# Formalising a Number Theory Textbook: Lessons Learnt

Lawrence C Paulson

*Pittsposium, 22 August 2023 – work funded by the ERC Advanced Grant ALEXANDRIA (Project GA 742178)*

# Formalising maths – up to 2015

- *A machine-checked proof of the odd order theorem*, using Coq (Gonthier et al.)
- … *of Gödel's incompleteness theorems*, using Isabelle (Paulson)
- … *of the Kepler conjecture*, using HOL Light and Isabelle (Hales et al.)

# The Lean phenomenon (2017–)

- **Sophisticated** definitions: schemes, perfectoid spaces
- Big libraries of advanced mathematics (mathlib)
- *Liquid tensor experiment*: verifying the brand-new work of a Fields medallist

Experiments to confirm *"that a proof assistant can handle complexity …, which is rather different from formalising a long proof about simple objects."* — Kevin Buzzard

# ALEXANDRIA

(ERC Project GA 742178)

Aim: to support working mathematicians

… by developing tools and libraries

What sorts of mathematics—and proofs—can we formalise?

*Using Isabelle/HOL, by the way*

# Some of our topics

quantum computation • projective geometry • counting roots • Budan–Fourier theorem • algebraically closed fields

ordinal partition theory

Grothendieck schemes

Szemerédi's regularity lemma

Roth: arithmetic progressions

Balog–Szemerédi–Gowers theorem, Khovanskii's theorem …

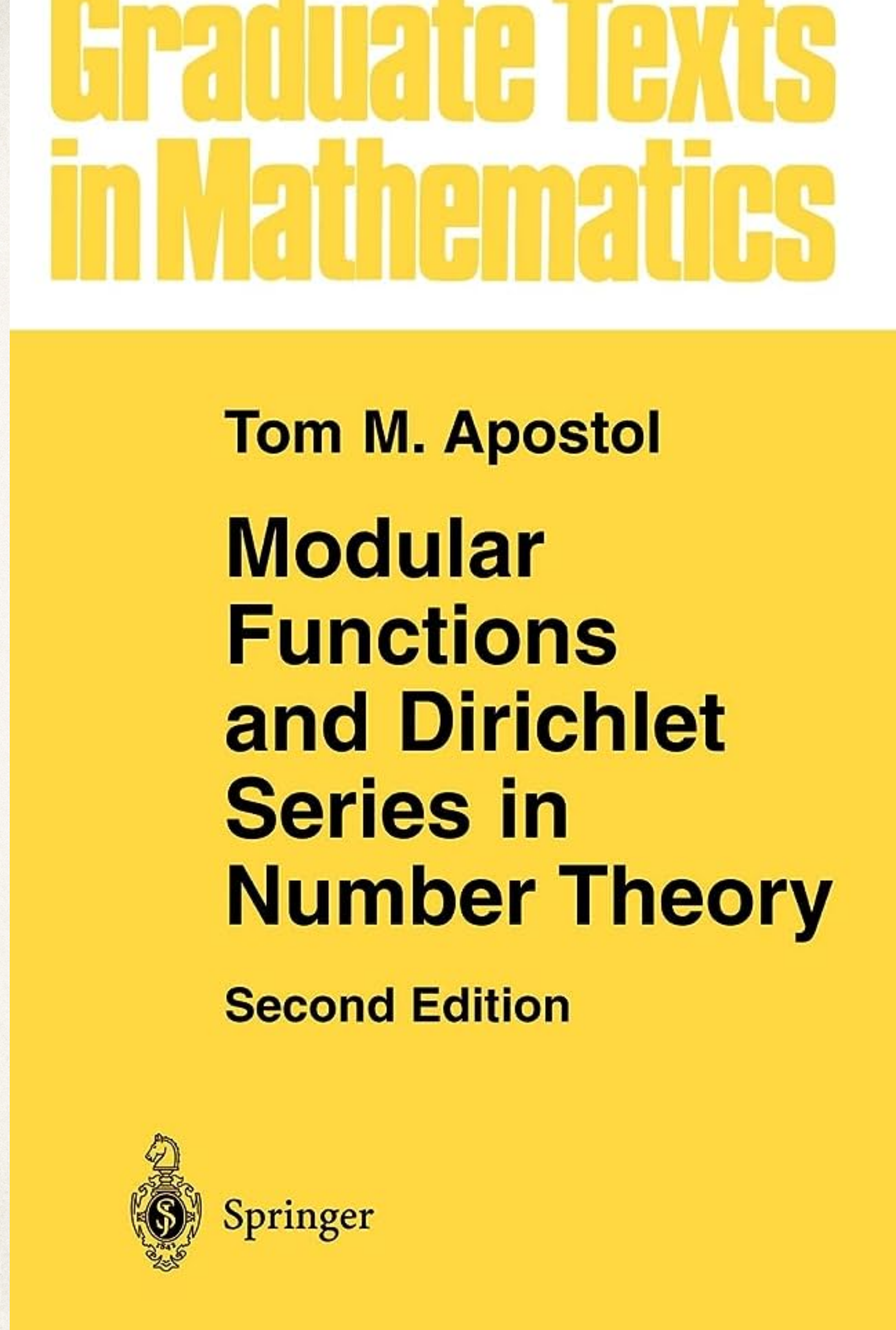
$\omega$-categories

*Aiming for variety; trying to test the limits*

# Number theory *(why not?)*

- Elliptic and modular functions
