

The Irrationality of $\zeta(5)$

Alex Hyman

October 29, 2026

Abstract

We formalise the proof that $\zeta(5)$ is irrational from A. Fauzan’s 2026 preprint [2], following the Lean 4/Mathlib formalisation by domino14 [1], of which this entry is a port. The argument builds integer polynomials Q_n with $0 < Q_n(\zeta(5)) < e^{-cn^2}$ as Hankel determinants of a rational functional: a positive moment representation of $\zeta(5)$ gives positivity, p -adic estimates through unimodular bases in two prime ranges and a uniform asymptotic for the valuations give the integrality factor, and a logarithmic-energy estimate for an explicit measure gives the archimedean bound, proving irrationality. The main theorem is $\text{zeta } 5 \notin \mathbb{Q}$ for the *zeta* of the entry `Zeta_Function`; the only oracle is *holds*, from the 72 numeric inequalities discharged by *approximation*. The port is not literal: Lean’s dependently typed *Fin* n matrices and Σ -indexed bases become `Jordan_Normal_Form` matrices over explicit index lists, and the p -adic field $\mathbb{Q}_p$ is replaced by truncated rational series with congruences modulo powers of p , so that the whole development lives in `HOL` over $\mathbb{Q}$ without `Types-To-Sets`; Lean’s kernel computation on 1052 dyadic intervals becomes *approximation* with splitting.

Thirteen theories are independent of the proof and reusable: a calculus for lower bounds on p -adic valuations of rationals and polynomials with a mod- p unimodularity criterion (*unimodular_criterion*), the Vandermonde determinant for `Jordan_Normal_Form` matrices (*det_vandermonde_jnf*) and positivity of Gram determinants, Riemann-sum limits (*outer_prime_sum_bound*) of sums over primes from the prime number theorem, the log-sine integral and the circle average of $\ln|z - a|$ (*ln_sin_integral*, *circle_avg_log*), the arcsine law and its potential (*arcsine_potential*), Andréief’s identity for σ -finite measures (*andreief*), and the zero-mass logarithmic energy inequality on $\mathbb{C}$ (*log_energy_zero_mass_nonpos*).

The port was an experiment in AI proof engineering: an orchestration model (Claude Fable 5.1) wrote Isar skeletons with fact hints, proof agents (Claude Opus 5.5) closed about 1,100 leaves interactively in Isabelle/jEdit, and automated scripts harvested *try0* and *sledgehammer* results to reduce context load on the agents. The problem was chosen because its final statement is short and is expressed with

existing AFP definitions, so the result is easy to audit. The formalisation effort spanned 3 days of continuous work with a fair amount of human intervention to keep Fable and the agents on track, give them Isabelle-related hints, insist on legible proofs, and oversee the structure of the project. The author has audited the files and takes full responsibility for their contents.

Relation to the Lean formalisation

The definitions, statements and proof structure follow the Lean project theory by theory (each Isabelle theory names its Lean counterparts). The main departures:

- The p -adic field $\mathbb{Q}_p$ of the paper’s Sections 3.1–3.2 is not constructed. Every p -adically convergent series is replaced by its length- M partial sum (the `__tr` definitions) and the identities become congruences modulo powers of p , so the development stays in HOL over $\mathbb{Q}$ without Types-To-Sets (theories `Zeta5_Truncated_Expansions`, `Zeta5_Pole_Distribution`).
- Lean’s *Fin* n matrices and Σ -indexed bases become `Jordan_Normal_Form` matrices with explicit index lists (`inner_idx`, `outer_idx`); dependent types were never needed, only bookkeeping.
- Lean checks the potential inequality (A.9) by kernel computation on 1052 dyadic intervals; here it is 52 region lemmas by *approximation* with splitting, and the 16 energy enclosures (A.10) are per-term *approximation* runs after rescaling the logarithms into $[1, 2)$.
- Mathlib facts with no HOL/AFP counterpart were proved from scratch and are the general theories listed in the abstract; the moment representation (Proposition 2.2) is derived from the Laplace transform of $\sin$ and the cotangent partial-fraction formula of the AFP rather than from a Hurwitz-zeta integral, the prime number theorem is the AFP’s (*var asymptotics*), the von Staudt–Clausen facts come from the entry `Bernoulli`, and the rational valuations from `Kummer_Congruence`.
- The zero-mass energy inequality (Lemma 6.2) is stated with explicit hypotheses (a finite dominating measure with $\ln|z - w|$ integrable on the product and a null diagonal), which is what the paper’s “finite energy, compact support” has to mean for signed measures.

Contents

1	A calculus for lower bounds on p-adic valuations of rationals and polynomials	8
----------	---	----------

1.1	Definitions	8
1.2	Basic closure properties	8
1.3	The ultrametric inequality for <i>qmultiplicity</i> (not in the AFP)	9
1.4	Valuations of powers and products	11
2	Vandermonde and Gram determinants for JNF matrices	12
3	Taylor coefficients of a rational polynomial at a point	13
4	Determinants of p-integral matrices and a unimodularity criterion	14
5	Legendre's formula for the p-adic valuation of $n!$	15
6	Riemann-sum limits of sums over primes from the prime number theorem	16
6.1	Chebyshev's ϑ over cells	16
6.2	Small primes: $\psi - \vartheta$ and the valuation of 24	17
6.3	Step majorants on a uniform partition	18
6.4	Dominated convergence for the majorants	20
6.5	The Riemann-sum bounds	21
7	Interval integrals of piecewise polynomial and rational functions	22
7.1	Generic piece lemmas	22
8	Gamma-type integrals, the Laplace transform of $\sin$ and the $\coth$ series	24
8.1	Gamma integrals and the interchange of $\int$ and $\sum$	24
8.2	The S -series and the Laplace transform of $\sin$	26
8.3	The pole integral	27
9	Substitutions in interval integrals with finite endpoints	28
10	The log-sine integral and circle averages of $\ln z - a$	30
11	The arcsine distribution and its logarithmic potential	32
11.1	The arcsine measure	33
12	Logarithmic energy of measures on $\mathbb{C}$ and the zero-mass energy inequality	36
13	Andreief's identity (continuous Cauchy–Binet)	42

14 Definitions of the construction	43
14.1 Generic helpers	44
14.2 Section 2.1 Parameters (2.1)	44
14.3 Section 2.1 The functional μ_X (2.2), (2.3)	44
14.4 Section 2.1 The matrix, determinant and normalisation (2.4), (2.5)	45
14.5 Section 3 The functional τ_X	45
14.6 Section 3.1-3.2 The p -adic extension, in truncated rational form	46
14.7 Section 3.3 Small primes	48
14.8 Section 4.1 The inner range	48
14.9 Section 4.2 The outer range	50
14.10 Section 5 Normalisation (5.1), (5.2), (2.6)	51
14.11 Section 5.1-5.3 Limiting functions (real-valued; Lean names- pace <i>Lim</i>)	52
14.12 Section 6 The real determinant	54
15 The functionals μ_X and τ_X: algebra and partial fractions	55
15.1 Linearity	55
15.2 Well-definedness: common factors cancel	56
15.3 Partial fractions (Lagrange decomposition)	57
15.4 (3.1) The pullback identity	58
15.5 τ on polynomials	58
15.6 (3.1) The pullback identity: proof	59
16 Integer-valued polynomials and the bound (3.9)	62
16.1 Binomial polynomials	62
16.2 The coefficients of $\text{binom}(x, n)$	64
16.3 Newton interpolation	64
16.4 (3.9) and (3.8)	65
17 The far-pole constant and Lemma 3.3	66
17.1 Bernoulli valuations (von Staudt-Clausen, from the AFP) . .	66
17.2 Section 3.1 The far-pole constant C_p	67
17.3 Section 3.3 Lemma 3.3 and the small-prime bound	68
17.4 Counting multiples in an interval	68
17.5 Valuations of integers as counts	69
17.6 Partial fractions with linear poles	70
17.7 Valuations of integers	70
17.8 The product-difference estimate	71
17.9 Lemma 3.3	71

18 The small-prime bound (3.12)	72
18.1 Section 3.3 Integer-valued basis polynomials	72
18.2 The determinant identity (3.11)	74
18.3 The small-prime bound (3.12)	75
19 The truncated p-adic layer and Lemma 3.1	76
19.1 Truncated expansions of $1/(z - s)$ as polynomials	76
19.2 The near residues	78
19.3 The analytic part	79
19.4 Lemma 3.1 with far poles, truncated rational form	81
20 The distribution formula (3.7) and Lemma 3.2	82
20.1 Raabe's multiplication formula	82
20.2 Harmonic increments and the pole sums	83
20.3 The pole values of $\tau^{\widehat{\{ext\}}}$ - Y on the distributed poles	84
20.4 Partial fractions and the substitution $x = a + p z$	84
20.5 Lemma 3.2	85
21 The inner range: Proposition 4.1	85
21.1 Section 4.1 The inner range	86
21.2 Extracting powers of p from $g(c + p z)$	88
21.3 The inner entry bounds (4.2)/(4.3)	90
22 The outer range: Lemma 4.2 and Proposition 4.3	95
22.1 Section 4.2 The outer range	96
22.2 The modified functional $\mu^{\widehat{0-X}}$ and the structure of the outer basis	98
22.3 Arithmetic of the pole classes	100
22.4 Valuations at the poles	101
22.5 The two small poles $a, p - a$	104
22.6 The zero class	105
22.7 The entry bound (4.12)	105
22.8 The closed form (4.14) of $\gamma^{\widehat{p-out}}$	106
22.9 Lemma 4.2	110
22.10 Proposition 4.3	111
22.11 Proposition 4.3 for $p > K$	115
23 The determinant construction and the moment representa- tion of $\zeta(5)$	117
23.1 (2.9): degree and leading coefficient of Δ - K	117
23.2 Proposition 2.2: the positive integral representation	119
23.3 Moments and the pole values	120
24 Exact rational constants	123

25 The uniform estimate (5.7) in the inner range	124
25.1 Floors and $v\text{-}p(S\text{-}K)$ in the inner range	125
25.2 The Riemann-sum identity for the z -integral	126
25.3 Exact class counts	127
25.4 The discrete decomposition of $\gamma\text{-}p\text{-}\widehat{in}$	127
25.5 Discrete sum versus the integral	129
25.6 The comparison functions	130
25.7 Assembly	131
26 The explicit integrals of Section 5	132
26.1 The closed form $R(x) = x F(x) + Q(x)$ (B.1), (5.13)	132
26.2 $\int_{-\{1/3\}}^{\{1/2\}} d(y) dy = 9/640$, the mean of P , and $ C < 16$	136
26.3 (5.10): $\int_{-\{1/3\}}^{\{2\lambda\}} \text{outerIntegrand} = I\text{-out}$ by 11 affine pieces	137
26.4 (5.18): $\int_{-\{3\}}^{\{20\}} R(x)/x^3 dx$ by 143 affine pieces	138
26.5 Integrability on $[3, \infty)$ and the tails (5.14)-(5.17)	150
26.6 Continuity off a countable set, and boundedness	155
27 Normalisation and the asymptotics of $Q_{K,M}$: Propositions 5.1 and 5.2	157
27.1 The small-prime sum	157
27.2 Standing hypotheses and integrality	157
27.3 Legendre's formula and the uniformity estimates	158
27.4 Proposition 5.1	158
27.5 The outer range of the uniformity estimate (Lean: Legendre5)	158
27.6 Exact integrals and tails	161
27.7 Prime sums via the prime number theorem	162
27.8 Continuity of the limiting functions off a countable set	163
27.9 Proposition 5.2 and (5.21)	163
28 The comparison measure ϱ and its logarithmic potential	165
28.1 Table 1	166
28.2 Elementary enclosures	168
28.3 (A.9): the potential inequality on the half-line	169
28.4 Ingredients of (6.9) that live here	170
29 Numeric enclosures: (A.9), (A.10) and Lemma 6.1	171
29.1 Elementary enclosures (A.10)	171
29.2 (A.9): the region check on $[0, 2]$	173
29.3 (6.9) ingredient	185

30 The archimedean bound: Proposition 6.3	185
30.1 (6.11) and Lemma 6.2	185
30.2 (6.12) and the one-coordinate bound	186
30.3 (6.9) The bound for every configuration	187
30.4 (6.14), (6.15) and Proposition 6.3	192
31 The main theorem: $\zeta(5)$ is irrational	194

```

theory Rational-Padic-Valuations
  imports Kummer-Congruence.Rat-Congruence Jordan-Normal-Form.Determinant
  HOL-Library.Log-Nat
begin

```

1 A calculus for lower bounds on p -adic valuations of rationals and polynomials

The p -adic valuation of a rational number is *qmultiplicity* from the AFP entry `Kummer_Congruence`. This theory provides the predicate *vge* p x b ($x = 0$ or $v_p(x) \geq b$) and its coefficientwise version *vpGge* p A b for polynomials (the Gauss valuation), together with their closure under sums, products, powers, polynomial evaluation, division by monic polynomials and the Leibniz terms of determinants, the ultrametric inequality for *qmultiplicity* (absent from the AFP), and the valuations of powers and products. Nothing here depends on the irrationality proof.

1.1 Definitions

The polynomial indeterminate.

abbreviation $pX :: \text{rat poly}$ **where** $pX \equiv \text{Polynomial.monom } 1 \ 1$

The p -adic valuation of a rational (Mathlib: *padicValRat*).

definition $vp :: \text{nat} \Rightarrow \text{rat} \Rightarrow \text{int}$ **where**
 $vp \ p \ x = \text{qmultiplicity } (\text{int } p) \ x$

$\lfloor \log_p n \rfloor$ (Mathlib's *Nat.log* $p \ n$; 0 for $n = 0$ or $p \leq 1$).

definition $\text{nat-log} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat}$ **where**
 $\text{nat-log } p \ n = \text{floorlog } p \ n - 1$

$x = 0 \vee b \leq v_p(x)$.

definition $vge :: \text{nat} \Rightarrow \text{rat} \Rightarrow \text{rat} \Rightarrow \text{bool}$ **where**
 $vge \ p \ x \ b \longleftrightarrow (x \neq 0 \longrightarrow b \leq \text{of-int } (vp \ p \ x))$

$v_p \hat{G}(A) \geq b$: every nonzero coefficient has valuation at least b .

definition $vpGge :: \text{nat} \Rightarrow \text{rat poly} \Rightarrow \text{rat} \Rightarrow \text{bool}$ **where**
 $vpGge \ p \ A \ b \longleftrightarrow (\forall i. \text{Polynomial.coeff } A \ i \neq 0 \longrightarrow b \leq \text{of-int } (vp \ p \ (\text{Polynomial.coeff } A \ i)))$

1.2 Basic closure properties

lemma *prime-multiplicity-prime*:
fixes $p \ q :: 'a :: \text{factorial-semiring}$
assumes $\text{prime } p \ \text{prime } q$

shows $\text{multiplicity } p \ q = (\text{if } p = q \text{ then } 1 \text{ else } 0)$
 $\langle \text{proof} \rangle$

lemma *vge-zero*: $\text{vge } p \ 0 \ b \ \langle \text{proof} \rangle$

lemma *vge-mono*: $\text{vge } p \ x \ b \implies b' \leq b \implies \text{vge } p \ x \ b'$
 $\langle \text{proof} \rangle$

1.3 The ultrametric inequality for *qmultiplicity* (not in the AFP)

lemma *qmultiplicity-power-int*:

assumes *prime* p

shows $\text{qmultiplicity } (\text{int } p) \ (\text{of-nat } p \ \text{powi } k) = k$

$\langle \text{proof} \rangle$

lemma *qmultiplicity-nonneg-add*:

assumes *prime* p $0 \leq \text{qmultiplicity } (\text{int } p) \ x$ $0 \leq$

$\text{qmultiplicity } (\text{int } p) \ y$ $x + y \neq 0$

shows $0 \leq \text{qmultiplicity } (\text{int } p) \ (x + y)$

$\langle \text{proof} \rangle$

lemma *qmultiplicity-add-ge*:

assumes *prime* p $x \neq 0$ $y \neq 0$ $x + y \neq 0$

shows $\min (\text{qmultiplicity } (\text{int } p) \ x) (\text{qmultiplicity } (\text{int } p) \ y) \leq$

$\text{qmultiplicity } (\text{int } p) \ (x + y)$

$\langle \text{proof} \rangle$

lemma *vge-add*:

assumes *prime* p $\text{vge } p \ x \ b$ $\text{vge } p \ y \ b$

shows $\text{vge } p \ (x + y) \ b$

$\langle \text{proof} \rangle$

lemma *vge-neg*: $\text{vge } p \ x \ b \implies \text{vge } p \ (- \ x) \ b \ \langle \text{proof} \rangle$

lemma *vge-sum*:

assumes *prime* p *finite* I $\bigwedge i. i \in I \implies \text{vge } p \ (f \ i) \ b$

shows $\text{vge } p \ (\sum i \in I. f \ i) \ b$

$\langle \text{proof} \rangle$

lemma *vge-mul*:

assumes *prime* p $\text{vge } p \ x \ a$ $\text{vge } p \ y \ b$

shows $\text{vge } p \ (x * y) \ (a + b)$

$\langle \text{proof} \rangle$

lemma *vge-one*: $\text{vge } p \ 1 \ 0 \ \langle \text{proof} \rangle$

lemma *vge-pow*: $\text{prime } p \implies \text{vge } p \ x \ 0 \implies \text{vge } p \ (x \wedge^n) \ 0$

$\langle \text{proof} \rangle$

lemma *vge-inv-p*: $\text{prime } p \implies \text{vge } p \ (1 / \text{of-nat } p) \ (- \ 1)$

$\langle \text{proof} \rangle$

lemma *vge-of-int*: $\text{prime } p \implies \text{vge } p \ (\text{of-int } n) \ 0 \ \langle \text{proof} \rangle$

lemma *vpGge-iff*: $\text{vpGge } p \ A \ b \longleftrightarrow (\forall i. \text{vge } p \ (\text{Polynomial.coeff } A \ i) \ b)$

$\langle \text{proof} \rangle$
lemma *vpGge-zero*: $\text{vpGge } p \ 0 \ b \ \langle \text{proof} \rangle$
lemma *vpGge-mono*: $\text{vpGge } p \ A \ b \implies b' \leq b \implies \text{vpGge } p \ A \ b'$
 $\langle \text{proof} \rangle$
lemma *vpGge-add*: $\text{prime } p \implies \text{vpGge } p \ A \ b \implies$
 $\text{vpGge } p \ B \ b \implies \text{vpGge } p \ (A + B) \ b \ \langle \text{proof} \rangle$
lemma *vpGge-neg*: $\text{vpGge } p \ A \ b \implies \text{vpGge } p \ (-A) \ b \ \langle \text{proof} \rangle$
lemma *vpGge-sum*:
assumes $\text{prime } p \ \text{finite } I \ \bigwedge i. i \in I \implies \text{vpGge } p \ (f \ i) \ b$
shows $\text{vpGge } p \ (\sum i \in I. f \ i) \ b$
 $\langle \text{proof} \rangle$
lemma *vpGge-C*: $\text{vge } p \ c \ b \implies \text{vpGge } p \ [:c:] \ b$
 $\langle \text{proof} \rangle$
lemma *vpGge-one*: $\text{vpGge } p \ 1 \ 0 \ \langle \text{proof} \rangle$
lemma *vpGge-mul*: $\text{prime } p \implies \text{vpGge } p \ A \ a \implies$
 $\text{vpGge } p \ B \ b \implies \text{vpGge } p \ (A * B) \ (a + b)$
 $\langle \text{proof} \rangle$
lemma *vpGge-prod*:
assumes $\text{prime } p \ \text{finite } I \ \bigwedge i. i \in I \implies \text{vpGge } p \ (f \ i) \ (b \ i)$
shows $\text{vpGge } p \ (\prod i \in I. f \ i) \ (\sum i \in I. b \ i)$
 $\langle \text{proof} \rangle$

Determinant bound from entry bounds: if every Leibniz term has valuation at least B , so does the determinant (Lean: *vpGge-det-of-terms*). Proof via *Determinant.det-def'*.

lemma *vpGge-det-of-terms*:
assumes $\text{prime } p \ A \in \text{carrier-mat } n \ n$
and $\bigwedge \sigma. \sigma \text{ permutes } \{0..<n\} \implies$
 $\text{vpGge } p \ (\prod i = 0..<n. A \ \$\$ (i, \sigma \ i)) \ B$
shows $\text{vpGge } p \ (\text{Determinant.det } A) \ B$
 $\langle \text{proof} \rangle$

The intended content of *vpGge-div-monic*, with monicity written as *lead-coeff* $Q = 1$.

lemma *vpGge-div-lead1*:
assumes p : $\text{prime } p$ **and** $Q1$: $\text{lead-coeff } Q = 1$ **and** Qi : $\text{vpGge } p \ Q \ 0$
shows $\text{vpGge } p \ P \ 0 \implies \text{vpGge } p \ (P \text{ div } Q) \ 0$
 $\langle \text{proof} \rangle$

Division of an integral polynomial by an integral monic polynomial is integral (monicity written as *lead-coeff* $Q = 1$; *monic* is not a constant in the base image).

lemma *vpGge-div-monic*:
 $\text{prime } p \implies \text{vpGge } p \ P \ 0 \implies \text{lead-coeff } Q = 1 \implies$
 $\text{vpGge } p \ Q \ 0 \implies \text{vpGge } p \ (P \text{ div } Q) \ 0$
 $\langle \text{proof} \rangle$

lemma *vge-poly-eval*:

$prime\ p \implies vpGge\ p\ P\ 0 \implies vge\ p\ x\ 0 \implies$
 $vge\ p\ (poly\ P\ x)\ 0\ \langle proof \rangle$

1.4 Valuations of powers and products

lemma *vp-power-rat*:

assumes $prime\ p\ x \neq 0$
shows $vp\ p\ (x \wedge n) = int\ n * vp\ p\ x$
 $\langle proof \rangle$

lemma *vp-powi-rat*:

assumes $prime\ p\ x \neq 0$
shows $vp\ p\ (x\ powi\ k) = k * vp\ p\ x$
 $\langle proof \rangle$

lemma *vp-prod-rat*:

assumes $prime\ p\ finite\ I \wedge i. i \in I \implies f\ i \neq 0$
shows $vp\ p\ (\prod i \in I. f\ i) = (\sum i \in I. vp\ p\ (f\ i))$
 $\langle proof \rangle$

lemma *vpGge-C-vp*: $vpGge\ p\ [:c:] (of-int\ (vp\ p\ c))$
 $\langle proof \rangle$

Composition with powers and with the identity polynomial pX .

lemma *pcompose-power-left*: $pcompose\ (p \wedge n)\ q = (pcompose\ p\ q) \wedge n$ **for** $p\ q ::$
 $rat\ poly$
 $\langle proof \rangle$

lemma *pcompose-pX*: $pcompose\ pX\ q = q$
 $\langle proof \rangle$

$v\text{-}p(1/j) \geq -\lfloor \log\text{-}p\ j \rfloor$.

lemma *vge-inv-nat*: $prime\ p \implies 1 \leq j \implies$
 $vge\ p\ (1\ /\ of\text{-}nat\ j) (\text{-}\ of\text{-}nat\ (nat\text{-}log\ p\ j))$
 $\langle proof \rangle$

lemma *nat-log-mono*: $m \leq n \implies nat\text{-}log\ p\ m \leq nat\text{-}log\ p\ n$
 $\langle proof \rangle$

lemma *vge-prod0*: $prime\ p \implies finite\ I \implies$
 $(\wedge i. i \in I \implies vge\ p\ (f\ i)\ 0) \implies$
 $vge\ p\ (\prod i \in I. f\ i)\ 0$
 $\langle proof \rangle$

Strict ultrametric inequality: $v(a) < v(u) \implies v(a + u) = v(a)$.

lemma *vp-add-eq-of-lt*:

```

    prime p  $\implies$  a  $\neq$  0  $\implies$  u  $\neq$  0  $\implies$ 
      vp p a < vp p u  $\implies$  a + u  $\neq$  0  $\wedge$  vp p (a + u) = vp p a
  <proof>

end

```

```

theory Vandermonde-Gram-Determinants
imports Jordan-Normal-Form.Determinant
begin

```

2 Vandermonde and Gram determinants for JNF matrices

The Vandermonde determinant $\det(x_i^j) = \prod_{i < j} (x_j - x_i)$ for the matrices of the `Jordan_Normal_Form` library (HOL-Analysis has it only for its own matrix type, and the AFP not at all), the factorisation of row scalings out of a determinant, and the positivity of the determinant of a positive definite (Gram) matrix, proved by a homotopy to the identity.

Vandermonde determinant for `Jordan_Normal_Form` matrices (absent from HOL and the AFP).

```

lemma det-diag-scale-rows:
  fixes d y :: nat  $\Rightarrow$  'a :: comm-ring-1
  shows Determinant.det (Matrix.mat n n ( $\lambda(i, j).$  d i * y i  $\wedge$  j))
    = ( $\prod$  i < n. d i) * Determinant.det (Matrix.mat n n ( $\lambda(i, j).$  y i  $\wedge$  j))
  <proof>

```

```

lemma det-vandermonde-step:
  fixes x :: nat  $\Rightarrow$  'a :: comm-ring-1
  shows Determinant.det (Matrix.mat (Suc n) (Suc n) ( $\lambda(i, j).$  x i  $\wedge$  j))
    = ( $\prod$  i < n. x (Suc i) - x 0) * Determinant.det (Matrix.mat n n ( $\lambda(i, j).$  x (Suc i)  $\wedge$  j))
  <proof>

```

```

lemma det-vandermonde-jnf:
  Determinant.det (Matrix.mat n n ( $\lambda(i, j).$  (x i :: 'a :: comm-ring-1)  $\wedge$  j))
    = ( $\prod$  i < n.  $\prod$  j  $\in$  {j. i < j  $\wedge$  j < n}. x j - x i)
  <proof>

```

A Gram matrix of linearly independent functions has positive determinant (used for $\Delta\text{-}K(\zeta(5)) > 0$ unless the Andreief route is taken).

```

lemma posdef-det-nonzero:
  fixes B :: real mat
  assumes B: B  $\in$  carrier-mat n n
  and pd:  $\bigwedge c :: nat \Rightarrow real. (\exists i < n. c i \neq 0) \implies$ 
    0 < ( $\sum$  i < n.  $\sum$  j < n. c i * B $$ (i, j) * c j)
  shows Determinant.det B  $\neq$  0

```

$\langle \text{proof} \rangle$

lemma *posdef-det-pos*:

assumes $A \in \text{carrier-mat } n \ n$

and $\bigwedge c :: \text{nat} \Rightarrow \text{real}. (\exists i < n. c \ i \neq 0) \implies$

$0 < (\sum i < n. \sum j < n. c \ i * A \ \$\$ (i, j) * c \ j)$

shows $0 < \text{Determinant.det } A$

$\langle \text{proof} \rangle$

end

theory *Polynomial-Taylor-Shift*

imports *Rational-Padic-Valuations*

begin

3 Taylor coefficients of a rational polynomial at a point

$\text{tay } P \ r \ i$ is the coefficient of X^i in $P(X + r)$. Linearity, the binomial formula for monomials, the behaviour under multiplication by $(X - r)^n$, and p -integrality of the Taylor coefficients of a p -integral polynomial at a p -integral point.

The i -th Taylor coefficient of P at r : $P(X + r) = \sum -i \text{tay } P \ r \ i \ X^i$.

definition $\text{tay} :: \text{rat poly} \Rightarrow \text{rat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$\text{tay } P \ r \ i = \text{Polynomial.coeff } (\text{pcompose } P \ (pX + [:r:])) \ i$

lemma *tay-add*: $\text{tay } (P + Q) \ r \ i = \text{tay } P \ r \ i + \text{tay } Q \ r \ i$

$\langle \text{proof} \rangle$

lemma *tay-smult*: $\text{tay } (\text{Polynomial.smult } c \ P) \ r \ i = c * \text{tay } P \ r \ i$

$\langle \text{proof} \rangle$

lemma *tay-shift-lib*: $\text{pcompose } ((pX - [:r:]) \wedge^n * Q) \ (pX + [:r:]) =$

$\text{Polynomial.monom } 1 \ n * \text{pcompose } Q \ (pX + [:r:])$

$\langle \text{proof} \rangle$

lemma *tay-sum*: $\text{tay } (\sum d \in I. f \ d) \ r \ i = (\sum d \in I. \text{tay } (f \ d) \ r \ i)$

$\langle \text{proof} \rangle$

lemma *tay-pX-pow*: $\text{tay } (pX \wedge^d) \ r \ i = (\text{if } i \leq d \text{ then of-nat } (d \text{ choose } i) * r \wedge^{(d - i)} \text{ else } 0)$

$\langle \text{proof} \rangle$

lemma *tay-eq-sum*: $\text{degree } P < h \implies$

$\text{tay } P \ r \ i = (\sum d < h. \text{Polynomial.coeff } P \ d * \text{tay } (pX \wedge^d) \ r \ i)$

$\langle \text{proof} \rangle$

lemma *tay-0-eq-poly*: $\text{tay } P \ r \ 0 = \text{poly } P \ r$
 $\langle \text{proof} \rangle$

$(X - r)^{\wedge n} Q$ has vanishing Taylor coefficients of order $< n$ at r , and the shifted ones are those of Q .

lemma *tay-pow-mult*: $\text{tay } ((pX - [:r:])^{\wedge n} * Q) \ r \ (n + i) = \text{tay } Q \ r \ i$
 $\langle \text{proof} \rangle$

lemma *tay-pow-mult-lt*: $i < n \implies \text{tay } ((pX - [:r:])^{\wedge n} * Q) \ r \ i = 0$
 $\langle \text{proof} \rangle$

lemma *vpGge-pcompose*: $\text{prime } p \implies \text{vpGge } p \ P \ 0 \implies$
 $\text{vpGge } p \ Q \ 0 \implies \text{vpGge } p \ (\text{pcompose } P \ Q) \ 0$
 $\langle \text{proof} \rangle$

lemma *vge-tay*: $\text{prime } p \implies \text{vpGge } p \ P \ 0 \implies \text{vge } p \ r \ 0 \implies$
 $\text{vge } p \ (\text{tay } P \ r \ i) \ 0$
 $\langle \text{proof} \rangle$

end

theory *Unimodular-Determinants*
imports *Rational-Padic-Valuations*
begin

4 Determinants of p -integral matrices and a unimodularity criterion

The determinant of a matrix with p -integral entries is p -integral; modulo p the determinant of a matrix that is lower triangular modulo p is the product of its diagonal; hence if $M \ V = T$ with M, V p -integral and T lower triangular modulo p with unit diagonal, then $\det M$ is a p -adic unit. This is the tool behind the unimodularity of the inner and outer bases of the irrationality proof, but it is stated for arbitrary matrices.

The determinant of a matrix with p -integral entries is p -integral.

lemma *vge-det-integral*:
assumes $\text{prime } p \ A \in \text{carrier-mat } n \ n \ \bigwedge i \ j. \ i < n \implies$
 $j < n \implies \text{vge } p \ (A \ \$\$ \ (i, j)) \ 0$
shows $\text{vge } p \ (\text{Determinant.det } A) \ 0$
 $\langle \text{proof} \rangle$

A permutation of $\{0..<n\}$ that is not the identity moves some i downwards (stated for *nat*; a version with an unaxiomatised *ord* type would be false).

lemma *permutes-not-id-exists-lt-nat*:

```

fixes  $\sigma :: \text{nat} \Rightarrow \text{nat}$ 
assumes  $\sigma$  permutes  $\{0..<n\}$   $\sigma \neq \text{id}$ 
shows  $\exists i < n. \sigma i < i$ 
<proof>

```

Modulo p , the determinant of a matrix whose entries below the diagonal are divisible by p is the product of the diagonal.

lemma *det-cong-diag*:

```

assumes  $p$ : prime  $p$  and  $T$ :  $T \in \text{carrier-mat } n \ n$ 
and int:  $\bigwedge i \ j. i < n \implies j < n \implies \text{vge } p \ (T \ \$\$ \ (i, j)) \ 0$ 
and low:  $\bigwedge i \ j. j < i \implies i < n \implies \text{vge } p \ (T \ \$\$ \ (i, j)) \ 1$ 
shows  $\text{vge } p \ (\text{Determinant.det } T - (\prod i < n. T \ \$\$ \ (i, i))) \ 1$ 
<proof>

```

The unimodularity criterion: if $M V = T$ with M, V p -integral and T upper triangular modulo p with unit diagonal, then $\text{det } M$ is a p -adic unit.

lemma *unimodular-criterion*:

```

assumes  $p$ : prime  $p$  and  $M$ :  $M \in \text{carrier-mat } n \ n$  and  $V$ :  $V \in \text{carrier-mat } n \ n$ 
and Mi:  $\bigwedge i \ j. i < n \implies j < n \implies \text{vge } p \ (M \ \$\$ \ (i, j)) \ 0$ 
and Vi:  $\bigwedge i \ j. i < n \implies j < n \implies \text{vge } p \ (V \ \$\$ \ (i, j)) \ 0$ 
and low:  $\bigwedge i \ j. j < i \implies i < n \implies$ 
   $\text{vge } p \ ((M * V) \ \$\$ \ (i, j)) \ 1$ 
and diag:  $\bigwedge i. i < n \implies (M * V) \ \$\$ \ (i, i) \neq 0 \wedge$ 
   $\text{vp } p \ ((M * V) \ \$\$ \ (i, i)) = 0$ 
shows  $\text{Determinant.det } M \neq 0 \wedge \text{vp } p \ (\text{Determinant.det } M) = 0$ 
<proof>

```

end

theory *Legendre-Factorial-Valuation*

```

imports Rational-Padic-Valuations Prime-Number-Theorem.Prime-Counting-Functions
begin

```

5 Legendre's formula for the p -adic valuation of $n!$

$v_p(n!) = \sum_{a \geq 1} \lfloor n / p^a \rfloor$, derived from the Legendre identity of the AFP entry `Prime_Number_Theorem`, in the two forms used later: with the *legendre-aux* function of that entry and with an explicit finite range of summation.

Legendre's formula $v_p(n!) = \sum_{a \geq 1} \lfloor n / p^a \rfloor$; exists as *IMO2019-Q4.multiplicity-prime-fact* with *legendre-aux*.

lemma *legendre-fact*:

```

fixes  $p :: \text{nat}$ 
assumes prime  $p$ 
shows  $\text{multiplicity } p \ (\text{fact } n) = \text{legendre-aux } (\text{real } n) \ p$ 
<proof>

```

Legendre's formula with any upper limit $B \geq n$ on the sum.

lemma *legendre-sum*:

assumes *prime* p $n \leq B$

shows *multiplicity* p (*fact* n) = $(\sum_{a=1..B. n \text{ div } p \wedge a}$

<proof>

end

theory *Prime-Sum-Limits*

imports *Rational-Padic-Valuations Prime-Number-Theorem.Prime-Number-Theorem*
HOL-Real-Asymp.Real-Asymp

begin

6 Riemann-sum limits of sums over primes from the prime number theorem

From the prime number theorem in the form $\vartheta(x) \sim x$ (the AFP's *ϑ -asymptotics*): for a bounded function φ on $[a, b]$ that is continuous off a countable set, $\sum_{aK < p \leq bK} \varphi(p/K) \ln p \leq (\int_a^b \varphi + \varepsilon) K$ for all large K , and the version in the variable $x = K/p$. The proof uses Chebyshev's ϑ over the cells of a uniform partition, step majorants of φ and dominated convergence as the mesh goes to zero. Also the bookkeeping $\psi - \vartheta$ for the valuations of small primes.

The prime number theorem in the form used (from *Prime-Number-Theorem. ϑ -asymptotics*).

lemma *pnt-theta*: $((\lambda x. \text{primes-theta } x / x) \longrightarrow 1)$ *at-top*

<proof>

6.1 Chebyshev's ϑ over cells

$\vartheta(x) = \sum -\{p \leq x\} \log p$ as a sum over a set of naturals.

lemma *theta-eq-sum*: $0 \leq x \implies \text{primes-theta } x = (\sum_{p \in \{p. \text{prime } p \wedge \text{real } p \leq x\}} \ln (\text{real } p))$

<proof>

lemma *finite-primes-le*: *finite* $\{p. \text{prime } p \wedge \text{real } p \leq x\}$

<proof>

The sum of $\log p$ over the primes in $(c, d]$ is $\vartheta(d) - \vartheta(c)$.

lemma *sum-cell*:

assumes $0 \leq c \leq d$

shows $(\sum_{p \in \{p. \text{prime } p \wedge c < \text{real } p \wedge \text{real } p \leq d\}} \ln (\text{real } p)) = \text{primes-theta } d - \text{primes-theta } c$

<proof>

lemma *theta-ratio-eq*: $0 < c \implies 0 < K \implies$

$c * (\text{primes-theta } (c * \text{real } K) / (c * \text{real } K)) = \text{primes-theta } (c * \text{real } K) / \text{real } K$
 $\langle \text{proof} \rangle$

$\vartheta(cK)/K \longrightarrow c$ along $K \in \mathbb{N}$.

lemma *theta-tendsto*:

assumes $0 \leq c$

shows $((\lambda K :: \text{nat. primes-theta } (c * \text{real } K) / \text{real } K) \longrightarrow c)$ *at-top*

$\langle \text{proof} \rangle$

lemma *cell-tendsto*:

assumes $0 \leq c \ 0 \leq d$

shows $((\lambda K :: \text{nat. (primes-theta } (d * \text{real } K) - \text{primes-theta } (c * \text{real } K)) / \text{real } K) \longrightarrow d - c)$ *at-top*

$\langle \text{proof} \rangle$

Eventually $\vartheta(dK) - \vartheta(cK) \leq (d - c + \delta) K$ resp. $\geq (d - c - \delta) K$.

lemma *cell-upper*:

assumes $0 \leq c \ 0 \leq d \ 0 < \delta$

shows $\forall_F K :: \text{nat in at-top. primes-theta } (d * \text{real } K) - \text{primes-theta } (c * \text{real } K) \leq (d - c + \delta) * \text{real } K$

$\langle \text{proof} \rangle$

lemma *cell-lower*:

assumes $0 \leq c \ 0 \leq d \ 0 < \delta$

shows $\forall_F K :: \text{nat in at-top. } (d - c - \delta) * \text{real } K \leq \text{primes-theta } (d * \text{real } K) - \text{primes-theta } (c * \text{real } K)$

$\langle \text{proof} \rangle$

6.2 Small primes: $\psi - \vartheta$ and the valuation of 24

$\psi(n) = \sum -\{p \leq n\} \lfloor \log p \rfloor \log p \ (\text{nat-log } p \ n = \text{floorlog } p \ n - 1 = \lfloor \log p \rfloor \log p)$.

lemma *card-powers-le*: $\text{prime } p \implies 0 < n \implies \text{card } \{i. 0 < i \wedge p^i \leq n\} = \text{nat-log } p \ n$

$\langle \text{proof} \rangle$

lemma *psi-eq-sum*:

$0 < n \implies \text{primes-psi } (\text{real } n) = (\sum p \in \{p. \text{prime } p \wedge p \leq n\}. \text{real } (\text{nat-log } p \ n) * \ln (\text{real } p))$

$\langle \text{proof} \rangle$

$\sum -\{p \leq N\} (\lfloor \log p \rfloor - 1) \log p = \psi(N) - \vartheta(N) \leq 2 \log N \sqrt{N}$.

lemma *psi-minus-theta-sum*:

assumes $2 \leq N$

shows $(\sum p \in \{p. \text{prime } p \wedge p \leq N\}. (\text{real } (\text{nat-log } p \ N) - 1) * \ln (\text{real } p)) \leq 2 * \ln (\text{real } N) * \text{sqrt } (\text{real } N)$

$\langle \text{proof} \rangle$

$\langle \text{proof} \rangle$

lemma *eventually-psi-theta-small*:

assumes $0 < \delta$

shows $\forall_F K :: \text{nat in at-top. } 2 * \ln (\text{real } (5 * K)) * \text{sqrt } (\text{real } (5 * K)) \leq \delta * \text{real } K$

$\langle \text{proof} \rangle$

lemma *mult24-log-le*:

prime $p \implies \text{real } (\text{multiplicity } p \text{ } (24 :: \text{nat})) * \ln (\text{real } p) \leq (\text{if } p \leq 24 \text{ then } \ln 24 \text{ else } 0)$

$\langle \text{proof} \rangle$

6.3 Step majorants on a uniform partition

Grid points of the uniform partition of $[a, b]$ into n cells.

definition $cx :: \text{real} \Rightarrow \text{real} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{real}$

where

$cx \ a \ b \ n \ i = a + (b - a) * \text{real } i / \text{real } n$

The supremum of φ over the closed i -th cell.

definition $cM :: (\text{real} \Rightarrow \text{real}) \Rightarrow \text{real} \Rightarrow \text{real} \Rightarrow \text{nat}$

$\Rightarrow \text{nat} \Rightarrow \text{real}$ **where**

$cM \ \varphi \ a \ b \ n \ i = \text{Sup } (\varphi \text{ ` } (\{cx \ a \ b \ n \ i..cx \ a \ b \ n \ (i + 1)\} \cap \{a..b\}))$

The step majorant of $\varphi + B$.

definition $cG :: (\text{real} \Rightarrow \text{real}) \Rightarrow \text{real} \Rightarrow \text{real} \Rightarrow \text{real}$

$\Rightarrow \text{nat} \Rightarrow \text{real} \Rightarrow \text{real}$ **where**

$cG \ \varphi \ a \ b \ B \ n \ y = (\sum \ i < n. \text{indicator } \{cx \ a \ b \ n \ i <..cx \ a \ b \ n \ (i + 1)\} \ y * (cM \ \varphi \ a \ b \ n \ i + B))$

lemma *cx-mono*: $a \leq b \implies i \leq j \implies cx \ a \ b \ n \ i \leq cx \ a \ b \ n \ j$

$\langle \text{proof} \rangle$

lemma *cx-zero*: $cx \ a \ b \ n \ 0 = a$ $\langle \text{proof} \rangle$

lemma *cx-self*: $0 < n \implies cx \ a \ b \ n \ n = b$ $\langle \text{proof} \rangle$

lemma *cx-succ-sub*: $0 < n \implies cx \ a \ b \ n \ (i + 1) - cx \ a \ b \ n \ i = (b - a) / \text{real } n$

$\langle \text{proof} \rangle$

lemma *cx-ge*: $a \leq b \implies a \leq cx \ a \ b \ n \ i$ $\langle \text{proof} \rangle$

lemma *cx-le*: $a \leq b \implies 0 < n \implies i \leq n \implies$

$cx \ a \ b \ n \ i \leq b$ $\langle \text{proof} \rangle$

lemma *cell-unique*:

assumes $a \leq b \ y \in \{cx \ a \ b \ n \ i <..cx \ a \ b \ n \ (i + 1)\} \ y \in \{cx \ a \ b \ n \ j <..cx \ a \ b \ n \ (j + 1)\}$

shows $i = j$

$\langle \text{proof} \rangle$

lemma *cell-exists*:

assumes $a < b \ 0 < n \ y \in \{a..b\}$
shows $\exists i < n. \ y \in \{cx \ a \ b \ n \ i..cx \ a \ b \ n \ (i + 1)\}$
 $\langle proof \rangle$

lemma *cM-bdd*:

fixes $\varphi :: real \Rightarrow real$
assumes $\bigwedge y. \ y \in \{a..b\} \implies |\varphi \ y| \leq B$
shows $bdd\text{-}above \ (\varphi \ ' \ (\{cx \ a \ b \ n \ i..cx \ a \ b \ n \ (i + 1)\} \cap \{a..b\}))$
 $\langle proof \rangle$

lemma *cM-le*:

assumes $\bigwedge y. \ y \in \{a..b\} \implies$
 $|\varphi \ y| \leq B \ 0 \leq B \ a \leq b \ 0 < n \ i < n$
shows $cM \ \varphi \ a \ b \ n \ i \leq B$
 $\langle proof \rangle$

lemma *cM-ge*:

assumes $\bigwedge y. \ y \in \{a..b\} \implies$
 $|\varphi \ y| \leq B \ a \leq b \ 0 < n \ i < n$
shows $-B \leq cM \ \varphi \ a \ b \ n \ i$
 $\langle proof \rangle$

lemma *le-cM*:

assumes $\bigwedge y. \ y \in \{a..b\} \implies$
 $|\varphi \ y| \leq B \ y \in \{cx \ a \ b \ n \ i..cx \ a \ b \ n \ (i + 1)\} \cap \{a..b\}$
shows $\varphi \ y \leq cM \ \varphi \ a \ b \ n \ i$
 $\langle proof \rangle$

lemma *cG-eval*:

assumes $a < b \ 0 < n \ y \in \{a..b\}$
shows $\exists i < n. \ y \in \{cx \ a \ b \ n \ i..cx \ a \ b \ n \ (i + 1)\} \wedge$
 $cG \ \varphi \ a \ b \ B \ n \ y = cM \ \varphi \ a \ b \ n \ i + B$
 $\langle proof \rangle$

lemma *cG-bounds*:

assumes $a < b \ \bigwedge y. \ y \in \{a..b\} \implies$
 $|\varphi \ y| \leq B \ 0 \leq B \ 0 < n \ y \in \{a..b\}$
shows $\varphi \ y + B \leq cG \ \varphi \ a \ b \ B \ n \ y \wedge 0 \leq cG \ \varphi \ a \ b \ B \ n \ y \wedge$
 $cG \ \varphi \ a \ b \ B \ n \ y \leq 2 * B$
 $\langle proof \rangle$

lemma *cG-measurable* [*measurable*]: $cG \ \varphi \ a \ b \ B \ n \in \text{borel-measurable borel}$
 $\langle proof \rangle$

At a continuity point of φ inside (a, b) , the majorants converge to $\varphi \ y + B$.

lemma *cG-tendsto*:

assumes $a < b \ \bigwedge y. \ y \in \{a..b\} \implies$
 $|\varphi \ y| \leq B \ y \in \{a..b\} \text{ isCont } \varphi \ y$

shows $((\lambda n. cG \varphi a b B n y) \longrightarrow \varphi y + B)$ *at-top*
 $\langle proof \rangle$

lemma *set-integral-sum-nat*:

fixes $f :: nat \Rightarrow real \Rightarrow real$

assumes $\bigwedge i. i \in I \implies \text{set-integrable } lborel A (f i)$

shows $\text{set-integrable } lborel A (\lambda x. \sum i \in I. f i x) \wedge$
 $\text{set-lebesgue-integral } lborel A (\lambda x. \sum i \in I. f i x) = (\sum i \in$
 $I. \text{set-lebesgue-integral } lborel A (f i))$

$\langle proof \rangle$

lemma *integral-cG*:

assumes $a < b \ 0 < n$

shows $\text{interval-lebesgue-integral } lborel (ereal a) (ereal b) (cG \varphi a b B n) = (\sum$
 $i <$

$n. (cM \varphi a b n i + B) * ((b - a) / real n))$

$\langle proof \rangle$

6.4 Dominated convergence for the majorants

lemma *ae-cG-tendsto*:

assumes $a < b \ \bigwedge y. y \in \{a..b\} \implies$

$|\varphi y| \leq B \text{ countable } D$

and $\bigwedge y. y \in \{a <..<b\} \implies y \notin D \implies \text{isCont } \varphi y$

shows $AE y \text{ in } lborel. y \in \{a <..<b\} \longrightarrow$

$((\lambda n. cG \varphi a b B n y) \longrightarrow \varphi y + B)$ *at-top*

$\langle proof \rangle$

φ (restricted to (a, b)) is Borel measurable and integrable.

lemma *phi-measurable*:

fixes $\varphi :: real \Rightarrow real$

assumes $\text{countable } D \ \bigwedge y. y \in \{a <..<b\} \implies y \notin D \implies$

$\text{isCont } \varphi y$

shows $(\lambda y. \text{indicator } \{a <..<b\} y * \varphi y) \in \text{borel-measurable borel}$

$\langle proof \rangle$

lemma *phi-integrable*:

fixes $\varphi :: real \Rightarrow real$

assumes $a < b \ \bigwedge y. y \in \{a..b\} \implies$

$|\varphi y| \leq B \text{ countable } D$

and $\bigwedge y. y \in \{a <..<b\} \implies y \notin D \implies \text{isCont } \varphi y$

shows $\text{interval-lebesgue-integrable } lborel (ereal a) (ereal b) \varphi$

$\langle proof \rangle$

lemma *integral-cG-tendsto*:

assumes $a < b \ \bigwedge y. y \in \{a..b\} \implies$

$|\varphi y| \leq B \ 0 \leq B \text{ countable } D$

and $\bigwedge y. y \in \{a <..<b\} \implies y \notin D \implies \text{isCont } \varphi y$

shows $((\lambda n. \text{interval-lebesgue-integral } lborel (ereal a) (ereal b) (cG \varphi a b B n))$

$\longrightarrow \text{interval-lebesgue-integral lborel (ereal } a) \text{ (ereal } b) (\lambda y.$
 $\varphi \ y + B)) \text{ at-top}$

$\langle \text{proof} \rangle$

The change of variables $x = 1/y$: $\int_{1/M}^{1/3} y f(1/y) \, dy = \int_{1/3}^M f(x)/x^3 \, dx$.

lemma *integral-inv-subst*:

fixes $f :: \text{real} \Rightarrow \text{real}$

assumes $3 \leq M$ $(\lambda x. \text{indicator } \{3 < .. < M\} \ x * f \ x) \in$
 $\text{borel-measurable borel } \bigwedge x. x \in \{3..M\} \implies |f \ x| \leq B d$

shows $\text{interval-lebesgue-integral lborel (ereal } (1 / M)) \text{ (ereal } (1 / 3)) (\lambda y. y * f$
 $(1 /$
 $y))$
 $= \text{interval-lebesgue-integral lborel (ereal } 3) \text{ (ereal } M) (\lambda x. f \ x / x^3)$

$\langle \text{proof} \rangle$

6.5 The Riemann-sum bounds

lemma *split2-aux*: $c * ((x + d) * k) = c * x * k + d * k * (c :: \text{real})$

$\langle \text{proof} \rangle$

Outer range, variable $y = p/K$: Riemann-sum upper bound for a bounded, almost-everywhere continuous φ (step majorants + the PNT cell estimates).

theorem *outer-prime-sum-bound*:

assumes $a: 0 < a$ **and** $ab: a \leq b$ **and** $Bd: \bigwedge y. y \in \{a..b\} \implies$
 $|\varphi \ y| \leq B d$ **and** $D: \text{countable } D$

and $\text{cont}: \bigwedge y. y \in \{a < .. < b\} \implies y \notin D \implies$
 $\text{isCont } \varphi \ y$ **and** $e: 0 < \varepsilon$

shows $\forall_F K$ *in at-top*.

$(\sum p \in \{p. p \leq \text{nat } (\text{floor } (b * \text{real } K)) \} \wedge \text{prime } p \wedge$
 $a * \text{real } K < \text{real } p \wedge \text{real } p \leq b * \text{real } K).$
 $\varphi (\text{real } p / \text{real } K) * \ln (\text{real } p))$
 $\leq (\text{interval-lebesgue-integral lborel (ereal } a) \text{ (ereal } b) \varphi + \varepsilon) * \text{real } K$

$\langle \text{proof} \rangle$

Inner range, variable $x = K/p$: substitute $y = 1/x$ in the outer bound.

theorem *inner-prime-sum-bound*:

assumes $M: 3 < M$ **and** $Bd: \bigwedge x. x \in \{3.. \text{real } M\} \implies$
 $|f \ x| \leq B d$ **and** $D: \text{countable } D$

and $\text{cont}: \bigwedge x. x \in \{3 < .. < \text{real } M\} \implies x \notin D \implies$
 $\text{isCont } f \ x$ **and** $e: 0 < \varepsilon$

shows $\forall_F K$ *in at-top*.

$(\sum p \in \{p. p \leq K \wedge \text{prime } p \wedge K < p * M \wedge$
 $3 * p \leq K\}. \text{real } p * f (\text{real } K / \text{real } p) * \ln (\text{real } p))$
 $\leq (\text{interval-lebesgue-integral lborel (ereal } 3) \text{ (ereal } (\text{real } M)) (\lambda x. f \ x /$
 $x^3) + \varepsilon) * \text{real } K^2$

$\langle \text{proof} \rangle$

end

```

theory Piecewise-Interval-Integrals
  imports HOL-Analysis.Analysis
begin

```

7 Interval integrals of piecewise polynomial and rational functions

Integrability and the value of *interval-lebesgue-integral* for functions that agree on an open interval with a quadratic polynomial, with $c_0 + c_1/x$, or with a constant, and the chaining of adjacent pieces. Together these give exact integrals of functions defined piecewise through *floor* and *frac*.

7.1 Generic piece lemmas

The integrand may be changed on the open interval.

```

lemma interval-integral-cong-Ioo:
  fixes  $f\ g :: \text{real} \Rightarrow \text{real}$ 
  assumes  $a \leq b \wedge x. x \in \{a < .. < b\} \implies f\ x = g\ x$ 
  shows  $\text{interval-lebesgue-integral}\ \text{lborel}\ (\text{ereal}\ a)\ (\text{ereal}\ b)\ f =$ 
   $\text{interval-lebesgue-integral}\ \text{lborel}\ (\text{ereal}\ a)\ (\text{ereal}\ b)\ g$ 
  <proof>

```

```

lemma interval-integrable-cong-Ioo:
  fixes  $f\ g :: \text{real} \Rightarrow \text{real}$ 
  assumes  $a \leq b \wedge x. x \in \{a < .. < b\} \implies$ 
   $f\ x = g\ x$ 
  shows  $\text{interval-lebesgue-integrable}\ \text{lborel}\ (\text{ereal}\ a)\ (\text{ereal}\ b)\ f$ 
  <proof>

```

A continuous integrand is integrable on a bounded interval.

```

lemma interval-integrable-continuous:
  fixes  $f :: \text{real} \Rightarrow \text{real}$ 
  assumes  $a \leq b$  continuous-on  $\{a..b\}$   $f$ 
  shows  $\text{interval-lebesgue-integrable}\ \text{lborel}\ (\text{ereal}\ a)\ (\text{ereal}\ b)\ f$ 
  <proof>

```

Quadratic piece: $\int_a^b (c_0 + c_1 x + c_2 x^2) dx$.

```

lemma piece-quad:
  fixes  $f :: \text{real} \Rightarrow \text{real}$ 
  assumes  $a \leq b \wedge x. x \in \{a < .. < b\} \implies f\ x = c_0 + c_1 * x + c_2 * x^2$ 
  shows  $\text{interval-lebesgue-integrable}\ \text{lborel}\ (\text{ereal}\ a)\ (\text{ereal}\ b)\ f \wedge$ 
   $\text{interval-lebesgue-integral}\ \text{lborel}\ (\text{ereal}\ a)\ (\text{ereal}\ b)\ f$ 
   $= (c_0 * b + c_1 * b^2 / 2 + c_2 * b^3 / 3) - (c_0 * a + c_1 * a^2 /$ 
   $2 + c_2 * a^3 /$ 
   $3)$ 

```

$\langle proof \rangle$

Rational piece: $\int -a \wedge b (A x + B) / x^3 dx$ for $0 < a$.

lemma *piece-rat*:

fixes $f :: real \Rightarrow real$

assumes $0 < a \leq b \wedge x. x \in \{a < .. < b\} \implies f x = A * x + B$

shows $interval\text{-}lebesgue\text{-}integrable\ lborel\ (ereal\ a)\ (ereal\ b)\ (\lambda x. f\ x / x^3) \wedge$
 $interval\text{-}lebesgue\text{-}integral\ lborel\ (ereal\ a)\ (ereal\ b)\ (\lambda x. f\ x / x^3)$
 $= (-A / b - B / (2 * b^2)) - (-A / a - B / (2 * a^2))$

$\langle proof \rangle$

Adjacent pieces add up.

lemma *chain*:

fixes $f :: real \Rightarrow real$

assumes $a \leq b \leq c$

and $interval\text{-}lebesgue\text{-}integrable\ lborel\ (ereal\ a)\ (ereal\ b)\ f \wedge$
 $interval\text{-}lebesgue\text{-}integral\ lborel\ (ereal\ a)\ (ereal\ b)\ f = v$

and $interval\text{-}lebesgue\text{-}integrable\ lborel\ (ereal\ b)\ (ereal\ c)\ f \wedge$
 $interval\text{-}lebesgue\text{-}integral\ lborel\ (ereal\ b)\ (ereal\ c)\ f = w$

shows $interval\text{-}lebesgue\text{-}integrable\ lborel\ (ereal\ a)\ (ereal\ c)\ f \wedge$
 $interval\text{-}lebesgue\text{-}integral\ lborel\ (ereal\ a)\ (ereal\ c)\ f = v + w$

$\langle proof \rangle$

lemma *const-piece*:

fixes $h :: real \Rightarrow real$

assumes $a \leq b \wedge z. z \in \{a < .. < b\} \implies h\ z = c$

shows $interval\text{-}lebesgue\text{-}integrable\ lborel\ (ereal\ a)\ (ereal\ b)\ h \wedge$
 $interval\text{-}lebesgue\text{-}integral\ lborel\ (ereal\ a)\ (ereal\ b)\ h = (b - a) * c$

$\langle proof \rangle$

lemma *floor-inv-eq*:

fixes $y :: real$

assumes $0 < y \text{ of-int } k * y \leq 1 \wedge 1 < (\text{of-int } k + 1) * y$

shows $\text{floor } (1 / y) = k$

$\langle proof \rangle$

lemma *frac-nat*:

fixes $u :: real$

assumes $real\ k \leq u \wedge u < real\ k + 1$

shows $\text{frac } u = u - real\ k$

$\langle proof \rangle$

end

theory *Laplace-Sin-Cot-Series*

imports *HOL-Analysis.Analysis Cotangent-PFD-Formula.Cotangent-PFD-Formula*

begin

8 Gamma-type integrals, the Laplace transform of *sin* and the *coth* series

Integrals $\int_0^\infty y^k e^{-cy} dy$ on the open half-line by the fundamental theorem of calculus, the interchange of $\int$ and $\sum$ for non-negative series, the Mittag-Leffler expansion of *coth* (from the AFP's cotangent partial-fraction formula), the series $\sum_l u / (u^2 + (2\pi l)^2)$, the Laplace transform $\int_0^\infty e^{-cy} \sin(ay) dy$, and the integrals $\Psi(a, c) = \int_0^\infty e^{-cy} y / (y^2 + a^2) dy$, $\Phi(a, c) = \int_0^\infty y^5 e^{-cy} / (y^2 + a^2) dy$ and the geometric pole sums.

