230/LIPIcs.ITP.2024.40.

21 Manuel Eberl, Anthony Bordg, Lawrence C. Paulson, and Wenda Li. Dedekind sums. *Archive of Formal Proofs*, April 2025. `https://isa-afp.org/entries/Dedekind_Sums.html`, Formal proof development.

22 John Harrison. Formalizing basic complex analysis. In R. Matuszewski and A. Zalewska, editors, *From Insight to Proof: Festschrift in Honour of Andrzej Trybulec*, volume 10(23) of *Studies in Logic, Grammar and Rhetoric*, pages 151–165. University of Bialystok, 2007.

23 John Harrison. Formalizing an analytic proof of the Prime Number Theorem (dedicated to Mike Gordon on the occasion of his 60th birthday). *Journal of Automated Reasoning*, 43(3):243–261, Oct 2009. `doi:10.1007/s10817-009-9145-6`.

24 Johannes Hölzl, Fabian Immler, and Brian Huffman. Type classes and filters for mathematical analysis in Isabelle/HOL. In Sandrine Blazy, Christine Paulin-Mohring, and David Pichardie, editors, *Interactive Theorem Proving*, pages 279–294, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

25 Serge Lang. *Elliptic Functions*. Graduate Texts in Mathematics. Springer New York, 1973. `doi:10.1007/978-1-4612-4752-4`.

26 David Loeffler and Michael Stoll. Formalizing zeta and L-functions in lean. *Annals of Formalized Mathematics*, Volume 1, July 2025. URL: `http://dx.doi.org/10.46298/afm.15328`, `doi:10.46298/afm.15328`.

27 Carl Ludwig Siegel. A simple proof of $\eta(-1/\tau) = \eta(\tau)\sqrt{\tau/i}$. *Mathematika*, 1(1):4, June 1954. `doi:10.1112/s0025579300000462`.

28 Jeremy Sylvestre. Formal Laurent series. Isabelle/HOL distribution, `HOL-Computational_Algebra.Formal_Laurent_Series`, 2019.

29 The Isabelle Community. `HOL-Complex_Analysis`. Isabelle/HOL distribution, 2026.

30 The mathlib community. The Lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020*, pages 367–381, 2020. `doi:10.1145/3372885.3373824`.