- The Dedekind eta function
- Approximation theorems (Kronecker's and others)
- The Riemann zeta function

*Lots of advanced material*



## 7.2 Dirichlet's approximation theorem

**Theorem 7.1.** *Given any real $\theta$ and any positive integer $N$, there exist integers $h$ and $k$ with $0 < k \leq N$ such that*

$$|k\theta - h| < \frac{1}{N}. \tag{1}$$

PROOF. Let $\{x\} = x - [x]$ denote the fractional part of $x$. Consider the $N + 1$ real numbers

$$0, \{\theta\}, \{2\theta\}, \ldots, \{N\theta\}.$$

All these numbers lie in the half open unit interval $0 \leq \{m\theta\} < 1$. Now divide the unit interval into $N$ equal half-open subintervals of length $1/N$. Then some subinterval must contain at least two of these fractional parts, say $\{a\theta\}$ and $\{b\theta\}$, where $0 \leq a < b \leq N$. Hence we can write

$$|\{b\theta\} - \{a\theta\}| < \frac{1}{N}. \tag{2}$$

But

$$\{b\theta\} - \{a\theta\} = b\theta - [b\theta] - a\theta + [a\theta] = (b - a)\theta - ([b\theta] - [a\theta]).$$

Therefore if we let

$$k = b - a \qquad \text{and} \qquad h = [b\theta] - [a\theta]$$

inequality (2) becomes

$$|k\theta - h| < \frac{1}{N}, \quad \text{with } 0 < k \leq N.$$

This proves the theorem. $\square$

- Unfortunately, the **simultaneous** version turned out to be necessary: approximate $\theta_1, \ldots, \theta_n$ as $|k\theta_i - h_i| < \dfrac{1}{N}$ where $k \leq N^n$.

- Proof obtained from Hardy and Wright, *An Introduction to the Theory of Numbers*.