8.1 Gamma integrals and the interchange of $\int$ and $\sum$

lemma *set-bm-cont: continuous-on UNIV f $\implies$*
set-borel-measurable lborel {0<..} (f :: real $\Rightarrow$ real)
<proof>

lemma *ftc-Ioi-nonneg:*
fixes *f F :: real $\Rightarrow$ real*
assumes *f: f $\in$ borel-measurable borel*
and *D: $\bigwedge x. 0 \leq x \implies (F \text{ has-real-derivative } f \ x) \text{ (at } x)$*
and *nn: $\bigwedge x. 0 \leq x \implies 0 \leq f \ x$*
and *T: (F $\longrightarrow$ T) at-top*
shows *set-integrable lborel {0<..} f $\wedge$ set-lebesgue-integral lborel {0<..} f = T - F 0*
<proof>

lemma *gam-deriv:*
fixes *c :: real*
shows *(($\lambda y. \exp(- (c * y)) * (\sum k \leq n. (c * y) ^ k / \text{fact } k)$) has-real-derivative*
*- c * $\exp(- (c * y)) * ((c * y) ^ n / \text{fact } n)$) (at y)*
<proof>

lemma *gam-lim:*
fixes *c :: real*
assumes *c: 0 < c*
shows *(($\lambda y. \exp(- (c * y)) * (\sum k \leq n. (c * y) ^ k / \text{fact } k)$) $\longrightarrow$ 0) at-top*
<proof>

lemma *exp-neg-lim: 0 < (c :: real) $\implies$*
*(($\lambda y. \exp(- (c * y))$) $\longrightarrow$ 0) at-top*
<proof>

lemma *gam-both:*
fixes *c :: real*
assumes *c: 0 < c*
shows *set-integrable lborel {0<..} ($\lambda y. y ^ n * \exp(- (c * y))$) $\wedge$*

$$\text{set-lebesgue-integral lborel } \{0 < ..\} (\lambda y. y^n * \exp(- (c * y))) = \text{fact } n / c^{(n+1)}$$

⟨proof⟩

lemma *gam-integrable*: $0 < (c::\text{real}) \implies$
 $\text{set-integrable lborel } \{0 < ..\} (\lambda y. y^n * \exp(- (c * y)))$
 ⟨proof⟩

lemma *gam*: $0 < (c::\text{real}) \implies$
 $\text{set-lebesgue-integral lborel } \{0 < ..\} (\lambda y. y^n * \exp(- (c * y))) = \text{fact } n / c^{(n+1)}$
 ⟨proof⟩

Interchange of $\int$ and $\sum$ for nonnegative integrable terms with summable integrals.

lemma *set-integral-sum-fin*:
fixes $f :: \text{nat} \Rightarrow \text{real} \Rightarrow \text{real}$
assumes $\bigwedge i. i \in I \implies \text{set-integrable lborel } A (f i)$
shows $\text{set-integrable lborel } A (\lambda x. \sum i \in I. f i x) \wedge$
 $\text{set-lebesgue-integral lborel } A (\lambda x. \sum i \in I. f i x) = (\sum i \in I. \text{set-lebesgue-integral lborel } A (f i))$
 ⟨proof⟩

lemma *set-integrable-cong-Ioi*:
 $\text{set-integrable lborel } \{0 < ..\} f \implies (\bigwedge x. 0 < x \implies f x = g x) \implies \text{set-integrable lborel } \{0 < ..\} (g :: \text{real} \Rightarrow \text{real})$
 ⟨proof⟩

lemma *set-integral-cong-Ioi*:
 $(\bigwedge x. 0 < x \implies f x = g x) \implies$
 $\text{set-lebesgue-integral lborel } \{0 < ..\} f = \text{set-lebesgue-integral lborel } \{0 < ..\} (g :: \text{real} \Rightarrow \text{real})$
 ⟨proof⟩

lemma *integral-suminf-nn*:
fixes $f :: \text{nat} \Rightarrow \text{real} \Rightarrow \text{real}$
assumes $\bigwedge n. \text{set-integrable lborel } \{0 < ..\} (f n) \wedge n y. 0 < y \implies 0 \leq f n y$
and $\bigwedge y. 0 < y \implies \text{summable } (\lambda n. f n y) \text{ summable } (\lambda n. \text{set-lebesgue-integral lborel } \{0 < ..\} (f n))$
shows $\text{set-integrable lborel } \{0 < ..\} (\lambda y. \sum n. f n y) \wedge$
 $\text{set-lebesgue-integral lborel } \{0 < ..\} (\lambda y. \sum n. f n y) = (\sum n. \text{set-lebesgue-integral lborel } \{0 < ..\} (f n))$
 ⟨proof⟩

Converse interchange: if the pointwise sum is integrable, the integrals sum to its integral.

lemma *suminf-integral-nn*:

fixes $f :: \text{nat} \Rightarrow \text{real} \Rightarrow \text{real}$
assumes $\bigwedge n. \text{set-integrable lborel } \{0 < ..\} (f \ n) \wedge n \ y. 0 < y \implies$
 $0 \leq f \ n \ y$
and $\bigwedge y. 0 < y \implies$
 $\text{summable } (\lambda n. f \ n \ y) \text{ set-integrable lborel } \{0 < ..\} (\lambda y. \sum n. f \ n \ y)$
shows $(\lambda n. \text{set-lebesgue-integral lborel } \{0 < ..\} (f \ n)) \text{ sums set-lebesgue-integral}$
 lborel
 $\{0 < ..\} (\lambda y. \sum n. f \ n \ y)$
 $\langle \text{proof} \rangle$

Mittag-Leffler for *coth* (from *Cotangent-PFD-Formula.cot-pfd-formula-real*).

lemma *coth-series*:

$0 < v \implies (\lambda n. 2 * v / (v^2 + (\text{real } n + 1)^2)) \text{ sums } (\pi * \cosh(\pi * v) / \sinh(\pi * v) - 1 / v)$
 $\langle \text{proof} \rangle$

8.2 The *S*-series and the Laplace transform of *sin*

lemma *S-series*:

$0 < u \implies (\lambda l. u / (u^2 + (2 * \pi * (\text{real } l + 1))^2)) \text{ sums } (1 / 4 + 1 / (2 * (\exp u - 1)) - 1 / (2 * u))$
 $\langle \text{proof} \rangle$

lemma *exp-integrable*: $0 < (a :: \text{real}) \implies$
 $\text{set-integrable lborel } \{0 < ..\} (\lambda u. \exp(- (a * u)))$
 $\langle \text{proof} \rangle$

lemma *laplace-sin-integrable*: $0 < (a :: \text{real}) \implies$
 $\text{set-integrable lborel } \{0 < ..\} (\lambda u. \exp(- (a * u)) * \sin(y * u))$
 $\langle \text{proof} \rangle$

$$\int_{-\infty}^{\infty} e^{-au} \sin(yu) \, du = y / (y^2 + a^2).$$

lemma *laplace-sin*: $0 < (a :: \text{real}) \implies$
 $\text{set-lebesgue-integral lborel } \{0 < ..\} (\lambda u. \exp(- (a * u)) * \sin(y * u)) =$
 $y / (y^2 + a^2)$
 $\langle \text{proof} \rangle$

$$\Psi(a, c) = \int_{-\infty}^{\infty} e^{-cy} y / (y^2 + a^2) \, dy.$$

definition *Psi* :: $\text{real} \Rightarrow \text{real} \Rightarrow \text{real}$ **where**

$Psi \ a \ c = \text{set-lebesgue-integral lborel } \{0 < ..\} (\lambda y. \exp(- (c * y)) * (y / (y^2 + a^2)))$

lemma *psi-integrable*: $0 < (a :: \text{real}) \implies 0 < c \implies$
 $\text{set-integrable lborel } \{0 < ..\} (\lambda y. \exp(- (c * y)) * (y / (y^2 + a^2)))$
 $\langle \text{proof} \rangle$

The symmetry $\Psi(a, c) = \Psi(c, a)$, by Fubini on $e^{-cy} e^{-au} \sin(yu)$.

lemma *psi-symm*: $0 < a \implies 0 < c \implies Psi \ a \ c = Psi \ c \ a$
 $\langle \text{proof} \rangle$

$$\Phi(a, c) = \int_0^\infty y^5 e^{-cy} / (y^2 + a^2) dy.$$

definition *Phi* :: real $\Rightarrow$ real $\Rightarrow$ real **where**

$$\Phi a c = \text{set-lebesgue-integral lborel } \{0 < ..\} (\lambda y. y^5 * \exp(- (c * y)) / (y^2 + a^2))$$

lemma *phi-split*:

fixes *a y* :: real **assumes** *a*: $0 < a$

$$\text{shows } y^5 * \exp(- (c * y)) / (y^2 + a^2) = y^3 * \exp(- (c * y)) - a^2 * (y * \exp(- (c * y))) + a^4 * (\exp(- (c * y)) * (y / (y^2 + a^2)))$$

$\langle \text{proof} \rangle$

lemma *phi-integrable*: $0 < (a::\text{real}) \implies 0 < c \implies$

$$\text{set-integrable lborel } \{0 < ..\} (\lambda y. y^5 * \exp(- (c * y)) / (y^2 + a^2))$$

$\langle \text{proof} \rangle$

lemma *phi-eq*: $0 < a \implies 0 < c \implies$

$$\Phi a c = 6 / c^4 - a^2 / c^2 + a^4 * \Psi a c$$

$\langle \text{proof} \rangle$

lemma *phi-symm*: $0 < a \implies 0 < c \implies c^4 * \Phi a c = a^4 * \Phi c a$

$\langle \text{proof} \rangle$

8.3 The pole integral

lemma *geom-pt*: $0 < u \implies (\lambda n. u^4 * \exp(- ((a + (\text{real } n + 1)) * u))) \text{ sums } (u^4 * \exp(- (a * u)) / (\exp u - 1))$

$\langle \text{proof} \rangle$

lemma *u-integral*:

assumes $0 < a (\lambda n. 1 / (a + (\text{real } n + 1))^5) \text{ sums } Z$

$$\text{shows set-integrable lborel } \{0 < ..\} (\lambda u. u^4 * \exp(- (a * u)) * (1 / 4 + 1 / (2 * (\exp u - 1)) - 1 / (2 * u))) \wedge \\ \text{set-lebesgue-integral lborel } \{0 < ..\} (\lambda u. u^4 * \exp(- (a * u)) * (1 / 4 + 1 / (2 * (\exp u - 1)) - 1 / (2 * u))) \\ = 6 / a^5 - 3 / a^4 + 12 * Z$$

$\langle \text{proof} \rangle$

end

theory *Interval-Integral-Substitutions*

imports *HOL-Analysis.Analysis*

begin

9 Substitutions in interval integrals with finite endpoints

Affine changes of variable and reflections for *interval-lebesgue-integral* with explicit endpoints (HOL-Analysis has the whole-line *lborel-integral-real-affine* and the monotone-substitution rules), restriction of integrability to a subinterval, joining of adjacent intervals, and the invariance $\int_0^{2\pi} g(x - \varphi) dx = \int_0^{2\pi} g$ of a 2π -periodic integrand.

Affine changes of variable in interval integrals with finite endpoints.

lemma *LBINT-affine-ind*:

fixes $a\ b\ c\ t\ x :: \text{real}$
assumes $c: 0 < c$
shows $\text{indicator } \{a <..<b\} (t + c * x) = (\text{indicator } \{(a - t) / c <..<(b - t) / c\} x :: \text{real})$
 $\langle \text{proof} \rangle$

lemma *LBINT-reflect-ind*:

fixes $a\ b\ t\ x :: \text{real}$
shows $\text{indicator } \{a <..<b\} (t + (-1) * x) = (\text{indicator } \{t - b <..<t - a\} x :: \text{real})$
 $\langle \text{proof} \rangle$

lemma *LBINT-reflect*:

fixes $f :: \text{real} \Rightarrow \text{real}$ **and** $a\ b\ t :: \text{real}$
assumes $ab: a \leq b$
shows $\text{interval-lebesgue-integral lborel } (ereal\ a) (ereal\ b) f$
 $= \text{interval-lebesgue-integral lborel } (ereal\ (t - b)) (ereal\ (t - a)) (\lambda x. f\ (t - x))$
 $\langle \text{proof} \rangle$

lemma *LBINT-reflect-int*:

fixes $f :: \text{real} \Rightarrow \text{real}$ **and** $a\ b\ t :: \text{real}$
assumes $ab: a \leq b$
shows $\text{interval-lebesgue-integrable lborel } (ereal\ a) (ereal\ b) f$
 $\longleftrightarrow \text{interval-lebesgue-integrable lborel } (ereal\ (t - b)) (ereal\ (t - a)) (\lambda x. f\ (t - x))$
 $\langle \text{proof} \rangle$

lemma *LBINT-affine-int*:

fixes $f :: \text{real} \Rightarrow \text{real}$ **and** $a\ b\ c\ t :: \text{real}$
assumes $c: 0 < c$ **and** $ab: a \leq b$
shows $\text{interval-lebesgue-integrable lborel } (ereal\ a) (ereal\ b) f$
 $\longleftrightarrow \text{interval-lebesgue-integrable lborel } (ereal\ ((a - t) / c)) (ereal\ ((b - t) / c)) (\lambda x. f\ (t + c * x))$
 $\langle \text{proof} \rangle$

lemma *LBINT-affine*:

fixes $f :: \text{real} \Rightarrow \text{real}$ **and** $a\ b\ c\ t :: \text{real}$
assumes $c: 0 < c$ **and** $ab: a \leq b$
shows $\text{interval-lebesgue-integral lborel (ereal a) (ereal b) f}$
 $= c * \text{interval-lebesgue-integral lborel (ereal ((a - t) / c)) (ereal ((b - t) /$
 $c)) (\lambda x. f (t + c * x))$
 $\langle \text{proof} \rangle$

lemma interval-integrable-sub:
fixes $f :: \text{real} \Rightarrow \text{real}$ **and** $a\ b\ c\ d :: \text{real}$
assumes $a \leq c$ $c \leq d$ $d \leq$
 b $\text{interval-lebesgue-integrable lborel (ereal a) (ereal b) f}$
shows $\text{interval-lebesgue-integrable lborel (ereal c) (ereal d) f}$
 $\langle \text{proof} \rangle$

lemma interval-integrable-join:
fixes $f :: \text{real} \Rightarrow \text{real}$ **and** $a\ b\ c :: \text{real}$
assumes $ab: a \leq b$ **and** $bc: b \leq c$
and $i1: \text{interval-lebesgue-integrable lborel (ereal a) (ereal b) f}$
and $i2: \text{interval-lebesgue-integrable lborel (ereal b) (ereal c) f}$
shows $\text{interval-lebesgue-integrable lborel (ereal a) (ereal c) f}$
 $\langle \text{proof} \rangle$

lemma periodic-shift-fun:
fixes $g :: \text{real} \Rightarrow \text{real}$ **and** $\varphi :: \text{real}$
assumes $\text{per}: \bigwedge x. g (x + 2 * \pi) = g x$
shows $(\lambda x. g (x - \varphi)) = (\lambda x. g (2 * \pi - \varphi + 1 * x))$
 $\langle \text{proof} \rangle$

lemma periodic-shift-int:
fixes $g :: \text{real} \Rightarrow \text{real}$ **and** $\varphi :: \text{real}$
assumes $\text{per}: \bigwedge x. g (x + 2 * \pi) = g x$
and $ig: \text{interval-lebesgue-integrable lborel (ereal 0) (ereal (2 * \pi)) g}$
and $p0: 0 \leq \varphi$ $\varphi \leq 2 * \pi$
shows $\text{interval-lebesgue-integrable lborel (ereal 0) (ereal (2 * \pi)) (\lambda x. g (x -$
 $\varphi))}$
 $\langle \text{proof} \rangle$

lemma periodic-shift-eq:
fixes $g :: \text{real} \Rightarrow \text{real}$ **and** $\varphi :: \text{real}$
assumes $\text{per}: \bigwedge x. g (x + 2 * \pi) = g x$
and $ig: \text{interval-lebesgue-integrable lborel (ereal 0) (ereal (2 * \pi)) g}$
and $p0: 0 \leq \varphi$ $\varphi \leq 2 * \pi$
shows $\text{interval-lebesgue-integral lborel (ereal (0)) (ereal (2 * \pi)) (\lambda x. g (x -$
 $\varphi)) = \text{interval-lebesgue-integral lborel (ereal (0)) (ereal (2 * \pi)) g}$
 $\langle \text{proof} \rangle$

end

theory *Log-Sine-Integral*
imports *Interval-Integral-Substitutions HOL-Complex-Analysis.Complex-Analysis*
begin

10 The log-sine integral and circle averages of $\ln$

$$|z - a|$$

Jordan's inequality $\sin \vartheta \geq 2\vartheta/\pi$ on $[0, \pi/2]$, integrability of $\ln$ near 0, the classical $\int_0^\pi \ln(\sin \vartheta) d\vartheta = -\pi \ln 2$, and the circle average $\int_0^{2\pi} \ln |e^{i\vartheta} - a| d\vartheta = 2\pi \ln(\max(1, |a|))$ for every complex a , including the singular case $|a| = 1$; the same for the normalised arclength measure *circ* on a circle of radius ε about c . This is the layer of Jensen's formula that HOL-Complex_Analysis lacks.

Jordan's inequality $\sin \vartheta \geq 2\vartheta/\pi$ on $[0, \pi/2]$: $\sin$ is concave there ($\sin'' = -\sin \leq 0$) and the chord through $(0, 0)$ and $(\pi/2, 1)$ lies below it.

lemma *sin-ge-two-over-pi*:
assumes $0 \leq \vartheta \leq \pi / 2$
shows $2 * \vartheta / \pi \leq \sin \vartheta$
 $\langle proof \rangle$

$\ln$ is integrable near 0: $\int_0^c (-\ln u) du = c - c \ln c < \infty$.

lemma *ln-integrable-near-zero*:
assumes $0 < c$
shows *set-integrable lborel* $\{0 <..<c\}$ $(\lambda u. \ln u)$
 $\langle proof \rangle$

The classical $\int_0^\pi \log \sin \vartheta d\vartheta = -\pi \log 2$; first the integrability.

lemma *ln-sin-integrable: interval-lebesgue-integrable lborel* $(ereal 0)$ $(ereal \pi)$
 $(\lambda \vartheta. \ln(\sin \vartheta))$
 $\langle proof \rangle$

lemma *ln-sin-integrable-half: interval-lebesgue-integrable lborel* $(ereal 0)$ $(ereal (\pi / 2))$ $(\lambda \vartheta. \ln(\sin \vartheta))$
 $\langle proof \rangle$

lemma *ln-cos-integrable-half: interval-lebesgue-integrable lborel* $(ereal 0)$ $(ereal (\pi / 2))$ $(\lambda u. \ln(\cos u))$
 $\langle proof \rangle$

lemma *ln-sin-integral: interval-lebesgue-integral lborel* $(ereal 0)$ $(ereal \pi)$ $(\lambda \vartheta. \ln(\sin \vartheta)) = -\pi * \ln 2$
 $\langle proof \rangle$

lemma *norm-1-minus-cis*: $\text{norm } (1 - \text{cis } \vartheta) \wedge 2 = (2 * \sin (\vartheta / 2)) \wedge 2$
 ⟨proof⟩

lemma *ln-norm-one-minus-cis*:
 assumes *th*: $0 < \vartheta \wedge \vartheta < 2 * \pi$
 shows $\ln (\text{norm } (1 - \text{cis } \vartheta)) = \ln 2 + \ln (\sin (\vartheta / 2))$
 ⟨proof⟩

$\int_{-0}^{2\pi} \log|1 - e^{i\vartheta}| d\vartheta = 0$: the singular case of the circle average.

lemma *circle-log-one*: *interval-lebesgue-integral lborel (ereal 0) (ereal (2 * pi))* $(\lambda \vartheta. \ln (\text{norm } (1 - \text{cis } \vartheta))) = 0$
 ⟨proof⟩

lemma *circle-log-one-integrable*: *interval-lebesgue-integrable lborel (ereal 0) (ereal (2 * pi))* $(\lambda \vartheta. \ln (\text{norm } (1 - \text{cis } \vartheta)))$
 ⟨proof⟩

Mean value of the holomorphic $\text{Ln } (1 - z/a)$ on the unit circle, $|a| > 1$.

lemma *circle-log-gt*:
 assumes $1 < \text{norm } a$
 shows *interval-lebesgue-integral lborel (ereal 0) (ereal (2 * pi))* $(\lambda \vartheta. \ln (\text{norm } (\text{cis } \vartheta - a))) = 2 * \pi * \ln (\text{norm } a)$
 ⟨proof⟩

lemma *circle-log-lt*:
 assumes $\text{norm } a < 1$
 shows *interval-lebesgue-integral lborel (ereal 0) (ereal (2 * pi))* $(\lambda \vartheta. \ln (\text{norm } (\text{cis } \vartheta - a))) = 0$
 ⟨proof⟩

A point of the unit circle as $\text{cis } \varphi$ with $\varphi \in [0, 2\pi]$.

lemma *cis-of-norm-one*:
 assumes $\text{norm } a = 1$
 obtains φ where $a = \text{cis } \varphi$ $0 \leq \varphi \wedge \varphi \leq 2 * \pi$
 ⟨proof⟩

lemma *norm-cis-minus-cis*: $\text{norm } (\text{cis } \vartheta - \text{cis } \varphi) = \text{norm } (1 - \text{cis } (\vartheta - \varphi))$
 ⟨proof⟩

lemma *circle-log-eq*:
 assumes $\text{norm } a = 1$
 shows *interval-lebesgue-integral lborel (ereal 0) (ereal (2 * pi))* $(\lambda \vartheta. \ln (\text{norm } (\text{cis } \vartheta - a))) = 0$
 ⟨proof⟩

lemma *circle-log-eq-integrable*:
 assumes $\text{norm } a = 1$
 shows *interval-lebesgue-integrable lborel (ereal 0) (ereal (2 * pi))*

$pi)) (\lambda \vartheta. \ln (\text{norm } (\text{cis } \vartheta - a)))$
 $\langle \text{proof} \rangle$

theorem *circle-avg-log*:

*interval-lebesgue-integral lborel (ereal 0) (ereal (2 *
 $pi)) (\lambda \vartheta. \ln (\text{norm } (\text{cis } \vartheta - a))) = 2 * pi * \ln (\max 1 (\text{norm } a))$*
 $\langle \text{proof} \rangle$

lemma *circle-log-integrable*:

*interval-lebesgue-integrable lborel (ereal 0) (ereal (2 *
 $pi)) (\lambda \vartheta. \ln (\text{norm } (\text{cis } \vartheta - a)))$*
 $\langle \text{proof} \rangle$

Normalised arclength on the circle of radius ε about c .

definition *circ* :: *complex* $\Rightarrow$ *real* $\Rightarrow$ *complex measure* **where**

circ $c \ \varepsilon = \text{distr } (\text{density lborel } (\lambda \vartheta. \text{ennreal } (\text{indicator } \{0..2 *
 $pi\} \ \vartheta / (2 * pi)))) \ \text{borel}$
 $(\lambda \vartheta. c + \text{of-real } \varepsilon * \text{cis } \vartheta)$$

The circle average of $\log|z - a|$ over the circle of radius ε about c : $\log \max(\varepsilon, |c - a|)$.

lemma *circ-log*:

assumes $0 < \varepsilon$
shows $\text{integral}^L (\text{circ } c \ \varepsilon) (\lambda z. \ln (\text{norm } (z - a))) =$
 $\ln (\max \varepsilon (\text{norm } (c - a)))$
 $\langle \text{proof} \rangle$

end

theory *Arcsine-Distribution*

imports *Log-Sine-Integral*

begin

11 The arcsine distribution and its logarithmic potential

The arcsine law on (a, b) with density $1 / (\pi \sqrt{(t - a)(b - t)})$, as the pushforward of the uniform distribution on $(0, \pi)$ under $\vartheta \mapsto (a+b)/2 - (b-a)/2 \cdot \cos \vartheta$; its logarithmic potential $U(t) = \int \ln |t - u| \, d\omega(u)$, which equals $\ln ((b - a)/4)$ on $[a, b]$ and has an explicit (Joukowski) form outside; and the bound $\omega[x - r, x + r] \leq 8 \sqrt{r} / (\pi \sqrt{(b - a)})$ on the mass of short intervals.

The arcsine probability density on (a, b) , and the measure.

definition *arcsine-dens* :: *real* $\Rightarrow$ *real* $\Rightarrow$ *real* $\Rightarrow$ *real* **where**

arcsine-dens $a \ b \ t = (\text{if } a < t \wedge t < b \text{ then } 1 / (pi * \text{sqrt } ((t - a) * (b - t)))$
 $\text{else } 0)$

definition $\text{arcsine} :: \text{real} \Rightarrow \text{real} \Rightarrow \text{real measure}$ **where**

$\text{arcsine } a \ b = \text{density lborel } (\lambda t. \text{ennreal } (\text{arcsine-dens } a \ b \ t))$

The logarithmic potential $\widehat{U^\mu}(t) = \int \log|t - u| \, d\mu(u)$ of a measure on the line.

definition $\text{logPot} :: \text{real measure} \Rightarrow \text{real} \Rightarrow \text{real}$ **where**

$\text{logPot } \mu \ t = \text{integral}^L \mu \ (\lambda u. \ln |t - u|)$

11.1 The arcsine measure

lemma arcsine-distr :

assumes $a < b$

shows $\text{arcsine } a \ b = \text{distr } (\text{density lborel } (\lambda \vartheta. \text{ennreal } (\text{indicator } \{0 < .. < \pi\} \ \vartheta / \pi))) \ \text{borel } (\lambda \vartheta. (a + b) / 2 - (b - a) / 2 * \cos \vartheta)$

$\langle \text{proof} \rangle$

Integration against the arcsine measure: $\int f \, d\omega = \pi^{-1} \int_{-1}^1 f(m - r \cos \vartheta) \, d\vartheta$ (substitution $t = m - r \cos \vartheta$: *has-integral-substitution*).

theorem integral-arcsine :

assumes $a < b \ f \in \text{borel-measurable borel}$

shows $\text{integral}^L (\text{arcsine } a \ b) f =$

$1 / \pi * \text{set-lebesgue-integral lborel } \{0 < .. < \pi\} (\lambda \vartheta. f ((a + b) / 2 - (b - a) / 2 * \cos \vartheta))$

$\langle \text{proof} \rangle$

lemma $\text{arcsine-sqrt-identity}$:

assumes $a < t < b$

shows $\text{sqrt } (1 - ((2 * t - a - b) / (b - a))^2) = 2 * \text{sqrt } ((t - a) * (b - t)) / (b - a)$

$\langle \text{proof} \rangle$

lemma $\text{arcsine-dens-integral}$:

assumes $ab: a < b$

shows $(\int^+ t. \text{ennreal } (\text{arcsine-dens } a \ b \ t) \ \partial \text{lborel}) = 1$

$\langle \text{proof} \rangle$

lemma $\text{arcsine-dens-measurable}$ [*measurable*]: $(\lambda t. \text{arcsine-dens } a \ b \ t) \in$

$\text{borel-measurable borel}$

$\langle \text{proof} \rangle$

theorem arcsine-univ : $a < b \implies \text{emeasure } (\text{arcsine } a \ b) \ \text{UNIV} = 1$

$\langle \text{proof} \rangle$

(A.1): the potential of the unit arcsine measure (Joukowski parameter, the integral of $\log|x - \cos \vartheta|$ over a period; alternatively via *Cauchy-integral-circlepath*).

The Joukowski radius $|w|$ with $w^2 + 1 = 2xw$: 1 for $|x| \leq 1$, else $|x| + \sqrt{x^2 - 1}$.

definition $\text{jouk} :: \text{real} \Rightarrow \text{real}$ **where**

$\text{jouk } x = (\text{if } |x| \leq 1 \text{ then } 1 \text{ else } |x| + \text{sqrt } (x^2 - 1))$

lemma $\text{jouk-ge-1}: 1 \leq \text{jouk } x$

$\langle \text{proof} \rangle$

lemma $\text{exists-w}: \exists w :: \text{complex}. w^2 + 1 = 2 * \text{of-real } x * w \wedge \text{norm } w = \text{jouk } x$

$\langle \text{proof} \rangle$

lemma joukowski :

assumes $w^2 + 1 = 2 * \text{of-real } x * w$

shows $\text{norm } (\text{cis } \vartheta - w) * \text{norm } (\text{cis } \vartheta - \text{cnj } w) = 2 * \text{norm } w * |x - \cos \vartheta|$

$\langle \text{proof} \rangle$

lemma $\text{cos-level-null}: \{\vartheta :: \text{real}. \cos \vartheta = x\} \in \text{null-sets lborel}$

$\langle \text{proof} \rangle$

lemma log-cos-pt :

assumes $w: w^2 + 1 = 2 * \text{of-real } x * w$ **and** $w1: 1 \leq \text{norm } w$ **and** $th: \cos \vartheta \neq x$

shows $\ln |x - \cos \vartheta| = \ln (\text{norm } (\text{cis } \vartheta - w)) + \ln (\text{norm } (\text{cis } \vartheta - \text{cnj } w)) - \ln 2 - \ln (\text{norm } w)$

$\langle \text{proof} \rangle$

lemma log-cos-ae :

assumes $w: w^2 + 1 = 2 * \text{of-real } x * w$ **and** $w1: 1 \leq \text{norm } w$

shows $\text{AE } \vartheta \text{ in lborel}. P \vartheta \longrightarrow$

$\ln |x - \cos \vartheta| = (\lambda \vartheta. \ln (\text{norm } (\text{cis } \vartheta - w)) + \ln (\text{norm } (\text{cis } \vartheta - \text{cnj } w)) - \ln 2 - \ln (\text{norm } w)) \vartheta$

$\langle \text{proof} \rangle$

lemma $\text{log-cos-meas}: (\lambda \vartheta :: \text{real}. \ln |x - \cos \vartheta|) \in$

$\text{borel-measurable borel}$

$\langle \text{proof} \rangle$

lemma $\text{log-cos-rhs-meas}: (\lambda \vartheta. \ln (\text{norm } (\text{cis } \vartheta - w)) + \ln (\text{norm } (\text{cis } \vartheta - \text{cnj } w)) - \ln 2 - \ln (\text{norm } w)) \in \text{borel-measurable borel}$

$\langle \text{proof} \rangle$

lemma $\text{log-cos-integrable}: \text{interval-lebesgue-integrable lborel } (\text{ereal } 0) (\text{ereal } (2 * \pi)) (\lambda \vartheta. \ln |x - \cos \vartheta|)$

$\langle \text{proof} \rangle$

$\int -0^{\wedge} \{2\pi\} \log |x - \cos \vartheta| \, d\vartheta = 2\pi(\log \text{jouk}(x) - \log 2).$

lemma log-cos-integral :

$\text{interval-lebesgue-integral lborel } (\text{ereal } 0) (\text{ereal } (2 * \pi)) (\lambda \vartheta. \ln |x -$

$\cos \vartheta|) = 2 * \pi * (\ln (\text{jouk } x) - \ln 2)$
 $\langle \text{proof} \rangle$

lemma *log-cos-half*:
*interval-lebesgue-integral lborel (ereal 0) (ereal pi) ($\lambda \vartheta. \ln |x - \cos \vartheta|$) = $\pi * (\ln (\text{jouk } x) - \ln 2)$*
 $\langle \text{proof} \rangle$

lemma *arcsine-integrable-ln*:
assumes *ab*: $a < b$
shows *integrable (arcsine a b) ($\lambda u. \ln |t - u|$)*
 $\langle \text{proof} \rangle$

lemma *dens-ln-meas*: $(\lambda u. \ln |t - u|) \in \text{borel-measurable borel}$
 $\langle \text{proof} \rangle$

lemma *dens-ln-integrable*:
assumes *ab*: $a < b$
shows *integrable lborel ($\lambda u. \arcsine\text{-dens } a \ b \ u * \ln |t - u|$)*
 $\langle \text{proof} \rangle$

lemma *dens-ln-integral*:
shows $(\int u. \arcsine\text{-dens } a \ b \ u * \ln |t - u| \ \partial \text{lborel}) = \text{logPot } (\arcsine \ a \ b) \ t$
 $\langle \text{proof} \rangle$

(A.1): the potential of the unit arcsine measure.

theorem *arcsine-potential*:
assumes $a < b$
shows $\text{logPot } (\arcsine \ a \ b) \ t =$
 $(\text{if } a \leq t \wedge t \leq b \text{ then } \ln ((b - a) / 4)$
 $\text{else } \ln ((|t - (a + b) / 2| + \text{sqrt } ((t - a) * (t - b))) / 2))$
 $\langle \text{proof} \rangle$

lemma *arcsine-dens-nonneg*: $0 \leq \arcsine\text{-dens } a \ b \ t$
 $\langle \text{proof} \rangle$

lemma *arcsine-finite*: $a < b \implies \text{finite-measure } (\arcsine \ a \ b)$
 $\langle \text{proof} \rangle$

lemma *arcsine-AE*: *AE x in arcsine a b. $a < x \wedge x < b$*
 $\langle \text{proof} \rangle$

lemma *abs-ln-bound*:
fixes $z :: \text{real}$
assumes $0 \leq z < 2$
shows $|\ln z| \leq 2 * \ln 2 - \ln z$
 $\langle \text{proof} \rangle$

lemma *arcsine-swap*:

fixes $a\ b\ c\ d\ L :: \text{real}$

assumes $ab: a < b\ 0 < a\ b < 2$ **and** $cd: c < d\ 0 < c\ d < 2$

and $bnd: \bigwedge x. 0 < x \implies x < 2 \implies$

$L \leq \text{logPot } (\text{arcsine } c\ d)\ x$

shows $\text{integral}^L (\text{arcsine } a\ b) (\text{logPot } (\text{arcsine } c\ d)) =$

$\text{integral}^L (\text{arcsine } c\ d) (\text{logPot } (\text{arcsine } a\ b))$

$\langle \text{proof} \rangle$

$\omega\text{-}\{[a,b]\}([x-r, x+r]) \leq 8\sqrt{r}/(\pi\sqrt{(b-a)}):$ the density is dominated by $(\pi\sqrt{((b-a)/2)})^{-1}((u-a)^{-1/2} + (b-u)^{-1/2})$.

lemma *cos-gap*:

fixes $s\ t :: \text{real}$

assumes $st: 0 \leq s\ s \leq t\ t \leq \pi$

shows $2 * ((t - s) / \pi) ^ 2 \leq \cos s - \cos t$

$\langle \text{proof} \rangle$

lemma *diam-measure*:

fixes $S :: \text{real set}$ **and** $D :: \text{real}$

assumes $ne: S \neq \{\}$ **and** $bdd: \forall x \in S. 0 \leq x$ **and** $dm: \bigwedge x\ y. x \in$

$S \implies y \in S \implies y - x \leq D$

shows $\text{emeasure lborel } S \leq \text{ennreal } D$

$\langle \text{proof} \rangle$

lemma *arcsine-Icc-le*:

assumes $a < b\ 0 \leq r$

shows $\text{emeasure } (\text{arcsine } a\ b) \{x - r..x + r\} \leq \text{ennreal } (8 * \text{sqrt } r / (\pi * \text{sqrt } (b - a)))$

$\langle \text{proof} \rangle$

lemma *arcsine-Icc-le40*:

assumes $a < b\ 1 / 225 < b - a\ 0 \leq r$

shows $\text{emeasure } (\text{arcsine } a\ b) \{x - r..x + r\} \leq \text{ennreal } (40 * \text{sqrt } r)$

$\langle \text{proof} \rangle$

end

theory *Logarithmic-Energy*

imports *Laplace-Sin-Cot-Series*

begin

12 Logarithmic energy of measures on $\mathbb{C}$ and the zero-mass energy inequality

The mutual logarithmic energy $I(\mu, \nu) = \int \int \ln |z - w| d\mu(z) d\nu(w)$ of finite measures on $\mathbb{C}$, the two-dimensional Gaussian integral $\int_{\mathbb{C}} \exp(-b|v|^2) dv = \pi/b$, the non-negativity of the energy of Gaussian kernels, the truncated

kernels $K_n \rightarrow \ln |z - w|$ obtained by integrating the Gaussian against ds/s (Frullani), and the main result *log-energy-zero-mass-nonpos*: for measures $\nu_1, \nu_2 \leq \eta$ of equal mass with $\ln |z - w|$ integrable on $\eta \otimes \eta$ and a null diagonal, $I(\nu_1) - 2 I(\nu_1, \nu_2) + I(\nu_2) \leq 0$.

Mutual logarithmic energy *integral integral* $\log|z - w| \, d\mu(z) \, d\nu(w)$ on $\mathbb{C}$.

definition *logEnergyC* :: *complex measure* $\Rightarrow$ *complex measure* $\Rightarrow$ *real* **where**
 $\text{logEnergyC } \mu \, \nu = \text{integral}^L \mu (\lambda z. \text{integral}^L \nu (\lambda w. \ln (\text{norm } (z - w))))$

Lemma 6.2 (zero-mass logarithmic energy), in the corrected form of the Lean proof: for finite measures $\nu_1, \nu_2 \leq \eta$ on $\mathbb{C}$ of equal mass, with $\log|z-w|$ integrable for $\eta \otimes \eta$ and the diagonal $\eta \otimes \eta$ -null, $I(\nu_1) - 2 I(\nu_1, \nu_2) + I(\nu_2) \leq 0$. (The literal statement with $\log 0 = 0$ is false for point masses; the diagonal hypothesis is what the paper uses.) Proof: Gaussian kernels $e^{-\frac{1}{2}|z-w|^2}$ have nonnegative energy (Fubini), integrate in s against ds/s to reach $\log$ (dominated convergence).

The Gaussian integral on $\mathbb{C}$: $\int e^{-\frac{1}{2}b|v|^2} \, dv = \pi/b$.

lemma *gauss-nn-C*:

fixes $b :: \text{real}$

assumes $b: 0 < b$

shows $(\int^+ v. \text{ennreal } (\exp (- b * (\text{norm } (v :: \text{complex})) ^ 2)) \, \partial \text{lborel}) = \text{ennreal } (\pi / b)$

<proof>

lemma *gauss-integral-C*:

assumes $0 < b$

shows $\text{integral}^L \text{lborel } (\lambda v :: \text{complex}. \exp (- b * (\text{norm } v) ^ 2)) = \pi / b$

<proof>

Convolution of two Gaussians: $\int e^{-\frac{1}{2}s|z-u|^2} e^{-\frac{1}{2}s|w-u|^2} \, du = \pi/(4s) e^{-\frac{1}{2}s|z-w|^2}$.

lemma *gauss-conv*:

assumes $0 < s$

shows $\text{integral}^L \text{lborel } (\lambda u :: \text{complex}. \exp (- 2 * s * (\text{norm } (z - u)) ^ 2) * \exp (- 2 * s * (\text{norm } (w - u)) ^ 2)) = \pi / (4 * s) * \exp (- s * (\text{norm } (z - w)) ^ 2)$

<proof>

definition *gPhi* :: *real* $\Rightarrow$ *complex measure* $\Rightarrow$ *complex* $\Rightarrow$ *real*

where

$\text{gPhi } s \, \mu \, u = \text{integral}^L \mu (\lambda z. \exp (- 2 * s * (\text{norm } (z - u)) ^ 2))$

definition *Eform* :: *complex measure* $\Rightarrow$ *complex measure* $\Rightarrow$ (*complex* $\times$ *complex* $\Rightarrow$ *real*) $\Rightarrow$ *real* **where**

$\text{Eform } \nu_1 \, \nu_2 \, k = \text{integral}^L (\nu_1 \otimes_M \nu_2) (k - 2 * \text{integral}^L (\nu_1 \otimes_M \nu_2) k +$

$\text{integral}^L (\nu_1 \otimes_M \nu_2) k +$

$$\text{integral}^L (\nu 2 \otimes_M \nu 2) k$$

lemma *gPhi-nn*:

fixes $\mu :: \text{complex measure}$

assumes *fm*: finite-measure μ **and** *sm*: sets $\mu = \text{sets borel}$ **and** *s*: $0 \leq s$

shows $\text{ennreal } (gPhi\ s\ \mu\ u) = (\int^+ z. \text{ennreal } (\exp (-2 * s * (\text{norm } (z - u)) ^ 2))\ \partial\mu)$

<proof>

lemma *gPhi-nonneg*: $0 \leq gPhi\ s\ \mu\ u$

<proof>

lemma *gPhi-meas*:

fixes $\mu :: \text{complex measure}$

assumes *fm*: finite-measure μ **and** *sm*: sets $\mu = \text{sets borel}$

shows $gPhi\ s\ \mu \in \text{borel-measurable borel}$

<proof>

lemma *par-exp*:

fixes $z\ w\ u :: \text{complex}$

shows $\exp (-2 * s * (\text{norm } (z - u)) ^ 2) * \exp (-2 * s * (\text{norm } (w - u)) ^ 2) =$

$\exp (-s * (\text{norm } (z - w)) ^ 2) * \exp (- (4 * s) * (\text{norm } (u - (z + w) / 2)) ^ 2)$

<proof>

lemma *gauss-shift-nn*:

fixes $b :: \text{real}$ **and** $m :: \text{complex}$

assumes *b*: $0 < b$

shows $(\int^+ u. \text{ennreal } (\exp (-b * (\text{norm } (u - m)) ^ 2))\ \partial\text{lborel}) = \text{ennreal } (\pi / b)$

<proof>

lemma *conv-nn*:

fixes $z\ w :: \text{complex}$

assumes *s*: $0 < s$

shows $(\int^+ u. \text{ennreal } (\exp (-2 * s * (\text{norm } (z - u)) ^ 2) * \exp (-2 * s * (\text{norm } (w - u)) ^ 2))\ \partial\text{lborel}) =$

$\text{ennreal } (\pi / (4 * s) * \exp (-s * (\text{norm } (z - w)) ^ 2))$

<proof>

Gaussian kernels have nonnegative energy: $E(e^{\sim\{-s|p-1 - p-2|\wedge 2\}}) = (4s/\pi) \int (\Phi-1 - \Phi-2)^{\wedge 2} \geq 0$.

lemma *gauss-pair-nn*:

fixes $\mu\ \nu :: \text{complex measure}$

assumes *fm*: finite-measure μ **and** *fn*: finite-measure ν **and** *sm*: sets $\mu = \text{sets borel}$ **and** *sn*: sets $\nu = \text{sets borel}$ **and** *s*: $0 < s$

shows $(\int^+ u. \text{ennreal } (gPhi\ s\ \mu\ u * gPhi\ s\ \nu\ u)\ \partial\text{lborel}) = \text{ennreal } (\pi / (4 * s)) * (\int^+ z. \int^+ w. \text{ennreal } (\exp (-s * (\text{norm } (z - w)) ^ 2)))$

$(\text{norm } (z - w)) \wedge 2)) \partial \nu \partial \mu)$
 $\langle \text{proof} \rangle$

lemma *gauss-pair*:

assumes *finite-measure* μ *finite-measure* ν *sets* $\mu = \text{sets borel}$ *sets* $\nu = \text{sets borel}$ $0 < s$
shows $\text{integral}^L (\mu \otimes_M \nu) (\lambda p. \exp (-s * (\text{norm } (\text{fst } p - \text{snd } p)) \wedge 2)) = 4 * s / \pi * \text{integral}^L \text{lborel } (\lambda u. gPhi s \mu u * gPhi s \nu u)$
 $\langle \text{proof} \rangle$

lemma *gPhi-prod-int*:

fixes $\mu \nu :: \text{complex measure}$
assumes *fm*: *finite-measure* μ **and** *fn*: *finite-measure* ν **and** *sm*: *sets* $\mu = \text{sets borel}$ **and** *sn*: *sets* $\nu = \text{sets borel}$ **and** $s: 0 < s$
shows $\text{integrable lborel } (\lambda u. gPhi s \mu u * gPhi s \nu u)$
 $\langle \text{proof} \rangle$

lemma *Eform-gauss-nonneg*:

assumes *finite-measure* $\nu 1$ *finite-measure* $\nu 2$ *sets* $\nu 1 = \text{sets borel}$ *sets* $\nu 2 = \text{sets borel}$ $0 < s$
shows $0 \leq Eform \nu 1 \nu 2 (\lambda p. \exp (-s * (\text{norm } (\text{fst } p - \text{snd } p)) \wedge 2))$
 $\langle \text{proof} \rangle$

Frullani-type kernel: $K\text{-}n(p) = (1/2)(\int -\{1/(n+1)\} \wedge \{n+1\} e^{-s}/s \, ds - \int -\{1/(n+1)\} \wedge \{n+1\} e^{-s|p-1 - p-2| \wedge 2}/s \, ds) \longrightarrow \log|p-1 - p-2|$.

definition $Kn :: \text{nat} \Rightarrow \text{complex} \times \text{complex} \Rightarrow \text{real}$ **where**

$Kn \, n \, p = 1 / 2 * (\text{interval-lebesgue-integral lborel } (\text{ereal } (1 / (\text{real } n + 1))))$
 $(\text{ereal } (\text{real } n + 1)) (\lambda s. \exp (-s) / s)$
 $- \text{interval-lebesgue-integral lborel } (\text{ereal } (1 / (\text{real } n + 1)))) (\text{ereal } (\text{real } n + 1)) (\lambda s. \exp (-s * (\text{norm } (\text{fst } p - \text{snd } p)) \wedge 2) / s))$

Helpers on $\int e^{-u}/u \, du$ for the kernels $K\text{-}n$.

lemma *ed-int*:

fixes $x \, y :: \text{real}$
assumes $0 < x$ $0 < y$
shows $\text{interval-lebesgue-integrable lborel } (\text{ereal } x) (\text{ereal } y) (\lambda u. \exp (-u) / u)$
and $\text{interval-lebesgue-integrable lborel } (\text{ereal } x) (\text{ereal } y) (\lambda u. 1 / u)$
 $\langle \text{proof} \rangle$

lemma *inv-ffc*:

fixes $x \, y :: \text{real}$
assumes $x: 0 < x$ **and** $y: 0 < y$
shows $\text{interval-lebesgue-integral lborel } (\text{ereal } (x)) (\text{ereal } (y)) (\lambda u. 1 / u) = \ln y - \ln x$
 $\langle \text{proof} \rangle$

lemma *ed-le*:
fixes $x\ y :: \text{real}$
assumes $x: 0 < x$ **and** $xy: x \leq y$
shows $0 \leq \text{interval-lebesgue-integral lborel } (\text{ereal } (x)) (\text{ereal } (y)) (\lambda u. \exp (- u) /$
 $u)$ **and** $\text{interval-lebesgue-integral lborel } (\text{ereal } (x)) (\text{ereal } (y)) (\lambda u. \exp (- u) /$
 $u) \leq \ln y - \ln x$
 $\langle \text{proof} \rangle$

lemma *ed-abs*:
fixes $x\ r :: \text{real}$
assumes $x: 0 < x$ **and** $r: 0 < r$
shows $|\text{interval-lebesgue-integral lborel } (\text{ereal } (x)) (\text{ereal } (x * r)) (\lambda u. \exp (- u) / u)| \leq |\ln r|$
 $\langle \text{proof} \rangle$

lemma *lbint-bound*:
fixes $x\ y\ C :: \text{real}$ **and** $g :: \text{real} \Rightarrow \text{real}$
assumes $gi: \text{interval-lebesgue-integrable lborel } (\text{ereal } x) (\text{ereal } y) g$ **and** $b: \bigwedge u. \min x\ y$
 $\leq u \implies u \leq \max x\ y \implies |g\ u| \leq C$
shows $|\text{interval-lebesgue-integral lborel } (\text{ereal } (x)) (\text{ereal } (y)) (g)| \leq$
 $C * |y - x|$
 $\langle \text{proof} \rangle$

lemma *Kn-eq*:
assumes $\text{fst } p \neq \text{snd } p$
shows $2 * Kn\ n\ p = \text{interval-lebesgue-integral lborel } (\text{ereal } (1 / (\text{real } n + 1)))$
 $(\text{ereal } (1 /$
 $(\text{real } n + 1) * (\text{norm } (\text{fst } p - \text{snd } p)) ^ 2)) (\lambda u. \exp (- u) / u) -$
 $\text{interval-lebesgue-integral lborel } (\text{ereal } (\text{real } n + 1)) (\text{ereal } ((\text{real } n + 1) * (\text{norm}$
 $(\text{fst } p -$
 $\text{snd } p)) ^ 2)) (\lambda u. \exp (- u) / u)$
 $\langle \text{proof} \rangle$

lemma *ed-near*:
fixes $x\ r :: \text{real}$
assumes $x: 0 < x$ **and** $r: 0 < r$
shows $|\text{interval-lebesgue-integral lborel } (\text{ereal } (x)) (\text{ereal } (x * r)) (\lambda u. \exp (- u) / u) - \ln r| \leq x * |r - 1|$
 $\langle \text{proof} \rangle$

lemma *ed-far*:
fixes $b\ r :: \text{real}$
assumes $b: 0 < b$ **and** $r: 0 < r$
shows $|\text{interval-lebesgue-integral lborel } (\text{ereal } (b)) (\text{ereal } (b * r)) (\lambda u. \exp (- u) / u)| \leq |r - 1| / (b * (\min 1\ r) ^ 2)$
 $\langle \text{proof} \rangle$

lemma *Kn-bound*: $\text{fst } p \neq \text{snd } p \implies$
 $|Kn\ n\ p| \leq 2 * |\ln (\text{norm } (\text{fst } p - \text{snd } p))|$
 $\langle \text{proof} \rangle$

lemma *Kn-tendsto*: $\text{fst } p \neq \text{snd } p \implies$
 $((\lambda n. Kn\ n\ p) \longrightarrow \ln (\text{norm } (\text{fst } p - \text{snd } p)))\ \text{at-top}$
 $\langle \text{proof} \rangle$

lemma *Kn-int-P*:
fixes $P :: (\text{complex} \times \text{complex})\ \text{measure}$
assumes fP : *finite-measure* P **and** sP : $\text{sets } P = \text{sets } (\text{borel } \otimes_M \text{ borel})$
shows $\text{integral}^L P (Kn\ n) = 1 / 2 * (\text{interval-lebesgue-integral } \text{lborel } (\text{ereal } (1 /$
 $(\text{real } n + 1))) (\text{ereal } (\text{real } n + 1)) (\lambda s. \exp (- s) / s) * \text{measure } P (\text{space } P) -$
 $\text{integral}^L \text{lborel } (\lambda s. \text{indicator } \{1 / (\text{real } n + 1) <..< \text{real } n + 1\} s / s *$
 $\text{integral}^L P (\lambda p. \exp (- s * (\text{norm } (\text{fst } p - \text{snd } p)) ^ 2)))$
and $\text{integrable } \text{lborel } (\lambda s. \text{indicator } \{1 / (\text{real } n + 1) <..< \text{real } n + 1\} s / s *$
 $\text{integral}^L P (\lambda p. \exp (- s * (\text{norm } (\text{fst } p - \text{snd } p)) ^ 2)))$
 $\langle \text{proof} \rangle$

lemma *Eform-Kn-nonpos*:
assumes *finite-measure* $\nu 1$ *finite-measure* $\nu 2$ $\text{sets } \nu 1 = \text{sets } \text{borel } \text{sets } \nu 2 =$
 $\text{sets } \text{borel } \text{emeasure } \nu 1\ UNIV = \text{emeasure } \nu 2\ UNIV$
shows $Eform\ \nu 1\ \nu 2\ (Kn\ n) \leq 0$
 $\langle \text{proof} \rangle$

Integrability passes to a smaller measure with the same sets.

lemma *integrable-le-measure*:
fixes $f :: 'a \Rightarrow \text{real}$
assumes PQ : $P \leq Q$ **and** s : $\text{sets } P = \text{sets } Q$ **and** fi : *integrable* $Q\ f$
shows *integrable* $P\ f$
 $\langle \text{proof} \rangle$

lemma *Kn-meas*: $Kn\ n \in \text{borel-measurable } (\text{borel } \otimes_M \text{ borel} :: (\text{complex} \times$
 $\text{complex})\ \text{measure})$
 $\langle \text{proof} \rangle$

Dominated convergence: $\int K\ n\ dP \longrightarrow \int \log|p-1 - p-2| dP$ for $P \leq Q$
with $\log\ Q$ -integrable and the diagonal Q -null.

lemma *Kn-integral-tendsto*:
assumes $P \leq Q$ $\text{sets } P = \text{sets } (\text{borel } \otimes_M \text{ borel})$ $\text{sets } Q =$
 $\text{sets } (\text{borel } \otimes_M \text{ borel})$
and *integrable* $Q\ (\lambda p :: \text{complex} \times \text{complex}. \ln (\text{norm } (\text{fst } p -$
 $\text{snd } p)))$ $\text{emeasure } Q\ \{p. \text{fst } p = \text{snd } p\} = 0$
shows $((\lambda n. \text{integral}^L P (Kn\ n)) \longrightarrow \text{integral}^L P$
 $(\lambda p. \ln (\text{norm } (\text{fst } p - \text{snd } p))))\ \text{at-top}$
 $\langle \text{proof} \rangle$

lemma *finite-le-measure*:
assumes $\nu \leq \eta$ $\text{sets } \nu = \text{sets } \eta$ *finite-measure* η

shows *finite-measure* ν
 $\langle \text{proof} \rangle$

lemma *pair-measure-mono*:

assumes $\nu \leq \eta$ $\nu' \leq \eta$ *sets* $\nu = \text{sets borel sets } \nu' =$
sets borel sets $\eta = \text{sets borel finite-measure } \eta$
shows $(\nu \otimes_M \nu') \leq (\eta \otimes_M \eta)$
 $\langle \text{proof} \rangle$

lemma *logEnergyC-prod*:

fixes $\mu \nu :: \text{complex measure}$
assumes *fm*: *finite-measure* μ **and** *fn*: *finite-measure* ν **and** *int*: *integrable* $(\mu$
 $\otimes_M \nu)$ $(\lambda p. \ln (\text{norm } (\text{fst } p - \text{snd } p)))$
shows *logEnergyC* $\mu \nu = \text{integral}^L (\mu \otimes_M \nu)$ $(\lambda p. \ln$
 $(\text{norm } (\text{fst } p - \text{snd } p)))$
 $\langle \text{proof} \rangle$

theorem *log-energy-zero-mass-nonpos*:

fixes $\nu 1 \nu 2 \eta :: \text{complex measure}$
assumes *finite-measure* η *sets* $\nu 1 = \text{sets borel sets } \nu 2 =$
sets borel sets $\eta = \text{sets borel}$
and $\nu 1 \leq \eta$ $\nu 2 \leq \eta$ *emeasure* $\nu 1 \text{ UNIV} = \text{emeasure } \nu 2 \text{ UNIV}$
and *integrable* $(\eta \otimes_M \eta)$ $(\lambda zw. \ln (\text{norm } (\text{fst } zw - \text{snd } zw)))$
and *emeasure* $(\eta \otimes_M \eta) \{zw. \text{fst } zw = \text{snd } zw\} = 0$
shows *logEnergyC* $\nu 1 \nu 1 - 2 * \text{logEnergyC } \nu 1 \nu 2 + \text{logEnergyC } \nu 2 \nu 2 \leq 0$
 $\langle \text{proof} \rangle$

end

theory *Andreief-Identity*

imports *Jordan-Normal-Form.Determinant HOL-Analysis.Analysis*
begin

13 Andreief's identity (continuous Cauchy–Binet)

For a σ -finite measure μ and functions φ_i, ψ_j with $\varphi_i \psi_j$ integrable, $\det [\int \varphi_i \psi_j d\mu] = (1/n!) \int \det [\varphi_a(x_b)] \det [\psi_a(x_b)] d\mu^{\otimes n}$, with the determinants of the *Jordan_Normal_Form* library and the product measure Pi_M ; also the transposition and column-scaling rules for determinants used with it.

The general continuous Cauchy-Binet (Andreief) identity: $\det [\int \varphi_i \psi_j d\mu] = (1/n!) \int \det [\varphi_a(x_b)] \det [\psi_a(x_b)] d\mu^{\otimes n}$. Proof: Leibniz expansion, symmetrisation over permutations, Fubini on Pi_M .

theorem *andreief*:

fixes $\mu :: \text{real measure}$ **and** $\varphi \psi :: \text{nat} \Rightarrow \text{real} \Rightarrow \text{real}$ **and**
 $n :: \text{nat}$
assumes *sf*: *sigma-finite-measure* μ
and *integ*: $\bigwedge i j. i < n \implies j < n \implies$

```

    integrable μ (λx. φ i x * ψ j x)
  shows Determinant.det (Matrix.mat n n (λ(i,
    j). integralL μ (λx. φ i x * ψ j x))) =
    1 / fact n * integralL (PiM {..n} (λ-. μ))
    (λx. Determinant.det (Matrix.mat n n (λ(a, b). φ a (x b))) *
      Determinant.det (Matrix.mat n n (λ(a, b). ψ a (x b))))
⟨proof⟩

(6.10): Δ-K(ζ(5)) = (1/h!) ∫-(0,∞)h ∏-(i<j) (y-i2 - y-j2)2 ∏-i
D-N(y-i2)6/D-K(y-i2) w(y-i) dy.

lemma andreief-det-swap:
  fixes f :: nat ⇒ nat ⇒ 'a :: comm-ring-1
  shows Determinant.det (Matrix.mat n n (λ(a, b). f b a)) =
    Determinant.det (Matrix.mat n n (λ(a, b). f a b))
⟨proof⟩

lemma andreief-det-scale-cols:
  fixes f :: nat ⇒ nat ⇒ 'a :: comm-ring-1 and c :: nat ⇒ 'a
  shows Determinant.det (Matrix.mat n n (λ(a, b). f a b * c b)) = (∏b < n c b) *
    Determinant.det (Matrix.mat n n (λ(a, b). f a b))
⟨proof⟩
end

theory Zeta5-Definitions
  imports Rational-Padic-Valuations Arcsine-Distribution Logarithmic-Energy
    Zeta-Function.Zeta-Function
    Kummer-Congruence.Rat-Congruence
    Jordan-Normal-Form.Determinant
    Jordan-Normal-Form.DL-Rank
    HOL-Computational-Algebra.Polynomial-FPS
    HOL-Library.Log-Nat
begin

```

14 Definitions of the construction

All definitions of the proof, transcribed from the Lean 4 theory *Defs* of the domino14/zeta5 formalisation, which fixed the conventions used throughout:

- A rational function in t is a numerator polynomial together with a finite set of simple poles: $\mu_X S P$ is $\mu_X(P(t) / \prod_{j \in S} (t + j^2))$ and $\tau_X S P$ is $\tau_X(P(x) / \prod_{r \in S} (x - r))$. Values are polynomials in $\mathbb{Q}[X]$; the indeterminate X is later specialised to $\zeta(5)$.
- The p -adic field $\mathbb{Q}_p$ of the paper's Sections 3.1–3.2 is not used. Every p -adically convergent series is replaced by its partial sum of length M (the *-tr* definitions) and the identities become congruences modulo high powers of p , so that the whole development stays in HOL over $\mathbb{Q}$.

- Matrices are those of the `Jordan_Normal_Form` library, indexed by explicit lists of index pairs instead of Lean's Σ -types. Equation and section numbers refer to Fauzan's paper.

14.1 Generic helpers

Evaluation of a rational polynomial at a real (Lean: `aeval x P`).

definition `real-eval :: rat poly  $\Rightarrow$  real  $\Rightarrow$  real` **where**
`real-eval P x = poly (map-poly of-rat P) x`

14.2 Section 2.1 Parameters (2.1)

definition `Nof :: nat  $\Rightarrow$  nat` **where** `Nof K = 3 * K div 40`
definition `hof :: nat  $\Rightarrow$  nat` **where** `hof K = 37 * K div 40`
definition `alpha-q :: rat` **where** `alpha-q = 3 / 40`
definition `lam-q :: rat` **where** `lam-q = 37 / 40`
definition `Hc-q :: rat` **where** `Hc-q = 1 + 2 * alpha-q`

The real number $\zeta(5)$; `zeta` is the AFP's Riemann zeta function.

definition `zeta5 :: real` **where** `zeta5 = Re (zeta 5)`

$$H\text{-}j^{\wedge\{5\}} = \sum \text{-}\{v=1\}^{\wedge j} v^{\wedge -5}.$$

definition `H5 :: nat  $\Rightarrow$  rat` **where** `H5 j = ( $\sum v = 1..j. 1 / \text{of-nat } v^{\wedge 5}$ )`

$$D\text{-}m(t) = \prod \text{-}\{j=1\}^{\wedge m} (t + j^{\wedge 2}).$$

definition `Dm :: nat  $\Rightarrow$  rat poly` **where** `Dm m = ( $\prod j = 1..m. pX + [\text{of-nat } j^{\wedge 2}]$ )`

14.3 Section 2.1 The functional `mu_X` (2.2), (2.3)

(2.2): $\text{mu}(t^{\wedge e}) = (-1)^{\wedge e} B\text{-}\{2e+2\} (2e+3)(2e+4)(2e+5)/24$, with $B\text{-}1 = -1/2$ (both Mathlib's `bernoulli` and the AFP's polymorphic `bernoulli` use this convention).

definition `muMono :: nat  $\Rightarrow$  rat` **where**
`muMono e = (-1)^{\wedge e} * bernoulli (2 * e + 2) *
 ((2 * of-nat e + 3) * (2 * of-nat e + 4) * (2 * of-nat e + 5)) / 24`

definition `muPoly :: rat poly  $\Rightarrow$  rat` **where**
`muPoly P = ( $\sum e \leq \text{degree } P. \text{Polynomial.coeff } P e * \text{muMono } e$ )`

$$(2.3): \text{mu}\text{-}X(1/(t+j^{\wedge 2})) = j^{\wedge 4}(X - H\text{-}j) - 1/4 + 1/(2j).$$

definition `muPole :: nat  $\Rightarrow$  rat poly` **where**
`muPole j = [\text{of-nat } j^{\wedge 4}] * (pX - [H5 j]) - [1 / 4:] + [1 / (2 * of-nat j):]`

definition `sqPoleProd :: nat set  $\Rightarrow$  rat poly` **where**

$$sqPoleProd\ S = (\prod_{j \in S} pX + [:of\text{-}nat\ j\ \wedge\ 2:])$$

Residue of $P/\prod_{k \in S}(t+k\wedge 2)$ at $t = -j\wedge 2$.

definition $sqResidue :: nat\ set \Rightarrow rat\ poly \Rightarrow nat \Rightarrow rat$ **where**

$$sqResidue\ S\ P\ j = poly\ P\ (-\ (of\text{-}nat\ j\ \wedge\ 2)) / (\prod_{k \in S - \{j\}} of\text{-}nat\ k\ \wedge\ 2 - (of\text{-}nat\ j\ \wedge\ 2))$$

$mu\text{-}X(P(t)/\prod_{j \in S}(t+j\wedge 2))$ by polynomial division and simple partial fractions (meaningful for finite S with $0 \notin S$).

definition $muX :: nat\ set \Rightarrow rat\ poly \Rightarrow rat\ poly$ **where**

$$muX\ S\ P = [:muPoly\ (P\ div\ sqPoleProd\ S):] + (\sum_{j \in S} [:sqResidue\ S\ P\ j:] * muPole\ j)$$

14.4 Section 2.1 The matrix, determinant and normalisation (2.4), (2.5)

$$(2.4): G\text{-}K(X) = [mu\text{-}X(D\text{-}N(t)\wedge 6\ t\wedge\{i+j\} / D\text{-}K(t))]\text{-}\{0 \leq i,j < h\}.$$

definition $GK :: nat \Rightarrow rat\ poly\ mat$ **where**

$$GK\ K = Matrix.mat\ (hof\ K)\ (hof\ K)\ (\lambda(i,j). muX\ \{1..K\}\ (Dm\ (Nof\ K)\ \wedge\ 6 * pX\ \wedge\ (i + j)))$$

definition $DeltaK :: nat \Rightarrow rat\ poly$ **where** $DeltaK\ K = Determinant.det\ (GK\ K)$

$$(2.5): S\text{-}K = (K!)\wedge\{2h\}\ 4\wedge\{h-1\} / ((N!)\wedge\{12h\} \prod_{i=1}^h \wedge\{h-1\} ((2i!)\wedge 2).$$

definition $SK :: nat \Rightarrow rat$ **where**

$$SK\ K = (fact\ K\ \wedge\ (2 * hof\ K) * 4\ \wedge\ (hof\ K - 1)) / (fact\ (Nof\ K)\ \wedge\ (12 * hof\ K) * (\prod_{i=1}^{hof\ K - 1} fact\ (2 * i)\ \wedge\ 2))$$

definition $FK :: nat \Rightarrow rat\ poly$ **where** $FK\ K = [:SK\ K:] * DeltaK\ K$

14.5 Section 3 The functional τ_X

$L(x\wedge k) = B\text{-}k$, extended linearly.

definition $Lfun :: rat\ poly \Rightarrow rat$ **where**

$$Lfun\ P = (\sum_{k \leq degree\ P} Polynomial.coeff\ P\ k * bernoulli\ k)$$

$\tau(P) = L(P''')/24$ on polynomials.

definition $tau :: rat\ poly \Rightarrow rat$ **where**

$$tau\ P = Lfun\ ((pderiv\ \wedge\ 3)\ P) / 24$$

$d(r) = r$ for $r \geq 0$ and $-r-1$ for $r < 0$.

definition $dIdx :: int \Rightarrow nat$ **where**

$$dIdx\ r = (if\ 0 \leq r\ then\ nat\ r\ else\ nat\ (-\ r - 1))$$

$$\tau\text{-}X(1/(x-r)) = H\text{-}\{d(r)\} - X.$$

definition $\text{tauPole} :: \text{int} \Rightarrow \text{rat poly}$ **where**
 $\text{tauPole } r = [\text{H5 } (dIdx \ r) :] - pX$

definition $\text{linPoleProd} :: \text{int set} \Rightarrow \text{rat poly}$ **where**
 $\text{linPoleProd } S = (\prod r \in S. pX - [: \text{of-int } r :])$

definition $\text{linResidue} :: \text{int set} \Rightarrow \text{rat poly} \Rightarrow \text{int} \Rightarrow \text{rat}$ **where**
 $\text{linResidue } S \ P \ r = \text{poly } P \ (\text{of-int } r) / (\prod s \in S - \{r\}. \text{of-int } r - \text{of-int } s)$

$\tau \cdot X(P(x)/\prod -\{r \in S\}(x-r))$ by polynomial division and simple partial fractions.

definition $\text{tauX} :: \text{int set} \Rightarrow \text{rat poly} \Rightarrow \text{rat poly}$ **where**
 $\text{tauX } S \ P = [: \text{tau } (P \text{ div } \text{linPoleProd } S) :] + (\sum r \in S. [: \text{linResidue } S \ P \ r :] * \text{tauPole } r)$

The fourth Taylor coefficient $g'''(0)/24$ of $g = P/Q$ at 0 (needs $Q(0) \neq 0$).

definition $\text{taylor4} :: \text{rat poly} \Rightarrow \text{rat poly} \Rightarrow \text{rat}$ **where**
 $\text{taylor4 } P \ Q = \text{fps-nth } (\text{fps-of-poly } P * \text{inverse } (\text{fps-of-poly } Q)) \ 4$

The poles $\pm j, j \in S$ (Lean: *signedPoles*).

definition $\text{signedPoles} :: \text{nat set} \Rightarrow \text{int set}$ **where**
 $\text{signedPoles } S = \text{int } ' S \cup (\lambda j. - \text{int } j) ' S$

The poles $-K \leq r \leq K, r \neq 0$, of Lemma 3.3.

definition $\text{symPoles} :: \text{nat} \Rightarrow \text{int set}$ **where**
 $\text{symPoles } K = \{r. - \text{int } K \leq r \wedge r \leq \text{int } K \wedge r \neq 0\}$

A is p -integer-valued on $\mathbb{Z}$ (Lean: *IntValuedAt*).

definition $\text{IntValuedAt} :: \text{nat} \Rightarrow \text{rat poly} \Rightarrow \text{bool}$ **where**
 $\text{IntValuedAt } p \ A \longleftrightarrow$
 $(\forall x :: \text{int}. \text{poly } A \ (\text{of-int } x) \neq 0 \longrightarrow$
 $0 \leq \text{vp } p \ (\text{poly } A \ (\text{of-int } x)))$

14.6 Section 3.1-3.2 The p -adic extension, in truncated rational form

$\kappa \cdot d = d(d-1)(d-2) B-\{d-3\}/24$, so that $\tau(z^{\wedge}d) = \kappa \cdot d$; it is 0 for $d < 3$.

definition $\text{kappa} :: \text{nat} \Rightarrow \text{rat}$ **where**
 $\text{kappa } d = \text{of-nat } d * (\text{of-nat } d - 1) * (\text{of-nat } d - 2) * \text{bernoulli } (d - 3) / 24$

τ on polynomials through κ (equal to *tau*).

definition $\text{tauK} :: \text{rat poly} \Rightarrow \text{rat}$ **where**
 $\text{tauK } Q = (\sum d \leq \text{degree } Q. \text{Polynomial.coeff } Q \ d * \text{kappa } d)$

(3.5), truncated: the partial sum of length M of $\tau \cdot \{an\}(1/(z-s)) = -(1/4) \sum -\{k \geq 0\} \ C(k+3,3) \ B-k \ s^{\wedge}\{-k-4\}$ (for $v\text{-}p(s) < 0$ the k -th term has valuation $\geq k+3$, so the tail is $\equiv 0 \text{ mod } p^{\wedge}\{M+3\}$).

definition $\text{tauAnPole-tr} :: \text{nat} \Rightarrow \text{rat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$\text{tauAnPole-tr } p \ s \ M =$
 $-(1 / 4) * (\sum k < M. \text{of-nat } ((k + 3) \text{ choose } 3) * \text{bernoulli } k * s \text{ powi } (-$
 $(\text{int } k + 4)))$

(3.6), truncated: $C-p = \sum -\{a=1\} \wedge \{p-1\} \tau \wedge \{an\} (1/(x + a/p))$.

definition $Cp\text{-tr} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$Cp\text{-tr } p \ M = (\sum a = 1..p - 1. \text{tauAnPole-tr } p \ (- \text{of-nat } a / \text{of-nat } p) \ M)$

(3.6): $Y = p \wedge 5 \ X + C-p$.

definition $Yp\text{-tr} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat poly}$ **where**

$Yp\text{-tr } p \ M = [: \text{of-nat } p \wedge 5:] * pX + [: Cp\text{-tr } p \ M:]$

Value of $\tau \cdot Y \wedge \{ext\}$ on the simple pole $1/(z-s)$: near (integer) poles take $H-\{d(s)\} - Y$, far poles the truncated series.

definition $\text{tauPoleP-tr} :: \text{nat} \Rightarrow \text{rat poly} \Rightarrow \text{rat} \Rightarrow \text{nat}$

$\Rightarrow \text{rat poly}$ **where**

$\text{tauPoleP-tr } p \ Y \ s \ M =$
 $(\text{if } \text{snd } (\text{quotient-of } s) = 1 \text{ then } [:H5 \ (dIdx \ (\text{fst } (\text{quotient-of } s)))] - Y$
 $\text{else } [: \text{tauAnPole-tr } p \ s \ M:])$

definition $qPoleProd :: \text{rat set} \Rightarrow \text{rat poly}$ **where**

$qPoleProd \ S = (\prod s \in S. pX - [:s:])$

definition $qRes :: \text{rat set} \Rightarrow \text{rat poly} \Rightarrow \text{rat} \Rightarrow \text{rat}$ **where**

$qRes \ S \ P \ s = \text{poly } P \ s / (\prod s' \in S - \{s\}. s - s')$

$\tau \cdot Y \wedge \{ext\} (U(z) / \prod -\{s \in S\} (z-s))$ for distinct rational poles S , truncated at M .

definition $\text{tauExt-tr} :: \text{nat} \Rightarrow \text{rat poly} \Rightarrow \text{rat poly} \Rightarrow \text{rat set}$

$\Rightarrow \text{nat} \Rightarrow \text{rat poly}$ **where**

$\text{tauExt-tr } p \ Y \ U \ S \ M =$
 $[: \text{tauK } (U \text{ div } qPoleProd \ S):] + (\sum s \in S. [:qRes \ S \ U \ s:] * \text{tauPoleP-tr } p \ Y \ s$
 $M)$

$g(a + p \ x)$ written as $U(x) / \prod (x - s)$: the numerator $p \wedge \{-|S|\} P(a + p \ x)$.

definition $\text{distribNum} :: \text{nat} \Rightarrow \text{int set} \Rightarrow \text{rat poly} \Rightarrow \text{nat}$

$\Rightarrow \text{rat poly}$ **where**

$\text{distribNum } p \ S \ P \ a =$
 $[: \text{of-nat } p \text{ powi } (- \text{int } (\text{card } S)):] * pcompose \ P \ ([: \text{of-nat } a:] + [: \text{of-nat } p:] *$
 $pX)$

The poles $(r - a)/p$ of $g(a + p \ x)$.

definition $\text{distribPoles} :: \text{nat} \Rightarrow \text{int set} \Rightarrow \text{nat} \Rightarrow \text{rat set}$ **where**

$\text{distribPoles } p \ S \ a = (\lambda r. (\text{of-int } r - \text{of-nat } a) / \text{of-nat } p) ' S$

The Taylor coefficients of the analytic part $Q + \sum -\{s \in F\} \varrho \cdot s / (z-s)$.

definition $fCoeff :: rat \Rightarrow poly \Rightarrow rat \Rightarrow set \Rightarrow (rat \Rightarrow rat)$
 $\Rightarrow nat \Rightarrow rat$ **where**
 $fCoeff \ Q \ F \ \varrho \ d = Polynomial.coeff \ Q \ d - (\sum \ s \in F. \ \varrho \ s * inverse \ s \wedge (d + 1))$

14.7 Section 3.3 Small primes

$$q-0 = 1, q-i(t) = (-1)^i 2t D-\{i-1\}(t)/(2i)!.$$

definition $qBasis :: nat \Rightarrow rat \Rightarrow poly$ **where**
 $qBasis \ i = (if \ i = 0 \ then \ 1 \ else \ [:(-1)^i * 2 / fact \ (2 * i):] * pX * Dm \ (i - 1))$

$$f-i(t) = (D-N(t)/(N!)^2)^3 q-i(t).$$

definition $fBasis :: nat \Rightarrow nat \Rightarrow rat \Rightarrow poly$ **where**
 $fBasis \ K \ i = ([1 / fact \ (Nof \ K) \wedge 2:] * Dm \ (Nof \ K)) \wedge 3 * qBasis \ i$

14.8 Section 4.1 The inner range

$$l-A(a) = \#\{1 \leq j \leq A : j \equiv \pm a \pmod{p}\}.$$

definition $ell :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat$ **where**
 $ell \ p \ A \ a = card \ \{j \in \{1..A\}. \ j \bmod p = a \bmod p \vee (j + a) \bmod p = 0\}$

definition $mHalf :: nat \Rightarrow nat$ **where** $mHalf \ p = (p - 1) \div 2$

definition $L0 :: nat \Rightarrow nat$ **where** $L0 \ M = 4 * M + 10$

Right-hand side of (4.4): $h - L-0 + 3(N - m-N)$.

definition $rhs44 :: nat \Rightarrow nat \Rightarrow nat \Rightarrow int$ **where**
 $rhs44 \ K \ M \ p = int \ (hof \ K) - int \ (L0 \ M) + 3 * (int \ (Nof \ K) - int \ (Nof \ K \div p))$

(4.4): T and E (integer division by the positive number $m = (p-1)/2$).

definition $Tin :: nat \Rightarrow nat \Rightarrow nat \Rightarrow int$ **where** $Tin \ K \ M \ p = rhs44 \ K \ M \ p \div int \ (mHalf \ p)$

definition $Ein :: nat \Rightarrow nat \Rightarrow nat \Rightarrow int$ **where** $Ein \ K \ M \ p = rhs44 \ K \ M \ p \bmod int \ (mHalf \ p)$

$$b-a = 3 \ l-N(a).$$

definition $bIn :: nat \Rightarrow nat \Rightarrow nat \Rightarrow int$ **where** $bIn \ K \ p \ a = 3 * int \ (ell \ p \ (Nof \ K) \ a)$

Position of class a in the ordering by decreasing $l-K$, ties by increasing a .

definition $defaultPos :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat$ **where**
 $defaultPos \ K \ p \ a = card \ \{c \in \{1..mHalf \ p\}. \ ell \ p \ K \ a < ell \ p \ K \ c \vee (ell \ p \ K \ c = ell \ p \ K \ a \wedge c < a)\}$

$\varepsilon-a = 1$ for the first E classes in that ordering.

definition $epsIn :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat \Rightarrow int$

where

$epsIn\ K\ M\ p\ a =$
 $(if\ int\ (card\ \{c \in \{1..mHalf\ p\}. defaultPos\ K\ p\ c < defaultPos\ K\ p\ a\}) <$
 $Ein\ K\ M\ p\ then\ 1\ else\ 0)$

$L-a = T - b-a + \varepsilon-a$ for $a \geq 1$, and $L-0 = 4M + 10$.

definition $Lin :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat \Rightarrow int$

where

$Lin\ K\ M\ p\ a = (if\ a = 0\ then\ int\ (L0\ M)\ else\ Tin\ K\ M\ p - bIn\ K\ p\ a + epsIn$
 $K\ M\ p\ a)$

$Z-a = T + \varepsilon-a$.

definition $Zin :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat \Rightarrow int$

where $Zin\ K\ M\ p\ a = Tin\ K\ M\ p + epsIn\ K\ M\ p\ a$

(4.6), (4.7): the row weights $w-\{a,i\}$.

definition $wIn :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat \Rightarrow nat$

$\Rightarrow rat$ **where**

$wIn\ K\ M\ p\ a\ i =$
 $(if\ a = 0\ then$
 $Min\ (insert\ (2 * of-nat\ i + 6 * of-nat\ (Nof\ K\ div\ p) - of-nat\ (K\ div\ p) +$
 $1\ /\ 2)$
 $((\lambda c. of-int\ (Zin\ K\ M\ p\ c) - (of-nat\ (ell\ p\ K\ c) + 4) /\$
 $2) '\{1..mHalf\ p\}))$
 $else\ of-nat\ i + of-int\ (bIn\ K\ p\ a) - (of-nat\ (ell\ p\ K\ a) + 4) /\ 2)$

(4.8): $\gamma \cdot p \wedge i = 2 \sum -\{a=0\} \wedge m \sum -\{i < L-a\} w-\{a,i\}$.

definition $gammaIn :: nat \Rightarrow nat \Rightarrow nat \Rightarrow rat$ **where**

$gammaIn\ K\ M\ p = 2 * (\sum a \leq mHalf\ p. \sum i < nat\ (Lin\ K\ M\ p\ a). wIn\ K\ M$
 $p\ a\ i)$

Index list of the inner basis: pairs (a, i) with $0 \leq a \leq m, i < L-a$ (Lean's Σ -type $InnerIdx$, enumerated).

definition $inner-idx :: nat \Rightarrow nat \Rightarrow nat \Rightarrow (nat \times$

$nat)$ **list** **where**

$inner-idx\ K\ M\ p = concat\ (map\ (\lambda a. map\ (\lambda i. (a,$
 $i))\ [0..<nat\ (Lin\ K\ M\ p\ a)])\ [0..<mHalf\ p + 1])$

(4.5): $E-\{a,i\}(t) = \prod -\{c \neq a\} (t + c \wedge 2) \wedge \{L-c\} (t + a \wedge 2) \wedge i$.

definition $innerBasis :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat \times$

$nat \Rightarrow rat\ poly$ **where**

$innerBasis\ K\ M\ p\ x =$
 $(\prod c \in \{0..mHalf\ p\} - \{fst\ x\}. (pX + [:of-nat\ c \wedge 2:]) \wedge nat\ (Lin\ K\ M\ p\ c))$
 $*$
 $(pX + [:of-nat\ (fst\ x) \wedge 2:]) \wedge snd\ x$

The Gram matrix of $\mu-X(D-N \wedge 6 \cdot / D-K)$ in the inner basis.

definition $innerGram :: nat \Rightarrow nat \Rightarrow nat \Rightarrow rat\ poly\ mat$ **where**

$innerGram\ K\ M\ p = (let\ idx = inner-idx\ K\ M\ p\ in$
 $Matrix.mat\ (length\ idx)\ (length\ idx)$
 $(\lambda(x, y). muX\ \{1..K\}\ (Dm\ (Nof\ K)\ \wedge\ 6 * innerBasis\ K\ M\ p\ (idx\ !\ x) * innerBasis\ K\ M\ p\ (idx\ !\ y))))$

definition $wInIdx :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat \times nat \Rightarrow rat$ **where**
 $wInIdx\ K\ M\ p\ x = wIn\ K\ M\ p\ (fst\ x)\ (snd\ x)$

14.9 Section 4.2 The outer range

$r-p = max(0, K + 4N - 2p + 2)$ from (4.10) (truncated subtraction).

definition $rOut :: nat \Rightarrow nat \Rightarrow nat$ **where** $rOut\ K\ p =$
 $K + 4 * Nof\ K + 2 - 2 * p$

(4.14): $\gamma-p \hat{out}$, with $v = K - p \lfloor K/p \rfloor$, $u = max(0, N+v-p+1)$, $t-p = min(N, v) + u$.

definition $gammaOut :: nat \Rightarrow nat \Rightarrow int$ **where**
 $gammaOut\ K\ p = (let\ v = K\ mod\ p; u = Nof\ K + v + 1 - p; tp = min\ (Nof\ K)\ v + u\ in$
 $if\ K < 2 * p$
 $then - 7 * (int\ K - int\ p) + 6 * int\ tp - 1 - min\ (int\ (rOut\ K\ p))\ (int\ p - 1 - int\ (Nof\ K) + int\ u)$
 $else - 7 * (int\ K - int\ p) + 3 + 12 * int\ (Nof\ K) + 5 * int\ tp - min\ (int\ (rOut\ K\ p))\ (int\ p + int\ u))$

(4.9): the hypotheses of the outer-range estimate.

definition $OuterHyp :: nat \Rightarrow nat \Rightarrow bool$ **where**
 $OuterHyp\ K\ p \iff 7 \leq p \wedge p \leq K \wedge K < 3 * p \wedge$
 $2 * K < p \wedge 2 * Nof\ K < p \wedge 5 * Nof\ K \leq 2 * p - 2$

The poles of D -tail in the class $\pm a \pmod p$ ($a = 0$: multiples of p).

definition $outerClassPoles :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat\ set$ **where**
 $outerClassPoles\ K\ p\ a = \{j \in \{Nof\ K + 1..K\}. j\ mod\ p = a\ mod\ p \vee (j + a)\ mod\ p = 0\}$

definition $outerCount :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat$ **where**
 $outerCount\ K\ p\ a = card\ (outerClassPoles\ K\ p\ a)$

definition $outer-idx :: nat \Rightarrow nat \Rightarrow (nat \times nat)\ list$ **where**
 $outer-idx\ K\ p = concat\ (map\ (\lambda a. map\ (\lambda i. (a, i))\ [0..<outerCount\ K\ p\ a])\ [0..<mHalf\ p + 1])$

(4.11): rows $P-a\ q-\{a, i\}$ with $P-a = D-tail/Q-a$; the zero class is read as $P-0\ (t + p \wedge 2) \hat{i}$ (ambiguity recorded in the Lean NOTES, finding 1).

definition $outerBasis :: nat \Rightarrow nat \Rightarrow nat \times$

$\text{nat} \Rightarrow \text{rat poly}$ **where**
 $\text{outerBasis } K \ p \ x = (\text{let } a = \text{fst } x; \ i = \text{snd } x;$
 $\quad Pa = \text{sqPoleProd } (\{ \text{Nof } K + 1..K \} - \text{outerClassPoles } K \ p \ a) \text{ in}$
 $\quad \text{if } a = 0 \text{ then } Pa * (pX + [: \text{of-nat } p \wedge 2:]) \wedge i$
 $\quad \text{else } (\text{let } l = \text{ell } p \ K \ a \text{ in}$
 $\quad \quad \text{if } i < l - 2 \text{ then } Pa * (pX + [: \text{of-nat } a \wedge 2:]) \wedge i$
 $\quad \quad \text{else } Pa * \text{sqPoleProd } \{j \in \text{outerClassPoles } K \ p \ a. \ p <$
 $\quad \quad j\} * (pX + [: \text{of-nat } a \wedge 2:]) \wedge (i - (l - 2)))$

(4.12) and the zero-class weights.

definition $wOut :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \times \text{nat} \Rightarrow \text{rat}$ **where**
 $wOut \ K \ p \ x = (\text{let } a = \text{fst } x; \ i = \text{snd } x \text{ in}$
 $\quad \text{if } a = 0 \text{ then } (\text{if } \text{outerCount } K \ p \ 0 = 1 \text{ then } -1 / 2 \text{ else if } i = 0 \text{ then } -2$
 $\text{else } 0)$
 $\quad \text{else } (\text{let } l = \text{ell } p \ K \ a; \ d = (\text{if } a \leq \text{Nof } K \text{ then } 1 \text{ else } 0 :: \text{rat}) \text{ in}$
 $\quad \quad \text{if } i < l - 2 \text{ then } \min 0 \ (\text{of-nat } i + 3 * d - (\text{of-nat } l + 4) / 2) \text{ else } 0))$

The integer $c\text{-}e \equiv p \ \mu(t \wedge e) \pmod p$ in $[0, p)$, with $c\text{-}e = 0$ for $e < 2p-3$ ($(q \bmod)$ is the AFP's residue of a rational modulo an integer).

definition $cCorr :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**
 $cCorr \ p \ e = (\text{if } e < 2 * p - 3 \text{ then } 0 \text{ else of-int } ((\text{of-nat } p * \mu \text{Mono } e) \text{ qmod}$
 $\text{int } p))$

$\mu\text{-}X$ with the polynomial moments replaced by $\mu \wedge 0(t \wedge e) = \mu(t \wedge e) - c\text{-}e/p$.

definition $\mu Xmod :: \text{nat} \Rightarrow \text{nat set} \Rightarrow \text{rat poly} \Rightarrow \text{rat poly}$ **where**
 $\mu Xmod \ p \ S \ P =$
 $\quad [: \sum e \leq \text{degree } (P \text{ div } \text{sqPoleProd } S). \text{Polynomial.coef} (P \text{ div } \text{sqPoleProd } S)$
 $e *$
 $\quad (\mu \text{Mono } e - cCorr \ p \ e / \text{of-nat } p):]$
 $\quad + (\sum j \in S. [: \text{sqResidue } S \ P \ j:] * \mu \text{Pole } j)$

The matrix A of (4.10).

definition $Aout :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat poly mat}$ **where**
 $Aout \ K \ p = \text{Matrix.mat } (\text{hof } K) \ (\text{hof } K) \ (\lambda(i,$
 $\quad j). \mu Xmod \ p \ \{1..K\} \ (Dm \ (\text{Nof } K) \wedge 6 * pX \wedge (i + j)))$

A in the outer basis.

definition $\text{outerGram} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat poly mat}$ **where**
 $\text{outerGram } K \ p = (\text{let } idx = \text{outer-idx } K \ p \text{ in}$
 $\quad \text{Matrix.mat } (\text{length } idx) \ (\text{length } idx)$
 $\quad (\lambda(x, y). \mu Xmod \ p \ \{1..K\} \ (Dm \ (\text{Nof } K) \wedge 6 * \text{outerBasis } K \ p \ (idx ! x) *$
 $\quad \text{outerBasis } K \ p \ (idx ! y))))$

14.10 Section 5 Normalisation (5.1), (5.2), (2.6)

definition $vpS :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{int}$ **where** $vpS \ K \ p = vp \ p \ (SK \ K)$

(5.1): $L\text{-}p(K, M)$; $\gamma\text{-}p\widehat{\text{in}}$ is an integer (Lean *gammaIn-isInt*), the floor just keeps the definition total.

definition $Lp :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{int}$ **where**

$Lp\ K\ M\ p =$
 (if $p * M \leq K$ then $- 6 * \text{int}(\text{hof}\ K) * \text{int}(\text{nat-log}\ p\ (5 * K)) - \text{int}(\text{hof}\ K)$
 $*$
 $\text{int}(\text{multiplicity}\ p\ (24::\text{nat}))$
 else if $3 * p \leq K$ then $\text{vpS}\ K\ p + \text{floor}(\text{gammaIn}\ K\ M\ p)$
 else if $p \leq K$ then $\text{vpS}\ K\ p + \text{gammaOut}\ K\ p$
 else $\text{vpS}\ K\ p$)

(5.2): $m\text{-}\{K, M\} = \prod \{p \leq 2h\} p^{\wedge\{-L\text{-}p(K, M)\}}.$

definition $mKM :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$mKM\ K\ M = (\prod p \in \{p. p \leq 2 * \text{hof}\ K \wedge \text{prime}\ p\}. \text{of-nat}\ p\ \text{powi}\ (-Lp\ K\ M\ p))$

(2.6): $Q\text{-}\{K, M\} = m\text{-}\{K, M\}\ F\text{-}K.$

definition $QKM :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat poly}$ **where** $QKM\ K\ M =$

$[:mKM\ K\ M:] * FK\ K$

14.11 Section 5.1-5.3 Limiting functions (real-valued; Lean namespace *Lim*)

definition $\alpha\text{-}r :: \text{real}$ **where** $\alpha\text{-}r = 3 / 40$

definition $\text{lam-r} :: \text{real}$ **where** $\text{lam-r} = 37 / 40$

definition $Hc\text{-}r :: \text{real}$ **where** $Hc\text{-}r = 23 / 20$

definition $\text{pos-r} :: \text{real} \Rightarrow \text{real}$ **where** $\text{pos-r}\ v = \max\ v\ 0$

$l(x, z) = \lfloor x - z \rfloor + \lfloor x + z \rfloor + 1.$

definition $\text{ell-r} :: \text{real} \Rightarrow \text{real} \Rightarrow \text{real}$ **where**

$\text{ell-r}\ x\ z = \text{of-int}(\text{floor}(x - z)) + \text{of-int}(\text{floor}(x + z)) + 1$

(5.4): $\Gamma(x).$

definition $\text{Gam-r} :: \text{real} \Rightarrow \text{real}$ **where**

$\text{Gam-r}\ x = (\text{let}\ T = \text{of-int}(\text{floor}(2 * Hc\text{-}r * x)); s = Hc\text{-}r * x - T / 2;$
 $q = \text{of-int}(\text{floor}(2 * x)); \text{nplus} = (2 * x - q) / 2\ \text{in}$
 $\text{interval-lebesgue-integral}\ \text{lborel}\ (\text{ereal}\ 0)\ (\text{ereal}\ (1 / 2))$
 $(\lambda z. (T - 3 * \text{ell-r}(\alpha\text{-}r * x)\ z) * (T + 3 * \text{ell-r}(\alpha\text{-}r * x)\ z - \text{ell-r}$
 $x\ z -$
 $5))$
 $+ s * (2 * T - q - 5) + \text{pos-r}(s - \text{nplus}))$

$J(u) = m\ u - m(m+1)/4, m = \lfloor 2u \rfloor.$

definition $J\text{-}r :: \text{real} \Rightarrow \text{real}$ **where**

$J\text{-}r\ u = \text{of-int}(\text{floor}(2 * u)) * u - \text{of-int}(\text{floor}(2 * u)) * (\text{of-int}(\text{floor}(2 * u)) + 1) / 4$

(5.5): $N(x).$

definition $Nfun-r :: real \Rightarrow real$ **where**

$$Nfun-r\ x = 2 * lam-r * x * of-int\ (floor\ x) - 12 * lam-r * x * of-int\ (floor\ (alpha-r * x)) \\ - 2 * J-r\ (lam-r * x)$$

$$(5.6): R(x) = -\Gamma(x) - N(x).$$

definition $R-r :: real \Rightarrow real$ **where** $R-r\ x = -\ Gam-r\ x - Nfun-r\ x$

$$(5.8): R-0(y).$$

definition $R0-r :: real \Rightarrow real$ **where**

$$R0-r\ y = \\ (if\ 1 / 3 < y \wedge y < 1 / 2\ then \\ 8 - 9 * y - 8 * alpha-r - 5 * min\ alpha-r\ (1 - 2 * y) - 5 * pos-r\ (1 + \\ alpha-r - 3 * y) \\ else\ if\ 1 / 2 < y \wedge y < 1\ then \\ 7 * (1 - y) - 6 * min\ alpha-r\ (1 - y) - 6 * pos-r\ (1 + alpha-r - 2 * y) \\ + pos-r\ (1 + 4 * \\ alpha-r - 2 * y) \\ else\ 0)$$

$$(5.9): d(y).$$

definition $dfun-r :: real \Rightarrow real$ **where**

$$dfun-r\ y = (if\ 1 / 3 < y \wedge y < 1 / 2\ then\ pos-r\ ((1 + 4 * alpha-r - 3 * y) - \\ pos-r\ (1 + \\ alpha-r - 3 * y))\ else\ 0)$$

Integrand of (5.10).

definition $outer-integrand :: real \Rightarrow real$ **where**

$$outer-integrand\ y = R0-r\ y - dfun-r\ y - 2 * lam-r * of-int\ (floor\ (1 / y)) \\ + (\sum\ j = 1..5.\ pos-r\ (2 * lam-r - real\ j * y))$$

(5.12)-(5.13): fractional parts and the pieces P , C of the tail.

definition $G0-r :: real \Rightarrow real$ **where** $G0-r\ v = v * (1 - v) * (2 * v - 1) / 6$

definition $Pper :: real \Rightarrow real$ **where**

$$Pper\ x = 74 * frac\ (alpha-r * x) * (1 - frac\ (alpha-r * x)) - lam-r * frac\ x * \\ (1 - frac\ x)$$

definition $Cper :: real \Rightarrow real$ **where**

$$Cper\ x = 74 / alpha-r * G0-r\ (frac\ (alpha-r * x)) - lam-r * G0-r\ (frac\ x)$$

$$(5.10): I-out = 127751 / 96000.$$

definition $Iout :: rat$ **where** $Iout = 127751 / 96000$

$$(5.19).$$

definition $Astar :: rat$ **where** $Astar = 9928298118277006344769 / 7535670527041937280000$

$$(5.20).$$

definition $AM :: nat \Rightarrow rat$ **where**

$$AMM = Astar + 7 * lam-q / of-nat M - (2923 / 240 - 1 / 4) / of-nat M \wedge 2 + 32 / of-nat M \wedge 3$$

(6.4): the constant $Ubar$.

definition $Ubar :: rat$ **where** $Ubar = - 2733991 / 2000000$

14.12 Section 6 The real determinant

(2.10): $w(y) = (2\pi)^4 y^5 / 12 \cdot \sum_{l \geq 1} l^4 e^{-2\pi l y}$ (*suminf*; summable for $y > 0$).

definition $weight :: real \Rightarrow real$ **where**

$$weight\ y = (2 * \pi)^4 * y^5 / 12 * \text{suminf } (\lambda l. real\ (l + 1)^4 * \exp(-2 * \pi * real\ (l + 1) * y))$$

(6.1): the external field V .

definition $Vf :: real \Rightarrow real$ **where**

$$Vf\ t = 2 * \pi * \sqrt{t} + \text{integral } \{0..1\} (\lambda u. \ln(t + u^2)) - 6 * \text{integral } \{0..3/40\} (\lambda u. \ln(t + u^2))$$

Table 1, scaled by 10^{-12} : (a - j , b - j , c - j) for $j = 1, \dots, 16$.

definition $table1 :: (nat \times nat \times nat)$ *list* **where**

$$\begin{aligned} table1 = & [(3906748086, 8992695531, 10515596180), (2312248264, 15340997855, 29471737793), \\ & (1402286665, 25730180724, 42934365099), (881725356, 41909578246, 58204231966), \\ & (578197906, 65851089563, 69037621310), (396324613, 99481037884, 78873099189), \\ & (283911191, 144325727458, 84856120711), (212206188, 201105762729, 88396082127), \\ & (165097686, 269345996903, 88303382125), (133347132, 347089554156, 85472321255), \\ & (111522114, 430806704415, 78899184238), (96349355, 515561896511, 70353471918), \\ & (85815639, 595448778546, 58838976615), (78667711, 664241383483, 44421321106), \\ & (74129565, 716160577112, 30462865791), (71741310, 746637295669, 5959622577)] \end{aligned}$$

definition $tA :: nat \times nat \times nat \Rightarrow real$ **where** $tA\ e = real\ (fst\ e) / 10^{12}$

definition $tB :: nat \times nat \times nat \Rightarrow real$ **where** $tB\ e = real\ (fst\ (snd\ e)) / 10^{12}$

definition $tC :: nat \times nat \times nat \Rightarrow real$ **where** $tC\ e = real\ (snd\ (snd\ e)) / 10^{12}$

The comparison measure $\varrho = \sum c\text{-}j\ \omega\text{-}\{[a\text{-}j, b\text{-}j]\}$ of Lemma 6.1, as one density w.r.t. Lebesgue measure (Lean sums the sixteen scaled measures; the two agree).

definition $\rho :: real\ measure$ **where**

$$\rho = \text{density } lborel\ (\lambda t. \text{ennreal } (\sum e \leftarrow table1. tC\ e * \arcsine\text{-dens } (tA\ e) (tB\ e)\ t))$$

$$I(mu) = \text{integral } \text{integral } \log|t - u| \ dmu(t) \ dmu(u).$$

definition $\logEnergy :: \text{real measure} \Rightarrow \text{real}$ **where**
 $\logEnergy \mu = \text{integral}^L \mu (\lambda t. \logPot \mu t)$

$M-0 = -1329/200.$

definition $M0c :: \text{rat}$ **where** $M0c = -1329 / 200$

(6.3): $C* = -2\lambda + 12\alpha\lambda(1 - \log \alpha) + 3\lambda^2 - 2\lambda^2 \log(2\lambda).$

definition $Cstar :: \text{real}$ **where**

$Cstar = -2 * lam-r + 12 * alpha-r * lam-r * (1 - \ln alpha-r) + 3 * lam-r^2 - 2 * lam-r^2 * \ln (2 * lam-r)$

The partial masses $S_j = \sum_{i \leq j} c_i$ of Appendix A.

definition $Spart :: \text{nat} \Rightarrow \text{real}$ **where** $Spart j =$
 $(\sum e \leftarrow \text{take } j \text{ table1. } tC e)$

end

theory *Zeta5-Functionals*
imports *Zeta5-Definitions*
begin

15 The functionals μ_X and τ_X : algebra and partial fractions

Well-definedness (a common factor of numerator and pole product cancels), linearity, the Lagrange partial-fraction decomposition, τ on polynomials and the pullback identity (3.1) of the paper. Corresponds to the Lean theories *Functionals* and parts of *Distribution*.

15.1 Linearity

lemma *muPoly-eq-sum*:

assumes $\text{degree } P \leq N$

shows $\text{muPoly } P = (\sum e \leq N. \text{Polynomial.coeff } P e * \text{muMono } e)$

<proof>

lemma *muPoly-add*: $\text{muPoly } (P + Q) = \text{muPoly } P + \text{muPoly } Q$

<proof>

lemma *muPoly-smult*: $\text{muPoly } (\text{Polynomial.smult } c P) = c * \text{muPoly } P$

<proof>

lemma *Lfun-eq-sum*:

assumes $\text{degree } P \leq N$

shows $\text{Lfun } P = (\sum k \leq N. \text{Polynomial.coeff } P k * \text{bernoulli } k)$

$\langle proof \rangle$

lemma *Lfun-add*: $Lfun (P + Q) = Lfun P + Lfun Q$
 $\langle proof \rangle$

lemma *Lfun-smult*: $Lfun (Polynomial.smult c P) = c * Lfun P$
 $\langle proof \rangle$

lemma *tau-add*: $tau (P + Q) = tau P + tau Q$
 $\langle proof \rangle$

lemma *tau-smult*: $tau (Polynomial.smult c P) = c * tau P$
 $\langle proof \rangle$

lemma *sqResidue-add*: $sqResidue S (P + Q) j = sqResidue S P j + sqResidue S Q j$
 $\langle proof \rangle$

lemma *sqResidue-smult*: $sqResidue S (Polynomial.smult c P) j = c * sqResidue S P j$
 $\langle proof \rangle$

lemma *linResidue-add*: $linResidue S (P + Q) r = linResidue S P r + linResidue S Q r$
 $\langle proof \rangle$

lemma *linResidue-smult*: $linResidue S (Polynomial.smult c P) r = c * linResidue S P r$
 $\langle proof \rangle$

lemma *muX-add*: $muX S (P + Q) = muX S P + muX S Q$
 $\langle proof \rangle$

lemma *smult-sum-right*: $Polynomial.smult c (\sum i \in S. f i) = (\sum i \in S. Polynomial.smult c (f i))$
 $\langle proof \rangle$

lemma *muX-C-mul*: $muX S ([:c:] * P) = [:c:] * muX S P$
 $\langle proof \rangle$

lemma *tauX-add*: $tauX S (P + Q) = tauX S P + tauX S Q$
 $\langle proof \rangle$

lemma *tauX-C-mul*: $tauX S ([:c:] * P) = [:c:] * tauX S P$
 $\langle proof \rangle$

15.2 Well-definedness: common factors cancel

mu-X depends only on the rational function (Lean: *muX-mul-cancel*).

lemma *muX-mul-cancel*:
 $finite\ S \implies j \notin S \implies$
 $muX\ (insert\ j\ S)\ (P * (pX + [:of-nat\ j\ ^\wedge\ 2:])) = muX\ S\ P$
 $\langle proof \rangle$

lemma *muX-mul-cancel-set*:
 $finite\ S \implies finite\ T \implies T \cap S = \{\} \implies$
 $muX\ (T \cup S)\ (P * sqPoleProd\ T) = muX\ S\ P$
 $\langle proof \rangle$

15.3 Partial fractions (Lagrange decomposition)

$P = \Pi\ (P\ div\ \Pi) + \sum\ -s\ res-s\ \prod\ -\{s' \neq s\}\ (X - s')$ (Lean: *pt-lagrange*).

lemma *pX-minus-const*: $pX - [:s:] = [-\ s,\ 1:]$
 $\langle proof \rangle$

lemma *qPoleProd-lead-coeff*: $finite\ S \implies lead-coeff\ (qPoleProd\ S) = 1$
 $\langle proof \rangle$

Monicity is written as $lead-coeff\ - = 1$ (*monic* is not a constant in the base image).

lemma *qPoleProd-monic*: $finite\ S \implies lead-coeff\ (qPoleProd\ S) = 1$
 $\langle proof \rangle$

lemma *degree-qPoleProd*: $finite\ S \implies degree\ (qPoleProd\ S) = card\ S$
 $\langle proof \rangle$

lemma *poly-qPoleProd*: $poly\ (qPoleProd\ T)\ x = (\prod\ t \in T.\ x - t)$
 $\langle proof \rangle$

lemma *poly-eq-0-of-roots*:
fixes $Q :: rat\ poly$
assumes $finite\ S\ degree\ Q < card\ S \wedge s.\ s \in S \implies poly\ Q\ s = 0$
shows $Q = 0$
 $\langle proof \rangle$

lemma *lagrange-decomp-aux*:
assumes $S: finite\ S$
shows $P = qPoleProd\ S * (P\ div\ qPoleProd\ S) + (\sum\ s \in S.\ [:qRes\ S\ P\ s:] * qPoleProd\ (S - \{s\}))$
 $\langle proof \rangle$

lemma *lagrange-decomp*:
 $finite\ S \implies P = qPoleProd\ S * (P\ div\ qPoleProd\ S) + (\sum\ s \in S.\ [:qRes\ S\ P\ s:] * qPoleProd\ (S - \{s\}))$
 $\langle proof \rangle$

15.4 (3.1) The pullback identity

The pullback identity (3.1) is stated and proved at the end of this theory.