- Still, an elementary proof by the pigeon hole principle, easily formalised (**almost** on a single slide!)

```
theorem Dirichlet_approx_simult:
  fixes ϑ :: "nat ⇒ real" and N n :: nat
  assumes "N > 0"
  obtains q p where "0<q" "q ≤ int (N^n)" and "⋀i. i<n ⟹ ¦of_int q * ϑ i - of_int(p i)¦ < 1/N"
proof -
  have lessN: "nat ⌊x * real N⌋ < N" if "0 ≤ x" "x < 1" for x
  proof -
    have "⌊x * real N⌋ < N"
      using that by (simp add: assms floor_less_iff)
    with assms show ?thesis by linarith
  qed
  define interv where "interv ≡ λk. {real k/N..< Suc k/N}"
  define fracs where "fracs ≡ λk. map (λi. frac (real k * ϑ i)) [0..<n]"
  define X where "X ≡ fracs ` {..N^n}"
  define Y where "Y ≡ set (List.n_lists n (map interv [0..<N]))"
  have interv_iff: "interv k = interv k' ⟷ k=k'" for k k'
    using assms by (auto simp: interv_def Ico_eq_Ico divide_strict_right_mono)
  have in_interv: "x ∈ interv (nat ⌊x * real N⌋)" if "x≥0" for x
    using that assms by (simp add: interv_def divide_simps) linarith
  have False
    if non: "∀a b. b ≤ N^n ⟶ a < b ⟶ ¬(∀i<n. ¦frac (real b * ϑ i) - frac (real a * ϑ i)¦ < 1/N)"
  proof - [35 lines]
  qed
  then obtain a b where "a<b" "b ≤ N^n" and *: "⋀i. i<n ⟹ ¦frac (real b * ϑ i) - frac (real a * ϑ i)¦ < 1/N"
    by blast
  let ?k = "b-a"
  let ?h = "λi. ⌊b * ϑ i⌋ - ⌊a * ϑ i⌋"
  show ?thesis
  proof
    fix i
    assume "i<n"
    have "frac (b * ϑ i) - frac (a * ϑ i) = ?k * ϑ i - ?h i"
      using ‹a < b› by (simp add: frac_def left_diff_distrib' of_nat_diff)
    then show "¦of_int ?k * ϑ i - ?h i¦ < 1/N"
      by (metis "*" ‹i < n› of_int_of_nat_eq)
  qed (use ‹a < b› ‹b ≤ N^n› in auto)
qed
```

# The chapter continues …

- refinements to Dirichlet's approximation theorem
- Liouville's approximation theorem (done elsewhere)
- Kronecker's approximation theorem
- … and the simultaneous version of Kronecker
- Advanced examples, e.g. to *periodic functions*

**Theorem 7.13.** *If $f$ has three periods $\omega_1, \omega_2, \omega_3$ which are linearly independent over the integers, then $f$ has arbitrarily small nonzero periods.*

PROOF. Suppose first that $\omega_2/\omega_1$ is real. If $\omega_2/\omega_1$ is rational then $\omega_1$ and $\omega_2$ are linearly dependent over the integers, hence $\omega_1, \omega_2, \omega_3$ are also dependent, contradicting the hypothesis. If $\omega_2/\omega_1$ is irrational, then $f$ has arbitrarily small nonzero periods by Theorem 7.12.

Now suppose $\omega_2/\omega_1$ is not real. Geometrically, this means that $\omega_1$ and $\omega_2$ are not collinear with the origin. Hence $\omega_3$ can be expressed as a linear combination of $\omega_1$ and $\omega_2$ with real coefficients, say

$$\omega_3 = \alpha\omega_1 + \beta\omega_2, \quad \text{where } \alpha \text{ and } \beta \text{ are real.}$$

Now we consider three cases:

(a) Both $\alpha$ and $\beta$ rational.
(b) One of $\alpha$, $\beta$ rational, the other irrational.
(c) Both $\alpha$ and $\beta$ irrational.

Case (a) implies $\omega_1, \omega_2, \omega_3$ are dependent over the integers, contradicting the hypothesis.

For case (b), assume $\alpha$ is rational, say $\alpha = a/b$, and $\beta$ is irrational. Then we have

$$\omega_3 = \frac{a}{b}\omega_1 + \beta\omega_2, \qquad \text{so} \qquad b\omega_3 - a\omega_1 = \beta(b\omega_2).$$

This gives us two periods $b\omega_3 - a\omega_1$ and $b\omega_2$ with irrational ratio, hence $f$ has arbitrarily small periods. The same argument works, of course, if $\beta$ is rational and $\alpha$ is irrational.

Now consider case (c), both $\alpha$ and $\beta$ irrational. Here we consider two subcases.