15.5 τ on polynomials

$\tau(z \hat{d}) = \kappa \cdot d$, and $\text{tau}K = \text{tau}$.

lemma *pX-pow-monom*: $pX \hat{d} = \text{Polynomial.monom } 1 \ d$
 $\langle \text{proof} \rangle$

lemma *Lfun-monom*: $Lfun (\text{Polynomial.monom } c \ k) = c * \text{bernoulli } k$
 $\langle \text{proof} \rangle$

lemma *tau-X-pow-eq-kappa*: $\text{tau } (pX \hat{d}) = \kappa \ d$
 $\langle \text{proof} \rangle$

lemma *tau-zero*: $\text{tau } 0 = 0$
 $\langle \text{proof} \rangle$

lemma *tau-sum*: $\text{tau } (\sum i \in S. f \ i) = (\sum i \in S. \text{tau } (f \ i))$
 $\langle \text{proof} \rangle$

lemma *tau-monom*: $\text{tau } (\text{Polynomial.monom } c \ d) = c * \kappa \ d$
 $\langle \text{proof} \rangle$

lemma *tauK-eq-tau*: $\text{tau}K \ Q = \text{tau } Q$
 $\langle \text{proof} \rangle$

lemma *sum-binomial-bernoulli-lt*:
 $(\sum k < n. \text{of-nat } (n \ \text{choose } k) * \text{bernoulli } k) = (\text{if } n = 1 \text{ then } 1 \text{ else } (0 :: \text{rat}))$
 $\langle \text{proof} \rangle$

lemma *kappa-0*: $\kappa \ 0 = 0$ **and** *kappa-1*: $\kappa \ 1 = 0$ **and** *kappa-2*: $\kappa \ 2 = 0$
and *kappa-Suc-0*: $\kappa \ (\text{Suc } 0) = 0$ **and** *kappa-Suc-Suc-0*: $\kappa \ (\text{Suc } (\text{Suc } 0)) = 0$
 $\langle \text{proof} \rangle$

lemma *kappa-Suc3*:
 $\kappa \ (\text{Suc } (\text{Suc } (\text{Suc } j))) = \text{of-nat } (\text{Suc } (\text{Suc } (\text{Suc } j)) * \text{Suc } (\text{Suc } j) * \text{Suc } j) * \text{bernoulli } j / 24$
 $\langle \text{proof} \rangle$

lemma *choose-falling3*:
 $(\text{Suc } (\text{Suc } (\text{Suc } m)) \ \text{choose } \text{Suc } (\text{Suc } (\text{Suc } j))) * (\text{Suc } (\text{Suc } (\text{Suc } j)) * \text{Suc } (\text{Suc } j) * \text{Suc } j)$
 $= \text{Suc } (\text{Suc } (\text{Suc } m)) * \text{Suc } (\text{Suc } m) * \text{Suc } m * (m \ \text{choose } j)$
 $\langle \text{proof} \rangle$

lemma *sum-choose-kappa-aux*:

$(\sum d \leq n. \text{of-nat } (n \text{ choose } d) * \text{kappa } d) = (\text{if } n = 4 \text{ then } 1 \text{ else } 0) + \text{kappa } n$
 $\langle \text{proof} \rangle$

lemma *tau-uminus*: $\text{tau } (- P) = - \text{tau } P$

$\langle \text{proof} \rangle$

lemma *tau-diff*: $\text{tau } (P - Q) = \text{tau } P - \text{tau } Q$

$\langle \text{proof} \rangle$

lemma *tau-of-nat-mult*: $\text{tau } (\text{of-nat } c * P) = \text{of-nat } c * \text{tau } P$

$\langle \text{proof} \rangle$

lemma *tau-shift-pow*: $\text{tau } ((pX + 1) \wedge n) = (\text{if } n = 4 \text{ then } 1 \text{ else } 0) + \text{kappa } n$

$\langle \text{proof} \rangle$

lemma *tau-fwd-monom*:

$\text{tau } (\text{pcompose } (\text{Polynomial.monom } c \ n) (pX + 1) - \text{Polynomial.monom } c \ n) =$
 $(\text{if } n = 4 \text{ then } c \text{ else } 0)$

$\langle \text{proof} \rangle$

lemma *tau-fwd-aux*: $\text{tau } (\text{pcompose } f (pX + 1) - f) = \text{Polynomial.coeff } f \ 4$

$\langle \text{proof} \rangle$

(3.3) for polynomials: $\tau(f(x+1) - f(x)) = f''''(0)/24 = [x^4] f$ (Lean: *tau-fwd*).

lemma *tau-fwd*: $\text{tau } (\text{pcompose } f (pX + 1) - f) = \text{Polynomial.coeff } f \ 4$

$\langle \text{proof} \rangle$

$\sum \{d \leq n\} C(n, d) \kappa \cdot d = [n = 4] + \kappa \cdot n.$

lemma *sum-choose-kappa*:

$(\sum d \leq n. \text{of-nat } (n \text{ choose } d) * \text{kappa } d) = (\text{if } n = 4 \text{ then } 1 \text{ else } 0) + \text{kappa } n$

$\langle \text{proof} \rangle$

Every polynomial is a forward difference.

lemma *pX-shift-pow-diff*:

$\text{pcompose } (pX \wedge m) (pX + 1) - pX \wedge m = (\sum k < m. \text{Polynomial.monom } (\text{of-nat } (m \text{ choose } k)) \ k)$

$\langle \text{proof} \rangle$

lemma *exists-antidiff-aux*: $\exists g. \text{pcompose } g (pX + 1) - g = f$

$\langle \text{proof} \rangle$

lemma *exists-antidiff*: $\exists g. \text{pcompose } g (pX + 1) - g = f$

$\langle \text{proof} \rangle$

15.6 (3.1) The pullback identity: proof

definition *pullbackR* :: $\text{nat set} \Rightarrow \text{rat poly} \Rightarrow \text{rat poly}$ **where**

$\text{pullbackR } S \ P = \text{tauX } (\text{signedPoles } S) \ ([:(-1) \wedge \text{card } S:] * pX \wedge 5 * \text{pcompose } P \ (- \ (pX \wedge 2)))$

lemma *muX-zero*: $\text{muX } S \ 0 = 0$
 $\langle \text{proof} \rangle$

lemma *muX-sum*: $\text{muX } S \ (\sum i \in I. f \ i) = (\sum i \in I. \text{muX } S \ (f \ i))$
 $\langle \text{proof} \rangle$

lemma *tauX-zero*: $\text{tauX } T \ 0 = 0$
 $\langle \text{proof} \rangle$

lemma *pullbackR-add*: $\text{pullbackR } S \ (P + Q) = \text{pullbackR } S \ P + \text{pullbackR } S \ Q$
 $\langle \text{proof} \rangle$

lemma *pullbackR-C-mul*: $\text{pullbackR } S \ ([:a:] * P) = [:a:] * \text{pullbackR } S \ P$
 $\langle \text{proof} \rangle$

lemma *pullbackR-zero*: $\text{pullbackR } S \ 0 = 0$
 $\langle \text{proof} \rangle$

lemma *pullbackR-sum*: $\text{pullbackR } S \ (\sum i \in I. f \ i) = (\sum i \in I. \text{pullbackR } S \ (f \ i))$
 $\langle \text{proof} \rangle$

lemma *pcompose-sq-factor*:
 $\text{pcompose } (pX + [:of\text{-nat } j \wedge 2:]) \ (- \ (pX \wedge 2))$
 $= [: - \ 1:] * ((pX - [:of\text{-int } (int \ j):]) * (pX - [:of\text{-int } (- \ int \ j):]))$
 $\langle \text{proof} \rangle$

lemma *const-poly-power*: $[:a:] \wedge n = [:a \wedge n:]$
 $\langle \text{proof} \rangle$

lemma *minus-one-poly*: $(- \ 1 :: \text{rat poly}) = [: - \ 1:]$
 $\langle \text{proof} \rangle$

lemma *pcompose-sqPoleProd*:
assumes S : *finite* S **and** $S0$: $0 \notin S$
shows $\text{pcompose } (\text{sqPoleProd } S) \ (- \ (pX \wedge 2)) = [:(-1) \wedge \text{card } S:] * \text{linPoleProd } (\text{signedPoles } S)$
 $\langle \text{proof} \rangle$

lemma *kappa-odd-muMono*: $(- \ 1) \wedge e * \text{kappa } (2 * e + 5) = \text{muMono } e$
 $\langle \text{proof} \rangle$

lemma *tau-pullback-monom*:
 $\text{tau } (pX \wedge 5 * \text{pcompose } (\text{Polynomial.monom } c \ e) \ (- \ (pX \wedge 2))) = c * \text{muMono } e$
 $\langle \text{proof} \rangle$

lemma *tau-pullback-poly*: $\text{tau } (pX \wedge 5 * \text{pcompose } Q \text{ } (- (pX \wedge 2))) = \text{muPoly } Q$
 $\langle \text{proof} \rangle$

lemma *sqPoleProd-nonzero*: $\text{finite } S \implies \text{sqPoleProd } S \neq 0$
 $\langle \text{proof} \rangle$

lemma *linPoleProd-nonzero*: $\text{finite } T \implies \text{linPoleProd } T \neq 0$
 $\langle \text{proof} \rangle$

lemma *muX-poly-mult*:
assumes S : *finite* S
shows $\text{muX } S \text{ } (\text{sqPoleProd } S * Q) = [\text{muPoly } Q]$
 $\langle \text{proof} \rangle$

lemma *tauX-poly-mult*:
assumes T : *finite* T
shows $\text{tauX } T \text{ } (G * \text{linPoleProd } T) = [\text{tau } G]$
 $\langle \text{proof} \rangle$

lemma *pullback-poly*:
assumes S : *finite* S **and** $S0$: $0 \notin S$
shows $\text{muX } S \text{ } (\text{sqPoleProd } S * Q) = \text{pullbackR } S \text{ } (\text{sqPoleProd } S * Q)$
 $\langle \text{proof} \rangle$

lemma *degree-pX-plus-const*: $\text{degree } (pX + [:a:]) = 1$
 $\langle \text{proof} \rangle$

lemma *degree-pX-minus-const*: $\text{degree } (pX - [:a:]) = 1$
 $\langle \text{proof} \rangle$

lemma *pX-plus-const-nonzero*: $pX + [:a:] \neq 0$
 $\langle \text{proof} \rangle$

lemma *pX-minus-const-nonzero*: $pX - [:a:] \neq 0$
 $\langle \text{proof} \rangle$

lemma *muX-single-pole*:
assumes S : *finite* S **and** j : $j \in S$
shows $\text{muX } S \text{ } (\text{sqPoleProd } (S - \{j\})) = \text{muPole } j$
 $\langle \text{proof} \rangle$

lemma *quintic-division-identity*:
fixes $x \ A :: 'a :: \text{comm-ring-1}$
shows $x \wedge 5 = ((x - A) * (x - - A)) * (x \wedge 3 + A \wedge 2 * x) + A \wedge 4 * x$
 $\langle \text{proof} \rangle$

lemma *H5-Suc-pred*: $j \neq 0 \implies H5 \ j = H5 \ (j - 1) + 1 \ / \ \text{of-nat } j \wedge 5$
 $\langle \text{proof} \rangle$

lemma *pullbackR-single-pole*:
 assumes S : *finite* S and $S0$: $0 \notin S$ and j : $j \in S$
 shows $\text{pullbackR } S (\text{sqPoleProd } (S - \{j\})) = \text{muPole } j$
 $\langle \text{proof} \rangle$

lemma *sq-lagrange*:
 assumes S : *finite* S
 shows $P = \text{sqPoleProd } S * (P \text{ div } \text{sqPoleProd } S) + (\sum j \in S. [\text{sqResidue } S P j:] * \text{sqPoleProd } (S - \{j\}))$
 $\langle \text{proof} \rangle$

theorem *pullback-aux*:
 assumes S : *finite* S and $S0$: $0 \notin S$
 shows $\text{muX } S P = \text{pullbackR } S P$
 $\langle \text{proof} \rangle$

$\text{mu-X}(R) = \tau\text{-X}(x^5 R(-x^2))$; the numerator picks up $(-1)^{|S|}$ because $\prod_{j \in S} (j^2 - x^2) = (-1)^{|S|} \prod_{r=\pm j} (x - r)$.

theorem *pullback*:
 assumes *finite* S $0 \notin S$
 shows $\text{muX } S P = \text{tauX } (\text{signedPoles } S) ([(-1)^{\text{card } S}] * pX^5 * \text{pcompose } P (- (pX^2)))$
 $\langle \text{proof} \rangle$

end

theory *Zeta5-IntValued*
 imports *Zeta5-Functionals*
 begin

16 Integer-valued polynomials and the bound (3.9)

Binomial polynomials, forward differences and Newton interpolation, used as a self-contained replacement for the $\mathbb{Z}_p$ -analytic arguments of Section 3.3 of the paper: values at integers with valuation bounds give coefficient bounds ((3.8) and (3.9), *tau-vge-of-values*, *diffQuot-vge*). Lean theory *IntValued*.

lemma *IntValuedAt-vge*: $\text{IntValuedAt } p A \implies \text{vge } p (\text{poly } A (\text{of-int } x)) 0$
 $\langle \text{proof} \rangle$

16.1 Binomial polynomials

$\text{binom}(x, k) = x(x-1) \cdots (x-k+1)/k!$.

definition $\text{bp} :: \text{nat} \Rightarrow \text{rat poly}$ **where**
 $\text{bp } k = \text{Polynomial.smult } (1 / \text{fact } k) (\prod i < k. pX - [\text{of-nat } i])$

lemma *bp-0*: $\text{bp } 0 = 1$

$\langle proof \rangle$

lemma *bp-Suc*: $bp\ (Suc\ k) = Polynomial.smult\ (1\ /\ (of\text{-}nat\ k + 1))\ (bp\ k * (pX - [:of\text{-}nat\ k:]))$
 $\langle proof \rangle$

lemma *degree-bp-le*: $degree\ (bp\ k) \leq k$
 $\langle proof \rangle$

$binom(x, k)$ is HOL's (*gchoose*).

lemma *poly-bp*: $poly\ (bp\ k)\ a = a\ gchoose\ k$
 $\langle proof \rangle$

$binom(n, k)$ at naturals.

lemma *bp-eval-nat*: $poly\ (bp\ k)\ (of\text{-}nat\ n) = of\text{-}nat\ (n\ choose\ k)$
 $\langle proof \rangle$

$binom(-(t+1), k) = (-1)^k binom(t+k, k)$.

lemma *bp-eval-neg*: $poly\ (bp\ k)\ (-\ (of\text{-}nat\ t + 1)) = (-1)^k * of\text{-}nat\ ((t + k)\ choose\ k)$
 $\langle proof \rangle$

Binomial polynomials are integer-valued on $\mathbb{Z}$.

lemma *bp-eval-int*: $\exists z::int. poly\ (bp\ k)\ (of\text{-}int\ m) = of\text{-}int\ z$
 $\langle proof \rangle$

Two polynomials agreeing on all naturals are equal.

lemma *poly-eq-of-eval-nat*:
fixes $P\ Q :: rat\ poly$
assumes $\bigwedge n::nat. poly\ P\ (of\text{-}nat\ n) = poly\ Q\ (of\text{-}nat\ n)$
shows $P = Q$
 $\langle proof \rangle$

Pascal: $\Delta\ binom(x, k+1) = binom(x, k)$.

lemma *bp-fwd*: $pcompose\ (bp\ (Suc\ k))\ (pX + 1) - bp\ (Suc\ k) = bp\ k$
 $\langle proof \rangle$

$binom(x, k+1) = (x/(k+1))\ binom(x-1, k)$.

lemma *bp-shift*: $bp\ (Suc\ k) = Polynomial.smult\ (1\ /\ (of\text{-}nat\ k + 1))\ (pX * pcompose\ (bp\ k)\ (pX - 1))$
 $\langle proof \rangle$

$\tau(binom(x, k)) = [x^4]\ binom(x, k+1)$.

lemma *tau-bp*: $\tau\ (bp\ k) = Polynomial.coeff\ (bp\ (Suc\ k))\ 4$
 $\langle proof \rangle$

16.2 The coefficients of $\text{binom}(x, n)$

Weighted Gauss bound: $v\text{-}p(\text{coeff}\text{-}m\ P) \geq -m\ c$.

definition $WB :: \text{nat} \Rightarrow \text{rat} \Rightarrow \text{rat poly} \Rightarrow \text{bool}$ **where**

$WB\ p\ c\ P \longleftrightarrow (\forall m. \text{vge}\ p\ (\text{Polynomial.coeff}\ P\ m)\ (-\ \text{of-nat}\ m * c))$

lemma $WB\text{-mul}$: $\text{prime}\ p \implies WB\ p\ c\ P \implies WB\ p\ c\ Q \implies$

$WB\ p\ c\ (P * Q)$

$\langle \text{proof} \rangle$

lemma $WB\text{-one}$: $WB\ p\ c\ 1$

$\langle \text{proof} \rangle$

lemma $WB\text{-prod}$:

$\text{prime}\ p \implies \text{finite}\ I \implies (\bigwedge i. i \in I \implies$

$WB\ p\ c\ (f\ i)) \implies WB\ p\ c\ (\prod i \in I. f\ i)$

$\langle \text{proof} \rangle$

$u\ X - v$ with $v\text{-}p(u) \geq -c$, $v\text{-}p(v) \geq 0$.

lemma $WB\text{-linear}$: $\text{prime}\ p \implies \text{vge}\ p\ u\ (-\ c) \implies$

$\text{vge}\ p\ v\ 0 \implies WB\ p\ c\ [-\ v, u]$

$\langle \text{proof} \rangle$

lemma poly-bp-factor :

fixes $a :: \text{rat}$

shows $\text{poly}\ ([:-0, 1 / (\text{of-nat}\ m + 1):] * (\prod i < m. [-1, 1 / (\text{of-nat}\ i + 1):]))$

$a =$

$a\ \text{gchoose}\ \text{Suc}\ m$

$\langle \text{proof} \rangle$

$\text{binom}(x, m+1) = (x/(m+1)) \prod_{i < m} (x/(i+1) - 1).$

lemma bp-factor : $\text{bp}\ (\text{Suc}\ m) = [-0, 1 / (\text{of-nat}\ m + 1):] * (\prod i < m. [-1, 1 / (\text{of-nat}\ i + 1):])$

$\langle \text{proof} \rangle$

$v\text{-}p(\lceil x \rceil_4\ \text{binom}(x, n)) \geq -4 \lfloor \log\text{-}p\ n \rfloor.$

lemma bp-coeff4 :

assumes p : $\text{prime}\ p$

shows $\text{vge}\ p\ (\text{Polynomial.coeff}\ (\text{bp}\ n)\ 4)\ (-\ 4 * \text{of-nat}\ (\text{nat-log}\ p\ n))$

$\langle \text{proof} \rangle$

16.3 Newton interpolation

Forward differences $\Delta^k f(y)$ with step 1.

fun $\text{fd} :: \text{rat poly} \Rightarrow \text{rat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$\text{fd}\ f\ y\ 0 = \text{poly}\ f\ y$

$\mid \text{fd}\ f\ y\ (\text{Suc}\ k) = \text{fd}\ f\ (y + 1)\ k - \text{fd}\ f\ y\ k$

lemma *fd-vge*:

assumes *prime* $p \wedge i. i \leq k \implies vge\ p\ (poly\ f\ (y + of\text{-}nat\ i))\ b$

shows $vge\ p\ (fd\ f\ y\ k)\ b$

<proof>

$$f(y + n) = \sum_{k \leq n} C(n, k) \Delta^k f(y).$$

lemma *newton-eval*: $poly\ f\ (y + of\text{-}nat\ n) = (\sum_{k \leq n. of\text{-}nat\ (n\ choose\ k) * fd\ f\ y\ k)$

<proof>

Newton's forward-difference formula as a polynomial identity.

lemma *newton*:

assumes $degree\ f \leq D$

shows $f = (\sum_{k \leq D. [:fd\ f\ y\ k:] * pcompose\ (bp\ k)\ (pX - [:y:]))$

<proof>

lemma *pcompose-pX-minus-0*: $pcompose\ P\ (pX - [:0:]) = P$

<proof>

16.4 (3.9) and (3.8)

(3.9), in the form used: if $deg\ f \leq D$ and f is p^{-a} -integral at $D+1$ consecutive integers, then $v\text{-}p(\tau(f)) \geq -a - 4 \lfloor \log\text{-}p(D+1) \rfloor$ (Lean: *tau-vge-of-values*; the paper's $-v\text{-}p(24)$ term is not needed).

theorem *tau-vge-of-values*:

assumes p : *prime* p **and** dfD : $degree\ f \leq D$

and hv : $\bigwedge i. i \leq D \implies vge\ p\ (poly\ f\ (of\text{-}int\ y + of\text{-}nat\ i))\ (-\ a)$

shows $vge\ p\ (tau\ f)\ (-\ a - 4 * of\text{-}nat\ (nat\text{-}log\ p\ (D + 1)))$

<proof>

(3.8): difference quotients of integer-valued polynomials of degree $\leq d$ lose at most $\lfloor \log\text{-}p\ max(1, d) \rfloor$ (Lean: *diffQuot-vge*).

theorem *diffQuot-vge*:

assumes p : *prime* p **and** A : *IntValuedAt* $p\ A$ **and** dA : $degree\ A \leq d$ **and** nr : $n \neq r$

shows $vge\ p\ ((poly\ A\ (of\text{-}int\ n) - poly\ A\ (of\text{-}int\ r)) / (of\text{-}int\ n - of\text{-}int\ r))$
 $(- of\text{-}nat\ (nat\text{-}log\ p\ (max\ 1\ d)))$

<proof>

end

theory *Zeta5-Far-Poles*

imports *Zeta5-IntValued Legendre-Factorial-Valuation*

begin

17 The far-pole constant and Lemma 3.3

Section 3 of the paper: the valuations of the Bernoulli numbers (von Staudt–Clausen, from the AFP), the far-pole constant C_p of Section 3.1, counting lemmas for multiples and valuations of integers, partial fractions with linear poles, the product-difference estimate and Lemma 3.3 (*far-pole-valuation-bound*). Lean theories *Section3*, *Lemma33*, *MuMod*.

17.1 Bernoulli valuations (von Staudt–Clausen, from the AFP)

$v_p(\kappa-d) \geq -1$ for odd p (false for $p = 2$: $\kappa-3 = 1/4$). Follows from *Bernoulli-FPS.vonStaudt-Clausen* / *Bernoulli-FPS.prime-dvd-bernoulli-denom-iff*: the denominator of $B-n$ is squarefree.

lemma *multiplicity-24*:
assumes *prime p p ≠ 2*
shows *multiplicity p (24::nat) = (if p = 3 then 1 else 0)*
<proof>

The denominator of a Bernoulli number is squarefree (von Staudt–Clausen):
 $v_p(B-n) \geq -1$.

lemma *vp-bernoulli-ge*:
assumes *prime p (bernoulli n :: rat) ≠ 0*
shows $-1 \leq v_p p (bernoulli\ n)$
<proof>

$B-n$ is p -integral unless $(p-1) \mid n$ (for odd p).

lemma *vp-bernoulli-nonneg*:
assumes *prime p p ≠ 2 ¬ (p-1) dvd n*
shows $0 \leq v_p p (bernoulli\ n)$
<proof>

lemma *three-dvd-consec*: $(3::int) \text{ dvd } m * (m-1) * (m-2)$
<proof>

lemma *kappa-eq*: $kappa\ d = of_int\ (int\ d * (int\ d - 1) * (int\ d - 2)) * bernoulli\ (d-3) / 24$
<proof>

lemma *vp-24*: $prime\ p \implies p \neq 2 \implies v_p p\ 24 = (if\ p = 3\ then\ 1\ else\ 0)$
<proof>

lemma *kappa-padicVal-ge*:
assumes *prime p p ≠ 2 kappa d ≠ 0*
shows $-1 \leq v_p p (kappa\ d)$
<proof>

$\kappa \cdot d \in \mathbb{Z}\text{-}p$ for $d \leq p + 1$, $p \geq 7$ (in fact for $d \leq 4p - 2$).

lemma *kappa-integral*:

assumes *prime* p $7 \leq p$ $d \leq p + 1$ $\kappa d \neq 0$

shows $0 \leq v_p p (\kappa d)$

<proof>

The polynomial moments: $v_p(\mu(t^e)) \geq -1$, and p -integral for $e < 2p - 3$.

lemma *muMono-eq*:

$\mu\text{Mono } e = (-1)^e * (\text{bernoulli } (2 * e + 2) * \text{of-int } ((2 * \text{int } e + 3) * (2 * \text{int } e + 4) * (2 * \text{int } e + 5)) / 24)$

<proof>

lemma *muMono-padicVal*:

assumes *prime* p $7 \leq p$ $\mu\text{Mono } e \neq 0$

shows $-1 \leq v_p p (\mu\text{Mono } e) \wedge (e < 2 * p - 3 \longrightarrow 0 \leq v_p p (\mu\text{Mono } e))$

<proof>

The modified moments $\mu(t^e) - c \cdot e/p$ are p -integral (Lean: *muMod-vge*).

lemma *vge-one-of-qcong-0*:

assumes *prime* p $[z = 0] \text{ (qmod int } p)$

shows $v_p p z \geq 1$

<proof>

lemma *muMod-vge*: *prime* $p \implies 7 \leq p \implies$

$v_p p (\mu\text{Mono } e - c\text{Corr } p e / \text{of-nat } p) \geq 0$

<proof>

17.2 Section 3.1 The far-pole constant C_p

Section 3.2: $C_p \in p^5 \mathbb{Z}\text{-}p$; every partial sum already has valuation ≥ 5 (the $k = 0$ term uses $\sum_{a=1}^{p-1} a^{-4} \equiv 0 \pmod{p}$, Lean: *pt-invPowSum-vge*).

lemma *vge-of-nat*: *prime* $p \implies v_p p (\text{of-nat } n) \geq 0$

<proof>

lemma *vge-p-self*: *prime* $p \implies v_p p (\text{of-nat } p) \geq 1$

<proof>

lemma *vge-dvd-nat*: *prime* $p \implies p \text{ dvd } n \implies v_p p (\text{of-nat } n) \geq 1$

<proof>

lemma *vge-inverse-unit*: *prime* $p \implies \neg p \text{ dvd } a \implies$

$v_p p (\text{inverse } (\text{of-nat } a)) \geq 0$

<proof>

lemma *vge-pow4-diff*:
assumes *prime p vge p x 0 vge p y 0 vge p (x - y) 1*
shows *vge p (x ^ 4 - y ^ 4) 1*
 $\langle proof \rangle$

lemma *sum-pow4-mod-prime*:
fixes *p :: nat*
assumes *p: prime p 7 ≤ p*
shows *p dvd (∑ c = 1..p - 1. c ^ 4)*
 $\langle proof \rangle$

lemma *invPowSum-vge*: *prime p ⇒ 7 ≤ p ⇒*
vge p (∑ a = 1..p - 1. inverse (of-nat a) ^ 4) 1
 $\langle proof \rangle$

lemma *vge-p-pow*: *prime p ⇒ vge p (of-nat p ^ n) (of-nat n)*
 $\langle proof \rangle$

lemma *vge-small-unit*:
assumes *prime p 7 ≤ p 0 < c c < 7*
shows *vge p (inverse (of-nat c)) 0*
 $\langle proof \rangle$

lemma *powi-neg-frac*:
assumes *a ≠ 0 p ≠ 0*
shows *(- of-nat a / of-nat p :: rat) powi (- (int k + 4))*
 $= (- 1) ^ (k + 4) * of-nat p ^ (k + 4) * inverse (of-nat a) ^ (k + 4)$
 $\langle proof \rangle$

lemma *Cp-tr-vge*: *prime p ⇒ 7 ≤ p ⇒ vge p (Cp-tr p M) 5*
 $\langle proof \rangle$

17.3 Section 3.3 Lemma 3.3 and the small-prime bound

Lemma 3.3, (3.10): if A is integer-valued with $\deg A \leq d$ and $g = (K!)^2 A(x) / \prod_{\{0 < |r| \leq K\}} (x - r)$, then $v\text{-}p \wedge G(\tau\text{-}X(g)) \geq -6 \lfloor \log\text{-}p \max(2K, d+1) \rfloor - v\text{-}p(24)$. Proof: the residues are $\pm (K!)^2 r A(r) / ((K+r)!(K-r)!)$, root counting modulo p^j , two-case estimate.

lemma *vge-diff*: *prime p ⇒ vge p x b ⇒ vge p y b ⇒*
vge p (x - y) b
 $\langle proof \rangle$

17.4 Counting multiples in an interval

At most $2K \operatorname{div} q + 1$ elements of $[-K, K]$ lie in one residue class modulo q .

lemma *card-filter-dvd-Icc-le*:
assumes $0 < q$

shows $\text{card } \{s \in \{- \text{int } K .. \text{int } K\}. \text{int } q \text{ dvd } (x - s)\} \leq 2 * K \text{ div } q + 1$
 <proof>

lemma *two-mul-div-le-nat*: $0 < q \implies 2 * K \text{ div } q \leq 2 * (K \text{ div } q) + (1 :: \text{nat})$
 <proof>

lemma *card-filter-dvd-le*:

$0 < q \implies T \subseteq \{- \text{int } K .. \text{int } K\} \implies$
 $\text{card } \{s \in T. \text{int } q \text{ dvd } (x - s)\} \leq 2 * K \text{ div } q + 1$
 <proof>

If $x0 \in [-K, K] - T$ lies in the residue class, the count drops by one.

lemma *card-filter-dvd-le-excl*:

$0 < q \implies T \subseteq \{- \text{int } K .. \text{int } K\} \implies$
 $x0 \in \{- \text{int } K .. \text{int } K\} \implies x0 \notin T \implies$
 $\text{int } q \text{ dvd } (x - x0) \implies$
 $\text{card } \{s \in T. \text{int } q \text{ dvd } (x - s)\} \leq 2 * K \text{ div } q$
 <proof>

lemma *lt-pow-nat-log-succ*: $\text{prime } p \implies 0 < n \implies$
 $n < p \wedge (\text{nat-log } p \ n + 1)$
 <proof>

lemma *div-eq-zero-of-gt-nat-log*: $\text{prime } p \implies \text{nat-log } p \ (2 * K) < j \implies$
 $2 * K \text{ div } p \wedge j = 0$
 <proof>

17.5 Valuations of integers as counts

lemma *multiplicity-int-eq-card*:

assumes $\text{prime } p \ z \neq 0 \ \text{multiplicity } (\text{int } p) \ z < B$
shows $\text{multiplicity } (\text{int } p) \ z = \text{card } \{j \in \{1 .. < B\}. \text{int } p \wedge j \text{ dvd } z\}$
 <proof>

lemma *sum-multiplicity-le*:

assumes $\text{prime } p \ \text{finite } T \ \bigwedge s. s \in T \implies x - s \neq 0$
and $\bigwedge s. s \in T \implies \text{multiplicity } (\text{int } p) \ (x - s) < B$
and $\bigwedge j. j \in \{1 .. < B\} \implies$
 $\text{card } \{s \in T. \text{int } p \wedge j \text{ dvd } (x - s)\} \leq c \ j$
shows $(\sum s \in T. \text{multiplicity } (\text{int } p) \ (x - s)) \leq (\sum j \in \{1 .. < B\}. c \ j)$
 <proof>

The factorial ratio $(K!) \wedge 2 / \prod \{-s \in T\} (x - s)$, from per-level counts: if at each level j at most $2 \lfloor K/p \wedge j \rfloor + e \ [j \leq L0]$ of the $x - s$ are divisible by $p \wedge j$, the ratio has $v\text{-}p \geq -e \ L0$, where $L0 = \lfloor \log\text{-}p \ 2K \rfloor$.

lemma *vge-factorial-sq-div-prod*:

assumes p : $\text{prime } p$ **and** T : $\text{finite } T$ **and** x : $\bigwedge s. s \in T \implies$
 $x - s \neq 0$
and hc : $\bigwedge j. 1 \leq j \implies \text{card } \{s \in T. \text{int } p \wedge j \text{ dvd } (x - s)\} \leq$
 $2 * (K \text{ div } p \wedge j) + (\text{if } j \leq \text{nat-log } p \ (2 * K) \text{ then } e \text{ else } 0)$

shows $vge\ p\ (fact\ K\ \wedge\ 2\ /\ (\prod\ s \in$
 $T.\ of-int\ x - of-int\ s))\ (\neg\ of-nat\ (e * nat-log\ p\ (2 * K)))$
 $\langle proof \rangle$

17.6 Partial fractions with linear poles

lemma *degree-div-le-self*:

fixes $G\ M :: rat\ poly$

assumes $M \neq 0$

shows $degree\ (G\ div\ M) \leq degree\ G$

$\langle proof \rangle$

lemma *linPoleProd-eq-qPoleProd*: $linPoleProd\ S = qPoleProd\ (of-int\ 'S)$

$\langle proof \rangle$

lemma *degree-linPoleProd*: $finite\ S \implies degree\ (linPoleProd\ S) = card\ S$

$\langle proof \rangle$

lemma *lead-coeff-linPoleProd*: $finite\ S \implies lead-coeff\ (linPoleProd\ S) = 1$

$\langle proof \rangle$

lemma *linPoleProd-nonzero*: $finite\ S \implies linPoleProd\ S \neq 0$

$\langle proof \rangle$

lemma *poly-linPoleProd*: $poly\ (linPoleProd\ S)\ y = (\prod\ r \in S.\ y - of-int\ r)$

$\langle proof \rangle$

Lagrange: $P\ mod\ \prod_{r \in S} (x - r) = \sum_{r \in S} -r\ res-r\ \prod_{s \neq r} (x - s).$

lemma *mod-linPoleProd*:

assumes $finite\ S$

shows $P\ mod\ linPoleProd\ S = (\sum\ r \in S.\ [:linResidue\ S\ P\ r:] * linPoleProd\ (S$
 $- \{r\}))$

$\langle proof \rangle$

Evaluating the partial-fraction decomposition away from the poles.

lemma *poly-div-linPoleProd*:

assumes $finite\ S\ \bigwedge r. r \in S \implies y - of-int\ r \neq 0$

shows $poly\ (P\ div\ linPoleProd\ S)\ y =$

$poly\ P\ y\ /\ (\prod\ r \in S.\ y - of-int\ r) - (\sum\ r \in$
 $S.\ linResidue\ S\ P\ r\ /\ (y - of-int\ r))$

$\langle proof \rangle$

17.7 Valuations of integers

lemma *vp-int-le-nat-log*:

$prime\ p \implies z \neq 0 \implies$

$nat\ |z| \leq M \implies vp\ p\ (of-int\ z) \leq int\ (nat-log\ p\ M)$

$\langle proof \rangle$

lemma *lt-vp-of-dvd*:

$\text{prime } p \implies z \neq 0 \implies \text{int } p \wedge (k + 1) \text{ dvd } z \implies$
 $\text{int } k < \text{vp } p \text{ (of-int } z)$
 $\langle \text{proof} \rangle$

lemma *vge-inv-int*:

$\text{prime } p \implies z \neq 0 \implies$
 $\neg \text{int } p \wedge (k + 1) \text{ dvd } z \implies \text{vge } p \text{ (1 / of-int } z) \text{ (- of-nat } k)$
 $\langle \text{proof} \rangle$

The pole values $H\{(5)\}$ - m for $m \leq K$ have $v\text{-}p \geq -5 \lfloor \log\text{-}p \ K \rfloor$.

lemma *vge-H5*: $\text{prime } p \implies m \leq K \implies$

$\text{vge } p \text{ (H5 } m) \text{ (- 5 * of-nat (nat-log } p \ K))}$
 $\langle \text{proof} \rangle$

lemma *vpGge-pX*: $\text{vpGge } p \text{ pX } 0$

$\langle \text{proof} \rangle$

17.8 The product-difference estimate

$v(\prod (a\text{-}i + u) - \prod a\text{-}i) \geq v(u) - L + \sum v(a\text{-}i)$ when every $v(a\text{-}i) \leq L < v(u)$.

lemma *vge-prod-add-sub-prod*:

assumes p : *prime* p **and** I : *finite* I **and** u : $u \neq 0$

and $a0$: $\bigwedge i. i \in I \implies$

$a\ i \neq 0$ **and** aL : $\bigwedge i. i \in I \implies \text{of-int } (\text{vp } p \text{ (} a\ i)) \leq L$

and Lu : $L < \text{of-int } (\text{vp } p \ u)$

shows $\text{vge } p \text{ ((} \prod i \in I. a\ i + u) - (\prod i \in I. a\ i))$
 $\text{(of-int } (\text{vp } p \ u) - L + (\sum i \in I. \text{of-int } (\text{vp } p \text{ (} a\ i))))$

$\langle \text{proof} \rangle$

17.9 Lemma 3.3

lemma *symPoles-subset*: $\text{symPoles } K \subseteq \{- \text{int } K .. \text{int } K\}$

$\langle \text{proof} \rangle$

lemma *finite-symPoles*: *finite* ($\text{symPoles } K$)

$\langle \text{proof} \rangle$

lemma *symPoles-abs-sub-le*: $r \in \text{symPoles } K \implies$

$s \in \text{symPoles } K \implies \text{nat } |r - s| \leq 2 * K$

$\langle \text{proof} \rangle$

lemma *dIdx-le-symPoles*: $r \in \text{symPoles } K \implies \text{dIdx } r \leq K$

$\langle \text{proof} \rangle$

theorem *far-pole-valuation-bound*:

assumes p : *prime* p **and** A : *IntValuedAt* p A **and** dA : *degree* $A \leq d$

shows $\text{vpGge } p \text{ (tauX (symPoles } K) ([\text{:fact } K \wedge 2:] * A))$

```

      (- 6 * of-nat (nat-log p (max (2 * K) (d + 1)))) - of-nat (multiplicity p
(24::nat)))
⟨proof⟩

end

theory Zeta5-Small-Primes
  imports Zeta5-Far-Poles
begin

```

18 The small-prime bound (3.12)

Section 3.3 of the paper: the basis polynomials $f_i(-x^2)$ are integer-valued, the determinant identity (3.11), and the small-prime bound (3.12) derived from Lemma 3.3. Lean theory *SmallPrimes*.

18.1 Section 3.3 Integer-valued basis polynomials

A takes integer values at integers.

definition *IntEval* :: *rat poly* $\Rightarrow$ *bool* **where**
IntEval $A \longleftrightarrow (\forall x::\text{int}. \exists z::\text{int}. \text{poly } A (\text{of-int } x) = \text{of-int } z)$

lemma *IntEval-IntValuedAt*: *prime* $p \implies \text{IntEval } A \implies \text{IntValuedAt } p \ A$
 ⟨proof⟩

lemma *IntEval-mult*: *IntEval* $A \implies \text{IntEval } B \implies \text{IntEval } (A * B)$
 ⟨proof⟩

lemma *IntEval-power*: *IntEval* $A \implies \text{IntEval } (A \wedge n)$
 ⟨proof⟩

lemma *IntEval-add*: *IntEval* $A \implies \text{IntEval } B \implies \text{IntEval } (A + B)$
 ⟨proof⟩

lemma *IntEval-C-int*: *IntEval* $[:\text{of-int } z:]$
 ⟨proof⟩

lemma *IntEval-pX*: *IntEval* pX
 ⟨proof⟩

binom($s \ x + m, k$) is integer-valued ($s, m \in \mathbb{Z}$).

lemma *IntEval-bp-pcompose*: *IntEval* (*pcompose* (*bp* k) $[:\text{of-int } m, \text{of-int } s:]$)
 ⟨proof⟩

lemma *poly-bp*: *poly* (*bp* k) $y = (\prod i < k. y - \text{of-nat } i) / \text{fact } k$
 ⟨proof⟩

$$\prod_{j=1}^N (j^2 - x^2) = \prod_{k < N} (N - k - x)(x + N - k).$$

lemma *prod-Icc-sq-sub*:

$$\left(\prod_{j=1}^N (j^2 - x^2) + \text{of-nat } j^2 \right) = \left(\prod_{k < N} (N - k - x)(x + N - k) + \text{of-nat } N - x - \text{of-nat } k \right) * (x + \text{of-nat } N - \text{of-nat } k) :: \text{rat}$$

<proof>

$$D-N(-x^2)/(N!)^2 = \text{binom}(N - x, N) \text{binom}(N + x, N).$$

lemma *Dm-pcompose-eq*:

$$\text{Polynomial.smult } (1 / \text{fact } N^2) (\text{pcompose } (Dm \ N) (- (pX^2))) = \text{pcompose } (bp \ N) [: \text{of-nat } N, -1:] * \text{pcompose } (bp \ N) [: \text{of-nat } N, 1:]$$

<proof>

lemma *IntEval-Dm-pcompose*: $\text{IntEval } (\text{Polynomial.smult } (1 / \text{fact } N^2) (\text{pcompose } (Dm \ N) (- (pX^2))))$

<proof>

lemma *E1-eq*:

$$\left(\prod_{k < 2 * m + 2} (x + (\text{of-nat } m + 1) - \text{of-nat } k) \right) = (x + \text{of-nat } m + 1) * x * \left(\prod_{j=1}^m (x^2 - \text{of-nat } j^2) :: \text{rat} \right)$$

<proof>

lemma *E2-eq*:

$$\left(\prod_{k < 2 * m + 2} (x + \text{of-nat } m - \text{of-nat } k) \right) = x * (x - \text{of-nat } m - 1) * \left(\prod_{j=1}^m (x^2 - \text{of-nat } j^2) :: \text{rat} \right)$$

<proof>

$$q-\{m+1\}(-x^2) = \text{binom}(x + m + 1, 2m + 2) + \text{binom}(x + m, 2m + 2).$$

lemma *qBasis-pcompose-eq*:

$$\text{pcompose } (qBasis \ (\text{Suc } m)) (- (pX^2)) = \text{pcompose } (bp \ (2 * m + 2)) [: \text{of-nat } m + 1, 1:] + \text{pcompose } (bp \ (2 * m + 2)) [: \text{of-nat } m, 1:]$$

<proof>

lemma *IntEval-qBasis*: $\text{IntEval } (\text{pcompose } (qBasis \ i) (- (pX^2)))$

<proof>

lemma *IntEval-fBasis*: $\text{IntEval } (\text{pcompose } (fBasis \ K \ i) (- (pX^2)))$

<proof>

$f-i(-x^2)$ is integer-valued (binomial identities $q-i(-x^2) = C(x+i, 2i) + C(x+i-1, 2i)$, $D-N(-x^2)/(N!)^2 = C(N-x, N) C(N+x, N)$).

theorem *fBasis-intValued*: $\text{prime } p \implies$

$$\text{IntValuedAt } p (\text{pcompose } (fBasis \ K \ i) (- (pX^2)))$$

<proof>

18.2 The determinant identity (3.11)

lemma *degree-Dm*: $\text{degree } (Dm\ m) = m$
 $\langle \text{proof} \rangle$

lemma *lead-coeff-Dm*: $\text{lead-coeff } (Dm\ m) = 1$
 $\langle \text{proof} \rangle$

lemma *Dm-nonzero*: $Dm\ m \neq 0$
 $\langle \text{proof} \rangle$

The leading coefficient $(-1)^i 2 / (2i)!$ of $q\text{-}i$ (and 1 for $i = 0$).

definition *qLead* :: $\text{nat} \Rightarrow \text{rat}$ **where**
 $qLead\ i = (\text{if } i = 0 \text{ then } 1 \text{ else } (-1)^i 2 / \text{fact } (2 * i))$

lemma *degree-qBasis-le*: $\text{degree } (qBasis\ i) \leq i$
 $\langle \text{proof} \rangle$

lemma *coeff-qBasis-self*: $\text{Polynomial.coeff } (qBasis\ i)\ i = qLead\ i$
 $\langle \text{proof} \rangle$

lemma *qBasis-eq-sum*:
 $i < h \implies qBasis\ i = (\sum_{k < h} k < h. \text{Polynomial.smult } (\text{Polynomial.coeff } (qBasis\ i)\ k) (pX^k))$
 $\langle \text{proof} \rangle$

The coefficient matrix of the $q\text{-}i$, lower triangular.

definition *Qc* :: $\text{nat} \Rightarrow \text{rat mat}$ **where**
 $Qc\ h = \text{Matrix.mat } h\ h\ (\lambda(i, k). \text{Polynomial.coeff } (qBasis\ i)\ k)$

lemma *Qc-carrier*: $Qc\ h \in \text{carrier-mat } h\ h$
 $\langle \text{proof} \rangle$

lemma *det-Qc*: $\text{Determinant.det } (Qc\ h) = (\prod_{i < h} qLead\ i)$
 $\langle \text{proof} \rangle$

lemma *qLead-sq-prod*: $(\prod_{i < h} qLead\ i)^2 = 4^{h-1} / (\prod_{i = 1..h-1} \text{fact } (2 * i)^2)$
 $\langle \text{proof} \rangle$

lemma *fBasis-mult*:
 $fBasis\ K\ i * fBasis\ K\ j = \text{Polynomial.smult } ((1 / \text{fact } (\text{Nof } K)^2)^6) (Dm\ (\text{Nof } K)^6 * (qBasis\ i * qBasis\ j))$
 $\langle \text{proof} \rangle$

lemma *muX-fBasis*:
assumes $i < \text{hof } K\ j < \text{hof } K$
shows $\text{muX } \{1..K\} (fBasis\ K\ i * fBasis\ K\ j) = \text{Polynomial.smult } ((1 / \text{fact } (\text{Nof } K)^2)^6)$

$$(\sum k < \text{hof } K. \sum l < \text{hof } K. [:Qc (\text{hof } K) \$\$ (i, k) * Qc (\text{hof } K) \$\$ (j, l) :] * GK K \$\$ (k, l))$$

⟨proof⟩

lemma *SK-eq-lead*:

$$SK K = (\text{fact } K \wedge 2 * (1 / \text{fact } (\text{Nof } K) \wedge 2) \wedge 6) \wedge \text{hof } K * (\prod i < \text{hof } K. qLead i) \wedge 2$$

⟨proof⟩

The matrix of (3.11) is $c \cdot Q G Q^T$ with $c = (K!) \wedge 2 / (N!) \wedge \{12\}$.

lemma *fBasis-matrix-eq*:

$$\begin{aligned} & \text{Matrix.mat } (\text{hof } K) (\text{hof } K) (\lambda(i, j). [: \text{fact } K \wedge 2 :] * \mu X \{1..K\} (fBasis K i * fBasis K j)) = \\ & [: \text{fact } K \wedge 2 * (1 / \text{fact } (\text{Nof } K) \wedge 2) \wedge 6 :] \cdot_m \\ & (\text{map-mat } (\lambda q. [: q :]) (Qc (\text{hof } K)) * GK K * \\ & \text{transpose-mat } (\text{map-mat } (\lambda q. [: q :]) (Qc (\text{hof } K)))) \end{aligned}$$

⟨proof⟩

lemma *comm-ring-hom-pCons*: $\text{comm-ring-hom } (\lambda q :: 'a :: \text{comm-ring-1}. [: q :]) \langle proof \rangle$

lemma *det-map-mat-C*:

$$M \in \text{carrier-mat } n \implies \text{Determinant.det } (\text{map-mat } (\lambda q. [: q :]) M) = [: \text{Determinant.det } M :]$$

⟨proof⟩

(3.11): $F-K = \text{det}[(K!) \wedge 2 \mu X (f-i f-j / D-K)]$.

theorem *F-eq-det-fBasis*:

$$\begin{aligned} & \text{assumes } 40 \text{ dvd } K \\ & \text{shows } FK K = \text{Determinant.det } (\text{Matrix.mat } (\text{hof } K) (\text{hof } K) \\ & \quad (\lambda(i, j). [: \text{fact } K \wedge 2 :] * \mu X \{1..K\} (fBasis K i * fBasis K j))) \end{aligned}$$

⟨proof⟩

18.3 The small-prime bound (3.12)

lemma *degree-fBasis-le*: $\text{degree } (fBasis K i) \leq 3 * \text{Nof } K + i$
 ⟨proof⟩

lemma *signedPoles-Icc*: $\text{signedPoles } \{1..K\} = \text{symPoles } K$
 ⟨proof⟩

Each entry of the matrix in (3.11) satisfies the Lemma 3.3 bound.

lemma *fBasis-entry-vge*:

$$\begin{aligned} & \text{assumes } p: \text{prime } p \text{ and } K: 40 \text{ dvd } K \text{ and } i: i < \text{hof } K \text{ and } j: j < \text{hof } K \\ & \text{shows } vpGge p ([: \text{fact } K \wedge 2 :] * \mu X \{1..K\} (fBasis K i * fBasis K j)) \\ & \quad (- 6 * \text{of-nat } (\text{nat-log } p (5 * K)) - \text{of-nat } (\text{multiplicity } p (24 :: \text{nat}))) \end{aligned}$$

⟨proof⟩

(3.12): $v-p \wedge G(F-K) \geq -6h \lfloor \log-p(5K) \rfloor - h v-p(24)$ for every prime p .

theorem *vpG-F-ge*:
assumes *p*: prime *p* **and** *K*: 40 dvd *K*
shows *vpGge p (FK K) (- 6 * of-nat (hof K) * of-nat (nat-log p (5 * K))*
 *- of-nat (hof K) * of-nat (multiplicity p (24::nat)))*
 ⟨*proof*⟩
end

theory *Zeta5-Truncated-Expansions*
imports *Zeta5-Far-Poles HOL-Computational-Algebra.Polynomial-FPS*
begin

19 The truncated p -adic layer and Lemma 3.1

Section 3.1 of the paper (Lean theory *PadicTau*). Lean works in $\mathbb{Q}_p$ with convergent series; here every truncated series is a polynomial, so the difference identity (3.3) for a far pole comes with an explicit error polynomial whose coefficients are divisible by p^{N+1} . The near residues and the analytic part (handled with formal power series) are shown to be integral, and Lemma 3.1 is proved in this truncated rational form (*tauX-far-pole-valuation*).

19.1 Truncated expansions of $1/(z - s)$ as polynomials

farPoly s N = $-\sum_{d < N} s^{-(d+1)} z^d$, the degree $< N$ truncation of $1/(z - s)$.

definition *farPoly* :: *rat* $\Rightarrow$ *nat* $\Rightarrow$ *rat poly* **where**
farPoly s N = $-(\sum_{d < N}. \text{Polynomial.smult } (\text{inverse } s^{(d+1)}) (pX^{(d)})$

lemma *coeff-farPoly*:
Polynomial.coeff (farPoly s N) d = (if $d < N$ then $-(\text{inverse } s^{(d+1)})$ else 0)
 ⟨*proof*⟩

lemma *degree-farPoly-lt*: $0 < N \implies \text{degree } (\text{farPoly } s \ N) < N$
 ⟨*proof*⟩

lemma *tau-farPoly*: $\tau (\text{farPoly } s \ N) = -(\sum_{d < N}. \text{kappa } d * \text{inverse } s^{(d+1)})$
 ⟨*proof*⟩

The truncated series (3.5) is τ of the truncated expansion.

lemma *tauAnPole-tr-eq-tau*: $\tau \text{AnPole-tr } p \ s \ M = \tau (\text{farPoly } s \ (M + 3))$
 ⟨*proof*⟩

lemma *tauAnPole-tr-eq-sum*: $\tau \text{AnPole-tr } p \ s \ M = -(\sum_{d < M + 3}. \text{kappa } d * \text{inverse } s^{(d+1)})$

$\langle \text{proof} \rangle$

$$(z - s) \text{farPoly } s \ N = 1 - s^{\wedge\{-N\}} z^{\wedge N}.$$

lemma *farPoly-mul*:

$$s \neq 0 \implies (pX - [:s:]) * \text{farPoly } s \ N = \\ 1 - \text{Polynomial.smult } (\text{inverse } s^{\wedge N}) (pX^{\wedge N})$$

$\langle \text{proof} \rangle$

The shifted-pole correction $\text{farPoly } s \ N \ (z + 1) - \text{farPoly } (s - 1) \ N$, as an explicit polynomial whose coefficients are divisible by $p^{\wedge\{N+1\}}$ when $v\text{-}p(s) < 0$.

definition *hPoly* :: *rat* $\Rightarrow$ *nat* $\Rightarrow$ *rat poly* **where**

$$\text{hPoly } s \ N = \text{Polynomial.smult } (\text{inverse } (s * (s - 1))) \\ (\sum i < N. (\text{Polynomial.smult } (\text{inverse } (s - 1)) \ pX)^{\wedge i} * \\ (\text{Polynomial.smult } (\text{inverse } s) \ (pX + 1))^{\wedge (N - 1 - i)})$$

lemma *vp-sub-one-lt*: *prime* $p \implies v\text{p } p \ s < 0 \implies s - 1 \neq 0 \wedge$

$$v\text{p } p \ (s - 1) < 0$$

$\langle \text{proof} \rangle$

lemma *vpGge-pow*: *prime* $p \implies v\text{pGge } p \ A \ a \implies$

$$v\text{pGge } p \ (A^{\wedge n}) \ (\text{of-nat } n * a)$$

$\langle \text{proof} \rangle$

lemma *vge-inverse-of-vp-lt*: *prime* $p \implies v\text{p } p \ s < 0 \implies$

$$v\text{ge } p \ (\text{inverse } s) \ 1$$

$\langle \text{proof} \rangle$

lemma *smult-as-C-mult*: $\text{Polynomial.smult } c \ P = [:c:] * P$

$\langle \text{proof} \rangle$

lemma *vpGge-hPoly*:

assumes *prime* $p \ v\text{p } p \ s < 0$

shows $v\text{pGge } p \ (\text{hPoly } s \ N) \ (\text{of-nat } (N + 1))$

$\langle \text{proof} \rangle$

lemma *farPoly-shift*:

assumes $s \neq 0 \ s - 1 \neq 0$

shows $p\text{compose } (\text{farPoly } s \ N) \ (pX + 1) - \text{farPoly } (s - 1) \ N = \text{hPoly } s \ N$

$\langle \text{proof} \rangle$

lemma *vge-kappa-m4*: *prime* $p \implies v\text{ge } p \ (\text{kappa } d) \ (-4)$

$\langle \text{proof} \rangle$

lemma *vge-tau-of-vpGge*: *prime* $p \implies v\text{pGge } p \ P \ b \implies$

$$v\text{ge } p \ (\text{tau } P) \ (b - 4)$$

$\langle \text{proof} \rangle$

lemma *coeff-farPoly-4*: $5 \leq N \implies$

Polynomial.coeff (farPoly s N) 4 = - (s powi (- 5))
<proof>

The difference identity (3.3) for a far pole, with explicit error: the discrepancy equals $\tau(h)$ and has valuation $\geq M$.

lemma *tauAnPole-tr-sub-eq*:

assumes *p*: prime *p* **and** *s*: *vp p s < 0* **and** *s0*: *s ≠ 0* **and** *M2*: $2 \leq M$
shows *vge p (tauAnPole-tr p s M - tauAnPole-tr p (s - 1) M - s powi (- 5))*
(of-nat M)
<proof>

The difference identity (3.3) for a far pole: $\tau^{\sim}\{an\}(1/(z-s)) - \tau^{\sim}\{an\}(1/(z-(s-1))) = s^{\sim}\{-5\}$ holds in $\mathbf{Q}\text{-}p$; for the partial sums it holds modulo any prescribed power of p once M is large (Lean: *tauAnPole-sub*).

lemma *tauAnPole-tr-sub*:

assumes prime *p* *vp p s < 0* *s ≠ 0*
shows $\exists M0. \forall M \geq M0. vge p (tauAnPole-tr p s M - tauAnPole-tr p (s - 1) M - s powi (- 5)) B$
<proof>

19.2 The near residues

lemma *vp-of-int-nonneg*: prime *p* $\implies of-int r \neq (0 :: rat) \implies 0 \leq vp p (of-int r)$
<proof>

lemma *far-ne-int*: prime *p* $\implies vp p s = -1 \implies s \neq of-int r$
<proof>

lemma *far-disj*: prime *p* $\implies (\bigwedge s. s \in F \implies vp p s = -1) \implies of-int 'T \cap F = \{\}$
<proof>

An integer minus a far pole has valuation exactly -1 .

lemma *vp-int-sub-far*:

prime *p* $\implies vp p s = -1 \implies of-int r - s \neq 0 \wedge vp p (of-int r - s) = -1$
<proof>

lemma *vp-int-sub-near*:

prime *p* $\implies \neg int p dvd (r - r') \implies of-int r - of-int r' \neq (0 :: rat) \wedge vp p (of-int r - of-int r') = 0$
<proof>

lemma *vp-neg-p-powi*: prime *p* $\implies vp p ((- of-nat p) powi (- int n)) = - int n$
<proof>

The near residues are integral (Lean: *pt-near-res-vge*): poles T distinct modulo p , far poles F with $v_p(s) = -1$, numerator $(-p)^{\wedge\{-|F|\}}$ U with U integral.

lemma *near-res-vge*:

assumes p : prime p **and** T : finite T **and** F : finite F
and hT : $\bigwedge r s. r \in T \implies s \in T \implies$
 $r \neq s \implies \neg \text{int } p \text{ dvd } (r - s)$
and hF : $\bigwedge s. s \in F \implies$
 $v_p p s = -1$ **and** U : $v_p \text{Gge } p \ U \ 0$ **and** r : $r \in T$
shows $vge \ p \ (qRes \ (of\text{-}int \ ' \ T \cup F) \ ([:(- \ of\text{-}nat \ p) \ powi \ (- \ int \ (card \ F)):] \ * \ U) \ (of\text{-}int \ r)) \ 0$
 $\langle proof \rangle$

19.3 The analytic part

$-1/(X - s) = \sum s^{\wedge\{-(d+1)\}} X^{\wedge d}$ as a formal power series.

definition *farSeries* :: $rat \Rightarrow rat \text{ fps}$ **where**

farSeries $s = Abs\text{-}fps \ (\lambda d. \text{inverse } s^{\wedge (d + 1)})$

lemma *X-sub-C-mul-farSeries*: $s \neq 0 \implies$

$fps\text{-of-poly} \ (pX - [:s:]) \ * \ farSeries \ s = -1$
 $\langle proof \rangle$

The Taylor coefficients of $Q + \sum_{s \in F} \varrho\text{-}s/(z - s)$: $\Pi\text{-}F \cdot f = \Pi\text{-}F \ Q + \sum \varrho\text{-}s \ \Pi\text{-}\{F - s\}$.

lemma *qPoleProd-mul-fCoeff*:

assumes $finite \ F \ \bigwedge s. s \in F \implies s \neq 0$
shows $fps\text{-of-poly} \ (qPoleProd \ F) \ * \ Abs\text{-}fps \ (fCoeff \ Q \ F \ \varrho) =$
 $fps\text{-of-poly} \ (qPoleProd \ F \ * \ Q + (\sum s \in F. [: \varrho \ s:] \ * \ qPoleProd \ (F - \{s\})))$
 $\langle proof \rangle$

If $\Psi f = N$ as power series, with $\Psi(0)$ a unit, the other coefficients of Ψ in $p\mathbb{Z}\text{-}p$, N integral and $\equiv 0 \pmod{p}$ beyond degree $p+1$, then so is f .

lemma *series-vge*:

assumes p : prime p **and** $P0$: $Polynomial.coeff \ \Psi \ 0 \neq$
 0 **and** $P0v$: $v_p \ p \ (Polynomial.coeff \ \Psi \ 0) = 0$
and $P1$: $\bigwedge n. 1 \leq n \implies vge \ p \ (Polynomial.coeff \ \Psi \ n) \ 1$
and $N0$: $v_p \text{Gge } p \ N \ 0$ **and** $N1$: $\bigwedge d. p + 1 < d \implies$
 $vge \ p \ (Polynomial.coeff \ N \ d) \ 1$
and mul : $fps\text{-of-poly} \ \Psi \ * \ Abs\text{-}fps \ f = fps\text{-of-poly} \ N$
shows $vge \ p \ (f \ d) \ 0 \wedge (p + 1 < d \implies vge \ p \ (f \ d) \ 1)$
 $\langle proof \rangle$

The shape of $\Psi = \prod (p \ s - p \ z)$: unit constant term, other coefficients in $p\mathbb{Z}\text{-}p$.

definition *PsiShape* :: $nat \Rightarrow rat \text{ poly} \Rightarrow bool$ **where**

PsiShape $p \ P \longleftrightarrow Polynomial.coeff \ P \ 0 \neq 0 \wedge$

$$vp\ p\ (Polynomial.coeff\ P\ 0) = 0 \wedge \\ (\forall n. 1 \leq n \longrightarrow vge\ p\ (Polynomial.coeff\ P\ n)\ 1)$$

lemma *PsiShape-one*: $PsiShape\ p\ 1$
 $\langle proof \rangle$

lemma *PsiShape-vpGge*: $prime\ p \implies PsiShape\ p\ P \implies vpGge\ p\ P\ 0$
 $\langle proof \rangle$

lemma *PsiShape-mult*: $prime\ p \implies PsiShape\ p\ P \implies$
 $PsiShape\ p\ Q \implies PsiShape\ p\ (P * Q)$
 $\langle proof \rangle$

lemma *PsiShape-prod*:
 $prime\ p \implies finite\ I \implies (\bigwedge i. i \in I \implies$
 $PsiShape\ p\ (f\ i)) \implies PsiShape\ p\ (\prod i \in I. f\ i)$
 $\langle proof \rangle$

A factor $p\ s - p\ z$ with $v\text{-}p(s) = -1$.

lemma *PsiShape-factor*: $prime\ p \implies vp\ p\ s = -1 \implies$
 $PsiShape\ p\ [:of\text{-}nat\ p * s, -\ of\text{-}nat\ p:]$
 $\langle proof \rangle$

Division by an integral monic polynomial preserves " $\equiv 0 \pmod p$ " beyond degree $p+1$.

lemma *degree-div-le-rat*: $degree\ (x\ div\ y) \leq degree\ (x :: rat\ poly)$
 $\langle proof \rangle$

lemma *div-lead1-high*:
assumes p : $prime\ p$ **and** $R0$: $vpGge\ p\ R\ 0$ **and** $R1$: $\bigwedge d. p + 1 < d \implies$
 $vge\ p\ (Polynomial.coeff\ R\ d)\ 1$
and $Q1$: $lead\text{-}coeff\ Q = 1$ **and** $Q0$: $vpGge\ p\ Q\ 0$ **and** d : $p + 1 < d$
shows $vge\ p\ (Polynomial.coeff\ (R\ div\ Q)\ d)\ 1$
 $\langle proof \rangle$

lemma *card-le-prime-of-distinct-mod*:
assumes $prime\ p$ $finite\ T$ $\bigwedge r\ s. r \in T \implies s \in T \implies$
 $r \neq s \implies \neg int\ p\ dvd\ (r - s)$
shows $card\ T \leq p$
 $\langle proof \rangle$

lemma *vpGge-qPoleProd-int*:
 $prime\ p \implies finite\ A \implies A \subseteq of\text{-}int\ 'T \implies$
 $vpGge\ p\ (qPoleProd\ A)\ 0$
 $\langle proof \rangle$

The analytic part is integral (Lean: *pt-far-vge*): every κ - d f - d is p -integral, f - d the Taylor coefficients of $Q + \sum_{s \in F} -\{s \in F\} \varrho\text{-}s / (z - s)$.

lemma *far-vge*:

assumes p : prime p **and** $p7$: $7 \leq p$ **and** T : finite T **and** F : finite F
and hT : $\bigwedge r s. r \in T \implies s \in T \implies$
 $r \neq s \implies \neg \text{int } p \text{ dvd } (r - s)$
and hF : $\bigwedge s. s \in F \implies \text{vp } p \text{ } s = -1$
and $U0$: $\text{vpGge } p \text{ } U \text{ } 0$ **and** $U1$: $\bigwedge d. p + 1 < d \implies$
 $\text{vge } p \text{ } (\text{Polynomial.coeff } U \text{ } d) \text{ } 1$
shows $\text{vge } p \text{ } (\text{kappa } d * \text{fCoeff } ([:(- \text{ of-nat } p) \text{ powi } (- \text{ int } (\text{card } F))]) *$
 $U) \text{ div } \text{qPoleProd } (\text{of-int } ' T \cup F))$
 $F (\text{qRes } (\text{of-int } ' T \cup F) ([:(- \text{ of-nat } p) \text{ powi } (- \text{ int } (\text{card } F))]) *$
 $U)) \text{ } d) \text{ } 0$
 $\langle \text{proof} \rangle$

19.4 Lemma 3.1 with far poles, truncated rational form

lemma tauPoleP-tr-near : $\text{tauPoleP-tr } p \text{ } Y \text{ } (\text{of-int } r) \text{ } M = [:\text{H5 } (d\text{Idx } r):] - Y$
 $\langle \text{proof} \rangle$

lemma far-denom-ne-1 : $\text{prime } p \implies \text{vp } p \text{ } s = -1 \implies$
 $\text{snd } (\text{quotient-of } s) \neq 1$
 $\langle \text{proof} \rangle$

lemma tauPoleP-tr-far : $\text{prime } p \implies \text{vp } p \text{ } s = -1 \implies$
 $\text{tauPoleP-tr } p \text{ } Y \text{ } s \text{ } M = [:\text{tauAnPole-tr } p \text{ } s \text{ } M:]$
 $\langle \text{proof} \rangle$

lemma vge-H5-small : $\text{prime } p \implies n < p \implies \text{vge } p \text{ } (\text{H5 } n) \text{ } 0$
 $\langle \text{proof} \rangle$

Lemma 3.1 with far poles, rational form (Lean: *lemma-3-1-rat*): with Y integral, near poles T distinct modulo p and $d(r) < p$, far poles F with $v\text{-}p(s) = -1$, numerator $(-p) \sim \{-|F|\} U$ with U integral and $\equiv 0 \pmod{p}$ beyond degree $p+1$, the truncated $\tau \sim \{ext\}\text{-}Y$ is integral. The truncation must cover the polynomial part: $\text{deg } U \leq M$.

lemma sum-const-poly : $(\sum i \in I. [:\text{f } i:]) = [:\sum i \in I. \text{f } i:]$
 $\langle \text{proof} \rangle$

theorem $\text{tauX-far-pole-valuation}$:

assumes p : prime p **and** $p7$: $7 \leq p$ **and** T : finite T **and** F : finite F
and hT : $\bigwedge r s. r \in T \implies s \in T \implies$
 $r \neq s \implies \neg \text{int } p \text{ dvd } (r - s)$ **and** hd : $\bigwedge r. r \in$
 $T \implies d\text{Idx } r < p$
and hF : $\bigwedge s. s \in F \implies \text{vp } p \text{ } s = -1$
and Y : $\text{vpGge } p \text{ } Y \text{ } 0$
and $U0$: $\text{vpGge } p \text{ } U \text{ } 0$ **and** $U1$: $\bigwedge d. p + 1 < d \implies$
 $\text{vge } p \text{ } (\text{Polynomial.coeff } U \text{ } d) \text{ } 1$
and dU : $\text{degree } U \leq M$
shows $\text{vpGge } p \text{ } (\text{tauExt-tr } p \text{ } Y ([:(- \text{ of-nat } p) \text{ powi } (- \text{ int } (\text{card } F))]) *$
 $U) (\text{of-int } ' T \cup F) \text{ } M) \text{ } 0$
 $\langle \text{proof} \rangle$

end

theory *Zeta5-Pole-Distribution*
imports *Zeta5-Truncated-Expansions*
begin

20 The distribution formula (3.7) and Lemma 3.2

Section 3.2 of the paper (Lean theory *Distribution*): a Raabe-type multiplication formula for τ on polynomials, the sum over the residue classes $a < p$ of the truncated pole values (by induction on the pole, with the truncation error controlled), compatibility of partial fractions with the substitution $x = a + p z$, and Lemma 3.2 (*tauX-distribution-formula*).

20.1 Raabe's multiplication formula

lemma *Lfun-uminus*: $Lfun \ (-P) = -Lfun \ P$
 $\langle proof \rangle$

lemma *Lfun-sub*: $Lfun \ (P - Q) = Lfun \ P - Lfun \ Q$
 $\langle proof \rangle$

lemma *Lfun-zero*: $Lfun \ 0 = 0$
 $\langle proof \rangle$

lemma *Lfun-sum*: $Lfun \ (\sum i \in I. f \ i) = (\sum i \in I. Lfun \ (f \ i))$
 $\langle proof \rangle$

lemma *sum-const-poly*: $(\sum i \in I. [:f \ i:]) = [: \sum i \in I. f \ i:]$
 $\langle proof \rangle$

lemma *Lfun-pX-pow*: $Lfun \ (pX \wedge n) = bernoulli \ n$
 $\langle proof \rangle$

lemma *Lfun-fwd-monom*:
 $Lfun \ (pcompose \ (Polynomial.monom \ c \ n) \ (pX + 1) - Polynomial.monom \ c \ n)$
 $= (if \ n =$
 $\quad 1 \text{ then } c \text{ else } 0)$
 $\langle proof \rangle$

$L(f(x+1) - f(x)) = f'(0)$: the defining recursion of the Bernoulli numbers.

lemma *Lfun-fwd*: $Lfun \ (pcompose \ f \ (pX + 1) - f) = poly \ (pderiv \ f) \ 0$
 $\langle proof \rangle$

lemma *pderiv-pcompose-affine*:
 $pderiv \ (pcompose \ Q \ ([:a:] + [:c:] * pX)) =$

*Polynomial.smult c (pcompose (pderiv Q) ([:a:] + [:c:] * pX))*
 $\langle \text{proof} \rangle$

lemma *Lfun-raabe*:

$(\sum a < p. \text{Lfun } (\text{pcompose } f ([:\text{of-nat } a:] + [:\text{of-nat } p:] * pX))) = \text{of-nat } p * \text{Lfun } f$
 $\langle \text{proof} \rangle$

lemma *tau-raabe*:

$(\sum a < p. \text{tau } (\text{pcompose } Q ([:\text{of-nat } a:] + [:\text{of-nat } p:] * pX))) = \text{of-nat } p \wedge 4 * \text{tau } Q$
 $\langle \text{proof} \rangle$

20.2 Harmonic increments and the pole sums

lemma *H5-dIdx-sub*: $H5 \text{ (dIdx } n) - H5 \text{ (dIdx } (n - 1)) = (\text{if } n = 0 \text{ then } 0 \text{ else } 1 / \text{of-int } n \wedge 5)$
 $\langle \text{proof} \rangle$

The scalar part of the truncated τ - Y^{ext} ($1/(z - n/p)$).

definition *phi-tr* :: $\text{nat} \Rightarrow \text{int} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$\text{phi-tr } p \ n \ M = (\text{if } \text{int } p \ \text{dvd } n \text{ then } H5 \text{ (dIdx } (n \ \text{div } \text{int } p)) - \text{Cp-tr } p \ M$
 $\text{else } \text{tauAnPole-tr } p \ (\text{of-int } n / \text{of-nat } p) \ M)$

lemma *vp-int-div-p*: $\text{prime } p \implies \neg \text{int } p \ \text{dvd } n \implies$

$\text{vp } p \ (\text{of-int } n / \text{of-nat } p) = -1 \wedge (\text{of-int } n / \text{of-nat } p :: \text{rat}) \neq 0$
 $\langle \text{proof} \rangle$

lemma *phi-tr-sub*:

assumes p : *prime* p

shows $\exists M0. \forall M \geq M0. \text{vge } p \ (\text{phi-tr } p \ n \ M - \text{phi-tr } p \ (n - \text{int } p) \ M$
 $- \text{of-nat } p \wedge 5 * (H5 \text{ (dIdx } n) - H5 \text{ (dIdx } (n - 1)))) B$

$\langle \text{proof} \rangle$

definition *Gsum-tr* :: $\text{nat} \Rightarrow \text{int} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$Gsum-tr \ p \ r \ M = (\sum a < p. \text{phi-tr } p \ (r - \text{int } a) \ M)$

lemma *Gsum-tr-step*: $0 < p \implies$

$Gsum-tr \ p \ n \ M - Gsum-tr \ p \ (n - 1) \ M = \text{phi-tr } p \ n \ M - \text{phi-tr } p \ (n - \text{int } p) \ M$

$\langle \text{proof} \rangle$

lemma *Gsum-tr-zero*: $\text{prime } p \implies Gsum-tr \ p \ 0 \ M = 0$

$\langle \text{proof} \rangle$

lemma *Gsum-tr-eq*:

assumes p : *prime* p

shows $\exists M0. \forall M \geq M0. \text{vge } p \ (Gsum-tr \ p \ r \ M - \text{of-nat } p \wedge 5 * H5 \text{ (dIdx } r))$
 B

$\langle proof \rangle$

20.3 The pole values of $\tau^{\wedge\{ext\}}\text{-}Y$ on the distributed poles

lemma *quotient-of-int-div-prime*:

assumes $prime\ p \neg int\ p\ dvd\ n$
shows $snd\ (quotient\text{-}of\ (of\text{-}int\ n\ /\ of\text{-}nat\ p)) \neq 1$
 $\langle proof \rangle$

lemma *tauPoleP-tr-int-div*:

assumes $prime\ p$
shows $tauPoleP\text{-}tr\ p\ (Yp\text{-}tr\ p\ M)\ (of\text{-}int\ n\ /\ of\text{-}nat\ p)\ M =$
 $[phi\text{-}tr\ p\ n\ M:] - (if\ int\ p\ dvd\ n\ then\ [:of\text{-}nat\ p\ ^\wedge\ 5:] * pX\ else\ 0)$
 $\langle proof \rangle$

lemma *sum-tauPoleP-tr*:

assumes $p: prime\ p$
shows $\exists M0. \forall M \geq M0.$
 $vpGge\ p\ ((\sum a < p. tauPoleP\text{-}tr\ p\ (Yp\text{-}tr\ p\ M)\ ((of\text{-}int\ r - of\text{-}nat\ a) /\ of\text{-}nat\ p)\ M)$
 $- [:of\text{-}nat\ p\ ^\wedge\ 5:] * ([H5\ (dIdx\ r):] - pX))\ B$
 $\langle proof \rangle$

20.4 Partial fractions and the substitution $x = a + p\ z$

$\tau^{\wedge\{ext\}}$ of a rational function given by an explicit partial fraction decomposition.

lemma *tauExt-tr-decomp*:

assumes $finite\ S\ inj\text{-}on\ f\ S$
and $U = Q' * qPoleProd\ (f\ 'S) + (\sum r \in S. [:q\ r:] * qPoleProd\ (f\ '(S - \{r\})))$
shows $tauExt\text{-}tr\ p\ Y\ U\ (f\ 'S)\ M = [:tau\ Q':] + (\sum r \in S. [:q\ r:] * tauPoleP\text{-}tr\ p\ Y\ (f\ r)\ M)$
 $\langle proof \rangle$

lemma *distrib-inj*: $0 < p \implies$

$inj\ (\lambda r. (of\text{-}int\ r - of\text{-}nat\ a) /\ (of\text{-}nat\ p :: rat))$
 $\langle proof \rangle$

$$(\prod_{r \in T} (x - r))(a + p\ z) = p^{\wedge\{|T|\}} \prod_{r \in T} (z - (r - a)/p).$$

lemma *linPoleProd-distrib*:

assumes $0 < p\ finite\ T$
shows $pcompose\ (linPoleProd\ T)\ ([:of\text{-}nat\ a:] + [:of\text{-}nat\ p:] * pX) =$
 $Polynomial.smult\ (of\text{-}nat\ p\ ^\wedge\ card\ T)\ (qPoleProd\ (distribPoles\ p\ T\ a))$
 $\langle proof \rangle$

lemma *summand-eq*:

assumes $p: prime\ p$ **and** $S: finite\ S$
shows $tauExt\text{-}tr\ p\ Y\ (distribNum\ p\ S\ P\ a)\ (distribPoles\ p\ S\ a)\ M =$

$$[:\text{tau } (p\text{compose } (P \text{ div } \text{linPoleProd } S) ([:\text{of-nat } a:] + [:\text{of-nat } p:] * pX)):]$$

$$+ (\sum r \in S. [:\text{linResidue } S \ P \ r / \text{of-nat } p:] * \text{tauPoleP-tr } p \ Y ((\text{of-int } r - \text{of-nat } a) / \text{of-nat } p) \ M)$$

$$\langle \text{proof} \rangle$$

20.5 Lemma 3.2

lemma *finite-eventually-all*:
assumes *finite* $S \wedge r. r \in S \implies$
 $\exists M0::\text{nat}. \forall M \geq M0. Q \ r \ M$
shows $\exists M0. \forall r \in S. \forall M \geq M0. Q \ r \ M$
 $\langle \text{proof} \rangle$

lemma *C-mul-diff-C-mul*: $[:c:] * (X - [:k:] * T) = [:c:] * X - [:c * k:] * (T :: \text{rat poly})$
 $\langle \text{proof} \rangle$

lemma *distribution-formula-aux*:
fixes $c \ k \ t :: \text{rat}$ **and** $A :: \text{rat poly}$ **and** $x :: 'a \Rightarrow \text{rat}$ **and** $T :: 'a \Rightarrow \text{rat poly}$
assumes $ck: c * k = 1$
shows $[:t:] + (\sum r \in S. [:\text{x } r:] * T \ r) - [:c:] * ([:k * t:] + A) =$
 $- [:c:] * (A - (\sum r \in S. [:\text{x } r * k:] * T \ r))$
 $\langle \text{proof} \rangle$

$\tau \cdot X(g) = p^{-4} \sum_{a < p} \tau \cdot Y^{\text{ext}}(g(a + p \ x))$ with $Y = p^5 X + C \cdot p$
(Lean: *lemma-3-2'*); the truncated right-hand side agrees with the left-hand side modulo any prescribed power of p once M is large.

theorem *tauX-distribution-formula*:
assumes p : *prime* p **and** $p7: 7 \leq p$ **and** S : *finite* S
shows $\exists M0. \forall M \geq M0.$

$$\text{vpGge } p \ (\text{tauX } S \ P - [:\text{of-nat } p \ \text{powi } (- \ 4):] * (\sum a < p. \text{tauExt-tr } p \ (Yp\text{-tr } p \ M) (\text{distribNum } p \ S \ P \ a) (\text{distribPoles } p \ S \ a) \ M))$$

$$B$$
 $\langle \text{proof} \rangle$

end

theory *Zeta5-Inner-Range*
imports *Zeta5-Small-Primes* *Zeta5-Pole-Distribution* *Polynomial-Taylor-Shift* *Unimodular-Determinants*
begin

21 The inner range: Proposition 4.1

Section 4.1 of the paper: the inner basis, extraction of powers of p from $g(c + p \ z)$, the entry bounds (4.2) and (4.3), and the unimodularity of the

inner Gram matrix (Proposition 4.1, *DeltaK-vpGge-inner*). Lean theories *Section4*, *InnerBasis*, *InnerEntries*, *InnerFinal*.

21.1 Section 4.1 The inner range

(4.1): the inner range.

definition *InnerHyp* :: $\text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{bool}$ **where**
 $\text{InnerHyp } K \ M \ p \iff 40 \leq M \wedge 40 \text{ dvd } K \wedge 0 < K \wedge$
 $200 * M \wedge^2 \leq K \wedge K < p * M \wedge 3 * p \leq K$

Under (4.1): $p > 200M$ and $p \wedge^2 > 5K$.

lemma *innerHyp-bounds*:

assumes *InnerHyp* $K \ M \ p$

shows $200 * M < p \wedge 5 * K < p \wedge^2$

<proof>

(4.4): $0 \leq E < m$ and $mT + E = h - L - 0 + 3(N - m - N)$.

lemma *TE-spec*:

assumes *prime* p *InnerHyp* $K \ M \ p$

shows $0 \leq \text{Ein } K \ M \ p \wedge \text{Ein } K \ M \ p < \text{int } (m\text{Half } p) \wedge$

$\text{int } (m\text{Half } p) * \text{Tin } K \ M \ p + \text{Ein } K \ M \ p = \text{rhs}_{44} \ K \ M \ p$

<proof>

(4.8): $\gamma - p \wedge^{\text{in}}$ is an integer (twice a sum of half-integers).

lemma *two-wIn-Ints*: $2 * w\text{In } K \ M \ p \ a \ i \in (\mathbb{Z} :: \text{rat set})$

<proof>

lemma *gammaIn-isInt*: $\exists n :: \text{int}. \text{gammaIn } K \ M \ p = \text{of-int } n$

<proof>

Section 4.1: the dimensions $L - a$ are nonnegative and $L - 0 + \sum -\{a \geq 1\} L - a = h$.

lemma *card-cong-class-le*:

assumes $0 < p \ A \subseteq \{..N\} \wedge x \ y. x \in A \implies$

$y \in A \implies x \bmod p = y \bmod p$

shows $\text{card } A \leq N \text{ div } p + 1$

<proof>

lemma *ell-le*:

assumes $0 < p$

shows $\text{ell } p \ N \ a \leq 2 * (N \text{ div } p) + 2$

<proof>

lemma *Lin-nonneg*: *prime* $p \implies \text{InnerHyp } K \ M \ p \implies$

$a \leq m\text{Half } p \implies 0 \leq \text{Lin } K \ M \ p \ a$

<proof>

lemma *card-multiples-upto*:

assumes $0 < p$

shows $\text{card } \{j \in \{1..N\}. p \text{ dvd } j\} = N \text{ div } p$

<proof>

lemma *sum-ell*:

assumes *prime* p $2 < p$

shows $(\sum a = 1..m\text{Half } p. \text{ ell } p \ N \ a) = N - N \text{ div } p$

<proof>

lemma *rank-props*:

fixes $r :: 'a \Rightarrow 'a \Rightarrow \text{bool}$

assumes A : *finite* A **and** *irr*: $\bigwedge x. \neg r \ x \ x$ **and** *tr*: $\bigwedge x \ y \ z. r \ x \ y$

$\implies r \ y \ z \implies r \ x \ z$

and *tot*: $\bigwedge x \ y. x \in A \implies y \in A \implies$

$x \neq y \implies r \ x \ y \vee r \ y \ x$

defines $\text{rk} \equiv \lambda x. \text{card } \{c \in A. r \ c \ x\}$

shows $\bigwedge x \ y. x \in A \implies y \in A \implies$

$\text{rk } x < \text{rk } y \longleftrightarrow r \ x \ y$

and *bij-betw* $\text{rk } A \ \{..<\text{card } A\}$

<proof>

lemma *sum-epsIn*:

assumes *prime* p *InnerHyp* $K \ M \ p$

shows $(\sum a = 1..m\text{Half } p. \text{ epsIn } K \ M \ p \ a) = \text{Ein } K \ M \ p$

<proof>

lemma *sum-Lin*: *prime* $p \implies \text{InnerHyp } K \ M \ p \implies$

$(\sum a \leq m\text{Half } p. \text{ Lin } K \ M \ p \ a) = \text{int } (\text{hof } K)$

<proof>

lemma *length-inner-idx*: *prime* $p \implies \text{InnerHyp } K \ M \ p \implies$

$\text{length } (\text{inner-idx } K \ M \ p) = \text{hof } K$

<proof>

(4.5): the inner basis is $\mathbb{Z}$ - p -unimodular: the coefficient matrix of the basis polynomials has a determinant that is a p -adic unit (CRT basis lemma over $\mathbb{Z}/p\mathbb{Z}$).

The index list is lexicographically ordered: an earlier position has a smaller class, or the same class and a smaller exponent.

lemma *inner-idx-sorted*:

sorted-wrt $(\lambda u \ v. \text{fst } u < \text{fst } v \vee (\text{fst } u = \text{fst } v \wedge \text{snd } u < \text{snd } v))$

$(\text{concat } (\text{map } (\lambda a. \text{map } (\lambda i. (a, i)) [0..<f \ a]) [0..<n]))$

<proof>

lemma *inner-idx-lex*:

assumes $y < x < \text{length } (\text{inner-idx } K \ M \ p)$

shows $\text{fst } (\text{inner-idx } K \ M \ p \ ! \ y) < \text{fst } (\text{inner-idx } K \ M \ p \ ! \ x) \vee$

$(fst (inner-idx K M p ! y) = fst (inner-idx K M p ! x) \wedge$
 $snd (inner-idx K M p ! y) < snd (inner-idx K M p ! x))$
 $\langle proof \rangle$

lemma *vpGge-innerBasis*: $prime\ p \implies vpGge\ p\ (innerBasis\ K\ M\ p\ x)\ 0$
 $\langle proof \rangle$

Shapes of pulled-back numerators (Lean: *FarGood*, *Decomp*).

definition *FarGood* :: $nat \Rightarrow rat\ poly \Rightarrow bool$ **where**
 $FarGood\ p\ F \iff vpGge\ p\ F\ 0 \wedge (\forall d. 1 \leq d \longrightarrow$
 $vge\ p\ (Polynomial.coeff\ F\ d)\ 1)$

definition *Decomp* :: $nat \Rightarrow nat \Rightarrow nat \Rightarrow rat\ poly \Rightarrow$
 $bool$ **where**
 $Decomp\ p\ e\ n\ Q \iff (\exists N\ F. Q = [:of-nat\ p\ \wedge e:] * N * F \wedge$
 $vpGge\ p\ N\ 0 \wedge degree\ N \leq n \wedge FarGood\ p\ F)$

The number of p 's in $j^2 - (c + p z)^2 = (j - c - p z)(j + c + p z)$.

definition *omg* :: $nat \Rightarrow nat \Rightarrow nat \Rightarrow nat$ **where**
 $omg\ p\ c\ j = (if\ int\ p\ dvd\ (int\ j - int\ c)\ then\ 1\ else\ 0) + (if\ int\ p\ dvd\ (int\ j +$
 $int\ c)\ then\ 1\ else\ 0)$

The exponent of p extracted from the pulled-back numerator at the class c .

definition *eNum* :: $nat \Rightarrow nat \Rightarrow nat\ set \Rightarrow (nat \Rightarrow$
 $nat) \Rightarrow nat$ **where**
 $eNum\ p\ c\ J\ k = 5 * (if\ int\ p\ dvd\ int\ c\ then\ 1\ else\ 0) + (\sum\ j \in J. k\ j * omg\ p$
 $c\ j)$

The near poles of the class c : $r \in \pm[1, K]$ with $r \equiv c \pmod{p}$.

definition *nearCount* :: $nat \Rightarrow nat \Rightarrow nat \Rightarrow nat$ **where**
 $nearCount\ p\ K\ c = card\ \{r \in signedPoles\ \{1..K\}. int\ p\ dvd\ (r - int\ c)\}$

21.2 Extracting powers of p from $g(c + p z)$

lemma *FarGood-one*: $FarGood\ p\ 1$
 $\langle proof \rangle$

lemma *FarGood-mult*: $prime\ p \implies FarGood\ p\ F \implies$
 $FarGood\ p\ G \implies FarGood\ p\ (F * G)$
 $\langle proof \rangle$

lemma *Decomp-one*: $Decomp\ p\ 0\ 0\ 1$
 $\langle proof \rangle$

lemma *Decomp-mult*:
 $prime\ p \implies Decomp\ p\ e\ n\ Q \implies Decomp\ p\ e'\ n'\ Q' \implies$
 $Decomp\ p\ (e + e')\ (n + n')\ (Q * Q')$
 $\langle proof \rangle$

lemma *Decomp-pow*: $\text{prime } p \implies \text{Decomp } p \text{ e } n \ Q \implies$
 $\text{Decomp } p \ (k * e) \ (k * n) \ (Q \wedge k)$
 $\langle \text{proof} \rangle$

lemma *Decomp-C-unit*: $\text{prime } p \implies \text{Decomp } p \text{ e } n \ Q \implies$
 $\text{vge } p \ u \ 0 \implies \text{Decomp } p \text{ e } n \ ([:u:] * Q)$
 $\langle \text{proof} \rangle$

A linear factor $\alpha + \sigma \ p \ z$ ($\sigma = \pm 1$) is $p \cdot (\text{near})$ if $p \mid \alpha$, and far-good otherwise.

lemma *Decomp-linear*:
assumes $\text{prime } p \ \sigma = 1 \vee \sigma = -1$
shows $\text{Decomp } p \ (\text{if int } p \text{ dvd } \alpha \text{ then } 1 \text{ else } 0) \ (\text{if int } p \text{ dvd } \alpha \text{ then } 1 \text{ else } 0)$
 $[:\text{of-int } \alpha, \text{of-int } (\sigma * \text{int } p):]$
 $\langle \text{proof} \rangle$

lemma *Decomp-prod*:
 $\text{prime } p \implies \text{finite } J \implies (\bigwedge j. j \in J \implies$
 $\text{Decomp } p \ (e \ j) \ (e \ j) \ (f \ j)) \implies$
 $\text{Decomp } p \ (\sum j \in J. e \ j) \ (\sum j \in J. e \ j) \ (\prod j \in J. f \ j)$
 $\langle \text{proof} \rangle$

The pulled-back numerator $\varepsilon \ x^5 \prod -j \ (j^2 - x^2)^{\{k-j\}}$ at $x = c + p \ z$: every factor $j^2 - (c + p \ z)^2 = (j - c - p \ z)(j + c + p \ z)$ contributes $\text{omg } p \ c \ j$ powers of p .

lemma *decomp-pullback*:
assumes p : $\text{prime } p$ **and** J : $\text{finite } J$ **and** ε : $\text{vge } p \ \varepsilon \ 0$
shows $\text{Decomp } p \ (\text{eNum } p \ c \ J \ k) \ (\text{eNum } p \ c \ J \ k)$
 $(\text{pcompose } ([:\varepsilon:] * pX^5 * \text{pcompose } (\prod j \in$
 $J. (pX + [:\text{of-nat } j^2:] \wedge k \ j) \ (- (pX^2))))$
 $([:\text{of-nat } c:] + [:\text{of-nat } p:] * pX))$
 $\langle \text{proof} \rangle$

lemma *tauExt-tr-C-mul*: $\text{tauExt-tr } p \ Y \ ([:a:] * U) \ S \ M = [a:] * \text{tauExt-tr } p \ Y \ U$
 $S \ M$
 $\langle \text{proof} \rangle$

lemma *vpGge-Yp-tr*: $\text{prime } p \implies 7 \leq p \implies \text{vpGge } p \ (Yp\text{-tr } p \ M) \ 0$
 $\langle \text{proof} \rangle$

lemma *coeff-high-vge*:
assumes $\text{prime } p \ \text{vpGge } p \ N \ 0 \ \text{FarGood } p \ F \ \text{degree } N < d$
shows $\text{vge } p \ (\text{Polynomial.coeff } (N * F) \ d) \ 1$
 $\langle \text{proof} \rangle$

One summand of (3.7). If $P(c + p \ z) = p^e \ N \ F$ (*Decomp*) with $e \leq p + 1$, the class- c summand has valuation $\geq e - \#\{\text{near poles}\}$, for every truncation length $M \geq \deg P$.

theorem *summand-bound-tr*:

assumes p : prime p **and** $p7$: $7 \leq p$ **and** $K1$: $2 * K < p^2$ **and** $K2$: $K + p < p^2$
and S : finite S **and** hS : $\bigwedge r. r \in S \implies$
 $|r| \leq \text{int } K$ **and** c : $c < p$
and D : *Decomp* p e e ($p\text{compose } P$ ($[:\text{of-nat } c:] + [:\text{of-nat } p:] * pX$)) **and** e : $e \leq p + 1$
and dP : *degree* $P \leq M$
shows $vpGge$ p ($\tau\text{Ext-tr } p$ ($Yp\text{-tr } p$ M) ($\text{distribNum } p$ S P c) ($\text{distribPoles } p$ S c) M)
 $(\text{of-int } (\text{int } e - \text{int } (\text{card } \{r \in S. \text{int } p \text{ dvd } (r - \text{int } c)\})))$
 $\langle \text{proof} \rangle$

lemma *finite-signedPoles*: finite $S \implies$ finite (*signedPoles* S)
 $\langle \text{proof} \rangle$

lemma *signedPoles-abs-le*: $r \in \text{signedPoles } \{1..K\} \implies |r| \leq \text{int } K$
 $\langle \text{proof} \rangle$

lemma *nearCount-eq-card*: $\text{nearCount } p$ K $c = \text{card } \{r \in \text{signedPoles } \{1..K\}. \text{int } p \text{ dvd } (r - \text{int } c)\}$
 $\langle \text{proof} \rangle$

The inner-range entry bound, generic form (Lean: *entry-generic*): if every class c gives $B + 4 \leq e\text{-}c - n\text{-}c$ with $e\text{-}c \leq p + 1$, then $v\text{-}p^2 G(\mu\text{-}X(\prod (t + j^2)^{\wedge \{k-j\} / D-K})) \geq B$. Uses (3.1), Lemma 3.2 and the summand bounds.

theorem *entry-generic*:

assumes p : prime p **and** $p7$: $7 \leq p$ **and** $K1$: $2 * K < p^2$ **and** $K2$: $K + p < p^2$ **and** J : finite J
and hB : $\bigwedge c. c < p \implies$
 $B + 4 \leq \text{of-nat } (e\text{Num } p$ c J $k) - \text{of-nat } (\text{nearCount } p$ K $c)$
and $hdeg$: $\bigwedge c. c < p \implies e\text{Num } p$ c J $k \leq p + 1$
shows $vpGge$ p ($\mu\text{X } \{1..K\}$ ($\prod j \in J. (pX + [:\text{of-nat } j^2:]^{\wedge k})$) B)
 $\langle \text{proof} \rangle$

21.3 The inner entry bounds (4.2)/(4.3)

The class of a residue: $\text{cls } p$ $j = \min(j \bmod p, p - j \bmod p)$.

definition $\text{cls} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat}$ **where** $\text{cls } p$ $j = \min(j \bmod p) (p - j \bmod p)$

Exponent of $t + j^2$ in the inner row $E\text{-}x$.

definition $\text{nu} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \times \text{nat} \Rightarrow \text{nat}$ **where**
 $\text{nu } K$ M p x $j = (\text{if } j \leq m\text{Half } p \text{ then } (\text{if } j = \text{fst } x \text{ then } \text{snd } x \text{ else } \text{nat } (\text{Lin } K$ M p $j)) \text{ else } 0)$

The index set and the exponents of the numerator $D\text{-}N^6 E\text{-}x E\text{-}y$.

definition $Jset :: nat \Rightarrow nat \Rightarrow nat \text{ set}$ **where** $Jset\ K\ p = \{1..Nof\ K\} \cup \{..mHalf\ p\}$

definition $kexp :: nat \Rightarrow nat \Rightarrow nat \Rightarrow nat \times nat \Rightarrow nat \times nat \Rightarrow nat \Rightarrow nat$ **where**
 $kexp\ K\ M\ p\ x\ y\ j = 6 * (if\ j \in \{1..Nof\ K\}\ then\ 1\ else\ 0) + nu\ K\ M\ p\ x\ j + nu\ K\ M\ p\ y\ j$

Multiplicity of a class: 2 for the zero class, 1 otherwise.

definition $mult :: nat \Rightarrow nat$ **where** $mult\ c = (if\ c = 0\ then\ 2\ else\ 1)$

lemma $mem-inner-idx$:
 $x \in set\ (inner-idx\ K\ M\ p) \longleftrightarrow fst\ x \leq mHalf\ p \wedge$
 $snd\ x < nat\ (Lin\ K\ M\ p\ (fst\ x))$
 $\langle proof \rangle$

lemma $innerBasis-eq-prod$:
assumes $fst\ x \leq mHalf\ p$
shows $innerBasis\ K\ M\ p\ x = (\prod\ j \leq mHalf\ p. (pX + [:of-nat\ j\ ^\ 2:])) \wedge nu\ K\ M\ p\ x\ j$
 $\langle proof \rangle$

lemma $numerator-eq$:
assumes $fst\ x \leq mHalf\ p$ $fst\ y \leq mHalf\ p$
shows $Dm\ (Nof\ K) \wedge 6 * innerBasis\ K\ M\ p\ x * innerBasis\ K\ M\ p\ y =$
 $(\prod\ j \in Jset\ K\ p. (pX + [:of-nat\ j\ ^\ 2:])) \wedge kexp\ K\ M\ p\ x\ y\ j$
 $\langle proof \rangle$

lemma $cls-le$: $odd\ p \implies cls\ p\ j \leq mHalf\ p$
 $\langle proof \rangle$

lemma $cls-small$: $odd\ p \implies j \leq mHalf\ p \implies cls\ p\ j = j$
 $\langle proof \rangle$

lemma $mod-add-zero-iff-aux$:
fixes $r\ c\ p :: nat$
assumes $r < p$ $c < p$
shows $(r + c) \bmod p = 0 \longleftrightarrow r + c = 0 \vee r + c = p$
 $\langle proof \rangle$

lemma $cls-eq-iff$:
assumes $odd\ p$ $a \leq mHalf\ p$
shows $cls\ p\ j = a \longleftrightarrow j \bmod p = a \vee j \bmod p + a = p$
 $\langle proof \rangle$

lemma $omg-eq$:
assumes $odd\ p$ $c < p$
shows $omg\ p\ c\ j = (if\ cls\ p\ j = cls\ p\ c\ then\ mult\ c\ else\ 0)$
 $\langle proof \rangle$

lemma *sum-omg*:

assumes *odd* p $c < p$

shows $(\sum j = 1..A. \text{omg } p \ c \ j) = \text{mult } c * \text{ell } p \ A \ (\text{cls } p \ c)$

<proof>

lemma *nearCount-eq*:

assumes *prime* p

shows $\text{nearCount } p \ K \ c = (\sum j = 1..K. \text{omg } p \ c \ j)$

<proof>

lemma *cls-zero*: $\text{cls } p \ 0 = 0$

<proof>

lemma *cls-pos*: $c \neq 0 \implies c < p \implies 1 \leq \text{cls } p \ c$

<proof>

lemma *ell-zero-eq*: $0 < p \implies \text{ell } p \ A \ 0 = A \ \text{div } p$

<proof>

lemma *eNum-eq*:

assumes *odd* p $c < p$

shows $eNum \ p \ c \ (Jset \ K \ p) \ (kexp \ K \ M \ p \ x \ y) =$

$5 * (\text{if } c = 0 \text{ then } 1 \text{ else } 0) +$

$\text{mult } c * (6 * \text{ell } p \ (\text{Nof } K) \ (\text{cls } p \ c) + \text{nu } K \ M \ p \ x \ (\text{cls } p \ c) + \text{nu } K \ M \ p$

$y \ (\text{cls } p \ c))$

<proof>

lemma *count-mod-ge*: $0 < p \implies 1 \leq r \implies r < p \implies$

$A \ \text{div } p \leq \text{card } \{j \in \{1..A\}. j \ \text{mod } p = r\}$

<proof>

lemma *count-mod-le*: $0 < p \implies 1 \leq r \implies r < p \implies$

$\text{card } \{j \in \{1..A\}. j \ \text{mod } p = r\} \leq A \ \text{div } p + 1$

<proof>

lemma *ell-bounds*:

assumes *odd* p $1 \leq a \leq mHalf \ p$

shows $2 * (A \ \text{div } p) \leq \text{ell } p \ A \ a \wedge \text{ell } p \ A \ a \leq 2 * (A \ \text{div } p) + 2$

<proof>

lemma *hyp-facts*:

assumes *prime* p *InnerHyp* $K \ M \ p$

shows $7 \leq p \wedge \text{odd } p \wedge 2 * mHalf \ p + 1 = p \wedge K \ \text{div } p < M \wedge$

$\text{Nof } K \ \text{div } p < M$

<proof>

lemma *Tin-le*:

assumes *prime* p *InnerHyp* $K \ M \ p$

shows $Tin\ K\ M\ p \leq 4 * int\ M$
 $\langle proof \rangle$

lemma *Lin-le*:
assumes $prime\ p\ InnerHyp\ K\ M\ p\ a \leq mHalf\ p$
shows $Lin\ K\ M\ p\ a \leq 4 * int\ M + 10$
 $\langle proof \rangle$

lemma *nu-le*:
assumes $prime\ p\ InnerHyp\ K\ M\ p\ x \in set\ (inner-idx\ K\ M\ p)$
shows $nu\ K\ M\ p\ x\ j \leq 4 * M + 10$
 $\langle proof \rangle$

lemma *ellN-le*:
assumes $prime\ p\ InnerHyp\ K\ M\ p\ 1 \leq a\ a \leq mHalf\ p$
shows $ell\ p\ (Nof\ K)\ a \leq M$
 $\langle proof \rangle$

lemma *eps-key*:
assumes $prime\ p\ InnerHyp\ K\ M\ p\ a \in \{1..mHalf\ p\}\ b \in \{1..mHalf\ p\}$
shows $2 * (epsIn\ K\ M\ p\ a - epsIn\ K\ M\ p\ b) \leq 2 + int\ (ell\ p\ K\ a) - int\ (ell\ p\ K\ b)$
 $\langle proof \rangle$

Half-weight at an ordinary source b .

lemma *half-ord*:
assumes $prime\ p\ InnerHyp\ K\ M\ p\ x \in set\ (inner-idx\ K\ M\ p)\ 1 \leq b\ b \leq mHalf\ p$
shows $wInIdx\ K\ M\ p\ x \leq of-nat\ (nu\ K\ M\ p\ x\ b) + 3 * of-nat\ (ell\ p\ (Nof\ K)\ b)$
 $-$
 $(of-nat\ (ell\ p\ K\ b) + 4) / 2$
 $\langle proof \rangle$

Half-weight at the zero source.

lemma *half-zero*:
assumes $prime\ p\ InnerHyp\ K\ M\ p\ x \in set\ (inner-idx\ K\ M\ p)$
shows $wInIdx\ K\ M\ p\ x \leq 2 * of-nat\ (nu\ K\ M\ p\ x\ 0) + 6 * of-nat\ (Nof\ K\ div\ p) -$
 $of-nat\ (K\ div\ p) + 1 / 2$
 $\langle proof \rangle$

(4.2)/(4.3): every entry of the inner Gram matrix satisfies the weights.

theorem *innerGram-entry-bound*:
assumes p : $prime\ p$ **and** H : $InnerHyp\ K\ M\ p$ **and** x : $x < length\ (inner-idx\ K\ M\ p)$ **and** y : $y <$
 $length\ (inner-idx\ K\ M\ p)$
shows $vpGge\ p\ (innerGram\ K\ M\ p\ \$\$ (x, y))$
 $(wInIdx\ K\ M\ p\ (inner-idx\ K\ M\ p\ !\ x) + wInIdx\ K\ M\ p\ (inner-idx\ K\ M\ p\ !\ y))$

<proof>

Multiplying by a p -adic unit does not change Gauss-valuation bounds.

lemma *vpGge-of-unit-mul*:

assumes *prime* p $u \neq 0$ $vp\ p\ u = 0$ $vpGge\ p\ ([:u:] * P)$ b
shows $vpGge\ p\ P\ b$

<proof>

$\sum -i\ (w\ (\sigma\ i) + w\ i) = 2 \sum -i\ w\ i$ for a permutation σ of $\{0..<n\}$.

lemma *sum-permute-add*:

assumes σ *permutes* $\{0..<n\}$
shows $(\sum\ i = 0..<n.\ w\ (\sigma\ i) + w\ i) = 2 * (\sum\ i = 0..<n.\ (w\ i :: rat))$

<proof>

The Gram matrix of a basis B (rows = coefficient vectors) is $B\ G\ B^T$, and its determinant is $\det(B)^2 \det(G)$; a Gauss bound on the Gram determinant transfers to $\det\ G$ when $\det\ B$ is a p -adic unit.

lemma *det-gram-transfer*:

assumes p : *prime* p **and** G : $G \in \text{carrier-mat } n\ n$ **and** B : $B \in \text{carrier-mat } n\ n$
and $\det B$: $\text{Determinant.det } B \neq 0$ $vp\ p\ (\text{Determinant.det } B) = 0$
and gram : $vpGge\ p\ (\text{Determinant.det } (\text{map-mat } (\lambda q. [:q:])\ B * G * \text{transpose-mat } (\text{map-mat } (\lambda q. [:q:])\ B)))$ b
shows $vpGge\ p\ (\text{Determinant.det } G)$ b

<proof>

$\gamma\text{-}p\hat{\text{in}} = 2 \sum -\{x \in \text{idx}\}\ w\text{-}x$, the double sum written over the index list.

lemma *sum-list-concat-aux*: $\text{sum-list } (\text{concat } xss) =$

$\text{sum-list } (\text{map } \text{sum-list } (xss :: 'a :: \text{monoid-add list list}))$

<proof>

lemma *gammaIn-eq-sum-idx*:

$\text{gammaIn } K\ M\ p = 2 * (\sum\ x < \text{length } (\text{inner-idx } K\ M\ p).\ w\text{InIdx } K\ M\ p\ (\text{inner-idx } K\ M\ p\ !\ x))$

<proof>

lemma *degree-innerBasis-lt*:

assumes *prime* p $\text{InnerHyp } K\ M\ p\ x \in \text{set } (\text{inner-idx } K\ M\ p)$
shows $\text{degree } (\text{innerBasis } K\ M\ p\ x) < \text{hof } K$

<proof>

The inner Gram matrix is $B\ G\text{-}K\ B^T$ for the coefficient matrix B of the inner basis.

lemma *innerGram-eq-conj*:

assumes p : *prime* p **and** H : $\text{InnerHyp } K\ M\ p$
defines $B \equiv \text{Matrix.mat } (\text{hof } K)\ (\text{hof } K)\ (\lambda(x, d).\ \text{Polynomial.coeff } (\text{innerBasis } K\ M\ p\ (\text{inner-idx } K\ M\ p\ !\ x))\ d)$
shows $\text{innerGram } K\ M\ p = \text{map-mat } (\lambda q. [:q:])\ B * G\ K\ K * \text{transpose-mat } (\text{map-mat } (\lambda q. [:q:])\ B)$

<proof>

(4.5): the inner basis is $\mathbb{Z}$ - p -unimodular: the coefficient matrix of the basis polynomials has a determinant that is a p -adic unit. Proof by the Taylor-matrix criterion (*unimodular-criterion*): expanding row $E-\{a,j\}$ at the point $-c^2$ to order i gives an upper triangular matrix with the units $\prod -\{c \neq a\} (c^2 - a^2)^{L-c}$ on the diagonal.

theorem *innerBasis-unimodular*:

assumes p : prime p **and** H : *InnerHyp* K M p

defines $B \equiv \text{Matrix.mat } (\text{hof } K) (\text{hof } K) (\lambda(x,$

$d).$ *Polynomial.coeff* (*innerBasis* K M p (*inner-idx* K M p ! x)) d)

shows *Determinant.det* $B \neq 0 \wedge \text{vp } p$ (*Determinant.det* B) = 0

<proof>

Proposition 4.1 from the entry bounds (unimodular change of basis + *vpGge-det-of-terms*).

theorem *DeltaK-vpGge-inner-of-entries*:

assumes p : prime p **and** H : *InnerHyp* K M p

and *ent*: $\bigwedge x y. x < \text{length } (\text{inner-idx } K M p) \implies$

$y < \text{length } (\text{inner-idx } K M p) \implies$

$\text{vpGge } p$ (*innerGram* $K M p$ $\$ (x, y)$)

$(\text{wInIdx } K M p (\text{inner-idx } K M p ! x) + \text{wInIdx } K M p (\text{inner-idx } K M$

$p ! y))$

shows $\text{vpGge } p$ (*DeltaK* K) (*gammaIn* $K M p$)

<proof>

Proposition 4.1: under (4.1), $v\text{-}p^{\wedge}G(\Delta\text{-}K) \geq \gamma\text{-}p^{\wedge}in$.

theorem *DeltaK-vpGge-inner*: prime $p \implies \text{InnerHyp } K M p \implies$

$\text{vpGge } p$ (*DeltaK* K) (*gammaIn* $K M p$)

<proof>

end

theory *Zeta5-Outer-Range*

imports *Zeta5-Inner-Range BenOr-Kozen-Reif.More-Matrix*

begin

22 The outer range: Lemma 4.2 and Proposition 4.3

Section 4.2 of the paper: the decomposition (4.10), the outer basis (4.11) and its unimodularity, the arithmetic of the pole classes, the entry bound (4.12), the closed form (4.14) of γ_p^{out} , Lemma 4.2 (*det-vpGge-of-weighted-entries*) and Proposition 4.3 (*DeltaK-vpGge-outer*, *DeltaK-vpGge-large-prime*). Lean theories *MuMod*, *CRTBasis*, *OuterCount*, *OuterEntries*, *Lemma42*, *Prop43*, *Prop43Large*.

22.1 Section 4.2 The outer range

(4.9) holds when $K \geq 200M^2$ and $K/3 < p \leq K$.

lemma *outer-hyp-of-range:*

assumes $40 \leq M$ $40 \text{ dvd } K$ $200 * M^2 \leq K$ *prime* p $K < 3 * p$ $p \leq K$

shows *OuterHyp* K p

<proof>

(4.10): $G-K = A + p^{-1}L$ with L constant, integral, of rank $\leq r-p$ (rank over $\mathbb{Q}$, *vec-space.rank* of *Jordan_Normal_Form*).

lemma *cCorr-vge:* *prime* $p \implies \text{vge } p \text{ (cCorr } p \text{ } e) \text{ } 0$

<proof>

lemma *cCorr-of-lt:* $e < 2 * p - 3 \implies \text{cCorr } p \text{ } e = 0$

<proof>

$\mu X = \mu \hat{0} X + p^{-1} \sum -e \text{ } q \text{ } e \text{ } c \text{ } e$: the two functionals differ by the correction of the polynomial part.

lemma *$\mu X \text{ eq } \mu X \text{ mod-add}$:*

prime $p \implies \mu X \text{ } S \text{ } P = \mu X \text{ mod } p \text{ } S \text{ } P +$

$[(\sum e \leq \text{degree } (P \text{ div } \text{sqPoleProd } S). \text{Polynomial.coeff } (P \text{ div } \text{sqPoleProd } S))$

$e *$

$\text{cCorr } p \text{ } e) / \text{of-nat } p]$

<proof>

lemma *$pX \text{ plus-const-pCons}$:* $pX + [:c:] = [:c, 1:]$

<proof>

lemma *$vpGge \text{ mul0'}$:* *prime* $p \implies vpGge \text{ } p \text{ } A \text{ } 0 \implies$

$vpGge \text{ } p \text{ } B \text{ } 0 \implies vpGge \text{ } p \text{ } (A * B) \text{ } 0$

<proof>

lemma *$vpGge \text{ pow0'}$:* *prime* $p \implies vpGge \text{ } p \text{ } A \text{ } 0 \implies vpGge \text{ } p \text{ } (A \wedge n) \text{ } 0$

<proof>

lemma *$vpGge \text{ pX-plus-sq0}$:* *prime* $p \implies vpGge \text{ } p \text{ } (pX + [: \text{of-nat } n \wedge 2:]) \text{ } 0$

<proof>

lemma *$\text{lead-coeff-sqPoleProd0}$:* $\text{lead-coeff } (\text{sqPoleProd } S) = 1$

<proof>

lemma *$vpGge \text{ sqPoleProd0}$:* *prime* $p \implies vpGge \text{ } p \text{ } (\text{sqPoleProd } S) \text{ } 0$

<proof>

lemma *$vpGge \text{ Dm0}$:* *prime* $p \implies vpGge \text{ } p \text{ } (\text{Dm } m) \text{ } 0$

<proof>

lemma *degree-div-sub :*

fixes $P \text{ } Q :: \text{rat poly}$

assumes $Q \neq 0$
shows $\text{degree } (P \text{ div } Q) \leq \text{degree } P - \text{degree } Q$
 $\langle \text{proof} \rangle$

lemma *blocks-lex*:

fixes $f :: \text{nat} \Rightarrow \text{nat}$
defines $B \ n \equiv \text{concat } (\text{map } (\lambda a. \text{map } (\lambda i. (a, i)) [0..<f \ a]) [0..<n])$
shows $y < x \implies x < \text{length } (B \ n) \implies$
 $\text{fst } (B \ n ! y) < \text{fst } (B \ n ! x) \vee (\text{fst } (B \ n ! y) = \text{fst } (B \ n ! x) \wedge$
 $\text{snd } (B \ n ! y) < \text{snd } (B \ n ! x))$
 $\langle \text{proof} \rangle$

The polynomial quotients $Q\text{-}\{ij\} = D\text{-}N^6 t^{\wedge\{i+j\}} \text{ div } D\text{-}K$ are integral.

lemma *vpGge-quot*: $\text{prime } p \implies$
 $\text{vpGge } p \ ((Dm \ (Nof \ K) \wedge 6 * pX \wedge n) \text{ div } \text{sqPoleProd } \{1..K\}) \ 0$
 $\langle \text{proof} \rangle$

A matrix whose rows outside a set of k indices vanish has rank $\leq k$.

lemma *rank-le-card-nonzero-rows*:

assumes $L \in \text{carrier-mat } n \ n \ T \subseteq \{0..<n\} \wedge i \ j. i < n \implies$
 $i \notin T \implies j < n \implies L \ \$\$ (i, j) = 0$
shows $\text{vec-space.rank } n \ L \leq \text{card } T$
 $\langle \text{proof} \rangle$

(4.10): $G\text{-}K = A + p^{\wedge - 1} L$ with L constant, integral, of rank $\leq r\text{-}p$ (rank over $\mathbb{Q}$, vec-space.rank of $\text{Jordan_Normal_Form}$).

theorem *GK-outer-decomposition*:

assumes p : *prime* p **and** K : $40 \text{ dvd } K$ **and** H : *OuterHyp* $K \ p$
shows $\exists L :: \text{rat mat. } L \in \text{carrier-mat } (\text{hof } K) (\text{hof } K) \wedge$
 $GK \ K = Aout \ K \ p + \text{map-mat } (\lambda c. [c / \text{of-nat } p]) \ L \wedge$
 $(\forall i < \text{hof } K. \forall j < \text{hof } K. L \ \$\$ (i, j) \neq 0 \implies$
 $0 \leq \text{vp } p \ (L \ \$\$ (i, j))) \wedge$
 $\text{vec-space.rank } (\text{hof } K) \ L \leq rOut \ K \ p$
 $\langle \text{proof} \rangle$

lemma *mod-add-eq-0-iff*:

fixes $j \ a \ p :: \text{nat}$
assumes $0 < a \ a < p$
shows $(j + a) \text{ mod } p = 0 \iff j \text{ mod } p = p - a$
 $\langle \text{proof} \rangle$

lemma *sum-classes-card*:

assumes *prime* $p \ 2 < p$ *finite* X
shows $(\sum a \leq mHalf \ p. \text{card } \{j \in X. j \text{ mod } p = a \text{ mod } p \vee$
 $(j + a) \text{ mod } p = 0\}) = \text{card } X$
 $\langle \text{proof} \rangle$

lemma *length-outer-idx*: $\text{prime } p \implies 40 \text{ dvd } K \implies$

$\text{OuterHyp } K \ p \implies \text{length } (\text{outer-idx } K \ p) = \text{hof } K$

$\langle \text{proof} \rangle$

(4.11): the outer basis is $\mathbb{Z}$ - p -unimodular.

lemma *outer-idx-lex*:

assumes $y < x \leq \text{length } (\text{outer-idx } K \ p)$
shows $\text{fst } (\text{outer-idx } K \ p \ ! \ y) < \text{fst } (\text{outer-idx } K \ p \ ! \ x) \vee$
 $(\text{fst } (\text{outer-idx } K \ p \ ! \ y) = \text{fst } (\text{outer-idx } K \ p \ ! \ x) \wedge$
 $\text{snd } (\text{outer-idx } K \ p \ ! \ y) < \text{snd } (\text{outer-idx } K \ p \ ! \ x))$
 $\langle \text{proof} \rangle$

lemma *mem-outer-idx*: $x \in \text{set } (\text{outer-idx } K \ p) \iff \text{fst } x \leq m\text{Half } p \wedge$
 $\text{snd } x < \text{outerCount } K \ p \ (\text{fst } x)$
 $\langle \text{proof} \rangle$

lemma *vpGge-outerBasis*: $\text{prime } p \implies \text{vpGge } p \ (\text{outerBasis } K \ p \ x) \ 0$
 $\langle \text{proof} \rangle$

In the outer range every class $a \geq 1$ contains exactly the two poles $a, p - a$ below p , so $\#\{j \in C\text{-}a. \ p < j\} + 2 = \text{ell } p \ K \ a$ (Lean: *card-E-add-two*).

lemma *res-class0*:

assumes $a \leq m\text{Half } p \ 2 * m\text{Half } p + 1 = p \ j \bmod p = a \bmod p \vee (j + a) \bmod$
 $p = 0$
shows $j \bmod p = a \vee (1 \leq a \wedge j \bmod p = p - a)$
 $\langle \text{proof} \rangle$

lemma *card-class-high-add-two*:

assumes $\text{prime } p \ \text{OuterHyp } K \ p \ 1 \leq a \leq m\text{Half } p$
shows $\text{card } \{j \in \text{outerClassPoles } K \ p \ a. \ p < j\} + 2 = \text{ell } p \ K \ a$
 $\langle \text{proof} \rangle$

Modulo p , a pole $j \in C\text{-}a$ with $p < j$ satisfies $j^2 \equiv a^2$: the factor $t + j^2$ is $(t + a^2) + (j^2 - a^2)$ with $p \mid j^2 - a^2$.

lemma *class-sq-cong*:

assumes $\text{prime } p \ 1 \leq a \leq m\text{Half } p \ j \in \text{outerClassPoles } K \ p \ a$
shows $\text{vge } p \ (\text{of-nat } j^2 - \text{of-nat } a^2) \ 1$
 $\langle \text{proof} \rangle$

22.2 The modified functional $\mu^0\text{-}X$ and the structure of the outer basis

definition *tailPoles* :: $\text{nat} \Rightarrow \text{nat set}$ **where** $\text{tailPoles } K = \{\text{Nof } K + 1..K\}$

μ^0 on polynomials.

definition *muModPoly* :: $\text{nat} \Rightarrow \text{rat poly} \Rightarrow \text{rat}$ **where**