# Oops!

- Unfortunately, Apostol set things up for Kronecker's theorem when actually he needed Dirichlet's
- Despite including a redundant case analysis, he *didn't* establish the preconditions for Kronecker's theorem
- … and he hadn't bothered to present Dirichlet's in its simultaneous form

```
theorem
  fixes f:: "complex ⇒ complex" and ω1 ω2 ω3:: complex
  assumes ω: "is_periodic ω1 f" "is_periodic ω2 f" "is_periodic ω3 f"
    and indp: "module.independent (λr. (*) (complex_of_int r)) {ω1,ω2,ω3}"
    and dist: "distinct [ω1,ω2,ω3]"
    and "ε > 0"
  obtains ω where "is_periodic ω f" "0 < cmod ω" "cmod ω < ε"
proof -
  interpret C: Modules.module "(λr. (*) (complex_of_int r))"
    by (simp add: Modules.module.intro distrib_left mult.commute)
  have nz: "ω1 ≠ 0" "ω2 ≠ 0" "ω3 ≠ 0"
    using indp C.dependent_zero by force+
  show thesis
  proof (cases "ω2/ω1 ∈ ℝ") [16 lines]
  next
    case False
    then obtain α β where αβ: "ω3 = of_real α * ω1 + of_real β * ω2"
      using complex_is_Real_iff gen_lattice.ω1ω2_decompose gen_lattice.intro by blast
    show ?thesis
    proof (cases "α ∈ ℚ")
      case True
      then obtain m1 n1 where mn1: "α = of_int m1 / of_int n1" and "n1 > 0"
        by (meson Rats_cases')
      show ?thesis
      proof (cases "β ∈ ℚ")
        case True
        then obtain m2 n2 where mn2: "β = of_int m2 / of_int n2" and "n2 > 0"
          by (meson Rats_cases')
        have "of_int(m1*n2)*ω1 + of_int(m2*n1)*ω2 + of_int(-n1*n2)*ω3 = 0"
          using αβ ‹n1 > 0› ‹n2 > 0› by (simp add: mn1 mn2 add_frac_eq)
        then have "C.dependent {ω1,ω2,ω3}" [5 lines]
        with indp show ?thesis
          by blast
      next
        case False
        define ω where "ω ≡ n1 * ω3 - m1 * ω1"
        have "ω = β * (n1 * ω2)"
          using ‹n1 > 0› by (simp add: ω_def αβ mn1 algebra_simps)
        moreover have "is_periodic ω f" "is_periodic (n1 * ω2) f"
          by (simp_all add: ω ω_def is_periodic_diff is_periodic_times_int)
        ultimately show ?thesis
          using that ‹β ∉ ℚ› nz ‹0 < n1› ‹ε > 0› small_periods_real_irrational [of "n1*ω2" f ω ε]
          by auto
      qed
```