$\text{muModPoly } p \ Q = (\sum \ e \leq \text{degree } Q. \ \text{Polynomial.coeff } Q \ e * (\text{muMono } e -$
 $\text{cCorr } p \ e /$
 $\text{of-nat } p))$

lemma *muXmod-eq*:

$\text{muXmod } p \ S \ P = [\text{muModPoly } p \ (P \ \text{div} \ \text{sqPoleProd } S):] + (\sum j \in S. [\text{sqResidue } S \ P \ j:] * \text{muPole } j)$
 $\langle \text{proof} \rangle$

lemma muModPoly-vge : $\text{prime } p \implies \gamma \leq p \implies$
 $\text{vpGge } p \ Q \ 0 \implies \text{vge } p \ (\text{muModPoly } p \ Q) \ 0$
 $\langle \text{proof} \rangle$

lemma $\text{muModPoly-sub-muPoly}$:
 $\text{muModPoly } p \ Q = \text{muPoly } Q - (\sum e \leq \text{degree } Q. \text{Polynomial.coeff } Q \ e * (\text{cCorr } p \ e \ / \ \text{of-nat } p))$
 $\langle \text{proof} \rangle$

lemma muXmod-as-muX :
 $\text{muXmod } p \ S \ P = \text{muX } S \ P - [\sum e \leq \text{degree } (P \ \text{div} \ \text{sqPoleProd } S). \text{Polynomial.coeff } (P \ \text{div} \ \text{sqPoleProd } S) \ e * (\text{cCorr } p \ e \ / \ \text{of-nat } p):]$
 $\langle \text{proof} \rangle$

lemma $\text{lead-coeff-sqPoleProd}$: $\text{finite } S \implies \text{lead-coeff } (\text{sqPoleProd } S) = 1$
 $\langle \text{proof} \rangle$

lemma vpGge-sqPoleProd : $\text{prime } p \implies \text{vpGge } p \ (\text{sqPoleProd } S) \ 0$
 $\langle \text{proof} \rangle$

lemma vpGge-mul0 : $\text{prime } p \implies \text{vpGge } p \ A \ 0 \implies$
 $\text{vpGge } p \ B \ 0 \implies \text{vpGge } p \ (A * B) \ 0$
 $\langle \text{proof} \rangle$

lemma vpGge-pow0 : $\text{prime } p \implies \text{vpGge } p \ A \ 0 \implies \text{vpGge } p \ (A \wedge^n) \ 0$
 $\langle \text{proof} \rangle$

lemma vpGge-pX-plus-sq : $\text{prime } p \implies \text{vpGge } p \ (pX + [\text{of-nat } n \wedge 2:]) \ 0$
 $\langle \text{proof} \rangle$

lemma vpGge-Dm : $\text{prime } p \implies \text{vpGge } p \ (\text{Dm } m) \ 0$
 $\langle \text{proof} \rangle$

lemma wOut-nonpos : $\text{wOut } K \ p \ x \leq 0$
 $\langle \text{proof} \rangle$

lemma wOut-halfInt : $\exists k::\text{int}. 2 * \text{wOut } K \ p \ x = \text{of-int } k$
 $\langle \text{proof} \rangle$

$\mu\wedge^0\text{-X}$ also depends only on the rational function.

lemma $\text{muXmod-mul-cancel-set}$:
 $\text{finite } T \implies \text{finite } S \implies T \cap S = \{\} \implies$
 $\text{muXmod } p \ (T \cup S) \ (P * \text{sqPoleProd } T) = \text{muXmod } p \ S \ P$
 $\langle \text{proof} \rangle$

lemma *muXmod-empty*: $\text{muXmod } p \ \{\} \ P = [\text{muModPoly } p \ P:]$
 $\langle \text{proof} \rangle$

lemma *sqPoleProd-union*: $\text{finite } s \implies \text{finite } t \implies$
 $s \cap t = \{\} \implies \text{sqPoleProd } (s \cup t) = \text{sqPoleProd } s * \text{sqPoleProd } t$
 $\langle \text{proof} \rangle$

lemma *sqPoleProd-Icc-split*: $\text{sqPoleProd } \{1..K\} = \text{Dm } (\text{Nof } K) * \text{sqPoleProd}$
 $(\text{tailPoles } K)$
 $\langle \text{proof} \rangle$

The q -part of an outer basis row: $\text{outerBasis} = P \cdot a \cdot \text{og}$.

definition *og* :: $\text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \times \text{nat} \Rightarrow \text{rat poly}$ **where**
 $\text{og } K \ p \ x = (\text{let } a = \text{fst } x; i = \text{snd } x \text{ in}$
 $\text{if } a = 0 \text{ then } (pX + [\text{of-nat } p \wedge 2:]) \wedge i$
 $\text{else if } i < \text{ell } p \ K \ a - 2 \text{ then } (pX + [\text{of-nat } a \wedge 2:]) \wedge i$
 $\text{else } \text{sqPoleProd } \{j \in \text{outerClassPoles } K \ p \ a. \ p <$
 $j\} * (pX + [\text{of-nat } a \wedge 2:]) \wedge (i - (\text{ell } p \ K \ a - 2)))$

lemma *outerBasis-eq*: $\text{outerBasis } K \ p \ x =$
 $\text{sqPoleProd } (\text{tailPoles } K - \text{outerClassPoles } K \ p \ (\text{fst } x)) * \text{og } K \ p \ x$
 $\langle \text{proof} \rangle$

lemma *og-vge*: $\text{prime } p \implies \text{vpGge } p \ (\text{og } K \ p \ x) \ 0$
 $\langle \text{proof} \rangle$

lemma *outerGram-apply*:
 $x < \text{length } (\text{outer-idx } K \ p) \implies y < \text{length } (\text{outer-idx } K \ p) \implies$
 $\text{outerGram } K \ p \ \$\$ (x, y) = \text{muXmod } p \ \{1..K\} \ (\text{Dm } (\text{Nof } K) \wedge 6 * \text{outerBasis}$
 $K \ p \ (\text{outer-idx } K \ p \ ! \ x) *$
 $\text{outerBasis } K \ p \ (\text{outer-idx } K \ p \ ! \ y))$
 $\langle \text{proof} \rangle$

22.3 Arithmetic of the pole classes

lemma *mem-class*: $j \in \text{outerClassPoles } K \ p \ a \iff \text{Nof } K + 1 \leq j \wedge$
 $j \leq K \wedge (j \bmod p = a \bmod p \vee (j + a) \bmod p = 0)$
 $\langle \text{proof} \rangle$

Facts implied by (4.9).

lemma *outer-facts*:
assumes $\text{prime } p \ \text{OuterHyp } K \ p$
shows $7 \leq p \wedge \text{odd } p \wedge 2 * \text{mHalf } p + 1 = p \wedge p \leq K \wedge K < 3 * p \wedge$
 $2 * \text{Nof } K < p \wedge$
 $(K < 2 * p \longrightarrow K \bmod p = K - p) \wedge (2 * p \leq K \longrightarrow$
 $K \bmod p = K - 2 * p)$
 $\langle \text{proof} \rangle$

lemma *res-class*:

assumes $a \leq mHalf\ p\ 2 * mHalf\ p + 1 = p\ j\ mod\ p = a\ mod\ p \vee (j + a)\ mod\ p = 0$

shows $j\ mod\ p = a \vee (1 \leq a \wedge j\ mod\ p = p - a)$

<proof>

lemma *class-disjoint*:

assumes $prime\ p\ OuterHyp\ K\ p\ a \leq mHalf\ p\ c \leq mHalf\ p\ a \neq c$

shows $outerClassPoles\ K\ p\ a \cap outerClassPoles\ K\ p\ c = \{\}$

<proof>

lemma *class-small*:

assumes $prime\ p\ OuterHyp\ K\ p\ 1 \leq a\ a \leq mHalf\ p\ j \in$

$outerClassPoles\ K\ p\ a\ j < p$

shows $j = a \vee j = p - a$

<proof>

lemma *class-not-dvd*:

assumes $prime\ p\ OuterHyp\ K\ p\ 1 \leq a\ a \leq mHalf\ p\ j \in outerClassPoles\ K\ p\ a$

shows $\neg p\ dvd\ j$

<proof>

lemma *pa-mem*:

assumes $prime\ p\ OuterHyp\ K\ p\ 1 \leq a\ a \leq mHalf\ p$

shows $p - a \in outerClassPoles\ K\ p\ a$

<proof>

lemma *a-mem-iff*:

assumes $prime\ p\ OuterHyp\ K\ p\ 1 \leq a\ a \leq mHalf\ p$

shows $a \in outerClassPoles\ K\ p\ a \longleftrightarrow Nof\ K < a$

<proof>

lemma *card-outerClass*:

assumes $prime\ p\ OuterHyp\ K\ p\ 1 \leq a\ a \leq mHalf\ p$

shows $card\ (outerClassPoles\ K\ p\ a) + (if\ a \leq Nof\ K\ then\ 1\ else\ 0) = ell\ p\ K\ a$

<proof>

lemma *zero-class*:

assumes $prime\ p\ OuterHyp\ K\ p$

shows $outerClassPoles\ K\ p\ 0 = (if\ 2 * p \leq K\ then\ \{p, 2 * p\}\ else\ \{p\})$

<proof>

22.4 Valuations at the poles

lemma *vge-inv-two-mul*: $prime\ p \implies \neg p\ dvd\ j \implies$

$p \neq 2 \implies vge\ p\ (1 / (2 * of\ nat\ j))\ 0$

<proof>

$\mu\text{-}X(1/(t+j^2))$ has coefficients of valuation $\geq \beta$ when $j^4 \nmid H\text{-}j$ and $1/(2j)$ do.

lemma *muPole-coeff0*: $\text{Polynomial.coeff } (\text{muPole } j) \ n =$
 (if $n = 1$ then $\text{of-nat } j^4$ else if $n =$
 0 then $-(\text{of-nat } j^4 * H5 \ j) - 1 / 4 + 1 / (2 * \text{of-nat } j)$ else 0)
 ⟨proof⟩

lemma *vge-pow-mul*: $\text{prime } p \implies \text{vge } p \ x \ b \implies$
 $\text{vge } p \ (x^n) \ (\text{of-nat } n * b)$
 ⟨proof⟩

lemma *nat-log-le-one-sq*: $\text{prime } p \implies K < p^2 \implies \text{nat-log } p \ K \leq 1$
 ⟨proof⟩

lemma *vge-of-int-dvd*: $\text{prime } p \implies \text{int } p \ \text{dvd } z \implies \text{vge } p \ (\text{of-int } z) \ 1$
 ⟨proof⟩

lemma *muPole-vge*:
 assumes $\text{prime } p \ \beta \leq 0 \ p \neq$
 $2 \ \text{vge } p \ (\text{of-nat } j^4 * H5 \ j) \ \beta \ \text{vge } p \ (1 / (2 * \text{of-nat } j)) \ \beta$
 shows $\text{vpGge } p \ (\text{muPole } j) \ \beta$
 ⟨proof⟩

lemma *muPole-vge-small*: $\text{prime } p \implies 1 \leq j \implies$
 $j < p \implies p \neq 2 \implies \text{vpGge } p \ (\text{muPole } j) \ 0$
 ⟨proof⟩

lemma *muPole-vge-mult*: $\text{prime } p \implies 7 \leq p \implies$
 $1 \leq t \implies t \leq 2 \implies \text{vpGge } p \ (\text{muPole } (t * p)) \ (-1)$
 ⟨proof⟩

lemma *nat-log-le-one-of-lt-sq*: $\text{prime } p \implies K < p^2 \implies$
 $\text{nat-log } p \ K \leq 1$
 ⟨proof⟩

lemma *muPole-vge-class*:
 assumes $\text{prime } p \ \text{OuterHyp } K \ p \ 1 \leq a \ a \leq mHalf \ p \ j \in \text{outerClassPoles } K \ p \ a$
 shows $\text{vpGge } p \ (\text{muPole } j) \ (-5)$
 ⟨proof⟩

$\mu^0\text{-X}(R / \prod_{j \in S} (t + j^2))$ is bounded by its residue terms, for integral R .

lemma *muXmod-vge-of-residues*:
 assumes $\text{prime } p \ 7 \leq p \ \text{finite } S \ \text{vpGge } p \ R \ 0 \ B \leq 0$
 and $\bigwedge j. j \in S \implies \text{vpGge } p \ ([:\text{sqResidue } S \ R \ j:] * \text{muPole } j) \ B$
 shows $\text{vpGge } p \ (\text{muXmod } p \ S \ R) \ B$
 ⟨proof⟩

lemma *sq-sub-vge*:
 assumes $\text{prime } p \ \text{OuterHyp } K \ p \ j \in \text{outerClassPoles } K \ p \ a$
 shows $\text{vge } p \ (\text{of-nat } a^2 - \text{of-nat } j^2) \ 1$
 ⟨proof⟩

lemma *eval-vge0*: $\text{prime } p \implies \text{vpGge } p \ P \ 0 \implies$
 $\text{vge } p \ x \ 0 \implies \text{vge } p \ (\text{poly } P \ x) \ 0$
 $\langle \text{proof} \rangle$

lemma *vge-neg-sq*: $\text{prime } p \implies \text{vge } p \ (- \ (\text{of-nat } j \wedge 2)) \ 0$
 $\langle \text{proof} \rangle$

lemma *vge-pow'*: $\text{prime } p \implies \text{vge } p \ x \ b \implies \text{vge } p \ (x \wedge n) \ (\text{of-nat } n * b)$
 $\langle \text{proof} \rangle$

lemma *vge-div-of-le*: $\text{prime } p \implies \text{vge } p \ x \ b \implies$
 $y \neq 0 \implies \text{of-int } (\text{vp } p \ y) \leq U \implies \text{vge } p \ (x / y) \ (b - U)$
 $\langle \text{proof} \rangle$

lemma *vp-int-le-one-of-lt-sq*: $\text{prime } p \implies z \neq 0 \implies$
 $\text{nat } |z| < p \wedge 2 \implies \text{vp } p \ (\text{of-int } z) \leq 1$
 $\langle \text{proof} \rangle$

lemma *D-eval-vge*:
assumes $\text{prime } p \ \text{OuterHyp } K \ p \ 1 \leq a \ j \in \text{outerClassPoles } K \ p \ a$
shows $\text{vge } p \ (\text{poly } (\text{Dm } (\text{Nof } K)) \ (- \ (\text{of-nat } j \wedge 2))) \ (\text{if } a \leq \text{Nof } K \text{ then } 1 \text{ else } 0)$
 $\langle \text{proof} \rangle$

lemma *node-factor-le*:
assumes $\text{prime } p \ \text{OuterHyp } K \ p \ 1 \leq a \ a \leq m\text{Half } p \ j \in$
 $\text{outerClassPoles } K \ p \ a \ k \in \text{outerClassPoles } K \ p \ a \ j \neq k$
shows $\text{vp } p \ (\text{of-nat } k \wedge 2 - \text{of-nat } j \wedge 2) \leq 1$
 $\langle \text{proof} \rangle$

lemma *node-prod-le*:
assumes $\text{prime } p \ \text{OuterHyp } K \ p \ 1 \leq a \ a \leq m\text{Half } p \ j \in \text{outerClassPoles } K \ p \ a$
shows $(\prod k \in \text{outerClassPoles } K \ p \ a - \{j\}. \text{of-nat } k \wedge 2 - \text{of-nat } j \wedge 2) \neq$
 $(0 :: \text{rat}) \wedge$
 $\text{of-int } (\text{vp } p \ (\prod k \in \text{outerClassPoles } K \ p \ a - \{j\}. \text{of-nat } k \wedge 2 -$
 $\text{of-nat } j \wedge 2)) \leq \text{of-nat } (\text{card } (\text{outerClassPoles } K \ p \ a)) - (1 :: \text{rat})$
 $\langle \text{proof} \rangle$

The class- a factor δ .

definition $\text{dlt} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where** $\text{dlt } K \ a = (\text{if } a \leq$
 $\text{Nof } K \text{ then } 1 \text{ else } 0)$

(4.12), ordinary rows: a same-class entry between rows $i, i' < l - 2$.

lemma *entry-ord*:
assumes p : $\text{prime } p$ **and** H : $\text{OuterHyp } K \ p$ **and** $a1$: $1 \leq a$ **and** am : $a \leq m\text{Half}$
 p
shows $\text{vpGge } p \ (\text{muXmod } p \ (\text{outerClassPoles } K \ p \ a))$
 $(\text{Dm } (\text{Nof } K) \wedge 5 * \text{sqPoleProd } (\text{tailPoles } K - \text{outerClassPoles } K \ p \ a) *$

$(pX +$
 $\quad [:of\text{-}nat\ a\ \wedge\ 2:] \wedge i * (pX + [:of\text{-}nat\ a\ \wedge\ 2:] \wedge i'))$
 $\quad (\min\ 0\ (of\text{-}nat\ i + of\text{-}nat\ i' + 6 * dlt\ K\ a - of\text{-}nat\ (ell\ p\ K\ a) - 4))$
 $\langle proof \rangle$

lemma *small-poles*:

assumes *prime* p *OuterHyp* $K\ p\ 1 \leq a\ a \leq mHalf\ p$
shows $\{j \in outerClassPoles\ K\ p\ a.\ j < p\} = (\text{if } a \leq Nof\ K \text{ then } \{p - a\} \text{ else } \{a, p - a\})$
 $\langle proof \rangle$

22.5 The two small poles $a, p - a$

$\sum -\{v=a\} \wedge \{p-a\} \ v \wedge -5 \equiv 0 \pmod{p}$, by pairing $v \leftrightarrow p - v$.

lemma *pair-sum-vge*:

assumes *prime* $p\ p \neq 2\ 1 \leq a\ 2 * a < p$
shows $vge\ p\ (\sum\ v = a..p - a.\ 1 / of\text{-}nat\ v \wedge 5)\ 1$
 $\langle proof \rangle$

The constant term of $\mu\text{-}X(1/(t+j^2))$.

definition $c0 :: nat \Rightarrow rat$ **where** $c0\ j =$
 $- (of\text{-}nat\ j \wedge 4 * H5\ j) - 1 / 4 + 1 / (2 * of\text{-}nat\ j)$

lemma *muPole-eq*: $\mu Pole\ j = [:c0\ j,\ of\text{-}nat\ j \wedge 4:]$
 $\langle proof \rangle$

lemma *muPole-coeff*: $Polynomial.coeff\ (\mu Pole\ j)\ n = (\text{if } n = 1 \text{ then } of\text{-}nat\ j \wedge 4 \text{ else } \text{if } n = 0 \text{ then } c0\ j \text{ else } 0)$
 $\langle proof \rangle$

lemma *H5-split*: $1 \leq a \implies a \leq b \implies$
 $H5\ b = H5\ (a - 1) + (\sum\ v = a..b.\ 1 / of\text{-}nat\ v \wedge 5)$
 $\langle proof \rangle$

The two-node congruence $\mu\text{-}X(1/(t+a^2)) \equiv \mu\text{-}X(1/(t+(p-a)^2)) \pmod{p}$ coefficientwise.

lemma *pole-congr*:

assumes *prime* $p\ p \neq 2\ 1 \leq a\ 2 * a < p$
shows $vge\ p\ (Polynomial.coeff\ (\mu Pole\ a)\ n - Polynomial.coeff\ (\mu Pole\ (p - a))\ n)\ 1$
 $\langle proof \rangle$

lemma *eval-sub-vge*:

assumes *prime* $p\ vpGge\ p\ R\ 0\ vge\ p\ x\ 0\ vge\ p\ y\ 0\ vge\ p\ (x - y)\ b$
shows $vge\ p\ (poly\ R\ x - poly\ R\ y)\ b$
 $\langle proof \rangle$

The divided difference at the two nodes $a, p - a$ is integral.

lemma *two-pole-vge*:

assumes p : prime p **and** $p7$: $7 \leq p$ **and** $a1$: $1 \leq a$ **and** $a2$: $2 * a < p$ **and** R : $vpGge\ p\ R\ 0$
shows $vpGge\ p\ (\mu Xmod\ p\ \{a, p - a\}\ R)\ 0$
 $\langle proof \rangle$

(4.12), rows $i \geq l - 2$: once $E-a$ is a factor, the entry is integral.

lemma *entry-large*:

assumes p : prime p **and** H : $OuterHyp\ K\ p$ **and** $a1$: $1 \leq a$ **and** am : $a \leq mHalf\ p$ **and** R : $vpGge\ p\ R\ 0$
shows $vpGge\ p\ (\mu Xmod\ p\ (outerClassPoles\ K\ p\ a)\ (R * sqPoleProd\ \{j \in outerClassPoles\ K\ p\ a.\ p < j\}))\ 0$
 $\langle proof \rangle$

22.6 The zero class

lemma *vp-three-sq*: prime $p \implies 7 \leq p \implies$
 $vp\ p\ (3 * of-nat\ p^2) \leq 2$
 $\langle proof \rangle$

The zero class with a single pole p .

lemma *entry-zero-one*:

assumes prime p $OuterHyp\ K\ p\ K < 2 * p$ $vpGge\ p\ R\ 0$
shows $vpGge\ p\ (\mu Xmod\ p\ (outerClassPoles\ K\ p\ 0)\ R)\ (-1)$
 $\langle proof \rangle$

The zero class with two poles $p, 2p$.

lemma *entry-zero-two*:

assumes prime p $OuterHyp\ K\ p\ 2 * p \leq K$ $vpGge\ p\ A\ 0$
shows $vpGge\ p\ (\mu Xmod\ p\ (outerClassPoles\ K\ p\ 0)\ (A * (pX + [:of-nat\ p^2:]^{\wedge i} * (pX + [:of-nat\ p^2:]^{\wedge i'})\ (\min\ 0\ (2 * (of-nat\ i + of-nat\ i') - 3))))$
 $\langle proof \rangle$

22.7 The entry bound (4.12)

lemma *min-add-le-min*: $\min\ 0\ A + \min\ 0\ B \leq \min\ 0\ (A + B)$ **for** $A\ B :: rat$
 $\langle proof \rangle$

The cancellation behind a same-class entry.

lemma *same-class-cancel*:

assumes finite Ca $Ca \subseteq tailPoles\ K$
shows $\mu Xmod\ p\ \{1..K\}\ (Dm\ (Nof\ K)^{\wedge 6} * (sqPoleProd\ (tailPoles\ K - Ca) * A) * (sqPoleProd\ (tailPoles\ K - Ca) * B)) =$
 $\mu Xmod\ p\ Ca\ (Dm\ (Nof\ K)^{\wedge 5} * sqPoleProd\ (tailPoles\ K - Ca) * A * B)$
 $\langle proof \rangle$

The cancellation behind a cross-class entry.

lemma *cross-class-cancel*:

assumes *finite Ca finite Cc* $Ca \cap Cc = \{\}$ $Ca \subseteq \text{tailPoles } K$ $Cc \subseteq \text{tailPoles } K$
shows $\text{muXmod } p \{1..K\} (Dm (Nof K) \wedge 6 * (\text{sqPoleProd } (\text{tailPoles } K - Ca) * A) * (\text{sqPoleProd } (\text{tailPoles } K - Cc) * B)) =$
 $[\text{muModPoly } p (Dm (Nof K) \wedge 5 * \text{sqPoleProd } (\text{tailPoles } K - (Ca \cup Cc)) * A * B):]$
 $\langle \text{proof} \rangle$

(4.12) and the zero-class weights: entries of A in the outer basis satisfy the weights. The longest Lean file of the proof (OuterEntries.lean, 1,045 lines): cross-class, ordinary and E - a rows, the two-node congruence $H\text{-}\{p-a\} \equiv H\text{-}\{a-1\} \pmod{p}$, the zero class.

theorem *outerGram-entry-bound*:

assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** H : *OuterHyp* K p **and** x : $x < \text{length } (\text{outer-idx } K p)$ **and** y : $y < \text{length } (\text{outer-idx } K p)$
shows $\text{vpGge } p (\text{outerGram } K p \$\$ (x, y)) (\text{wOut } K p (\text{outer-idx } K p ! x) + \text{wOut } K p (\text{outer-idx } K p ! y))$
 $\langle \text{proof} \rangle$

22.8 The closed form (4.14) of $\gamma\text{-}p^{\wedge}\text{out}$

definition *ind* :: $\text{bool} \Rightarrow \text{nat}$ **where** $\text{ind } P = (\text{if } P \text{ then } 1 \text{ else } 0)$

lemma *ind-le-one*: $\text{ind } P \leq 1$ $\langle \text{proof} \rangle$

lemma *ind-True*: $P \implies \text{ind } P = 1$ $\langle \text{proof} \rangle$

lemma *ind-False*: $\neg P \implies \text{ind } P = 0$ $\langle \text{proof} \rangle$

lemma *ind-mult*: $\text{ind } P * \text{ind } Q = \text{ind } (P \wedge Q)$ $\langle \text{proof} \rangle$

Membership in a class $\pm a \pmod{p}$ for $j < 3p$.

lemma *class-char*:

fixes $j a p$:: nat
assumes $1 \leq a < p$ $j < 3 * p$
shows $(j \bmod p = a \bmod p \vee (j + a) \bmod p = 0) \longleftrightarrow$
 $(j = a \vee j = p + a \vee j = 2 * p + a \vee j + a = p \vee j + a = 2 * p \vee j + a = 3 * p)$
 $\langle \text{proof} \rangle$

lemma *sum6*:

fixes f :: $\text{nat} \Rightarrow \text{nat}$
assumes *distinct* $[x1, x2, x3, x4, x5, x6]$
shows $(\sum x \in \{x1, x2, x3, x4, x5, x6\}. f x) = f x1 + f x2 + f x3 + f x4 + f x5 + f x6$
 $\langle \text{proof} \rangle$

The class $\pm a$ in $\{L..K\}$, as six indicators.

lemma *card-class*:

fixes $L K a p :: \text{nat}$

assumes $1 \leq a \ 2 * a < p \ K < 3 * p$

shows $\text{card } \{j \in \{L..K\}. j \bmod p = a \bmod p \vee (j + a) \bmod p = 0\} =$
 $\text{ind } (L \leq a \wedge a \leq K) + \text{ind } (L \leq p - a \wedge$
 $p - a \leq K) + \text{ind } (L \leq p + a \wedge p + a \leq K) +$
 $\text{ind } (L \leq 2 * p - a \wedge 2 * p - a \leq K) + \text{ind } (L \leq 2 * p + a \wedge$
 $2 * p + a \leq K) + \text{ind } (L \leq 3 * p - a \wedge 3 * p - a \leq K)$

$\langle \text{proof} \rangle$

lemma *ell-eq*:

assumes *prime* $p \ \text{OuterHyp } K \ p \ 1 \leq a \ a \leq m\text{Half } p$

shows $\text{ell } p \ K \ a = (\text{if } K < 2 * p \text{ then } 2 \text{ else } 4) + \text{ind } (a \leq K \bmod p) + \text{ind } (p$
 $\leq$
 $K \bmod p + a)$

$\langle \text{proof} \rangle$

lemma *outerCount-add*:

assumes *prime* $p \ \text{OuterHyp } K \ p \ 1 \leq a \ a \leq m\text{Half } p$

shows $\text{outerCount } K \ p \ a + \text{ind } (a \leq \text{Nof } K) = \text{ell } p \ K \ a$

$\langle \text{proof} \rangle$

lemma *outerCount-zero*:

assumes *prime* $p \ \text{OuterHyp } K \ p$

shows $\text{outerCount } K \ p \ 0 = (\text{if } K < 2 * p \text{ then } 1 \text{ else } 2)$

$\langle \text{proof} \rangle$

The weight (4.12) of row i of a class with l poles and $\delta = d$.

definition $Wc :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$Wc \ l \ d \ i = (\text{if } i < l - 2 \text{ then } \min \ 0 \ (\text{of-nat } i + 3 * \text{of-nat } d - (\text{of-nat } l + 4) /$
 $2) \text{ else } 0)$

The two finite class computations: classes with $2 + A + B$ and $4 + A + B$ poles.

lemma *card-lt-Suc*: $\text{card } \{i. i < \text{Suc } n \wedge P \ i\} = \text{card } \{i. i < n \wedge$

$P \ i\} + (\text{if } P \ n \text{ then } 1 \text{ else } 0)$

$\langle \text{proof} \rangle$

lemma *cls2*:

assumes $A \leq 1 \ B \leq 1 \ d \leq 1$

shows $2 * (\sum i < 2 + A + B - d. Wc \ (2 + A + B) \ d \ i) =$
 $- 7 * (\text{of-nat } A + \text{of-nat } B) + 6 * \text{of-nat } d * (\text{of-nat } A + \text{of-nat } B) \wedge$
 $\text{card } \{i. i < 2 + A + B - d \wedge Wc \ (2 + A + B) \ d \ i = 0\} = 2 - d + d *$

$A * B$

$\langle \text{proof} \rangle$

lemma *cls4*:

assumes $A \leq 1 \ B \leq 1 \ d \leq 1$

shows $2 * (\sum i < 4 + A + B - d. Wc \ (4 + A + B) \ d \ i) =$

$- 14 - 7 * (\text{of-nat } A + \text{of-nat } B) + \text{of-nat } d * (12 + 5 * (\text{of-nat } A + \text{of-nat } B)) \wedge$
 $\text{card } \{i. i < 4 + A + B - d \wedge \text{Wc } (4 + A + B) \ d \ i = 0\} = 2 + d * A *$
 B
 $\langle \text{proof} \rangle$

The weight as a function of naturals.

definition $\text{Wn} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**

$\text{Wn } K \ p \ a \ i = (\text{if } a = 0 \text{ then } (\text{if } \text{outerCount } K \ p \ 0 = 1 \text{ then } - 1 / 2 \text{ else if } i =$
 $0 \text{ then } - 2 \text{ else } 0))$
 $\text{else } \text{Wc } (\text{ell } p \ K \ a) \ (\text{ind } (a \leq \text{Nof } K)) \ i)$

lemma $w\text{Out-eg}$: $w\text{Out } K \ p \ x = \text{Wn } K \ p \ (\text{fst } x) \ (\text{snd } x)$
 $\langle \text{proof} \rangle$

lemma sum-wOut : $(\sum x \leftarrow \text{outer-idx } K \ p. w\text{Out } K \ p \ x) = (\sum a \leq$
 $m\text{Half } p. \sum i < \text{outerCount } K \ p \ a. \text{Wn } K \ p \ a \ i)$
 $\langle \text{proof} \rangle$

lemma card-zero-wOut :

$\text{length } (\text{filter } (\lambda x. w\text{Out } K \ p \ x = 0) \ (\text{outer-idx } K \ p)) = (\sum a \leq$
 $m\text{Half } p. \text{card } \{i. i < \text{outerCount } K \ p \ a \wedge \text{Wn } K \ p \ a \ i = 0\})$
 $\langle \text{proof} \rangle$

lemma class-low :

assumes $\text{prime } p \ \text{OuterHyp } K \ p \ K < 2 * p \ 1 \leq a \leq m\text{Half } p$

shows $2 * (\sum i < \text{outerCount } K \ p \ a. \text{Wn } K \ p \ a \ i) =$
 $- 7 * (\text{of-nat } (\text{ind } (a \leq K \bmod p)) + \text{of-nat } (\text{ind } (p \leq$
 $K \bmod p + a))) + 6 * \text{of-nat } (\text{ind } (a \leq \text{Nof } K)) * (\text{of-nat } (\text{ind } (a \leq$
 $K \bmod p)) + \text{of-nat } (\text{ind } (p \leq K \bmod p + a))) \wedge$
 $\text{card } \{i. i < \text{outerCount } K \ p \ a \wedge$
 $\text{Wn } K \ p \ a \ i = 0\} = 2 - \text{ind } (a \leq \text{Nof } K) + \text{ind } (a \leq \text{Nof } K) * \text{ind } (a \leq$
 $K \bmod p) * \text{ind } (p \leq K \bmod p + a)$

$\langle \text{proof} \rangle$

lemma class-high :

assumes $\text{prime } p \ \text{OuterHyp } K \ p \ \neg K < 2 * p \ 1 \leq a \leq m\text{Half } p$

shows $2 * (\sum i < \text{outerCount } K \ p \ a. \text{Wn } K \ p \ a \ i) =$
 $- 14 - 7 * (\text{of-nat } (\text{ind } (a \leq K \bmod p)) + \text{of-nat } (\text{ind } (p \leq$
 $K \bmod p + a))) + \text{of-nat } (\text{ind } (a \leq \text{Nof } K)) * (12 + 5 * (\text{of-nat } (\text{ind } (a \leq$
 $K \bmod p)) + \text{of-nat } (\text{ind } (p \leq K \bmod p + a)))) \wedge$
 $\text{card } \{i. i < \text{outerCount } K \ p \ a \wedge$
 $\text{Wn } K \ p \ a \ i = 0\} = 2 + \text{ind } (a \leq \text{Nof } K) * \text{ind } (a \leq K \bmod p) * \text{ind } (p$
 $\leq$
 $K \bmod p + a)$
 $\langle \text{proof} \rangle$

The interval counts used in (4.14).

lemma *counts*:

assumes *prime p OuterHyp K p*

shows $\text{card } \{a \in \{1..m\text{Half } p\}. a \leq K \bmod p\} + \text{card } \{a \in \{1..m\text{Half } p\}. p \leq K \bmod p + a\} = K \bmod p \wedge$

$\text{card } \{a \in \{1..m\text{Half } p\}. a \leq \text{Nof } K \wedge$

$a \leq K \bmod p\} = \min (\text{Nof } K) (K \bmod p) \wedge$

$\text{card } \{a \in \{1..m\text{Half } p\}. a \leq \text{Nof } K \wedge$

$p \leq K \bmod p + a\} = \text{Nof } K + K \bmod p + 1 - p \wedge$

$\text{card } \{a \in \{1..m\text{Half } p\}. a \leq \text{Nof } K\} = \text{Nof } K \wedge$

$\text{card } \{a \in \{1..m\text{Half } p\}. (a \leq \text{Nof } K \wedge a \leq K \bmod p) \wedge$

$p \leq K \bmod p + a\} = \text{Nof } K + K \bmod p + 1 - p$

<proof>

The table after (4.14): summing (4.12) and applying Lemma 4.2 gives exactly $\gamma\text{-}p\hat{\text{out}}$. Pure combinatorics of the classes (Lean: OuterCount.lean, 444 lines).

lemma *ind-sum-nat: finite I $\implies$*

$(\sum a \in I. \text{ind } (P a)) = \text{card } \{a \in I. P a\}$

<proof>

lemma *ind-sum-rat: finite I $\implies$*

$(\sum a \in I. (\text{of-nat } (\text{ind } (P a)) :: \text{rat})) = \text{of-nat } (\text{card } \{a \in I. P a\})$

<proof>

lemma *two-minus-ind: $2 - \text{ind } P + \text{ind } P = (2 :: \text{nat})$*

<proof>

lemma *gamma-arith-low:*

fixes *X :: rat*

assumes *S: $2 * X = - 7 * (\text{of-nat } c1 + \text{of-nat } c2) + 6 * (\text{of-nat } c3 + \text{of-nat } c4)$*

and *c12: $c1 + c2 = v$ and v: $v = K - p$ and pK: $p \leq K$ and c3: $c3 =$*

min N v and c4: $c4 = u$

and *m: $2 * m + 1 = p$ and Nm: $N \leq 2 * m$*

shows $(\text{of-int } (- 7 * (\text{int } K - \text{int } p) + 6 * \text{int } (\text{min } N v + u) - 1 - \text{min } (\text{int } r) (\text{int } p - 1 -$

$\text{int } N + \text{int } u)) :: \text{rat})$

$= 2 * (- 1 / 2 + X) - \text{of-nat } (\text{min } r (2 * m - N + u))$

<proof>

lemma *gamma-arith-high:*

fixes *X :: rat*

assumes *S: $2 * X = - 14 * \text{of-nat } m - 7 * (\text{of-nat } c1 + \text{of-nat } c2) + 12 * \text{of-nat } c5 + 5 *$*

(of-nat c3 + of-nat c4)

and *c12: $c1 + c2 = v$ and v: $v = K - 2 * p$ and pK: $2 * p \leq K$ and c3: $c3 =$*

min N v and c4: $c4 = u$

and *c5: $c5 = N$ and m: $2 * m + 1 = p$*

shows $(\text{of-int } (- 7 * (\text{int } K - \text{int } p) + 3 + 12 * \text{int } N + 5 * \text{int } (\min N v + u) - \min (\text{int } r) (\text{int } p + \text{int } u)) :: \text{rat})$
 $= 2 * (- 2 + X) - \text{of-nat } (\min r (2 * m + 1 + u))$
 $\langle \text{proof} \rangle$
theorem *gammaOut-eq-sum*:
assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** H : *OuterHyp* K p
shows $\text{of-int } (\text{gammaOut } K p) =$
 $2 * (\sum x \leftarrow \text{outer-idx } K p. \text{wOut } K p x)$
 $- \text{of-nat } (\min (r\text{Out } K p) (\text{length } (\text{filter } (\lambda x. \text{wOut } K p x = 0) (\text{outer-idx } K p))))$
 $\langle \text{proof} \rangle$

22.9 Lemma 4.2

The weight arithmetic behind Lemma 4.2: for nonpositive half-integer weights and any U , $\sum \{i \in U\} (w \cdot i + 1/2) \leq \min(|U|, z)/2$, z the number of zero weights.

lemma *weight-loss-nat*:
fixes $n :: \text{nat}$ **and** $w :: \text{nat} \Rightarrow 'a :: \text{linordered-field}$
assumes $\bigwedge i. i < n \Rightarrow w \cdot i \leq 0$ $\bigwedge i. i < n \Rightarrow$
 $\exists k :: \text{int}. 2 * w \cdot i = \text{of-int } k \ U \subseteq \{..<n\}$
shows $(\sum i \in U. w \cdot i + 1 / 2) \leq \text{of-nat } (\min (\text{card } U) (\text{card } \{i. i < n \wedge w \cdot i = 0\})) / 2$
 $\langle \text{proof} \rangle$

lemma *weight-loss*:
fixes $n :: \text{nat}$ **and** $w :: \text{nat} \Rightarrow 'a :: \text{linordered-field}$
assumes $\bigwedge i. i < n \Rightarrow w \cdot i \leq 0$ $\bigwedge i. i < n \Rightarrow$
 $\exists k :: \text{int}. 2 * w \cdot i = \text{of-int } k \ U \subseteq \{..<n\}$
shows $(\sum i \in U. w \cdot i + 1 / 2) \leq \text{of-nat } (\min (\text{card } U) (\text{card } \{i. i < n \wedge w \cdot i = 0\})) / 2$
 $\langle \text{proof} \rangle$

A matrix with a nontrivial linear relation among its rows has determinant zero (over an integral domain: multilinearity in the row carrying a nonzero coefficient).

lemma *det-zero-of-row-relation*:
fixes $A :: 'a :: \text{idom } \text{mat}$
assumes A : $A \in \text{carrier-mat } n \ n$ **and** $i0$: $i0 < n$ **and** $c0$: $c \cdot i0 \neq 0$
and rel : $\bigwedge j. j < n \Rightarrow (\sum i = 0..<n. c \cdot i * A \ \$\$ (i, j)) = 0$
shows $\text{Determinant.det } A = 0$
 $\langle \text{proof} \rangle$

More than *rank* L rows of a rational matrix L satisfy a nontrivial linear relation.

lemma *rows-dependent*:

assumes L : $L \in \text{carrier-mat } n \ n$ **and** T : $T \subseteq \{0..<n\}$ **and** r : $\text{vec-space.rank } n$
 $L <$
 $\text{card } T$
shows $\exists c :: \text{nat} \Rightarrow \text{rat. } (\forall i. i \notin T \longrightarrow$
 $c \ i = 0) \wedge (\exists i \in T. c \ i \neq 0) \wedge$
 $(\forall j < n. (\sum i = 0..<n. c \ i * L \ \$\$ (i, j)) = 0)$
 $\langle \text{proof} \rangle$

Multilinear expansion of the determinant of a sum over rows: for every subset T of the rows, take the rows in T from B and the others from A .

lemma *det-add-rows-expand*:
fixes $A \ B :: 'a :: \text{comm-ring-1 mat}$
assumes A : $A \in \text{carrier-mat } n \ n$ **and** B : $B \in \text{carrier-mat } n \ n$
shows $\text{Determinant.det } (A + B) =$
 $(\sum T \in \text{Pow } \{0..<n\}. \text{Determinant.det } (\text{Matrix.mat } n \ n \ (\lambda(i, j).$
 $\text{if } i \in T \text{ then } B \ \$\$ (i, j) \text{ else } A \ \$\$ (i, j))))$
 $\langle \text{proof} \rangle$

Lemma 4.2: if $v(A \cdot ij) \geq w \cdot i + w \cdot j$ with nonpositive half-integer weights, L is integral of rank at most r , and exactly z weights are zero, then $v(\det(A + p \cdot \hat{-} 1L)) \geq 2 \sum w \cdot i - \min(r, z)$ (Gauss valuation; L constant). Proof by the row-multilinear expansion (*Determinant.det-linear-rows-sum*), not by complementary minors.

theorem *det-vpGge-of-weighted-entries*:
assumes p : $\text{prime } p$ **and** A : $A \in \text{carrier-mat } n \ n$ **and** L : $L \in \text{carrier-mat } n \ n$
and hw : $\bigwedge i. i < n \implies$
 $w \ i \leq 0$ **and** $hw2$: $\bigwedge i. i < n \implies \exists k :: \text{int. } 2 * w \ i = \text{of-int } k$
and hA : $\bigwedge i \ j. i < n \implies j < n \implies$
 $\text{vpGge } p \ (A \ \$\$ (i, j)) \ (w \ i + w \ j)$
and hL : $\bigwedge i \ j. i < n \implies j < n \implies$
 $L \ \$\$ (i, j) \neq 0 \implies 0 \leq \text{vp } p \ (L \ \$\$ (i, j))$
and hr : $\text{vec-space.rank } n \ L \leq r$
shows $\text{vpGge } p \ (\text{Determinant.det } (A + \text{map-mat } (\lambda c. [:c / \text{of-nat } p:]) \ L))$
 $(2 * (\sum i < n. w \ i) - \text{of-nat } (\min r \ (\text{card } \{i. i < n \wedge w \ i = 0\})))$
 $\langle \text{proof} \rangle$

22.10 Proposition 4.3

lemma *degree-outerBasis-lt*:
assumes $\text{prime } p$ $40 \ \text{dvd } K$ $\text{OuterHyp } K \ p \ x \in \text{set } (\text{outer-id } K \ p)$
shows $\text{degree } (\text{outerBasis } K \ p \ x) < \text{hof } K$
 $\langle \text{proof} \rangle$

Helpers for the unimodularity of the outer basis: congruences modulo p of polynomials and of Taylor coefficients. $\text{oroot } p \ a$ is the expansion point of class a (p for the zero class).

definition $\text{oroot} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat}$ **where** $\text{oroot } p \ a = (\text{if } a =$
 $0 \text{ then } p \text{ else } a)$

lemma *oroot-mod*: $\text{oroot } p \ a \ \text{mod } p = a \ \text{mod } p$
 $\langle \text{proof} \rangle$

lemma *oroot-add-mod*: $(k + \text{oroot } p \ a) \ \text{mod } p = (k + a) \ \text{mod } p$
 $\langle \text{proof} \rangle$

lemma *vpGge-tay1*:
assumes p : *prime* p **and** P : $\text{vpGge } p \ P \ 1$ **and** r : $\text{vge } p \ r \ 0$
shows $\text{vge } p \ (\text{tay } P \ r \ i) \ 1$
 $\langle \text{proof} \rangle$

lemma *tay-diff*: $\text{tay } (P - Q) \ r \ i = \text{tay } P \ r \ i - \text{tay } Q \ r \ i$
 $\langle \text{proof} \rangle$

lemma *vpGge-diff*: $\text{prime } p \implies \text{vpGge } p \ A \ b \implies$
 $\text{vpGge } p \ B \ b \implies \text{vpGge } p \ (A - B) \ b$
 $\langle \text{proof} \rangle$

lemma *vpGge-prod-diff*:
assumes p : *prime* p **and** S : *finite* S
and hf : $\bigwedge j. j \in S \implies$
 $\text{vpGge } p \ (f \ j) \ 0$ **and** hg : $\bigwedge j. j \in S \implies \text{vpGge } p \ (g \ j) \ 0$
and hfg : $\bigwedge j. j \in S \implies \text{vpGge } p \ (f \ j - g \ j) \ 1$
shows $\text{vpGge } p \ ((\prod j \in S. f \ j) - (\prod j \in S. g \ j)) \ 1$
 $\langle \text{proof} \rangle$

lemma *sq-cong-mod*:
assumes $\text{prime } p \ j \ \text{mod } p = a \ \text{mod } p \vee (j + a) \ \text{mod } p = 0$
shows $\text{vge } p \ (\text{of-nat } j \ ^2 - \text{of-nat } a \ ^2) \ 1$
 $\langle \text{proof} \rangle$

lemma *sq-unit-mod*:
assumes p : *prime* p **and** nc : $\neg (k \ \text{mod } p = s \ \text{mod } p \vee (k + s) \ \text{mod } p = 0)$
shows $(\text{of-nat } k \ ^2 - \text{of-nat } s \ ^2 :: \text{rat}) \neq 0 \wedge$
 $\text{vp } p \ (\text{of-nat } k \ ^2 - \text{of-nat } s \ ^2) = 0$
 $\langle \text{proof} \rangle$

lemma *class-disjoint-m*:
assumes m : $2 * m\text{Half } p + 1 = p$ **and** a : $a \leq m\text{Half } p$ **and** c : $c \leq$
 $m\text{Half } p$ **and** ac : $a \neq c$
shows $\text{outerClassPoles } K \ p \ a \cap \text{outerClassPoles } K \ p \ c = \{\}$
 $\langle \text{proof} \rangle$

lemma *class-prod-cong*:
assumes p : *prime* p **and** S : $S \subseteq \text{outerClassPoles } K \ p \ c$
shows $\text{vpGge } p \ (\text{sqPoleProd } S - (pX - [:- (\text{of-nat } (\text{oroot } p \ c) \ ^2):]) \ ^{\text{card } S})$
 1
 $\langle \text{proof} \rangle$

lemma *oq-cong*:

assumes p : prime p
and cH : $1 \leq \text{fst } x \implies$
 $\text{card } \{j \in \text{outerClassPoles } K \ p \ (\text{fst } x). \ p < j\} = \text{ell } p \ K \ (\text{fst } x) - 2$
shows $\text{vpGge } p \ (\text{oq } K \ p \ x - (pX - [\text{of-nat } (\text{oroot } p \ (\text{fst } x)) \wedge 2]:]) \wedge \text{snd } x$
 1
 $\langle \text{proof} \rangle$

lemma *oq-cong-hyp*:

assumes p : prime p **and** H : *OuterHyp* $K \ p$ **and** x : $x \in \text{set } (\text{outer-idx } K \ p)$
shows $\text{vpGge } p \ (\text{oq } K \ p \ x - (pX - [\text{of-nat } (\text{oroot } p \ (\text{fst } x)) \wedge 2]:]) \wedge \text{snd } x$
 1
 $\langle \text{proof} \rangle$

Below the diagonal of the Taylor matrix of the outer basis the entries are divisible by p .

lemma *outer-tay-below*:

assumes p : prime p **and** m : $2 * m\text{Half } p + 1 = p$
and oqc : $\text{vpGge } p \ (\text{oq } K \ p \ (a, j) - (pX - [\text{of-nat } (\text{oroot } p \ a) \wedge 2]:]) \wedge j \ 1$
and a : $a \leq m\text{Half } p$ **and** c : $c \leq m\text{Half } p$ **and** ci : $i < \text{outerCount } K \ p \ c$
and lex : $c < a \vee (c = a \wedge i < j)$
shows $\text{vge } p \ (\text{tay } (\text{outerBasis } K \ p \ (a, j)) \ (- \ (\text{of-nat } (\text{oroot } p \ c) \wedge 2)) \ i) \ 1$
 $\langle \text{proof} \rangle$

The diagonal entries of the Taylor matrix of the outer basis are p -adic units.

lemma *outer-tay-diag*:

assumes p : prime p
and oqc : $\text{vpGge } p \ (\text{oq } K \ p \ (a, j) - (pX - [\text{of-nat } (\text{oroot } p \ a) \wedge 2]:]) \wedge j \ 1$
shows $\text{tay } (\text{outerBasis } K \ p \ (a, j)) \ (- \ (\text{of-nat } (\text{oroot } p \ a) \wedge 2)) \ j \neq 0 \wedge$
 $\text{vp } p \ (\text{tay } (\text{outerBasis } K \ p \ (a, j)) \ (- \ (\text{of-nat } (\text{oroot } p \ a) \wedge 2)) \ j) = 0$
 $\langle \text{proof} \rangle$

(4.11): the outer basis is $\mathbb{Z}$ - p -unimodular, by the Taylor-matrix criterion. Row (a, i) is expanded at $-a \wedge 2$ (at $-p \wedge 2$ for the zero class); below the diagonal the entries are divisible by p (the poles $j > p$ of a class satisfy $j \wedge 2 \equiv a \wedge 2$), and the diagonal entries are units.

theorem *outerBasis-unimodular*:

assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** H : *OuterHyp* $K \ p$
defines $B \equiv \text{Matrix.mat } (\text{hof } K) \ (\text{hof } K) \ (\lambda(x,$
 $d). \text{Polynomial.coeff } (\text{outerBasis } K \ p \ (\text{outer-idx } K \ p \ ! \ x)) \ d)$
shows $\text{Determinant.det } B \neq 0 \wedge \text{vp } p \ (\text{Determinant.det } B) = 0$
 $\langle \text{proof} \rangle$

lemma *muModPoly-eq-sum*:

assumes $\text{degree } Q \leq N$
shows $\text{muModPoly } p \ Q = (\sum e \leq$
 $N. \text{Polynomial.coeff } Q \ e * (\text{muMono } e - c\text{Corr } p \ e / \text{of-nat } p))$

$\langle \text{proof} \rangle$

lemma *muModPoly-add*: $\text{muModPoly } p (P + Q) = \text{muModPoly } p P + \text{muModPoly } p Q$
 $\langle \text{proof} \rangle$

lemma *muModPoly-smult*: $\text{muModPoly } p (\text{Polynomial.smult } c P) = c * \text{muModPoly } p P$
 $\langle \text{proof} \rangle$

lemma *muXmod-add*: $\text{muXmod } p S (P + Q) = \text{muXmod } p S P + \text{muXmod } p S Q$
 $\langle \text{proof} \rangle$

lemma *muXmod-C-mul*: $\text{muXmod } p S ([:c:] * P) = [:c:] * \text{muXmod } p S P$
 $\langle \text{proof} \rangle$

lemma *muXmod-zero*: $\text{muXmod } p S 0 = 0$
 $\langle \text{proof} \rangle$

lemma *muXmod-sum*: $\text{muXmod } p S (\sum i \in I. f i) = (\sum i \in I. \text{muXmod } p S (f i))$
 $\langle \text{proof} \rangle$

The Gram identity with the length and degree facts as hypotheses, so that it also applies for $p > K$.

lemma *outerGram-eq-conj-gen*:
assumes *lenH*: $\text{length } (\text{outer-idx } K p) = \text{hof } K$
and *dgH*: $\bigwedge x. x \in \text{set } (\text{outer-idx } K p) \implies \text{degree } (\text{outerBasis } K p x) < \text{hof } K$
defines $B \equiv \text{Matrix.mat } (\text{hof } K) (\text{hof } K) (\lambda(x, d). \text{Polynomial.coeff } (\text{outerBasis } K p (\text{outer-idx } K p ! x)) d)$
shows $\text{outerGram } K p = \text{map-mat } (\lambda q. [:q:]) B * \text{Aout } K p * \text{transpose-mat } (\text{map-mat } (\lambda q. [:q:]) B)$
 $\langle \text{proof} \rangle$

lemma *outerGram-eq-conj*:
assumes *p*: *prime* *p* **and** *K*: $40 \text{ dvd } K$ **and** *H*: *OuterHyp* *K* *p*
defines $B \equiv \text{Matrix.mat } (\text{hof } K) (\text{hof } K) (\lambda(x, d). \text{Polynomial.coeff } (\text{outerBasis } K p (\text{outer-idx } K p ! x)) d)$
shows $\text{outerGram } K p = \text{map-mat } (\lambda q. [:q:]) B * \text{Aout } K p * \text{transpose-mat } (\text{map-mat } (\lambda q. [:q:]) B)$
 $\langle \text{proof} \rangle$

lemma *gammaOut-eq-sum-idx*:
assumes *prime* *p* $40 \text{ dvd } K$ *OuterHyp* *K* *p*
shows $\text{of-int } (\text{gammaOut } K p) = 2 * (\sum x < \text{length } (\text{outer-idx } K p). \text{wOut } K p (\text{outer-idx } K p ! x)) - \text{of-nat } (\min (\text{rOut } K p) (\text{card } \{x. x < \text{length } (\text{outer-idx } K p) \} \wedge$

$wOut\ K\ p\ (outer\text{-}idx\ K\ p\ !\ x) = 0\})$

$\langle proof \rangle$

Proposition 4.3: under (4.9), $v\text{-}p\hat{G}(\Delta\text{-}K) \geq \gamma\text{-}p\hat{out}$. Assembly: change to the outer basis, split $G = A + p\hat{-}\hat{1}L$, bound the entries, apply Lemma 4.2, identify the bound.

lemma *vge-mat-mult0*:

assumes p : prime p **and** A : $A \in carrier\text{-}mat\ n\ n$ **and** B : $B \in carrier\text{-}mat\ n\ n$
and hA : $\forall i < n. \forall j < n. vge\ p\ (A\ \$\$ (i, j))\ 0$ **and** hB : $\forall i < n. \forall j < n. vge\ p\ (B\ \$\$ (i, j))\ 0$
and i : $i < n$ **and** j : $j < n$
shows $vge\ p\ ((A * B)\ \$\$ (i, j))\ 0$

$\langle proof \rangle$

lemma *mat-mult-entry*:

assumes $A \in carrier\text{-}mat\ n\ m$ $C \in carrier\text{-}mat\ m\ k$ $i < n$ $j < k$
shows $(A * C)\ \$\$ (i, j) = (\sum\ l = 0..<m. A\ \$\$ (i, l) * C\ \$\$ (l, j))$

$\langle proof \rangle$

theorem *DeltaK-vpGge-outer*:

assumes p : prime p **and** K : $40\ dvd\ K$ **and** H : $OuterHyp\ K\ p$
shows $vpGge\ p\ (DeltaK\ K)\ (of\text{-}int\ (\gamma Out\ K\ p))$

$\langle proof \rangle$

22.11 Proposition 4.3 for $p > K$

lemma *muX-eq-muXmod-of-lt*:

assumes prime p $degree\ (P\ div\ sqPoleProd\ S) < 2 * p - 3$
shows $muX\ S\ P = muXmod\ p\ S\ P$

$\langle proof \rangle$

For $p > K \geq 40$: p is odd and ≥ 7 , class $a \geq 1$ poles are among $a, p - a$, the zero class is empty.

lemma *large-facts*:

assumes prime p $40\ dvd\ K$ $0 < K$ $K < p$
shows $7 \leq p \wedge odd\ p \wedge 2 * mHalf\ p + 1 = p \wedge outerCount\ K\ p\ 0 = 0 \wedge$
 $(\forall a\ j. a \leq mHalf\ p \longrightarrow$
 $j \in outerClassPoles\ K\ p\ a \longrightarrow (j = a \vee j = p - a) \wedge$
 $Nof\ K + 1 \leq j \wedge j \leq K) \wedge$
 $(\forall a. a \leq mHalf\ p \longrightarrow ell\ p\ K\ a \leq 2) \wedge$
 $(\forall a. \{j \in outerClassPoles\ K\ p\ a. p < j\} = \{\})$

$\langle proof \rangle$

For $p > K$: the length of the outer index list, the degree bound and the congruence of the class factors.

lemma *length-outer-idx-large*:

assumes p : prime p **and** K : $40\ dvd\ K$ **and** $K0$: $0 < K$ **and** Kp : $K < p$
shows $length\ (outer\text{-}idx\ K\ p) = hof\ K$

$\langle proof \rangle$

lemma *degree-outerBasis-lt-large:*

assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** $K0$: $0 < K$ **and** Kp : $K < p$ **and** x :
 $x \in$
 $\text{set } (\text{outer-idx } K \ p)$
shows $\text{degree } (\text{outerBasis } K \ p \ x) < \text{hof } K$
 $\langle \text{proof} \rangle$

lemma *oq-cong-large:*

assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** $K0$: $0 < K$ **and** Kp : $K < p$ **and** x :
 $x \in$
 $\text{set } (\text{outer-idx } K \ p)$
shows $\text{vpGge } p \ (\text{oq } K \ p \ x - (pX - [\text{:- } (\text{of-nat } (\text{oroot } p \ (\text{fst } x)) \wedge 2):]) \wedge \text{snd } x)$
 1
 $\langle \text{proof} \rangle$

lemma *outerBasis-unimodular-large:*

assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** $K0$: $0 < K$ **and** Kp : $K < p$
defines $B \equiv \text{Matrix.mat } (\text{hof } K) \ (\text{hof } K) \ (\lambda(x,$
 $d). \text{Polynomial.coeff } (\text{outerBasis } K \ p \ (\text{outer-idx } K \ p \ ! \ x)) \ d)$
shows $\text{Determinant.det } B \neq 0 \wedge \text{vp } p \ (\text{Determinant.det } B) = 0$
 $\langle \text{proof} \rangle$

lemma *G-eq-Aout-large:*

assumes prime p $40 \text{ dvd } K$ $0 < K$ $K < p$
shows $GK \ K = Aout \ K \ p$
 $\langle \text{proof} \rangle$

lemma *large-class-entry:*

assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** $K0$: $0 < K$ **and** Kp : $K < p$ **and**
 $a1$: $1 \leq$
 a **and** am : $a \leq mHalf \ p$ **and** R : $\text{vpGge } p \ R \ 0$
shows $\text{vpGge } p \ (\text{muXmod } p \ (\text{outerClassPoles } K \ p \ a) \ R) \ 0$
 $\langle \text{proof} \rangle$

lemma *outerGram-int-large:*

assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** $K0$: $0 < K$ **and** Kp : $K < p$ **and** x :
 $x <$
 $\text{length } (\text{outer-idx } K \ p)$ **and** y : $y < \text{length } (\text{outer-idx } K \ p)$
shows $\text{vpGge } p \ (\text{outerGram } K \ p \ \$\$ \ (x, y)) \ 0$
 $\langle \text{proof} \rangle$

Proposition 4.3, second part: $v\text{-}p\text{-}\hat{G}(\Delta\text{-}K) \geq 0$ for $p > K$.

theorem *DeltaK-vpGge-large-prime:*

assumes p : prime p **and** K : $40 \text{ dvd } K$ **and** Kp : $K < p$
shows $\text{vpGge } p \ (\text{DeltaK } K) \ 0$
 $\langle \text{proof} \rangle$

end

```

theory Zeta5-Integral-Representation
  imports Zeta5-Outer-Range Vandermonde-Gram-Determinants Laplace-Sin-Cot-Series
    HOL-Real-Asymp.Real-Asymp
begin

```

23 The determinant construction and the moment representation of $\zeta(5)$

Section 2 of the paper: degree and leading coefficient of Δ_K (2.9) through the Vandermonde determinant, the positive integral representation $\mu_{\zeta(5)}(P) = \int P w$ of Proposition 2.2 (*muX-zeta5-integral*: moments from Euler's formula for $\zeta(2e + 2)$ and the pole values from the Laplace transform of *sin* and the cotangent expansion), and the positivity $\Delta_K(\zeta(5)) > 0$. Lean theories *Section2*, *Degree29*, *Prop22*.