- This first part covers when $\omega_2/\omega_1$ is real, and if not obtains real $\alpha$ and $\beta$ where $\omega_3 = \alpha\omega_1 + \beta\omega_2$.
- Then it considers whether $\alpha$ (or $\beta$) is rational.
- In the final case, both are irrational and there is a big calculation using Dirichlet's approximation theorem

```
      case False
      show ?thesis
      proof (cases "β ∈ ℚ") [11 lines]
      next
        case False
        show ?thesis
        proof -
          define ϑ where "ϑ ≡ case_nat α (λ_. β)"
          define δ where "δ ≡ ε / (1 + cmod ω1 + cmod ω2)"
          have "δ > 0"
            by (smt (verit, best) δ_def ‹ε > 0› divide_pos_pos norm_not_less_zero)
          obtain N where N: "1 / real N < δ" and "N>0"
            by (meson ‹0 < δ› nat_approx_posE zero_less_Suc)
          then obtain k q where kh: "⋀i. i < 2 ⟹ ¦of_int k * ϑ i - of_int (q i)¦ < δ" and "0 < k"
            by (metis Dirichlet_approx_simult[of N 2 ϑ] less_trans)
          define h1 where "h1 ≡ q 0" define h2 where "h2 ≡ q 1"
          have "cmod (k * α * ω1 - h1 * ω1) = cmod (k * α - h1) * cmod ω1"
            by (metis left_diff_distrib norm_mult of_real_diff of_real_of_int_eq)
          also have "… = abs (k * α - h1) * cmod ω1"
            by (metis norm_of_real)
          also have "… < δ * cmod ω1"
            using kh [of 0] by (simp add: ϑ_def nz h1_def)
          finally have 1: "norm (k * α * ω1 - h1 * ω1) < δ * cmod ω1" .
          have "cmod (k * β * ω2 - h2 * ω2) = cmod (k * β - h2) * cmod ω2"
            by (metis left_diff_distrib norm_mult of_real_diff of_real_of_int_eq)
          also have "… = abs (k * β - h2) * cmod ω2"
            by (metis norm_of_real)
          also have "… < δ * cmod ω2"
            using kh [of 1] by (simp add: ϑ_def nz h2_def)
          finally have 2: "cmod (k * β * ω2 - h2 * ω2) < δ * cmod ω2" .
          define ω where "ω ≡ k * ω3 - h1 * ω1 - h2 * ω2"
          have "ω = (k * α * ω1 - h1 * ω1) + (k * β * ω2 - h2 * ω2)"
            by (simp add: ω_def αβ algebra_simps)
          then have "cmod ω ≤ cmod(k * α * ω1 - h1 * ω1) + cmod(k * β * ω2 - h2 * ω2)"
            using norm_triangle_ineq by blast
          also have "… <  δ * cmod ω1 +  δ * cmod ω2"
            using "1" "2" by linarith
          also have "… < ε"
            using ‹ε > 0› nz
            by (simp add: δ_def divide_simps) (auto simp add: distrib_left pos_add_strict)
          finally have "cmod ω < ε" .
          have "is_periodic ω f"
            by (simp add: ω ω_def is_periodic_diff is_periodic_times_int)
          moreover have "ω ≠ 0" [9 lines]
          ultimately show ?thesis
            by (simp add: ‹cmod ω < ε› that)
        qed
      qed
    qed
  qed
qed
```

# Apostol's application to the Riemann zeta function

- Obtaining the inf and sup of $|\zeta(\sigma + it)|$ where $\sigma$ is held constant
- Apostol's proof contains a circularity that I broke with the help of an elaborate argument from *MathOverflow*
- You also need to understand that $s$ is synonymous with $\sigma + it$ *(except when it isn't)*

**Definition.** For fixed $\sigma$, we define

$$m(\sigma) = \inf_t |\zeta(\sigma + it)| \qquad \text{and} \qquad M(\sigma) = \sup_t |\zeta(\sigma + it)|,$$

where the infimum and supremum are taken over all real $t$.

**Theorem 7.11.** *For each fixed $\sigma > 1$ we have*

$$M(\sigma) = \zeta(\sigma) \qquad \textit{and} \qquad m(\sigma) = \frac{\zeta(2\sigma)}{\zeta(\sigma)}.$$

PROOF. For $\sigma > 1$ we have $|\zeta(\sigma + it)| \le \zeta(\sigma)$ so $M(\sigma) = \zeta(\sigma)$, the supremum being attained on the real axis. To obtain the result for $m(\sigma)$ we estimate the reciprocal $|1/\zeta(s)|$. For $\sigma > 1$ we have

$$\left|\frac{1}{\zeta(s)}\right| = \prod_p |1 - p^{-s}| \le \prod_p (1 + p^{-\sigma}) = \frac{\zeta(\sigma)}{\zeta(2\sigma)}. \tag{17}$$

Hence $|\zeta(s)| \ge \zeta(2\sigma)/\zeta(\sigma)$ so $m(\sigma) \ge \zeta(2\sigma)/\zeta(\sigma)$.

Now we wish to prove the reverse inequality $m(\sigma) \le \zeta(2\sigma)/\zeta(\sigma)$. The idea is to show that the inequality

$$|1 - p^{-s}| \le 1 + p^{-\sigma}$$

used in (17) is very nearly an equality for certain values of $t$. Now

$$1 - p^{-s} = 1 - p^{-\sigma - it} = 1 - p^{-\sigma}e^{-it\log p} = 1 + p^{-\sigma}e^{i(-t\log p - \pi)},$$