$G\text{-}K$ may be computed with the cancelled denominator $D\text{-}K/D\text{-}N$ and numerator $D\text{-}N^5$.

lemma *G-eq-cancelled*:

```

   $i < \text{hof } K \implies j < \text{hof } K \implies$ 
   $GK\ K\ \$\$ (i, j) = \text{muX } \{Nof\ K + 1..K\} (Dm\ (Nof\ K) \wedge 5 * pX \wedge (i + j))$ 
  <proof>

```

$G\text{-}K(X)$ has entries affine in X .

lemma *degree-muPole-le*: $\text{degree } (\text{muPole } j) \leq 1$
<proof>

lemma *muX-degree-le*:

```

  assumes finite S
  shows  $\text{degree } (\text{muX } S\ P) \leq 1$ 
  <proof>

```

23.1 (2.9): degree and leading coefficient of $\Delta\text{-}K$

A product of polynomials of degree ≤ 1 has degree $\leq \text{card } I$, and its top coefficient is the product of the X -coefficients.

lemma *coeff-prod-degree-le-1*:

```

  assumes  $\text{finite } I \wedge i. i \in I \implies \text{degree } (f\ i) \leq 1$ 
  shows  $\text{degree } (\prod i \in I. f\ i) \leq \text{card } I \wedge$ 
   $\text{Polynomial.coeff } (\prod i \in I. f\ i) (\text{card } I) = (\prod i \in$ 
   $I. \text{Polynomial.coeff } (f\ i)\ 1)$ 
  <proof>

```

$A + X\ B$ as a matrix of affine polynomials.

definition *affine-mat* :: $\text{rat mat} \Rightarrow \text{rat mat} \Rightarrow \text{rat poly mat}$ **where**

```

  affine-mat  $A\ B = \text{Matrix.mat } (\text{dim-row } A) (\text{dim-col } A) (\lambda(i, j). [A\ \$\$ (i, j), B$ 
   $\$ \$ (i,$ 

```

$j):])$

lemma *affine-mat-carrier*: $A \in \text{carrier-mat } n \ n \implies$
 $\text{affine-mat } A \ B \in \text{carrier-mat } n \ n$
 $\langle \text{proof} \rangle$

$\det(A + X \ B)$ has degree $\leq n$ and X^n -coefficient $\det B$.

lemma *det-affine-mat*:
assumes $A: A \in \text{carrier-mat } n \ n$ **and** $B: B \in \text{carrier-mat } n \ n$
shows $\text{degree } (\text{Determinant.det } (\text{affine-mat } A \ B)) \leq n \wedge$
 $\text{Polynomial.coeff } (\text{Determinant.det } (\text{affine-mat } A \ B)) \ n = \text{Determinant.det}$
 B
 $\langle \text{proof} \rangle$

The constant and X -coefficient matrices of G - K .

definition $GA :: \text{nat} \Rightarrow \text{rat mat}$ **where**
 $GA \ K = \text{Matrix.mat } (\text{hof } K) (\text{hof } K) (\lambda(i, j). \text{Polynomial.coeff } (GK \ K \ \$\$ (i,$
 $j)) \ 0)$

definition $GB :: \text{nat} \Rightarrow \text{rat mat}$ **where**
 $GB \ K = \text{Matrix.mat } (\text{hof } K) (\text{hof } K) (\lambda(i, j). \text{Polynomial.coeff } (GK \ K \ \$\$ (i,$
 $j)) \ 1)$

lemma *degree-le-1-pCons*:
assumes $d: \text{degree } p \leq 1$
shows $p = [\text{Polynomial.coeff } p \ 0, \text{Polynomial.coeff } p \ 1:]$
 $\langle \text{proof} \rangle$

lemma *GK-eq-affine*: $GK \ K = \text{affine-mat } (GA \ K) (GB \ K)$
 $\langle \text{proof} \rangle$

lemma *muPole-coeff-one*: $\text{Polynomial.coeff } (\text{muPole } j) \ 1 = \text{of-nat } j \ ^4$
 $\langle \text{proof} \rangle$

The residue weight at the pole j .

definition $wt :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{rat}$ **where**
 $wt \ K \ j = \text{of-nat } j \ ^4 * \text{poly } (Dm \ (Nof \ K)) \ (- \ (\text{of-nat } j \ ^2)) \ ^5 /$
 $(\prod \ k \in \{Nof \ K + 1..K\} - \{j\}. \text{of-nat } k \ ^2 - \text{of-nat } j \ ^2)$

lemma *GB-apply*:
assumes $i < \text{hof } K \ j < \text{hof } K$
shows $GB \ K \ \$\$ (i, j) =$
 $(\sum \ l \in \{Nof \ K + 1..K\}. (- \ (\text{of-nat } l \ ^2)) \ ^i * (- \ (\text{of-nat } l \ ^2)) \ ^j * \text{of-nat } l)$
 $\langle \text{proof} \rangle$

The Vandermonde sign identity $\prod -t \prod -\{s \neq t\} (v \ t - v \ s) = (-1)^{\wedge \{n(n-1)/2\}}$
 $(\prod -\{i < j\} (v \ j - v \ i))^2$.

lemma *prod-erase-sub*:

fixes $v :: \text{nat} \Rightarrow \text{rat}$
shows $(\prod t < n. \prod s \in \{..<n\} - \{t\}. v\ t - v\ s) =$
 $(-1)^{\wedge (n * (n - 1) \text{ div } 2)} * (\prod i < n. \prod j \in \{j. i < j \wedge$
 $j < n\}. v\ j - v\ i)^{\wedge 2}$
 $\langle \text{proof} \rangle$

lemma *Dm-eval-ne-zero*: $\text{Nof } K < j \implies \text{poly } (Dm\ (\text{Nof } K))\ (-\ (\text{of-nat } j)^{\wedge 2}) \neq$
 0
 $\langle \text{proof} \rangle$

lemma *hof-eq-diff*: $40 \text{ dvd } K \implies \text{hof } K = K - \text{Nof } K$
 $\langle \text{proof} \rangle$

lemma *field-cancel-aux*:
fixes $d\ c\ P :: \text{rat}$
assumes $d: d \neq 0$ **and** $c: c * c = 1$
shows $d * (P / (c * d^{\wedge 2})) * d = c * P$
 $\langle \text{proof} \rangle$

lemma *det-GB*:
assumes $40 \text{ dvd } K$
shows $\text{Determinant.det } (GB\ K) = (-1)^{\wedge (\text{hof } K * (\text{hof } K - 1) \text{ div } 2)} *$
 $(\prod j = \text{Nof } K + 1..K. \text{of-nat } j^{\wedge 4} * \text{poly } (Dm\ (\text{Nof } K))\ (-\ (\text{of-nat } j)^{\wedge$
 $2))^{\wedge 5})$
 $\langle \text{proof} \rangle$

(2.9): Δ - K has degree h and leading coefficient $(-1)^{\wedge \{h(h-1)/2\}} \prod \{-j=N+1\}^{\wedge K}$
 $j^{\wedge 4} D-N(-j^{\wedge 2})^{\wedge 5}$. The X -part of G - K is $V^{\wedge T} \text{diag}(w)\ V$ with V Vander-
monde.

theorem *Delta-degree-lead-coeff*:
assumes $40 \text{ dvd } K$
shows $\text{degree } (\text{DeltaK } K) = \text{hof } K \wedge$
 $\text{lead-coeff } (\text{DeltaK } K) = (-1)^{\wedge (\text{hof } K * (\text{hof } K - 1) \text{ div } 2)} *$
 $(\prod j = \text{Nof } K + 1..K. \text{of-nat } j^{\wedge 4} * \text{poly } (Dm\ (\text{Nof } K))\ (-\ (\text{of-nat } j)^{\wedge$
 $2))^{\wedge 5})$
 $\langle \text{proof} \rangle$

lemma *SK-pos*: $0 < SK\ K$
 $\langle \text{proof} \rangle$

23.2 Proposition 2.2: the positive integral representation

lemma *weight-summable*:
assumes $0 < y$
shows $\text{summable } (\lambda l. \text{real } (l + 1)^{\wedge 4} * \exp (-\ 2 * \pi i * \text{real } (l + 1) * y))$
 $\langle \text{proof} \rangle$

The weight is positive on $(0, \infty)$.

theorem *weight-pos*: $0 < y \implies 0 < \text{weight } y$

<proof>

lemma *weight-eq*: $\text{weight } y = (2 * \pi i)^4 * y^5 / 12 * (\sum l. \text{real } (l + 1)^4 * \exp(-2 * \pi i * \text{real } (l + 1) * y))$
<proof>

$\int_{-\infty}^{\infty} w(y)/(y^2 + a^2) dy = 1/(2a) - 1/4 + a^4 \sum_{n \geq 0} (a + n + 1)^{-5}$.

lemma *pole*:

assumes $0 < a$ $(\lambda n. 1 / (a + (\text{real } n + 1))^5)$ *sums* Z

shows *set-integrable lborel* $\{0 < ..\}$ $(\lambda y. \text{weight } y / (y^2 + a^2)) \wedge$
set-lebesgue-integral lborel $\{0 < ..\}$ $(\lambda y. \text{weight } y / (y^2 + a^2)) =$
 $1 / (2 * a) - 1 / 4 + a^4 * Z$

<proof>

23.3 Moments and the pole values

lemma *re-map-add*: $\text{map-poly } (\text{of-rat} :: \text{rat} \Rightarrow \text{real}) (P + Q) =$
 $\text{map-poly of-rat } P + \text{map-poly of-rat } Q$
<proof>

lemma *re-map-diff*: $\text{map-poly } (\text{of-rat} :: \text{rat} \Rightarrow \text{real}) (P - Q) =$
 $\text{map-poly of-rat } P - \text{map-poly of-rat } Q$
<proof>

lemma *re-map-mult*: $\text{map-poly } (\text{of-rat} :: \text{rat} \Rightarrow \text{real}) (P * Q) =$
 $\text{map-poly of-rat } P * \text{map-poly of-rat } Q$
<proof>

lemma *real-eval-add*: $\text{real-eval } (P + Q) x = \text{real-eval } P x + \text{real-eval } Q x$
<proof>

lemma *real-eval-diff*: $\text{real-eval } (P - Q) x = \text{real-eval } P x - \text{real-eval } Q x$
<proof>

lemma *real-eval-mult*: $\text{real-eval } (P * Q) x = \text{real-eval } P x * \text{real-eval } Q x$
<proof>

lemma *real-eval-const*: $\text{real-eval } [:c:] x = \text{of-rat } c$
<proof>

lemma *real-eval-zero*: $\text{real-eval } 0 x = 0$
<proof>

lemma *real-eval-one*: $\text{real-eval } 1 x = 1$
<proof>

lemma *real-eval-pX*: $\text{real-eval } pX x = x$

<proof>

lemma *real-eval-monom*: *real-eval* (*Polynomial.monom* *c n*) *x* = *of-rat* *c* * *x* ^{*n*}
<proof>

lemma *real-eval-smult*: *real-eval* (*Polynomial.smult* *c P*) *x* = *of-rat* *c* * *real-eval* *P x*
<proof>

lemma *real-eval-sum*: *real-eval* ($\sum i \in I. f\ i$) *x* = ($\sum i \in I. \text{real-eval } (f\ i)\ x$)
<proof>

lemma *real-eval-prod*: *real-eval* ($\prod i \in I. f\ i$) *x* = ($\prod i \in I. \text{real-eval } (f\ i)\ x$)
<proof>

lemma *real-eval-power*: *real-eval* (*P* ^{*n*}) *x* = *real-eval* *P x* ^{*n*}
<proof>

lemmas *real-eval-simps* = *real-eval-add* *real-eval-diff* *real-eval-mult* *real-eval-const* *real-eval-pX*
real-eval-monom
real-eval-smult *real-eval-sum* *real-eval-prod* *real-eval-power* *real-eval-zero* *real-eval-one*

lemma *val2-aux*:
fixes *W Q P F a s B* :: *real*
assumes *W* $\neq 0$ *Q* $\neq 0$ *P* $\neq 0$ *F* $\neq 0$
shows *W* / 12 * (*a* * *F*) / (*W* * (2 * *Q* * *P*)) * (*s* * *Q* * *P* * *B* / *F*) = *s* * *B*
 * *a* / 24
<proof>

lemma *moment-term*:
 (2 * *pi*) ⁴ / 12 * *real* (*l* + 1) ⁴ * (*y* ^(2 * *e* + 5) * *exp* (− ((2 * *pi* * *real* (*l* + 1)) *
y))) =
 (*y* ^(2 * *e*) * ((2 * *pi*) ⁴ * *y* ⁵ / 12)) * (*real* (*l* + 1) ⁴ * *exp* (− 2 * *pi*
 * *real* (*l* + 1) *
y))
<proof>

Moments: $\int_{-\infty}^{\infty} y^{2e} w(y) dy = \mu(t^e)$ (Euler's formula for $\zeta(2e+2)$:
Zeta-Function.zeta-even-nat; Gamma integrals: *Gamma-integral-real*).

lemma *moment*:
set-integrable lborel {0<..<} ($\lambda y. y^{(2 * e)} * \text{weight } y$) $\wedge$
set-lebesgue-integral lborel {0<..<} ($\lambda y. y^{(2 * e)} * \text{weight } y$) = *of-rat* (*muMono*
e)
<proof>

Polynomial part: $\int_{-\infty}^{\infty} A(y^2) w(y) dy = \mu(A)$.

lemma *poly-moment*:

set-integrable lborel $\{0 < ..\}$ $(\lambda y. \text{real-eval } A (y^2) * \text{weight } y) \wedge$
set-lebesgue-integral lborel $\{0 < ..\}$ $(\lambda y. \text{real-eval } A (y^2) * \text{weight } y) =$
of-rat $(\text{muPoly } A)$
 $\langle \text{proof} \rangle$

Pole part: $\int_{-\infty}^{\infty} w(y)/(y^2 + j^2) dy = j^4(\zeta(5) - H-j) - 1/4 + 1/(2j)$,
via the symmetry $c^4\Phi(a,c) = a^4\Phi(c,a)$ of $\Phi(a,c) = \int y^5 e^{-cy}/(y^2+a^2) dy$ (Fubini) and *coth-series*.

$\zeta(5) = \sum_{n \geq 1} n^{-5}$ as a real series, and its tails $\zeta(5) - H-j = \sum_{n \geq 0} (j + n + 1)^{-5}$.

lemma *zeta5-sums*: $(\lambda n. 1 / (\text{real } n + 1)^5) \text{ sums } \text{zeta5}$
 $\langle \text{proof} \rangle$

lemma *H5-eq-sum*: $\text{of-rat } (H5 \ j) = (\sum_{i < j} 1 / (\text{real } i + 1)^5)$
 $\langle \text{proof} \rangle$

lemma *zeta-tail*: $(\lambda n. 1 / (\text{real } j + (\text{real } n + 1))^5) \text{ sums } (\text{zeta5} - \text{of-rat } (H5 \ j))$
 $\langle \text{proof} \rangle$

lemma *pole-val*:

$j \neq 0 \implies$
set-integrable lborel $\{0 < ..\}$ $(\lambda y. \text{weight } y / (y^2 + \text{real } j^2)) \wedge$
set-lebesgue-integral lborel $\{0 < ..\}$ $(\lambda y. \text{weight } y / (y^2 + \text{real } j^2)) =$
real-eval $(\text{muPole } j) \ \text{zeta5}$
 $\langle \text{proof} \rangle$

lemma *real-eval-sqPoleProd-pos*:

assumes *finite* S $0 \notin S$ $0 \leq t$
shows $0 < \text{real-eval } (\text{sqPoleProd } S) \ t$
 $\langle \text{proof} \rangle$

Partial fractions for $P(t)/\prod_{j \in S} (t + j^2)$ at real $t \geq 0$.

lemma *partial-fractions-real*:

assumes *finite* S $0 \notin S$ $0 \leq t$
shows $\text{real-eval } P \ t / \text{real-eval } (\text{sqPoleProd } S) \ t =$
 $\text{real-eval } (P \ \text{div} \ \text{sqPoleProd } S) \ t + (\sum_{j \in S} \text{of-rat } (\text{sqResidue } S \ P \ j) / (t + \text{real } j^2))$
 $\langle \text{proof} \rangle$

lemma *rat-decomp*:

assumes *finite* S $0 \notin S$
shows $\text{real-eval } P \ (y^2) / \text{real-eval } (\text{sqPoleProd } S) \ (y^2) * \text{weight } y =$
 $\text{real-eval } (P \ \text{div} \ \text{sqPoleProd } S) \ (y^2) * \text{weight } y + (\sum_{j \in S} \text{of-rat } (\text{sqResidue } S \ P \ j) * (\text{weight } y / (y^2 + \text{real } j^2)))$
 $\langle \text{proof} \rangle$

lemma *rat-integrable*:

assumes *finite S* $0 \notin S$

shows *set-integrable lborel* $\{0 < ..\}$ $(\lambda y. \text{real-eval } P (y \wedge 2) /$
 $\text{real-eval } (\text{sqPoleProd } S) (y \wedge 2) * \text{weight } y)$

<proof>

Proposition 2.2, (2.10): $\mu\{\zeta(5)\}(R) = \int_{-\infty}^{\infty} R(y^2) w(y) dy$ for every R in the domain.

theorem *muX-zeta5-integral*:

assumes *S: finite S and S0: 0 ∉ S*

shows *real-eval (muX S P) zeta5 =*
 $\text{set-lebesgue-integral lborel } \{0 < ..\}$
 $(\lambda y. \text{real-eval } P (y \wedge 2) / \text{real-eval } (\text{sqPoleProd } S) (y \wedge 2) * \text{weight } y)$

<proof>

Proposition 2.2: $G\text{-}K(\zeta(5))$ is positive definite (stated with coefficient vectors).

theorem *G-zeta5-posdef*:

assumes *c: ∃ i < hof K. c i ≠ 0*

shows $0 < (\sum i < \text{hof } K. \sum j < \text{hof } K. c i * \text{real-eval } (GK K \$\$ (i, j)) \text{ zeta5}$
 $* c j)$

<proof>

Consequence: $\Delta\text{-}K(\zeta(5)) > 0$ (positive definite $\Rightarrow$ positive determinant; alternatively from Andreief with a positive integrand).

lemma *real-eval-hom: comm-ring-hom* $(\lambda P. \text{real-eval } P x)$

<proof>

theorem *Delta-zeta5-pos-aux: 0 < real-eval (DeltaK K) zeta5*

<proof>

theorem *Delta-zeta5-pos: 0 < real-eval (DeltaK K) zeta5*

<proof>

end

theory *Zeta5-Exact-Constants*

imports *Zeta5-Definitions*

begin

24 Exact rational constants

Appendix B of the paper: the exact rational values of A^* , A_M and the margins in (7.2), by rational arithmetic (Lean theory *AppendixB*).

lemma *Hc-eq: Hc-q = 23 / 20* *<proof>*

The cancellation of the quadratic coefficient of R (Appendix B.1).

lemma *quadratic-cancellation*:

$$2 * \text{lam-q} - 12 * \text{lam-q} * \text{alpha-q} + 2 * (\text{Hc-q}^2 - \text{Hc-q} - \text{lam-q}^2) - 18 \\ * \text{alpha-q}^2 + 6 * \\ \text{alpha-q} = 0 \text{ \langle proof \rangle}$$

lemma *lam-M0*: $\text{lam-q} * \text{M0c} = -49173 / 8000$ *\langle proof \rangle*

$$(5.19): A* = I\text{-out} + \int_3^{\{20\}} R/x^3 - 2689/48000.$$

lemma *Astar-eq*: $A\text{star} = I\text{out} + 322437603634266857629 / 7535670527041937280000$
 $- 2689 / 48000$
\langle proof \rangle

lemma *A200-eq*: $AM\ 200 = 127125602969131786927559 / 94195881588024216000000$
\langle proof \rangle

lemma *A100000-eq*: $AM\ 100000 = 7756864096839411316755964319057 / 58872425992515135000000000000000$
\langle proof \rangle

$$(7.2), M = 200: -1600(A_2\text{-}0\text{-}0 + U\text{bar}) > 139/5, \text{ with the exact margin.}$$

lemma *margin-200*:

$$-1600 * (AM\ 200 + U\text{bar}) - 139 / 5 = 3089837638249482469 / 58872425992515135000 \\ \wedge \\ 139 / 5 < -1600 * (AM\ 200 + U\text{bar}) \text{ \langle proof \rangle}$$

$$(7.2), M = 100000: -1600(A\text{-}1\text{-}0\text{-}0\text{-}0\text{-}0 + U\text{bar}) > 7907/100.$$

lemma *margin-100000*:

$$-1600 * (AM\ 100000 + U\text{bar}) - 7907 / 100 = \\ 29873543950273155160680943 / 3679526624532195937500000000 \wedge \\ 7907 / 100 < -1600 * (AM\ 100000 + U\text{bar}) \text{ \langle proof \rangle}$$

$$(6.4): U\text{bar} < -136699/100000.$$

lemma *U-lt*: $U\text{bar} < -136699 / 100000$ *\langle proof \rangle*

end

theory *Zeta5-Uniform-Asymptotics*

imports *Zeta5-Inner-Range Piecewise-Interval-Integrals*

begin

25 The uniform estimate (5.7) in the inner range

For fixed $M \geq 40$, $\gamma_p^{in} = p \Gamma(K/p) + O_M(1)$ and $v_p(S_K) = p N(K/p) + O_M(1)$ uniformly over the range (4.1), with the explicit constant $1000 M^2$ (*gammaIn-uniform-estimate*). Floors and $v_p(S_K)$, a Riemann-sum identity for the z -integral, exact class counts and the discrete decomposition of γ_p^{in} ; everything else is integer arithmetic. Lean theory *Uniform57*.

25.1 Floors and $v\text{-}p(S\text{-}K)$ in the inner range

lemma *floor-nat-div*: $\text{floor } (\text{real } n / \text{real } d) = \text{int } (n \text{ div } d)$
 $\langle \text{proof} \rangle$

Legendre with a single term: $v\text{-}p(n!) = \lfloor n/p \rfloor$ for $n < p^2$.

lemma *multiplicity-fact-small*:
assumes *prime* p $n < p^2$
shows *multiplicity* p (*fact* n) = $n \text{ div } p$
 $\langle \text{proof} \rangle$

Under (4.1) all factorial arguments are $< p^2$ (*innerHyp-bounds*: $5K < p^2$).

lemma *vpS-inner*:
assumes p : *prime* p **and** h : *InnerHyp* K M p
shows vpS K $p = 2 * \text{int } (\text{hof } K) * \text{int } (K \text{ div } p) - 12 * \text{int } (\text{hof } K) * \text{int } (Nof$
 $K \text{ div } p)$
 $- 2 * \text{int } (\sum i = 1..hof K - 1. 2 * i \text{ div } p)$
 $\langle \text{proof} \rangle$

$G_4(n) = 4 \text{ t } n - p \text{ t } (t + 1)$, $t = \lfloor 2n/p \rfloor$; $G_4(n)/4 = p \text{ J}(n/p)$.

definition $G_4 :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{int}$ **where**
 G_4 p $n = 4 * \text{int } (2 * n \text{ div } p) * \text{int } n - \text{int } p * \text{int } (2 * n \text{ div } p) * (\text{int } (2 * n$
 $\text{div } p) + 1)$

lemma *G4-step*:
assumes $2 \leq p$
shows $0 \leq G_4$ p $(n + 1) - G_4$ p $n - 4 * \text{int } (2 * n \text{ div } p) \wedge$
 G_4 p $(n + 1) - G_4$ p $n - 4 * \text{int } (2 * n \text{ div } p) \leq$
 $4 * (\text{int } (2 * (n + 1) \text{ div } p) - \text{int } (2 * n \text{ div } p))$
 $\langle \text{proof} \rangle$

lemma *G4-tele*:
assumes $2 \leq p$
shows $0 \leq G_4$ p $n - 4 * (\sum i < n. \text{int } (2 * i \text{ div } p)) \wedge$
 G_4 p $n - 4 * (\sum i < n. \text{int } (2 * i \text{ div } p)) \leq 4 * \text{int } (2 * n \text{ div } p)$
 $\langle \text{proof} \rangle$

lemma *sum-Icc-eq-range*: f $0 = (0 :: \text{int}) \implies 1 \leq (h :: \text{nat}) \implies$
 $(\sum i = 1..h - 1. f i) = (\sum i < h. f i)$
 $\langle \text{proof} \rangle$

$v\text{-}p(S\text{-}K) - p \text{ N}(K/p) = (G_4(h) - 4 \sum_{i < h} \lfloor 2i/p \rfloor)/2$ ($K = 40n$:
 $\lambda K/p = h/p$, $\alpha K/p = N/p$ exactly).

lemma *vpS-sub*:
assumes p : *prime* p **and** h : *InnerHyp* K M p
shows $of\text{-int } (vpS$ K $p) - \text{real } p * Nfun\text{-r } (\text{real } K / \text{real } p)$
 $= of\text{-int } (G_4$ p $(hof$ $K) - 4 * (\sum i < hof$ $K. \text{int } (2 * i \text{ div } p))) / 2$
 $\langle \text{proof} \rangle$

lemma *vpS-bound*:

assumes p : prime p **and** h : InnerHyp K M p
shows $|of-int (vpS K p) - real p * Nfun-r (real K / real p)| \leq 4 * real M$
 $\langle proof \rangle$

25.2 The Riemann-sum identity for the z -integral

lemma *floor-between*:

assumes $0 < p$ $of-int j / real p < y$ $y < (of-int j + 1) / real p$
shows $floor y = j \div int p$
 $\langle proof \rangle$

l on the a -th grid cell $(a/p, (a+1)/p)$.

definition $ellZ :: nat \Rightarrow nat \Rightarrow nat \Rightarrow int$ **where**

$ellZ p A a = (int A - int a - 1) \div int p + (int A + int a) \div int p + 1$

definition $gg :: int \Rightarrow int \Rightarrow int \Rightarrow int$ **where**

$gg T v l = (T - 3 * v) * (T + 3 * v - l - 5)$

lemma *ell-on-cell*:

assumes $0 < p$ $real a / real p < z$ $z < (real a + 1) / real p$
shows $ell-r (real A / real p) z = of-int (ellZ p A a)$
 $\langle proof \rangle$

definition $phiZ :: nat \Rightarrow nat \Rightarrow nat \Rightarrow int \Rightarrow real$

$\Rightarrow real$ **where**

$phiZ p N K T z = (of-int T - 3 * ell-r (real N / real p) z) * (of-int T + 3 * ell-r (real N / real p) z - ell-r (real K / real p) z - 5)$

lemma *phi-on-cell*:

assumes $0 < p$ $real a / real p < z$ $z < (real a + 1) / real p$
shows $phiZ p N K T z = of-int (gg T (ellZ p N a) (ellZ p K a))$
 $\langle proof \rangle$

lemma *integral-cell*:

assumes $0 < p$ $real a / real p \leq c$ $c \leq (real a + 1) / real p$
shows $interval-lebesgue-integrable lborel (ereal (real a / real p)) (ereal c) (phiZ p N K T) \wedge$
 $interval-lebesgue-integral lborel (ereal (real a / real p)) (ereal c) (phiZ p N K T)$
 $= (c - real a / real p) * of-int (gg T (ellZ p N a) (ellZ p K a))$
 $\langle proof \rangle$

$p \int -0^{1/2} \varphi = \sum -\{a < m\} gg(a) + gg(m)/2$ for $p = 2m + 1$.

lemma *integral-sum*:

assumes pm : $p = 2 * m + 1$

shows $\text{real } p * \text{interval-lebesgue-integral lborel } (\text{ereal } 0) (\text{ereal } (1 / 2)) (\text{phiZ } p$
 $N \ K \ T)$
 $= (\sum a < m. \text{of-int } (gg \ T \ (\text{ellZ } p \ N \ a) \ (\text{ellZ } p \ K \ a))) +$
 $\text{of-int } (gg \ T \ (\text{ellZ } p \ N \ m) \ (\text{ellZ } p \ K \ m)) / 2$
 $\langle \text{proof} \rangle$

25.3 Exact class counts

lemma *count-mod-eq*:
assumes $0 < p \ 1 \leq r \ r < p$
shows $\text{card } \{j \in \{1..A\}. j \bmod p = r\} = (A + p - r) \text{ div } p$
 $\langle \text{proof} \rangle$

lemma *ell-exact*:
assumes $\text{odd } p \ 1 \leq a \ a \leq m\text{Half } p$
shows $\text{ell } p \ A \ a = (A + p - a) \text{ div } p + (A + a) \text{ div } p$
 $\langle \text{proof} \rangle$

lemma *ell-succ-eq*:
assumes $\text{odd } p \ a + 1 \leq m\text{Half } p$
shows $\text{int } (\text{ell } p \ A \ (a + 1)) = \text{ellZ } p \ A \ a + ((\text{int } A + \text{int } a + 1) \text{ div } \text{int } p -$
 $(\text{int } A +$
 $\text{int } a) \text{ div } \text{int } p)$
 $\langle \text{proof} \rangle$

lemma *sum-disc*:
assumes $0 < p \ m < p$
shows $(\sum a < m. ((\text{int } A + \text{int } a + 1) \text{ div } \text{int } p - (\text{int } A + \text{int } a) \text{ div } \text{int } p))$
 ≤ 1
and $0 \leq (\text{int } A + \text{int } a + 1) \text{ div } \text{int } p - (\text{int } A + \text{int } a) \text{ div } \text{int } p$
 $\langle \text{proof} \rangle$

lemma *ell-cases*:
assumes $\text{odd } p \ 1 \leq a \ a \leq m\text{Half } p$
shows $\text{ell } p \ A \ a = 2 * A \text{ div } p \vee \text{ell } p \ A \ a = 2 * A \text{ div } p + 1$
 $\langle \text{proof} \rangle$

lemma *card-inter-of-chain*: $P \subseteq Q \vee Q \subseteq P \implies$
 $\text{finite } P \implies \text{finite } Q \implies \text{card } (P \cap Q) = \min (\text{card } P) (\text{card } Q)$
 $\langle \text{proof} \rangle$

lemma *sum-two-lin*: $(\sum i < L. 2 * (\text{of-nat } i + c)) =$
 $\text{of-nat } L * (\text{of-nat } L - 1) + 2 * \text{of-nat } L * (c :: \text{rat})$
 $\langle \text{proof} \rangle$

25.4 The discrete decomposition of $\gamma\text{-}p\hat{in}$

The number of classes with $l\text{-}K(a) = q + 1$, $q = \lfloor 2K/p \rfloor$.

definition $c1 :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat}$ **where**

$$c1\ K\ p = \text{card } \{a \in \{1..mHalf\ p\}. \text{ell } p\ K\ a = 2 * K\ \text{div } p + 1\}$$

lemma *sum-ellK*:

assumes *p*: prime *p* **and** *h*: InnerHyp *K M p*
shows $(\sum a = 1..mHalf\ p. \text{ell } p\ K\ a) = mHalf\ p * (2 * K\ \text{div } p) + c1\ K\ p$
 $\langle proof \rangle$

lemma *sum-ellK'*:

assumes *p*: prime *p* **and** *h*: InnerHyp *K M p*
shows $(\sum a = 1..mHalf\ p. \text{ell } p\ K\ a) = K - K\ \text{div } p$
 $\langle proof \rangle$

lemma *c1-le*: $c1\ K\ p \leq mHalf\ p$
 $\langle proof \rangle$

$\varepsilon\text{-}a \in \{0, 1\}$, and $\varepsilon\text{-}a = 1$ exactly when the rank of *a* is $< E$.

lemma *eps-cases*: $\text{epsIn } K\ M\ p\ a = 0 \vee \text{epsIn } K\ M\ p\ a = 1$
 $\langle proof \rangle$

lemma *eps-iff*:

assumes *p*: prime *p* **and** *h*: InnerHyp *K M p* **and** *a*: $a \in \{1..mHalf\ p\}$
shows $\text{epsIn } K\ M\ p\ a = 1 \iff \text{int } (\text{defaultPos } K\ p\ a) < \text{Ein } K\ M\ p$
 $\langle proof \rangle$

lemma *defaultPos-lt*:

assumes $a \in \{1..mHalf\ p\}$ $c \in \{1..mHalf\ p\}$ $\text{ell } p\ K\ c < \text{ell } p\ K\ a$
shows $\text{defaultPos } K\ p\ a < \text{defaultPos } K\ p\ c$
 $\langle proof \rangle$

$\sum -a\ \varepsilon\text{-}a\ l\text{-}K(a) = q\ E + \min(E, c\text{-}1)$: the classes with $\varepsilon = 1$ and those with $l\text{-}K = q + 1$ form a chain.

lemma *sum-if-const*: $\text{finite } A \implies B \subseteq A \implies$

$$(\sum x \in A. \text{if } x \in B \text{ then } c \text{ else } 0) = \text{int } (\text{card } B) * (c :: \text{int})$$

$\langle proof \rangle$

lemma *sum-eps-ell*:

assumes *p*: prime *p* **and** *h*: InnerHyp *K M p*
shows $(\sum a = 1..mHalf\ p. \text{epsIn } K\ M\ p\ a * \text{int } (\text{ell } p\ K\ a)) =$
 $\text{int } (2 * K\ \text{div } p) * \text{Ein } K\ M\ p + \min (\text{Ein } K\ M\ p) (\text{int } (c1\ K\ p))$
 $\langle proof \rangle$

The sum over the rows of class $a \geq 1$.

lemma *class-sum*:

assumes *p*: prime *p* **and** *h*: InnerHyp *K M p* **and** *a*: $a \in \{1..mHalf\ p\}$
shows $(\sum i < \text{nat } (\text{Lin } K\ M\ p\ a). 2 * wIn\ K\ M\ p\ a\ i)$
 $= \text{of-int } (\text{gg } (\text{Tin } K\ M\ p) (\text{int } (\text{ell } p\ (\text{Nof } K)\ a)) (\text{int } (\text{ell } p\ K\ a)) + \text{epsIn}$
 $K\ M\ p\ a * (2 * \text{Tin } K\ M\ p - \text{int } (\text{ell } p\ K\ a) - 4))$
 $\langle proof \rangle$

definition $Sd :: nat \Rightarrow nat \Rightarrow int \Rightarrow int$ **where**

$Sd\ K\ p\ T = (\sum\ a = 1..mHalf\ p.\ gg\ T\ (int\ (ell\ p\ (Nof\ K)\ a))\ (int\ (ell\ p\ K\ a)))$

$\gamma\text{-}in = 2\ \sum\ \{i < 4M+10\}\ w\text{-}\{0,i\} + [S\text{-}d(T) + E\ (2T - q - 4) - \min(E, c-1)]$.

lemma *gamma-decomp*:

assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$

shows $gammaIn\ K\ M\ p = 2 * (\sum\ i < 4 * M + 10.\ wIn\ K\ M\ p\ 0\ i)$
 $+ of\text{-}int\ (Sd\ K\ p\ (Tin\ K\ M\ p) + Ein\ K\ M\ p * (2 * Tin\ K\ M\ p - int\ (2$
 $* K\ div\ p) - 4) -$
 $\min\ (Ein\ K\ M\ p)\ (int\ (c1\ K\ p)))$

$\langle proof \rangle$

lemma *Tin-ge*:

assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$

shows $-1 \leq Tin\ K\ M\ p$

$\langle proof \rangle$

lemma *w0-bound*:

assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$ **and** i : $i < 4 * M + 10$

shows $|wIn\ K\ M\ p\ 0\ i| \leq 15 * of\text{-}nat\ M$

$\langle proof \rangle$

lemma *Z0-bound*:

assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$

shows $|2 * (\sum\ i < 4 * M + 10.\ wIn\ K\ M\ p\ 0\ i)| \leq 150 * of\text{-}nat\ M \wedge 2$

$\langle proof \rangle$

$p\ \Gamma(K/p)$ in terms of the z -integral of ϕiZ at $T\text{-}f = \lfloor 2H\text{-}c\ K/p \rfloor$.

lemma *Gam-eq*:

assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$

defines $Tf \equiv floor\ (2 * Hc\text{-}r * (real\ K / real\ p))$

and $s \equiv Hc\text{-}r * (real\ K / real\ p) - of\text{-}int\ (floor\ (2 * Hc\text{-}r * (real\ K / real\ p)))$
 $/\ 2$

shows $real\ p * Gam\text{-}r\ (real\ K / real\ p)$
 $= real\ p * interval\text{-}lebesgue\text{-}integral\ lborel\ (ereal\ 0)\ (ereal\ (1 /$
 $2))\ (\phi iZ\ p\ (Nof\ K)\ K\ Tf)$
 $+ real\ p * s * (2 * of\text{-}int\ Tf - real\ (2 * K\ div\ p) - 4)$
 $- \min\ (real\ p * s)\ (real\ K - real\ p * real\ (2 * K\ div\ p) / 2)$

$\langle proof \rangle$

25.5 Discrete sum versus the integral

lemma *sum-Icc-shift*: $(\sum\ a = 1..m.\ f\ a) = (\sum\ a < (m :: nat).\ f\ (a + 1))$

$\langle proof \rangle$

lemma *ellZ-bounds*:

assumes $0 < p\ a < p$

shows $0 \leq \text{ellZ } p \ A \ a \wedge \text{ellZ } p \ A \ a \leq 2 * \text{int } (A \ \text{div } p) + 2$
 $\langle \text{proof} \rangle$

lemma *disc-01*:

assumes $0 < p$
shows $(\text{int } A + \text{int } a + 1) \ \text{div } \text{int } p - (\text{int } A + \text{int } a) \ \text{div } \text{int } p = 0 \vee$
 $(\text{int } A + \text{int } a + 1) \ \text{div } \text{int } p - (\text{int } A + \text{int } a) \ \text{div } \text{int } p = 1$
 $\langle \text{proof} \rangle$

lemma *gg-lip*:

assumes $40 \leq M - 2 \leq T \ T \leq 4 * \text{int } M + 1 \ 0 \leq v \ v \leq$
 $2 * \text{int } M \ 0 \leq l \ l \leq 2 * \text{int } M$
 $dv = 0 \vee dv = 1 \ dl = 0 \vee dl = 1$
shows $|\text{gg } T \ (v + dv) \ (l + dl) - \text{gg } T \ v \ l| \leq 100 * \text{int } M * (dv + dl)$
 $\langle \text{proof} \rangle$

lemma *gg-bound*:

assumes $40 \leq M - 2 \leq T \ T \leq 4 * \text{int } M + 1 \ 0 \leq v \ v \leq$
 $2 * \text{int } M \ 0 \leq l \ l \leq 2 * \text{int } M$
shows $|\text{gg } T \ v \ l| \leq 150 * \text{int } M \wedge 2$
 $\langle \text{proof} \rangle$

$|S\text{-}d(T) - p \int -0 \sim \{1/2\} \ \varphi \cdot T| \leq 100 \ M \wedge 2$: per-cell comparison plus the last half cell.

lemma *S-vs-I*:

assumes p : *prime* p **and** h : *InnerHyp* $K \ M \ p$ **and** T : $-2 \leq T \ T \leq 4 * \text{int } M + 1$
shows $|\text{of-int } (Sd \ K \ p \ T) - \text{real } p * \text{interval-lebesgue-integral lborel } (\text{ereal } 0) (\text{ereal } (1 /$
 $2)) (\text{phiZ } p \ (\text{Nof } K) \ K \ T)| \leq 100 * \text{real } M \wedge 2$
 $\langle \text{proof} \rangle$

25.6 The comparison functions

definition $Dd :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{int} \Rightarrow \text{real} \Rightarrow \text{real}$

where
 $Dd \ K \ p \ T \ E = \text{of-int } (Sd \ K \ p \ T) + E * (2 * \text{of-int } T - \text{real } (2 * K \ \text{div } p) -$
 $4) -$
 $\min E \ (\text{real } (c1 \ K \ p))$

definition $Cc :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{int} \Rightarrow \text{real} \Rightarrow \text{real}$

where
 $Cc \ K \ p \ T \ \sigma = \text{real } p * \text{interval-lebesgue-integral lborel } (\text{ereal } 0) (\text{ereal } (1 /$
 $2)) (\text{phiZ } p \ (\text{Nof } K) \ K \ T)$
 $+ \sigma * (2 * \text{of-int } T - \text{real } (2 * K \ \text{div } p) - 4) - \min \sigma \ (\text{real } K -$
 $\text{real } p * \text{real } (2 * K \ \text{div } p) / 2)$

lemma *Dd-trans*:

assumes p : *prime* p **and** h : *InnerHyp* $K \ M \ p$

shows $Dd\ K\ p\ T\ (real\ (mHalf\ p)) = Dd\ K\ p\ (T + 1)\ 0$
 $\langle proof \rangle$

lemma *q-le*:
assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$
shows $2 * K\ div\ p \leq 2 * M$
 $\langle proof \rangle$

lemma *slope-bound*:
assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$ **and** T : $-2 \leq T\ T \leq 4 * int\ M + 1$
shows $|2 * of-int\ T - real\ (2 * K\ div\ p) - 4| \leq 11 * real\ M$
 $\langle proof \rangle$

lemma *Dd-lip*:
assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$ **and** T : $-2 \leq T\ T \leq 4 * int\ M + 1$
shows $|Dd\ K\ p\ T\ E1 - Dd\ K\ p\ T\ E2| \leq |E1 - E2| * (11 * real\ M + 1)$
 $\langle proof \rangle$

lemma *c1-close*:
assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$
shows $|real\ (c1\ K\ p) - (real\ K - real\ p * real\ (2 * K\ div\ p) / 2)| \leq 1$
 $\langle proof \rangle$

lemma *Dd-Cc*:
assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$ **and** T : $-2 \leq T\ T \leq 4 * int\ M + 1$
shows $|Dd\ K\ p\ T\ E - Cc\ K\ p\ T\ \sigma| \leq 100 * real\ M \wedge 2 + |E - \sigma| * (11 * real\ M + 1) + 1$
 $\langle proof \rangle$

25.7 Assembly

lemma *gamma-real*:
assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$
shows $of-rat\ (gammaIn\ K\ M\ p) = of-rat\ (2 * (\sum\ i < 4 * M + 10.\ wIn\ K\ M\ p\ 0\ i)) + Dd\ K\ p\ (Tin\ K\ M\ p)\ (of-int\ (Ein\ K\ M\ p))$
 $\langle proof \rangle$

The fill relation: $mT + E = m \cdot 2H-c\ K/p + \Delta$ with $|\Delta| \leq 8M$.

lemma *fill-rel*:
assumes p : *prime* p **and** h : *InnerHyp* $K\ M\ p$
shows $|(real\ (mHalf\ p) * of-int\ (Tin\ K\ M\ p) + of-int\ (Ein\ K\ M\ p)) - real\ (mHalf\ p) * (2 * Hc-r * (real\ K / real\ p))| \leq 8 * real\ M$
 $\langle proof \rangle$

lemma *m-large*:

assumes p : prime p **and** h : InnerHyp K M p
shows $100 * \text{real } M \leq \text{real } (m\text{Half } p)$
 $\langle \text{proof} \rangle$

$|\gamma\text{-in} - p \Gamma(K/p)| \leq 1000 M^2$: $T\text{-f} \in \{T - 1, T, T + 1\}$ and three cases.

theorem *gamma-bound*:

assumes p : prime p **and** h : InnerHyp K M p
shows $|\text{of-rat } (\text{gammaIn } K \text{ } M \text{ } p) - \text{real } p * \text{Gam-r } (\text{real } K / \text{real } p)| \leq$
 $1000 * \text{real } M^2$
 $\langle \text{proof} \rangle$

Lemma 5.7 with $C(M) = 1000 M^2$.

theorem *gammaIn-uniform-estimate*:

assumes $40 \leq M$
shows $\exists Cst. \forall K \text{ } p. \text{prime } p \longrightarrow \text{InnerHyp } K \text{ } M \text{ } p \longrightarrow$
 $|\text{of-rat } (\text{gammaIn } K \text{ } M \text{ } p) - \text{real } p * \text{Gam-r } (\text{real } K / \text{real } p)| \leq Cst \wedge$
 $|\text{of-int } (vpS \text{ } K \text{ } p) - \text{real } p * \text{Nfun-r } (\text{real } K / \text{real } p)| \leq Cst$
 $\langle \text{proof} \rangle$

end

theory *Zeta5-Explicit-Integrals*

imports *Zeta5-Definitions Piecewise-Interval-Integrals*
begin

26 The explicit integrals of Section 5

The closed form $R(x) = x F(x) + Q(x)$ with $-1/2 \leq Q \leq 13/8$ ((B.1), (5.13)), the exact integrals (5.10) and (5.18) as sums of affine pieces (the piece lemmas are generated from exact rational tables, mirroring the generated Lean files), the tails (5.14)–(5.17), and continuity of the limiting functions off a countable set. All integrals are *interval-lebesgue-integral* over *lborel*. Lean theories *Integrals5Base*, *Integrals5Gam*, *Integrals5*, *Integrals5Outer*, *Integrals5Inner*, *Integrals5Tail*, *RCont*.