so we need to show that $-t \log p - \pi$ is nearly an even multiple of $2\pi$ for certain values of $t$. For this we invoke Kronecker's theorem. Of course, there are infinitely many terms in the Euler product for $1/\zeta(s)$ and we cannot expect to make $-t \log p - \pi$ nearly an even multiple of $2\pi$ for *all* primes $p$. But we will be able to do this for enough primes to obtain the desired inequality.

```
theorem Inf_7_11:
  fixes σ:: real
  assumes "σ > 1"
  shows "(INF t. cmod (zeta(Complex σ t))) = Re (zeta (2 * σ)) / Re (zeta σ)" (is "Inf ?F = ?rhs")
proof (intro antisym)
  show rhs_le_INFF: "?rhs ≤ Inf ?F"
    by (metis Complex_eq UNIV_I empty_iff norm_zeta_same_Im_ge [OF assms] cINF_greatest)
  interpret Modules.module "(λr. (*) (real_of_int r))"
    by (simp add: Modules.module.intro distrib_left mult.commute)
  define pr where "pr ≡ enumerate {p::nat. prime p}"
    — ‹enumeration of the primes, starting from 0 (not 1 as in the text)›
  have [simp]: "strict_mono pr"
    by (simp add: pr_def primes_infinite strict_mono_enumerate)
  have prime_iff: "prime n ⟷ (∃k. n = pr k)" for n
    using enumerate_Ex enumerate_in_set pr_def primes_infinite by blast
  then have pnp: "prime (pr k)" for k
    using prime_iff by blast
  then have pr_gt1: "real (pr k) > 1" for k
    by (metis of_nat_1 of_nat_less_iff prime_gt_1_nat)
  have pr_gt: "n < pr n" for n [9 lines]
  define ϑ where "ϑ ≡ λk. - ln (pr k) / (2 * pi)"
  have "inj pr"
    by (simp add: strict_mono_imp_inj_on)
  then have injϑ: "inj ϑ"
    by (auto simp: inj_on_def ϑ_def pnp prime_gt_0_nat)
  have [simp]: "pr 0 = 2"
    by (simp add: pr_def enumerate.simps Least_equality prime_ge_2_nat)
  have prod_if_prime_eq: "(∏p≤pr n. if prime p then w p else 1) = (∏k≤n. w (pr k))" (is "?L=?R") [12 lines]
  have prod_if_prime_eq_real: "(∏p≤pr n. if prime p then w p else 1) = (∏k≤n. w (pr k))"  [9 lines]
  have zeta_nz: "zeta (Complex σ t) ≠ 0" for t
    using assms complex.sel(1) zeta_Re_gt_1_nonzero by presburger
  then obtain zeta_pos: "Re (zeta σ) > 0" "Re (zeta (of_real σ * 2)) > 0"
    by (smt (verit) Complex_eq Re_complex_of_real assms complex_of_real_def mult_2_right
           norm_zeta_same_Im_le of_real_add zero_less_norm_iff zeta_Re_gt_1_nonzero)
  then have rhs_pos: "?rhs > 0"
    by (auto simp: field_simps)
  with rhs_le_INFF have INFF_pos: "Inf ?F > 0"
    by linarith
```

- Here we see only the boilerplate from the first part of this 400 line proof.
- The main part is the calculation of the required *t*, including the removal of the circular dependence
- Apostol is good at conveying general ideas, but terrible with details
- … let's see some examples from Chapter 1

# Three trivial proofs

**Theorem 1.5.** *If an elliptic function f has no zeros in some period parallelogram, then f is constant.*

PROOF. Apply Theorem 1.4 to the reciprocal $1/f$. $\square$

Over 60 lines of dense calculations

**Theorem 1.6.** *The contour integral of an elliptic function taken along the boundary of any cell is zero.*

PROOF. The integrals along parallel edges cancel because of periodicity. $\square$

Over 100 lines

**Theorem 1.7.** *The sum of the residues of an elliptic function at its poles in any period parallelogram is zero.*

PROOF. Apply Cauchy's residue theorem to a cell and use Theorem 1.6. $\square$

Nearly 200 lines

# Remarks and conclusions

- We did chapters 1–3 and 7.
- The material is straightforward to formalise, once you understand the conventions
- … but errors and gaps waste lots of time.
- Expertise in the field you're formalising is necessary!