26.1 The closed form $R(x) = x F(x) + Q(x)$ (B.1), (5.13)

definition *ind* :: $\text{real} \Rightarrow \text{real} \Rightarrow \text{real}$ **where** $\text{ind } p \text{ } z = (\text{if } p <$
 $z \text{ then } 1 \text{ else } 0)$

definition *d0* :: $\text{real} \Rightarrow \text{real}$ **where** $d0 \text{ } u = \min u (1 - u)$

definition *es* :: $\text{real} \Rightarrow \text{real}$ **where** $\text{es } u = (\text{if } u \leq 1 / 2 \text{ then } 1 \text{ else } -1)$

lemma *ind-of-lt*: $p < z \implies \text{ind } p \text{ } z = 1$ **and** *ind-of-le*: $z \leq p \implies$
 $\text{ind } p \text{ } z = 0$
 $\langle \text{proof} \rangle$

lemma *es-cases*: $(es\ u = 1 \wedge d0\ u = u) \vee (es\ u = -1 \wedge d0\ u = 1 - u)$
 $\langle proof \rangle$

lemma *d0-mem*: $0 \leq u \implies u \leq 1 \implies 0 \leq d0\ u \wedge$
 $d0\ u \leq 1 / 2$
 $\langle proof \rangle$

lemma *es-pm*: $es\ u = 1 \vee es\ u = -1$
 $\langle proof \rangle$

Integral over $(0, 1/2)$ of a product of two step functions with steps at p and q .

lemma *step3*:
fixes $h :: real \Rightarrow real$
assumes $p: 0 \leq p \leq 1 / 2$ **and** $q: 0 \leq q \leq 1 / 2$
and $H: \bigwedge z. z \in \{0 < .. < 1 / 2\} \implies z \neq p \implies$
 $z \neq q \implies$
 $h\ z = (a0 + a1 * ind\ q\ z) * (b0 + b1 * ind\ q\ z + b2 * ind\ p\ z)$
shows *interval-lebesgue-integral lborel* $(ereal\ 0)\ (ereal\ (1 / 2))\ h$
 $= a0 * b0 / 2 + (a0 * b1 + a1 * b0 + a1 * b1) * (1 / 2 - q) + a0 * b2 * (1 / 2 - p) +$
 $a1 * b2 * (1 / 2 - \max\ p\ q)$
 $\langle proof \rangle$

$l(y, z) = 2[y] + 1 - es\{y\} \cdot ind(d0\{y\}, z)$ for $z \in (0, 1/2)$, $z \neq d0\{y\}$.

lemma *ell-step*:
assumes $z: z \in \{0 < .. < 1 / 2\}$ **and** $zp: z \neq d0\ (frac\ y)$
shows *ell-r* $y\ z = 2 * of-int\ (floor\ y) + 1 - es\ (frac\ y) * ind\ (d0\ (frac\ y))\ z$
 $\langle proof \rangle$

The z -integral in Γ .

lemma *gam-int*:
interval-lebesgue-integral lborel $(ereal\ 0)\ (ereal\ (1 / 2))$
 $(\lambda z. (T - 3 * ell-r\ (alpha-r * x)\ z) * (T + 3 * ell-r\ (alpha-r * x)\ z - ell-r\ x\ z - 5))$
 $= (let\ p = d0\ (frac\ x); q = d0\ (frac\ (alpha-r * x));$
 $a0 = T - 3 * (2 * of-int\ (floor\ (alpha-r * x)) + 1); a1 = 3 * es\ (frac\ (alpha-r * x));$
 $b0 = T + 3 * (2 * of-int\ (floor\ (alpha-r * x)) + 1) - (2 * of-int\ (floor\ x) + 1) - 5;$
 $b1 = -3 * es\ (frac\ (alpha-r * x)); b2 = es\ (frac\ x)\ in$
 $a0 * b0 / 2 + (a0 * b1 + a1 * b0 + a1 * b1) * (1 / 2 - q) + a0 * b2 * (1 / 2 - p) + a1 * b2 * (1 / 2 - \max\ p\ q))$
 $\langle proof \rangle$

$Q = R - x\ F$, eq. (5.13) with (B.1); arguments $\{x\}, \{\alpha x\}, \{2H-c\ x\}, \{2x\}, \{2\lambda x\}$.

definition $Qc :: real \Rightarrow real \Rightarrow real \Rightarrow real \Rightarrow real$

$\Rightarrow real$ **where**

$$\begin{aligned} Qc\ f\ g\ \tau\ \sigma\ \eta &= 9 * (d0\ g * (1 - 2 * d0\ g)) \\ &\quad - 3 * (es\ f * es\ g * (d0\ f + d0\ g - \max\ (d0\ f)\ (d0\ g) - 2 * d0\ f * d0\ g)) \\ &\quad + ((\tau \wedge 2 - \sigma * \tau) / 2 - pos\text{-}r\ ((\tau - \sigma) / 2)) + (\eta - \\ &\quad \eta \wedge 2) / 2 \end{aligned}$$

definition $Fx :: real \Rightarrow real$ **where**

$$Fx\ x = 4 * lam\text{-}r + 2 * lam\text{-}r * frac\ x - 12 * lam\text{-}r * frac\ (alpha\text{-}r * x)$$

The polynomial identities behind the three remaining sign cases of *R-eq*, with the fractional parts, the *max* and the *pos-r* term as variables.

lemma *R-eq-alg2*:

fixes $x\ fx\ fa\ fh\ f2\ fl\ mx\ pp :: real$

shows $- ((2 * Hc\text{-}r * x - fh - 3 * (2 * (alpha\text{-}r * x - fa) + 1)) * (2 * Hc\text{-}r * x - fh + 3 * (2 * (alpha\text{-}r * x - fa) + 1) - (2 * (x - fx) + 1) - 5) / 2 + ((2 * Hc\text{-}r * x - fh - 3 * (2 * (alpha\text{-}r * x - fa) + 1)) * (- 3 * - 1) + 3 * - 1 * (2 * Hc\text{-}r * x - fh + 3 * (2 * (alpha\text{-}r * x - fa) + 1) - (2 * (x - fx) + 1) - 5) + 3 * - 1 * (- 3 * - 1)) * (1 / 2 - (1 - fa))) + (2 * Hc\text{-}r * x - fh - 3 * (2 * (alpha\text{-}r * x - fa) + 1)) * 1 * (1 / 2 - fx) + 3 * - 1 * 1 * (1 / 2 - mx) + (Hc\text{-}r * x - (2 * Hc\text{-}r * x - fh) / 2) * (2 * (2 * Hc\text{-}r * x - fh) - (2 * x - f2) - 5) + pp) - (2 * lam\text{-}r * x * (x - fx) - 12 * lam\text{-}r * x * (alpha\text{-}r * x - fa) - 2 * ((2 * (lam\text{-}r * x) - fl) * (lam\text{-}r * x) - (2 * (lam\text{-}r * x) - fl) * (2 * (lam\text{-}r * x) - fl + 1) / 4)) =$

$$\begin{aligned} &x * (4 * lam\text{-}r + 2 * lam\text{-}r * fx - 12 * lam\text{-}r * fa) + (9 * ((1 - fa) * (1 - 2 * (1 - fa))) - 3 * \\ &\quad (1 * - 1 * (fx + (1 - fa) - mx - 2 * fx * (1 - fa))) + (((fh)^2 - f2 * fh) / 2 - pp) + \\ &\quad (fl - (fl)^2) / 2) \end{aligned}$$

<proof>

lemma *R-eq-alg3*:

fixes $x\ fx\ fa\ fh\ f2\ fl\ mx\ pp :: real$

shows $- ((2 * Hc\text{-}r * x - fh - 3 * (2 * (alpha\text{-}r * x - fa) + 1)) * (2 * Hc\text{-}r * x - fh + 3 * (2 * (alpha\text{-}r * x - fa) + 1) - (2 * (x - fx) + 1) - 5) / 2 + ((2 * Hc\text{-}r * x - fh - 3 * (2 * (alpha\text{-}r * x - fa) + 1)) * (- 3 * 1) + 3 * 1 * (2 * Hc\text{-}r * x - fh + 3 * (2 * (alpha\text{-}r * x - fa) + 1) - (2 * (x - fx) + 1) - 5) + 3 * 1 * (- 3 * 1)) * (1 / 2 - fa) + (2 * Hc\text{-}r * x - fh - 3 * (2 * (alpha\text{-}r * x - fa) + 1)) * - 1 * (1 / 2 - (1 - fx)) + 3 * 1 * - 1 * (1 / 2 - mx) + (Hc\text{-}r * x - (2 * Hc\text{-}r * x - fh) / 2) * (2 * (2 * Hc\text{-}r * x - fh) - (2 * x -$

$f2) - 5) + pp) - (2 * \\
\text{lam-r} * x * (x - fx) - 12 * \text{lam-r} * x * (\text{alpha-r} * x - fa) - 2 * ((2 * (\text{lam-r} \\
* x) - fl) * \\
(\text{lam-r} * x) - (2 * (\text{lam-r} * x) - fl) * (2 * (\text{lam-r} * x) - fl + 1) / 4)) = \\
x * (4 * \text{lam-r} + 2 * \text{lam-r} * fx - 12 * \text{lam-r} * fa) + (9 * (fa * (1 - 2 * fa)) \\
- 3 * (-1 * 1 * \\
(1 - fx + fa - mx - 2 * (1 - fx) * fa)) + (((fh)^2 - f2 * fh) / 2 - pp) + (fl \\
- \\
(fl)^2) / 2) \\
\langle \text{proof} \rangle$

lemma *R-eg-alg4*:

fixes $x \text{ fx fa fh f2 fl mx pp} :: \text{real}$
shows $- ((2 * \text{Hc-r} * x - fh - 3 * (2 * (\text{alpha-r} * x - fa) + 1)) * (2 * \text{Hc-r} \\
* x - fh + 3 * (2 * \\
(\text{alpha-r} * x - fa) + 1) - (2 * (x - fx) + 1) - 5) / 2 + ((2 * \text{Hc-r} * x - \\
fh - 3 * (2 * \\
(\text{alpha-r} * x - fa) + 1)) * (-3 * -1) + 3 * -1 * (2 * \text{Hc-r} * x - fh + 3 \\
* (2 * (\text{alpha-r} * x - \\
fa) + 1) - (2 * (x - fx) + 1) - 5) + 3 * -1 * (-3 * -1)) * (1 / 2 - (1 \\
- fa)) + (2 * \text{Hc-r} * \\
x - fh - 3 * (2 * (\text{alpha-r} * x - fa) + 1)) * -1 * (1 / 2 - (1 - fx)) + 3 \\
* -1 * -1 * (1 / 2 - \\
mx) + (\text{Hc-r} * x - (2 * \text{Hc-r} * x - fh) / 2) * (2 * (2 * \text{Hc-r} * x - fh) - (2 \\
* x - f2) - 5) + \\
pp) - (2 * \text{lam-r} * x * (x - fx) - 12 * \text{lam-r} * x * (\text{alpha-r} * x - fa) - 2 * \\
((2 * (\text{lam-r} * x) - \\
fl) * (\text{lam-r} * x) - (2 * (\text{lam-r} * x) - fl) * (2 * (\text{lam-r} * x) - fl + 1) / 4)) = \\
x * (4 * \text{lam-r} + 2 * \text{lam-r} * fx - 12 * \text{lam-r} * fa) + (9 * ((1 - fa) * (1 - \\
2 * (1 - fa))) - 3 * \\
(-1 * -1 * (1 - fx + (1 - fa) - mx - 2 * (1 - fx) * (1 - fa))) + (((fh)^2 \\
- f2 * fh) / \\
2 - pp) + (fl - (fl)^2) / 2) \\
\langle \text{proof} \rangle$

theorem *R-eg*:

$R\text{-r } x = x * Fx \text{ } x + Qc \text{ } (\text{frac } x) \text{ } (\text{frac } (\text{alpha-r} * x)) \text{ } (\text{frac } (2 * \text{Hc-r} * x)) \text{ } (\text{frac } \\
(2 * \\
x)) \text{ } (\text{frac } (2 * (\text{lam-r} * x))) \\
\langle \text{proof} \rangle$

lemma *Qc-bounds*:

assumes $0 \leq f \leq 1 \ 0 \leq g \leq 1 \ 0 \leq \tau \leq 1 \ 0 \leq \sigma \leq 1 \ 0 \leq \eta \leq 1$
shows $- 1 / 2 \leq Qc \text{ } f \text{ } g \text{ } \tau \text{ } \sigma \text{ } \eta \wedge \\
Qc \text{ } f \text{ } g \text{ } \tau \text{ } \sigma \text{ } \eta \leq 13 / 8 \\
\langle \text{proof} \rangle$

(5.12)-(5.14) for every real x .

theorem *R-decomp-bound-all:*

$-1/2 \leq R\text{-}r\ x - x * (4 * \text{lam-r} + 2 * \text{lam-r} * \text{frac}\ x - 12 * \text{lam-r} * \text{frac}(\text{alpha-r} * x)) \wedge$
 $R\text{-}r\ x - x * (4 * \text{lam-r} + 2 * \text{lam-r} * \text{frac}\ x - 12 * \text{lam-r} * \text{frac}(\text{alpha-r} * x))$
 $\leq 13/8$
 $\langle \text{proof} \rangle$

$R(x) = A\ x + B$ on a piece where the five floors are known.

lemma *R-on-piece:*

fixes $k1\ k2\ k3\ k4\ k5 :: \text{nat}$
assumes $\text{real}\ k1 \leq x\ x < \text{real}\ k1 + 1\ \text{real}\ k2 \leq \text{alpha-r} * x\ \text{alpha-r} * x < \text{real}\ k2 + 1$
 $\text{real}\ k3 \leq 2 * \text{Hc-r} * x\ 2 * \text{Hc-r} * x < \text{real}\ k3 + 1\ \text{real}\ k4 \leq 2 * x\ 2 * x < \text{real}\ k4 + 1$
 $\text{real}\ k5 \leq 2 * (\text{lam-r} * x)\ 2 * (\text{lam-r} * x) < \text{real}\ k5 + 1$
shows $R\text{-}r\ x = x * (4 * \text{lam-r} + 2 * \text{lam-r} * (x - \text{real}\ k1) - 12 * \text{lam-r} * (\text{alpha-r} * x - \text{real}\ k2))$
 $+ Qc\ (x - \text{real}\ k1)\ (\text{alpha-r} * x - \text{real}\ k2)\ (2 * \text{Hc-r} * x - \text{real}\ k3)$
 $(2 * x - \text{real}\ k4)\ (2 * (\text{lam-r} * x) - \text{real}\ k5)$
 $\langle \text{proof} \rangle$

26.2 $\int_{-1/3}^{1/2} d(y)\ dy = 9/640$, the mean of P , and $|C| < 16$

theorem *integral-dfun-eq:* $\text{interval-lebesgue-integral}\ \text{lborel}\ (\text{ereal}\ (1/3))\ (\text{ereal}\ (1/2))\ \text{dfun-r} = 9/640$
 $\langle \text{proof} \rangle$

lemma *fract-quad-piece:* $x \in \{\text{real}\ n <..< \text{real}\ n + 1\} \implies$
 $\text{frac}\ x * (1 - \text{frac}\ x) = (-\text{real}\ n - \text{real}\ n \wedge 2) + (1 + 2 * \text{real}\ n) * x + (-1) * x \wedge 2$
 $\langle \text{proof} \rangle$

lemma *fract-quad-integral:*

$\text{interval-lebesgue-integrable}\ \text{lborel}\ (\text{ereal}\ 0)\ (\text{ereal}\ (\text{real}\ n))\ (\lambda x. \text{frac}\ x * (1 - \text{frac}\ x)) \wedge$
 $\text{interval-lebesgue-integral}\ \text{lborel}\ (\text{ereal}\ 0)\ (\text{ereal}\ (\text{real}\ n))\ (\lambda x. \text{frac}\ x * (1 - \text{frac}\ x)) = \text{real}\ n / 6$
 $\langle \text{proof} \rangle$

Scaling $x \mapsto c\ x$ in an integral from 0.

lemma *integral-scale:*

fixes $g :: \text{real} \Rightarrow \text{real}$
assumes $c: 0 < c$ and $b: 0 \leq b$ and $\text{interval-lebesgue-integrable}\ \text{lborel}\ (\text{ereal}\ 0)$
 $(\text{ereal}\ (c * b))\ g$

shows *interval-lebesgue-integral lborel (ereal 0) (ereal b) ($\lambda x. g (c * x)$) =*
*(1 / c) * interval-lebesgue-integral lborel (ereal 0) (ereal (c * b)) g*
 ⟨proof⟩

lemma *integrable-scale:*

fixes *g :: real $\Rightarrow$ real*
assumes *c: 0 < c and b: 0 $\leq$ b and i: interval-lebesgue-integrable lborel (ereal*
0) (ereal
*(c * b)) g*
shows *interval-lebesgue-integrable lborel (ereal 0) (ereal b) ($\lambda x. g (c * x)$)*
 ⟨proof⟩

theorem *Pper-mean-eq: interval-lebesgue-integral lborel (ereal 0) (ereal 40) Pper*
/ 40 =
2923 / 240
 ⟨proof⟩

$|G_0(v)| \leq 81/5000$ on $[0, 1]$ and $|C(x)| < 16$.

lemma *G0-r-bound:*

assumes *0 $\leq v$ v $\leq$ 1*
shows *$|G_0-r v| \leq 81 / 5000$*
 ⟨proof⟩

theorem *Cper-bound: $|Cper x| < 16$*
 ⟨proof⟩

26.3 (5.10): $\int -\{1/3\}^{\wedge}\{2\lambda\}$ *outerIntegrand* = *I-out* by 11 affine pieces

On each piece *outerIntegrand* $y = c_0 + c_1 y$; $\lfloor 1/y \rfloor$ is constant (fact *fl*).
 The pieces were generated from Lean's *gen/gen-outer.py* (29 pieces, merged where the formula agrees).

lemma *pos-eq1: 0 $\leq v \implies pos-r v = v$* ⟨proof⟩

lemma *pos-eq0: v $\leq 0 \implies pos-r v = 0$* ⟨proof⟩

lemma *outer-piece-0: $y \in \{(1 / 3) <..<(43 / 120)\} \implies$*
*outer-integrand y = (279 / 40) + (- 9) * y*
 ⟨proof⟩

lemma *outer-piece-1: $y \in \{(43 / 120) <..<(37 / 100)\} \implies$*
*outer-integrand y = (451 / 40) + (- 21) * y*
 ⟨proof⟩

lemma *outer-piece-2: $y \in \{(37 / 100) <..<(13 / 30)\} \implies$*
*outer-integrand y = (377 / 40) + (- 16) * y*
 ⟨proof⟩

lemma *outer-piece-3*: $y \in \{(13 / 30) <..< (37 / 80)\} \implies$
outer-integrand $y = (429 / 40) + (- 19) * y$
 <proof>

lemma *outer-piece-4*: $y \in \{(37 / 80) <..< (1 / 2)\} \implies$
outer-integrand $y = (17 / 4) + (- 5) * y$
 <proof>

lemma *outer-piece-5*: $y \in \{(1 / 2) <..< (43 / 80)\} \implies$
outer-integrand $y = (51 / 10) + (- 3) * y$
 <proof>

lemma *outer-piece-6*: $y \in \{(43 / 80) <..< (37 / 60)\} \implies$
outer-integrand $y = (231 / 20) + (- 15) * y$
 <proof>

lemma *outer-piece-7*: $y \in \{(37 / 60) <..< (13 / 20)\} \implies$
outer-integrand $y = (97 / 10) + (- 12) * y$
 <proof>

lemma *outer-piece-8*: $y \in \{(13 / 20) <..< (37 / 40)\} \implies$
outer-integrand $y = (42 / 5) + (- 10) * y$
 <proof>

lemma *outer-piece-9*: $y \in \{(37 / 40) <..< 1\} \implies$ *outer-integrand* $y = 1 + (- 2) * y$
 <proof>

lemma *outer-piece-10*: $y \in \{1 <..< (37 / 20)\} \implies$
outer-integrand $y = (37 / 20) + (- 1) * y$
 <proof>

The pieces chained from $1/3$ to $2\lambda = 37/20$.

theorem *outer-integral-value*:
*interval-lebesgue-integral lborel (ereal (1 / 3)) (ereal (2 * lam-r)) outer-integrand*
 =
of-rat lout
 <proof>

26.4 (5.18): $\int_{-3}^{20} R(x)/x^3 dx$ by 143 affine pieces

On each piece $R(x) = A x + B$ (Lean *gen/gen-inner.py*; breakpoints are the multiples of $1/2, 20/3, 20/37, 10/23, 10/3, 20/43$ in $[3, 20]$). The first fact of each piece gives the floors ($\lfloor x \rfloor, \lfloor \alpha x \rfloor, \lfloor 2H-c x \rfloor, \lfloor 2x \rfloor, \lfloor 2\lambda x \rfloor$) to feed *R-on-piece*; after that the identity follows from *Qc-def, d0-def, es-def, pos-r-def* with min/max/if resolved by the linear side conditions.

lemma *inner-piece-0*: $x \in \{3 <..< (70 / 23)\} \implies$ *R-r* $x = (18 / 5) * x + (- 6)$
 <proof>

lemma inner-piece-1: $x \in \{(70 / 23) <..< (120 / 37)\} \implies$
 $R\text{-}r\ x = (49 / 20) * x + (- 5 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-2: $x \in \{(120 / 37) <..< (140 / 43)\} \implies$
 $R\text{-}r\ x = (283 / 40) * x + (- 35 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-3: $x \in \{(140 / 43) <..< (10 / 3)\} \implies$
 $R\text{-}r\ x = (283 / 40) * x + (- 35 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-4: $x \in \{(10 / 3) <..< (80 / 23)\} \implies$
 $R\text{-}r\ x = (277 / 40) * x + (- 17)$
 $\langle \text{proof} \rangle$

lemma inner-piece-5: $x \in \{(80 / 23) <..< (7 / 2)\} \implies$
 $R\text{-}r\ x = (231 / 40) * x + (- 13)$
 $\langle \text{proof} \rangle$

lemma inner-piece-6: $x \in \{(7 / 2) <..< (160 / 43)\} \implies$
 $R\text{-}r\ x = (271 / 40) * x + (- 33 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-7: $x \in \{(160 / 43) <..< (140 / 37)\} \implies$
 $R\text{-}r\ x = (71 / 20) * x + (- 9 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-8: $x \in \{(140 / 37) <..< (90 / 23)\} \implies$
 $R\text{-}r\ x = (27 / 5) * x + (- 23 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-9: $x \in \{(90 / 23) <..< 4\} \implies R\text{-}r\ x = (17 / 4) * x + (- 7)$
 $\langle \text{proof} \rangle$

lemma inner-piece-10: $x \in \{4 <..< (180 / 43)\} \implies R\text{-}r\ x = (17 / 5) * x + (- 11)$
 $\langle \text{proof} \rangle$

lemma inner-piece-11: $x \in \{(180 / 43) <..< (160 / 37)\} \implies$
 $R\text{-}r\ x = (17 / 5) * x + (- 11)$
 $\langle \text{proof} \rangle$

lemma inner-piece-12: $x \in \{(160 / 37) <..< (100 / 23)\} \implies$
 $R\text{-}r\ x = (321 / 40) * x + (- 31)$
 $\langle \text{proof} \rangle$

lemma inner-piece-13: $x \in \{(100 / 23) <..< (9 / 2)\} \implies$

$R\text{-}r\ x = (55 / 8) * x + (-26)$
 $\langle \text{proof} \rangle$

lemma inner-piece-14: $x \in \{(9 / 2) < .. < (200 / 43)\} \implies$
 $R\text{-}r\ x = (63 / 8) * x + (-61 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-15: $x \in \{(200 / 43) < .. < (110 / 23)\} \implies$
 $R\text{-}r\ x = (93 / 20) * x + (-31 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-16: $x \in \{(110 / 23) < .. < (180 / 37)\} \implies$
 $R\text{-}r\ x = (7 / 2) * x + (-10)$
 $\langle \text{proof} \rangle$

lemma inner-piece-17: $x \in \{(180 / 37) < .. < 5\} \implies R\text{-}r\ x = (107 / 20) * x + (-19)$
 $\langle \text{proof} \rangle$

lemma inner-piece-18: $x \in \{5 < .. < (220 / 43)\} \implies R\text{-}r\ x = (9 / 2) * x + (-24)$
 $\langle \text{proof} \rangle$

lemma inner-piece-19: $x \in \{(220 / 43) < .. < (120 / 23)\} \implies$
 $R\text{-}r\ x = (9 / 2) * x + (-24)$
 $\langle \text{proof} \rangle$

lemma inner-piece-20: $x \in \{(120 / 23) < .. < (200 / 37)\} \implies$
 $R\text{-}r\ x = (67 / 20) * x + (-18)$
 $\langle \text{proof} \rangle$

lemma inner-piece-21: $x \in \{(200 / 37) < .. < (11 / 2)\} \implies$
 $R\text{-}r\ x = (319 / 40) * x + (-43)$
 $\langle \text{proof} \rangle$

lemma inner-piece-22: $x \in \{(11 / 2) < .. < (240 / 43)\} \implies$
 $R\text{-}r\ x = (359 / 40) * x + (-97 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-23: $x \in \{(240 / 43) < .. < (130 / 23)\} \implies$
 $R\text{-}r\ x = (23 / 4) * x + (-61 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-24: $x \in \{(130 / 23) < .. < (220 / 37)\} \implies$
 $R\text{-}r\ x = (23 / 5) * x + (-24)$
 $\langle \text{proof} \rangle$

lemma inner-piece-25: $x \in \{(220 / 37) < .. < 6\} \implies R\text{-}r\ x = (129 / 20) * x + (-35)$

$\langle proof \rangle$

lemma inner-piece-26: $x \in \{6 < .. < (260 / 43)\} \implies R\text{-}r\ x = (28 / 5) * x + (-41)$

$\langle proof \rangle$

lemma inner-piece-27: $x \in \{(260 / 43) < .. < (140 / 23)\} \implies$

$$R\text{-}r\ x = (28 / 5) * x + (-41)$$

$\langle proof \rangle$

lemma inner-piece-28: $x \in \{(140 / 23) < .. < (240 / 37)\} \implies$

$$R\text{-}r\ x = (89 / 20) * x + (-34)$$

$\langle proof \rangle$

lemma inner-piece-29: $x \in \{(240 / 37) < .. < (13 / 2)\} \implies$

$$R\text{-}r\ x = (363 / 40) * x + (-64)$$

$\langle proof \rangle$

lemma inner-piece-30: $x \in \{(13 / 2) < .. < (280 / 43)\} \implies$

$$R\text{-}r\ x = (403 / 40) * x + (-141 / 2)$$

$\langle proof \rangle$

lemma inner-piece-31: $x \in \{(280 / 43) < .. < (150 / 23)\} \implies$

$$R\text{-}r\ x = (137 / 20) * x + (-99 / 2)$$

$\langle proof \rangle$

lemma inner-piece-32: $x \in \{(150 / 23) < .. < (20 / 3)\} \implies$

$$R\text{-}r\ x = (57 / 10) * x + (-42)$$

$\langle proof \rangle$

lemma inner-piece-33: $x \in \{(20 / 3) < .. < (160 / 23)\} \implies$

$$R\text{-}r\ x = (69 / 10) * x + (-50)$$

$\langle proof \rangle$

lemma inner-piece-34: $x \in \{(160 / 23) < .. < (300 / 43)\} \implies$

$$R\text{-}r\ x = (23 / 4) * x + (-42)$$

$\langle proof \rangle$

lemma inner-piece-35: $x \in \{(300 / 43) < .. < 7\} \implies R\text{-}r\ x = (23 / 4) * x + (-42)$

$\langle proof \rangle$

lemma inner-piece-36: $x \in \{7 < .. < (260 / 37)\} \implies R\text{-}r\ x = (49 / 10) * x + (-49)$

$\langle proof \rangle$

lemma inner-piece-37: $x \in \{(260 / 37) < .. < (170 / 23)\} \implies$

$$R\text{-}r\ x = (27 / 4) * x + (-62)$$

$\langle proof \rangle$

lemma inner-piece-38: $x \in \{(170 / 23) < .. < (320 / 43)\} \implies$

$$R\text{-}r\ x = (28 / 5) * x + (- 107 / 2)$$

$\langle proof \rangle$

lemma inner-piece-39: $x \in \{(320 / 43) < .. < (15 / 2)\} \implies$

$$R\text{-}r\ x = (19 / 8) * x + (- 59 / 2)$$

$\langle proof \rangle$

lemma inner-piece-40: $x \in \{(15 / 2) < .. < (280 / 37)\} \implies$

$$R\text{-}r\ x = (27 / 8) * x + (- 37)$$

$\langle proof \rangle$

lemma inner-piece-41: $x \in \{(280 / 37) < .. < (180 / 23)\} \implies R\text{-}r\ x = 8 * x + (- 72)$

$\langle proof \rangle$

lemma inner-piece-42: $x \in \{(180 / 23) < .. < (340 / 43)\} \implies$

$$R\text{-}r\ x = (137 / 20) * x + (- 63)$$

$\langle proof \rangle$

lemma inner-piece-43: $x \in \{(340 / 43) < .. < 8\} \implies R\text{-}r\ x = (137 / 20) * x + (- 63)$

$\langle proof \rangle$

lemma inner-piece-44: $x \in \{8 < .. < (300 / 37)\} \implies R\text{-}r\ x = 6 * x + (- 71)$

$\langle proof \rangle$

lemma inner-piece-45: $x \in \{(300 / 37) < .. < (190 / 23)\} \implies$

$$R\text{-}r\ x = (157 / 20) * x + (- 86)$$

$\langle proof \rangle$

lemma inner-piece-46: $x \in \{(190 / 23) < .. < (360 / 43)\} \implies$

$$R\text{-}r\ x = (67 / 10) * x + (- 153 / 2)$$

$\langle proof \rangle$

lemma inner-piece-47: $x \in \{(360 / 43) < .. < (17 / 2)\} \implies$

$$R\text{-}r\ x = (139 / 40) * x + (- 99 / 2)$$

$\langle proof \rangle$

lemma inner-piece-48: $x \in \{(17 / 2) < .. < (320 / 37)\} \implies$

$$R\text{-}r\ x = (179 / 40) * x + (- 58)$$

$\langle proof \rangle$

lemma inner-piece-49: $x \in \{(320 / 37) < .. < (200 / 23)\} \implies$

$$R\text{-}r\ x = (91 / 10) * x + (- 98)$$

$\langle proof \rangle$

lemma inner-piece-50: $x \in \{(200 / 23) < .. < (380 / 43)\} \implies$

$$R\text{-}r\ x = (159 / 20) * x + (- 88)$$

<proof>

lemma inner-piece-51: $x \in \{(380 / 43) < .. < 9\} \implies R\text{-}r\ x = (159 / 20) * x + (- 88)$

<proof>

lemma inner-piece-52: $x \in \{9 < .. < (210 / 23)\} \implies R\text{-}r\ x = (71 / 10) * x + (- 97)$

<proof>

lemma inner-piece-53: $x \in \{(210 / 23) < .. < (340 / 37)\} \implies$
 $R\text{-}r\ x = (119 / 20) * x + (- 173 / 2)$

<proof>

lemma inner-piece-54: $x \in \{(340 / 37) < .. < (400 / 43)\} \implies$
 $R\text{-}r\ x = (39 / 5) * x + (- 207 / 2)$

<proof>

lemma inner-piece-55: $x \in \{(400 / 43) < .. < (19 / 2)\} \implies$
 $R\text{-}r\ x = (183 / 40) * x + (- 147 / 2)$

<proof>

lemma inner-piece-56: $x \in \{(19 / 2) < .. < (220 / 23)\} \implies$
 $R\text{-}r\ x = (223 / 40) * x + (- 83)$

<proof>

lemma inner-piece-57: $x \in \{(220 / 23) < .. < (360 / 37)\} \implies$
 $R\text{-}r\ x = (177 / 40) * x + (- 72)$

<proof>

lemma inner-piece-58: $x \in \{(360 / 37) < .. < (420 / 43)\} \implies$
 $R\text{-}r\ x = (181 / 20) * x + (- 117)$

<proof>

lemma inner-piece-59: $x \in \{(420 / 43) < .. < 10\} \implies$
 $R\text{-}r\ x = (181 / 20) * x + (- 117)$

<proof>

lemma inner-piece-60: $x \in \{10 < .. < (440 / 43)\} \implies R\text{-}r\ x = (69 / 10) * x + (- 114)$

<proof>

lemma inner-piece-61: $x \in \{(440 / 43) < .. < (380 / 37)\} \implies$
 $R\text{-}r\ x = (147 / 40) * x + (- 81)$

<proof>

lemma inner-piece-62: $x \in \{(380 / 37) < .. < (240 / 23)\} \implies$
 $R\text{-}r\ x = (221 / 40) * x + (- 100)$

$\langle proof \rangle$

lemma inner-piece-63: $x \in \{(240 / 23) < .. < (21 / 2)\} \implies$
 $R-r x = (35 / 8) * x + (- 88)$
 $\langle proof \rangle$

lemma inner-piece-64: $x \in \{(21 / 2) < .. < (460 / 43)\} \implies$
 $R-r x = (43 / 8) * x + (- 197 / 2)$
 $\langle proof \rangle$

lemma inner-piece-65: $x \in \{(460 / 43) < .. < (400 / 37)\} \implies$
 $R-r x = (43 / 8) * x + (- 197 / 2)$
 $\langle proof \rangle$

lemma inner-piece-66: $x \in \{(400 / 37) < .. < (250 / 23)\} \implies$
 $R-r x = 10 * x + (- 297 / 2)$
 $\langle proof \rangle$

lemma inner-piece-67: $x \in \{(250 / 23) < .. < 11\} \implies$
 $R-r x = (177 / 20) * x + (- 136)$
 $\langle proof \rangle$

lemma inner-piece-68: $x \in \{11 < .. < (480 / 43)\} \implies R-r x = 8 * x + (- 147)$
 $\langle proof \rangle$

lemma inner-piece-69: $x \in \{(480 / 43) < .. < (260 / 23)\} \implies$
 $R-r x = (191 / 40) * x + (- 111)$
 $\langle proof \rangle$

lemma inner-piece-70: $x \in \{(260 / 23) < .. < (420 / 37)\} \implies$
 $R-r x = (29 / 8) * x + (- 98)$
 $\langle proof \rangle$

lemma inner-piece-71: $x \in \{(420 / 37) < .. < (23 / 2)\} \implies$
 $R-r x = (219 / 40) * x + (- 119)$
 $\langle proof \rangle$

lemma inner-piece-72: $x \in \{(23 / 2) < .. < (500 / 43)\} \implies$
 $R-r x = (259 / 40) * x + (- 261 / 2)$
 $\langle proof \rangle$

lemma inner-piece-73: $x \in \{(500 / 43) < .. < (270 / 23)\} \implies$
 $R-r x = (259 / 40) * x + (- 261 / 2)$
 $\langle proof \rangle$

lemma inner-piece-74: $x \in \{(270 / 23) < .. < (440 / 37)\} \implies$
 $R-r x = (213 / 40) * x + (- 117)$
 $\langle proof \rangle$

lemma inner-piece-75: $x \in \{(440 / 37) < .. < 12\} \implies$

$$R\text{-}r\ x = (199 / 20) * x + (-172)$$

$\langle proof \rangle$

lemma inner-piece-76: $x \in \{12 < .. < (520 / 43)\} \implies R\text{-}r\ x = (91 / 10) * x + (-184)$

$\langle proof \rangle$

lemma inner-piece-77: $x \in \{(520 / 43) < .. < (280 / 23)\} \implies$

$$R\text{-}r\ x = (47 / 8) * x + (-145)$$

$\langle proof \rangle$

lemma inner-piece-78: $x \in \{(280 / 23) < .. < (460 / 37)\} \implies$

$$R\text{-}r\ x = (189 / 40) * x + (-131)$$

$\langle proof \rangle$

lemma inner-piece-79: $x \in \{(460 / 37) < .. < (25 / 2)\} \implies$

$$R\text{-}r\ x = (263 / 40) * x + (-154)$$

$\langle proof \rangle$

lemma inner-piece-80: $x \in \{(25 / 2) < .. < (540 / 43)\} \implies$

$$R\text{-}r\ x = (303 / 40) * x + (-333 / 2)$$

$\langle proof \rangle$

lemma inner-piece-81: $x \in \{(540 / 43) < .. < (290 / 23)\} \implies$

$$R\text{-}r\ x = (303 / 40) * x + (-333 / 2)$$

$\langle proof \rangle$

lemma inner-piece-82: $x \in \{(290 / 23) < .. < (480 / 37)\} \implies$

$$R\text{-}r\ x = (257 / 40) * x + (-152)$$

$\langle proof \rangle$

lemma inner-piece-83: $x \in \{(480 / 37) < .. < 13\} \implies$

$$R\text{-}r\ x = (221 / 20) * x + (-212)$$

$\langle proof \rangle$

lemma inner-piece-84: $x \in \{13 < .. < (560 / 43)\} \implies R\text{-}r\ x = (51 / 5) * x + (-225)$

$\langle proof \rangle$

lemma inner-piece-85: $x \in \{(560 / 43) < .. < (300 / 23)\} \implies$

$$R\text{-}r\ x = (279 / 40) * x + (-183)$$

$\langle proof \rangle$

lemma inner-piece-86: $x \in \{(300 / 23) < .. < (40 / 3)\} \implies$

$$R\text{-}r\ x = (233 / 40) * x + (-168)$$

$\langle proof \rangle$

lemma inner-piece-87: $x \in \{(40 / 3) < .. < (310 / 23)\} \implies$

$$R-r x = (145 / 8) * x + (- 184)$$

<proof>

lemma inner-piece-88: $x \in \{(310 / 23) < .. < (580 / 43)\} \implies$
 $R-r x = (679 / 40) * x + (- 337 / 2)$
<proof>

lemma inner-piece-89: $x \in \{(580 / 43) < .. < (27 / 2)\} \implies$
 $R-r x = (679 / 40) * x + (- 337 / 2)$
<proof>

lemma inner-piece-90: $x \in \{(27 / 2) < .. < (500 / 37)\} \implies$
 $R-r x = (719 / 40) * x + (- 182)$
<proof>

lemma inner-piece-91: $x \in \{(500 / 37) < .. < (320 / 23)\} \implies$
 $R-r x = (793 / 40) * x + (- 207)$
<proof>

lemma inner-piece-92: $x \in \{(320 / 23) < .. < (600 / 43)\} \implies$
 $R-r x = (747 / 40) * x + (- 191)$
<proof>

lemma inner-piece-93: $x \in \{(600 / 43) < .. < 14\} \implies$
 $R-r x = (309 / 20) * x + (- 146)$
<proof>

lemma inner-piece-94: $x \in \{14 < .. < (520 / 37)\} \implies R-r x = (73 / 5) * x + (- 160)$
<proof>

lemma inner-piece-95: $x \in \{(520 / 37) < .. < (330 / 23)\} \implies$
 $R-r x = (769 / 40) * x + (- 225)$
<proof>

lemma inner-piece-96: $x \in \{(330 / 23) < .. < (620 / 43)\} \implies$
 $R-r x = (723 / 40) * x + (- 417 / 2)$
<proof>

lemma inner-piece-97: $x \in \{(620 / 43) < .. < (29 / 2)\} \implies$
 $R-r x = (723 / 40) * x + (- 417 / 2)$
<proof>

lemma inner-piece-98: $x \in \{(29 / 2) < .. < (540 / 37)\} \implies$
 $R-r x = (763 / 40) * x + (- 223)$
<proof>

lemma inner-piece-99: $x \in \{(540 / 37) < .. < (340 / 23)\} \implies$
 $R-r x = (837 / 40) * x + (- 250)$

$\langle proof \rangle$

lemma inner-piece-100: $x \in \{(340 / 23) < .. < (640 / 43)\} \implies$
 $R-r x = (791 / 40) * x + (- 233)$
 $\langle proof \rangle$

lemma inner-piece-101: $x \in \{(640 / 43) < .. < 15\} \implies$
 $R-r x = (331 / 20) * x + (- 185)$
 $\langle proof \rangle$

lemma inner-piece-102: $x \in \{15 < .. < (560 / 37)\} \implies$
 $R-r x = (157 / 10) * x + (- 200)$
 $\langle proof \rangle$

lemma inner-piece-103: $x \in \{(560 / 37) < .. < (350 / 23)\} \implies$
 $R-r x = (813 / 40) * x + (- 270)$
 $\langle proof \rangle$

lemma inner-piece-104: $x \in \{(350 / 23) < .. < (660 / 43)\} \implies$
 $R-r x = (767 / 40) * x + (- 505 / 2)$
 $\langle proof \rangle$

lemma inner-piece-105: $x \in \{(660 / 43) < .. < (31 / 2)\} \implies$
 $R-r x = (767 / 40) * x + (- 505 / 2)$
 $\langle proof \rangle$

lemma inner-piece-106: $x \in \{(31 / 2) < .. < (360 / 23)\} \implies$
 $R-r x = (807 / 40) * x + (- 268)$
 $\langle proof \rangle$

lemma inner-piece-107: $x \in \{(360 / 23) < .. < (580 / 37)\} \implies$
 $R-r x = (761 / 40) * x + (- 250)$
 $\langle proof \rangle$

lemma inner-piece-108: $x \in \{(580 / 37) < .. < (680 / 43)\} \implies$
 $R-r x = (167 / 8) * x + (- 279)$
 $\langle proof \rangle$

lemma inner-piece-109: $x \in \{(680 / 43) < .. < 16\} \implies$
 $R-r x = (353 / 20) * x + (- 228)$
 $\langle proof \rangle$

lemma inner-piece-110: $x \in \{16 < .. < (370 / 23)\} \implies R-r x = (84 / 5) * x + (-$
 $244)$
 $\langle proof \rangle$

lemma inner-piece-111: $x \in \{(370 / 23) < .. < (600 / 37)\} \implies$
 $R-r x = (313 / 20) * x + (- 451 / 2)$
 $\langle proof \rangle$

lemma inner-piece-112: $x \in \{(600 / 37) < .. < (700 / 43)\} \implies$
 $R\text{-}r\ x = (811 / 40) * x + (- 601 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-113: $x \in \{(700 / 43) < .. < (33 / 2)\} \implies$
 $R\text{-}r\ x = (811 / 40) * x + (- 601 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-114: $x \in \{(33 / 2) < .. < (380 / 23)\} \implies$
 $R\text{-}r\ x = (851 / 40) * x + (- 317)$
 $\langle \text{proof} \rangle$

lemma inner-piece-115: $x \in \{(380 / 23) < .. < (50 / 3)\} \implies$
 $R\text{-}r\ x = (161 / 8) * x + (- 298)$
 $\langle \text{proof} \rangle$

lemma inner-piece-116: $x \in \{(50 / 3) < .. < (720 / 43)\} \implies$
 $R\text{-}r\ x = (799 / 40) * x + (- 591 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-117: $x \in \{(720 / 43) < .. < (620 / 37)\} \implies$
 $R\text{-}r\ x = (67 / 4) * x + (- 483 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-118: $x \in \{(620 / 37) < .. < (390 / 23)\} \implies$
 $R\text{-}r\ x = (93 / 5) * x + (- 545 / 2)$
 $\langle \text{proof} \rangle$

lemma inner-piece-119: $x \in \{(390 / 23) < .. < 17\} \implies$
 $R\text{-}r\ x = (349 / 20) * x + (- 253)$
 $\langle \text{proof} \rangle$

lemma inner-piece-120: $x \in \{17 < .. < (740 / 43)\} \implies R\text{-}r\ x = (83 / 5) * x + (- 270)$
 $\langle \text{proof} \rangle$

lemma inner-piece-121: $x \in \{(740 / 43) < .. < (640 / 37)\} \implies$
 $R\text{-}r\ x = (83 / 5) * x + (- 270)$
 $\langle \text{proof} \rangle$

lemma inner-piece-122: $x \in \{(640 / 37) < .. < (400 / 23)\} \implies$
 $R\text{-}r\ x = (849 / 40) * x + (- 350)$
 $\langle \text{proof} \rangle$

lemma inner-piece-123: $x \in \{(400 / 23) < .. < (35 / 2)\} \implies$
 $R\text{-}r\ x = (803 / 40) * x + (- 330)$
 $\langle \text{proof} \rangle$

lemma inner-piece-124: $x \in \{(35 / 2) < .. < (760 / 43)\} \implies$
 $R\text{-}r\ x = (843 / 40) * x + (- 695 / 2)$
 $\langle proof \rangle$

lemma inner-piece-125: $x \in \{(760 / 43) < .. < (410 / 23)\} \implies$
 $R\text{-}r\ x = (357 / 20) * x + (- 581 / 2)$
 $\langle proof \rangle$

lemma inner-piece-126: $x \in \{(410 / 23) < .. < (660 / 37)\} \implies$
 $R\text{-}r\ x = (167 / 10) * x + (- 270)$
 $\langle proof \rangle$

lemma inner-piece-127: $x \in \{(660 / 37) < .. < 18\} \implies$
 $R\text{-}r\ x = (371 / 20) * x + (- 303)$
 $\langle proof \rangle$

lemma inner-piece-128: $x \in \{18 < .. < (780 / 43)\} \implies$
 $R\text{-}r\ x = (177 / 10) * x + (- 321)$
 $\langle proof \rangle$

lemma inner-piece-129: $x \in \{(780 / 43) < .. < (420 / 23)\} \implies$
 $R\text{-}r\ x = (177 / 10) * x + (- 321)$
 $\langle proof \rangle$

lemma inner-piece-130: $x \in \{(420 / 23) < .. < (680 / 37)\} \implies$
 $R\text{-}r\ x = (331 / 20) * x + (- 300)$
 $\langle proof \rangle$

lemma inner-piece-131: $x \in \{(680 / 37) < .. < (37 / 2)\} \implies$
 $R\text{-}r\ x = (847 / 40) * x + (- 385)$
 $\langle proof \rangle$

lemma inner-piece-132: $x \in \{(37 / 2) < .. < (800 / 43)\} \implies$
 $R\text{-}r\ x = (887 / 40) * x + (- 807 / 2)$
 $\langle proof \rangle$

lemma inner-piece-133: $x \in \{(800 / 43) < .. < (430 / 23)\} \implies$
 $R\text{-}r\ x = (379 / 20) * x + (- 687 / 2)$
 $\langle proof \rangle$

lemma inner-piece-134: $x \in \{(430 / 23) < .. < (700 / 37)\} \implies$
 $R\text{-}r\ x = (89 / 5) * x + (- 322)$
 $\langle proof \rangle$

lemma inner-piece-135: $x \in \{(700 / 37) < .. < 19\} \implies$
 $R\text{-}r\ x = (393 / 20) * x + (- 357)$
 $\langle proof \rangle$

lemma inner-piece-136: $x \in \{19 < .. < (820 / 43)\} \implies R\text{-}r\ x = (94 / 5) * x + (-$

376)
 $\langle \text{proof} \rangle$

lemma *inner-piece-137*: $x \in \{(820 / 43) < \dots < (440 / 23)\} \implies$
 $R\text{-}r \ x = (94 / 5) * x + (- 376)$
 $\langle \text{proof} \rangle$

lemma *inner-piece-138*: $x \in \{(440 / 23) < \dots < (720 / 37)\} \implies$
 $R\text{-}r \ x = (353 / 20) * x + (- 354)$
 $\langle \text{proof} \rangle$

lemma *inner-piece-139*: $x \in \{(720 / 37) < \dots < (39 / 2)\} \implies$
 $R\text{-}r \ x = (891 / 40) * x + (- 444)$
 $\langle \text{proof} \rangle$

lemma *inner-piece-140*: $x \in \{(39 / 2) < \dots < (840 / 43)\} \implies$
 $R\text{-}r \ x = (931 / 40) * x + (- 927 / 2)$
 $\langle \text{proof} \rangle$

lemma *inner-piece-141*: $x \in \{(840 / 43) < \dots < (450 / 23)\} \implies$
 $R\text{-}r \ x = (401 / 20) * x + (- 801 / 2)$
 $\langle \text{proof} \rangle$

lemma *inner-piece-142*: $x \in \{(450 / 23) < \dots < 20\} \implies$
 $R\text{-}r \ x = (189 / 10) * x + (- 378)$
 $\langle \text{proof} \rangle$

theorem *R-integral-3-20*:
interval-lebesgue-integral *lborel* (*ereal* 3) (*ereal* 20) ($\lambda x. R\text{-}r \ x / x^3$) =
 $322437603634266857629 / 7535670527041937280000$
 $\langle \text{proof} \rangle$

26.5 Integrability on $[\beta, \infty)$ and the tails (5.14)-(5.17)

The exceptional set $S = \mathbb{Z} \cup (40/3)\mathbb{Z}$ where the fractional parts jump.

definition $Sx :: \text{real set}$ **where** $Sx = \{x. x \in \mathbb{Z} \vee \text{alpha-r} * x \in \mathbb{Z}\}$

(5.15): $\Phi(x) = (P(x) - 2923/240)/x^2 + \lambda/x + 2C(x)/x^3$.

definition $\Phi :: \text{real} \Rightarrow \text{real}$ **where**

$\Phi x = (P_{\text{per}} x - 2923 / 240) / x^2 + \text{lam-r} / x + 2 * C_{\text{per}} x / x^3$

lemma *frac-measurable* [*measurable*]: (*frac* :: *real* $\Rightarrow$ *real*) $\in$ *borel-measurable* *borel*
 $\langle \text{proof} \rangle$

lemma *es-measurable* [*measurable*]: *es* $\in$ *borel-measurable* *borel*
 $\langle \text{proof} \rangle$

lemma *d0-measurable* [*measurable*]: *d0* $\in$ *borel-measurable* *borel*
 $\langle \text{proof} \rangle$

lemma *pos-measurable* [*measurable*]: *pos-r* $\in$ *borel-measurable borel*
 $\langle$ *proof* $\rangle$

lemma *R-measurable* [*measurable*]: *R-r* $\in$ *borel-measurable borel*
 $\langle$ *proof* $\rangle$

lemma *Fx-bounds*: $-37 / 5 \leq Fx\ x \wedge Fx\ x \leq 111 / 20$
 $\langle$ *proof* $\rangle$

lemma *Q-bounds*: $-1 / 2 \leq R-r\ x - x * Fx\ x \wedge R-r\ x - x * Fx\ x \leq 13 / 8$
 $\langle$ *proof* $\rangle$

lemma *R-abs-le*: $3 \leq x \implies |R-r\ x| \leq 9 * x$
 $\langle$ *proof* $\rangle$

lemma *R-div-bound*: $3 \leq x \implies |R-r\ x / x \wedge 3| \leq 9 / x \wedge 2$
 $\langle$ *proof* $\rangle$

lemma *inv-sq-integrable*: *set-integrable lborel* {*3..*} ($\lambda x :: \text{real. } 9 / x \wedge 2$)
 $\langle$ *proof* $\rangle$

theorem *R-div-cube-integrable*: *set-integrable lborel* {*3..*} ($\lambda x. R-r\ x / x \wedge 3$)
 $\langle$ *proof* $\rangle$

Derivatives of the fractional part off the integers.

lemma *frac-has-derivative*: $x \notin \mathbb{Z} \implies (\text{frac has-real-derivative } 1) (at\ x)$
 $\langle$ *proof* $\rangle$

lemma *frac-scaled-has-derivative*: $c * x \notin \mathbb{Z} \implies$
 $((\lambda x. \text{frac } (c * x)) \text{ has-real-derivative } c) (at\ x)$
 $\langle$ *proof* $\rangle$

lemma *Pper-deriv*: $x \notin Sx \implies (Pper \text{ has-real-derivative } (Fx\ x + lam-r)) (at\ x)$
 $\langle$ *proof* $\rangle$

lemma *G0-eq*: $G0-r = (\lambda v. v * (1 - v) * (2 * v - 1) / 6)$
 $\langle$ *proof* $\rangle$

lemma *G0-deriv*:
 $(G0-r \text{ has-real-derivative } (v * (1 - v) - 1 / 6)) (at\ v)$
 $\langle$ *proof* $\rangle$

lemma *Cper-deriv*: $x \notin Sx \implies$
 $(Cper \text{ has-real-derivative } (Pper\ x - 2923 / 240)) (at\ x)$
 $\langle$ *proof* $\rangle$

lemma *comp-frac-piece*:
fixes $g :: \text{real} \Rightarrow \text{real}$ **and** $m :: \text{int}$

assumes *continuous-on* $\{0..1\}$ $g \ g \ 0 = g \ 1$
shows *continuous-on* $\{of-int \ m..of-int \ m + 1\}$ $(\lambda x. \ g \ (frac \ x))$
 $\langle proof \rangle$

lemma *comp-frac-isCont*:
fixes $g :: real \Rightarrow real$
assumes *continuous-on* $\{0..1\}$ $g \ g \ 0 = g \ 1$
shows *isCont* $(\lambda x. \ g \ (frac \ x)) \ x$
 $\langle proof \rangle$

$g \circ frac$ is continuous when g is continuous on $[0,1]$ with $g \ 0 = g \ 1$ (Lean *ContinuousOn.comp-fract''*).

lemma *comp-frac-cont*:
fixes $g :: real \Rightarrow real$
assumes *continuous-on* $\{0..1\}$ $g \ g \ 0 = g \ 1$
shows *continuous-on* *UNIV* $(\lambda x. \ g \ (frac \ x))$
 $\langle proof \rangle$

lemma *u-cont: continuous-on UNIV* $(\lambda x::real. \ frac \ x * (1 - frac \ x))$
 $\langle proof \rangle$

lemma *u-cont-a: continuous-on UNIV* $(\lambda x. \ frac \ (alpha-r * x) * (1 - frac \ (alpha-r * x)))$
 $\langle proof \rangle$

lemma *Pper-cont: continuous-on UNIV Pper*
 $\langle proof \rangle$

lemma *G0-cont: continuous-on* $\{0..1\}$ *G0-r*
 $\langle proof \rangle$

lemma *G0-frac-cont: continuous-on UNIV* $(\lambda x. \ G0-r \ (frac \ x))$
 $\langle proof \rangle$

lemma *Cper-cont: continuous-on UNIV Cper*
 $\langle proof \rangle$

lemma *uq-bounds*: $0 \leq (v::real) \Longrightarrow v \leq 1 \Longrightarrow$
 $0 \leq v * (1 - v) \wedge v * (1 - v) \leq 1 / 4$
 $\langle proof \rangle$

lemma *Pper-abs-le*: $|Pper \ x - 2923 / 240| \leq 32$
 $\langle proof \rangle$

lemma *Phi-deriv*: $0 < x \Longrightarrow x \notin Sx \Longrightarrow$
 $(Phi \ has-real-derivative \ (Fx \ x / x ^ 2 - 6 * Cper \ x / x ^ 4)) \ (at \ x)$
 $\langle proof \rangle$

lemma *Phi-cont*: $0 < a \Longrightarrow continuous-on \{a..b\} \ Phi$

<proof>

lemma *Phi-abs-le*: $1 \leq x \implies |Phi\ x| \leq 65 / x$
<proof>

lemma *Sx-finite*: *finite* ($Sx \cap \{M..N\}$)
<proof>

lemma *set-integrable-bounded*:
 fixes $f :: real \Rightarrow real$
 assumes $A: A \in sets\ lborel\ emeasure\ lborel\ A < \infty$ **and** $f: f \in$
 borel-measurable borel
 and $b: \bigwedge x. x \in A \implies |f\ x| \leq B$
 shows *set-integrable lborel A f*
<proof>

lemma *interval-integrable-bounded*:
 fixes $f :: real \Rightarrow real$
 assumes $a \leq b$ $f \in borel-measurable\ borel$ $\bigwedge x. x \in \{a..b\} \implies$
 $|f\ x| \leq B$
 shows *interval-lebesgue-integrable lborel (ereal a) (ereal b) f*
<proof>

Measurability, bounds and integrability of the two parts of the tail integrand.

lemma *Fx-measurable [measurable]*: $Fx \in borel-measurable\ borel$
<proof>

lemma *Cper-measurable [measurable]*: $Cper \in borel-measurable\ borel$
<proof>

lemma *abs-div-ge1*:
 fixes $a\ d\ B :: real$
 assumes $d: 1 \leq d$ **and** $a: |a| \leq B$
 shows $|a / d| \leq B$
<proof>

lemma *g-bound*: $3 \leq x \implies |Fx\ x / x^2 - 6 * Cper\ x / x^4| \leq 104$
<proof>

lemma *h-bound*: $3 \leq x \implies$
 $|6 * Cper\ x / x^4 + (R-r\ x - x * Fx\ x) / x^3| \leq 98$
<proof>

lemma *g-meas*: $(\lambda x. Fx\ x / x^2 - 6 * Cper\ x / x^4) \in borel-measurable\ borel$
<proof>

lemma *h-meas*: $(\lambda x. 6 * Cper\ x / x^4 + (R-r\ x - x * Fx\ x) / x^3) \in$
 borel-measurable borel *<proof>*

lemma *g-integrable*:

assumes $M: \exists \leq M$ **and** $MN: M \leq N$
shows *interval-lebesgue-integrable lborel* (ereal M) (ereal N) $(\lambda x. Fx \ x / x^2 - 6 * Cper \ x / x^4)$
 $\langle proof \rangle$

lemma *h-integrable*:

assumes $M: \exists \leq M$ **and** $MN: M \leq N$
shows *interval-lebesgue-integrable lborel* (ereal M) (ereal N) $(\lambda x. 6 * Cper \ x / x^4 + (R-r \ x - x * Fx \ x) / x^3)$
 $\langle proof \rangle$

lemma *g-set-integrable*:

assumes $M: \exists \leq M$ **and** $MN: M \leq N$
shows *set-integrable lborel* $\{M..N\}$ $(\lambda x. Fx \ x / x^2 - 6 * Cper \ x / x^4)$
 $\langle proof \rangle$

lemma *interval-integral-mono-real*:

fixes $f \ g :: real \Rightarrow real$
assumes $ab: a \leq b$ **and** $f: interval-lebesgue-integrable lborel$ (ereal a) (ereal b) f
and $g: interval-lebesgue-integrable lborel$ (ereal a) (ereal b) g **and** $fg: \bigwedge x. x \in \{a..b\} \implies f \ x \leq g \ x$
shows *interval-lebesgue-integral lborel* (ereal a) (ereal b) $f \leq interval-lebesgue-integral lborel$ (ereal a) (ereal b) g
 $\langle proof \rangle$

lemma *pt-upper*: $\exists \leq x \implies$

$6 * Cper \ x / x^4 + (R-r \ x - x * Fx \ x) / x^3 \leq 96 / x^4 + 13 / 8 / x^3$
 $\langle proof \rangle$

lemma *pt-lower*: $\exists \leq x \implies$

$(-96) / x^4 + (-1 / 2) / x^3 \leq 6 * Cper \ x / x^4 + (R-r \ x - x * Fx \ x) / x^3$
 $\langle proof \rangle$

lemma *inv34-integrable*:

assumes $M: 0 < M$ **and** $MN: M \leq N$
shows *interval-lebesgue-integrable lborel* (ereal M) (ereal N) $(\lambda x. a / x^4 + b / x^3)$
 $\langle proof \rangle$

(5.15): $\int -M^N R / x^3 = \Phi(N) - \Phi(M) + \int -M^N (6C / x^4 + Q / x^3).$

lemma *tail-identity*:

assumes $M: \exists \leq M$ **and** $MN: M \leq N$
shows *interval-lebesgue-integral lborel* (ereal M) (ereal N) $(\lambda x. R-r \ x / x^3)$
 $= \Phi N - \Phi M + interval-lebesgue-integral lborel$ (ereal M) (ereal N)
 $(\lambda x. 6 * Cper \ x / x^4 + (R-r \ x - x * Fx \ x) / x^3)$

$C_{per} x / x^4 + (R-r x - x * Fx x) / x^3$
 $\langle proof \rangle$

lemma *integral-inv34*:

assumes $0 < M \leq N$
shows *interval-lebesgue-integral lborel* (*ereal* M) (*ereal* N) $(\lambda x. a / x^4 + b / x^3)$
 $= (- a / (3 * N^3) - b / (2 * N^2)) - (- a / (3 * M^3) - b / (2 * M^2))$
 $\langle proof \rangle$

The tail bounds, uniformly in $M \geq 3$.

lemma *tail-bounds*:

assumes $M: 3 \leq M$
shows $- \Phi M - 32 / M^3 - 1 / (4 * M^2) \leq$
set-lebesgue-integral lborel $\{M < ..\}$ $(\lambda x. R-r x / x^3)$
and *set-lebesgue-integral lborel* $\{M < ..\}$ $(\lambda x. R-r x / x^3) \leq$
 $- \Phi M + 32 / M^3 + 13 / (16 * M^2)$
 $\langle proof \rangle$

lemma *Phi-20*: $\Phi 20 = (37 / 2 - 2923 / 240) / 400 + 37 / 800$
 $\langle proof \rangle$

(5.16) (tight: $P(20) = 37/2$, $C(20) = 0$).

theorem *R-tail-20-bound*: *set-lebesgue-integral lborel* $\{20 < ..\}$ $(\lambda x. R-r x / x^3)$
 $\leq$
 $- 2689 / 48000$
 $\langle proof \rangle$

(5.17): for $40 \mid M$, $\Phi(M) = -(2923/240)/M^2 + \lambda/M$.

theorem *R-tail-M-bound*:

assumes $40 \text{ dvd } M$ $0 < M$
shows $- \lambda_{M-r} / \text{real } M + (2923 / 240 - 1 / 4) / \text{real } M^2 - 32 / \text{real } M^3$
 $\leq \text{set-lebesgue-integral lborel } \{\text{real } M < ..\} (\lambda x. R-r x / x^3)$
 $\langle proof \rangle$

26.6 Continuity off a countable set, and boundedness

D-R: the points where some $c x$ ($c \in \{1, 2, \alpha, 2\alpha, 2H-c, 2\lambda\}$) is an integer.

definition *DR* :: *real set* **where**

$DR = (\bigcup c \in \{1, 2, \alpha, 2\alpha, 2H-c, 2\lambda\}. (\lambda n :: \text{int. of-int } n / c) \text{ `UNIV})$

lemma *DR-countable*: *countable* *DR*

$\langle proof \rangle$

A function that agrees with a continuous one on an open neighbourhood is continuous there.

lemma *isCont-local*:

fixes $f\ g :: \text{real} \Rightarrow \text{real}$

assumes $\text{open } S\ y \in S \wedge z. z \in S \implies f\ z = g\ z\ \text{isCont } g\ y$

shows $\text{isCont } f\ y$

<proof>

lemma *frac-isCont*: $(y :: \text{real}) \notin \mathbb{Z} \implies \text{isCont } \text{frac } y$

<proof>

lemma *es-isCont*: $u \neq 1 / 2 \implies \text{isCont } \text{es } u$

<proof>

lemma *d0-cont*: $\text{isCont } d0\ u$ **and** *pos-cont*: $\text{isCont } \text{pos-r } u$

<proof>

lemma *isCont-R-form*:

fixes $a\ b\ c\ d\ e :: \text{real} \Rightarrow \text{real}$ **and** $x :: \text{real}$

assumes $\text{isCont } a\ x\ \text{isCont } b\ x\ \text{isCont } c\ x\ \text{isCont } d\ x\ \text{isCont } e\ x$

$\text{isCont } (\lambda x. \text{es } (a\ x))\ x\ \text{isCont } (\lambda x. \text{es } (b\ x))\ x$

shows $\text{isCont } (\lambda x. x * (4 * \text{lam-r} + 2 * \text{lam-r} * a\ x - 12 * \text{lam-r} * b\ x) +$

$Qc\ (a\ x)\ (b\ x)\ (c\ x)\ (d\ x)\ (e\ x))\ x$

<proof>

Every ingredient of *R-eq* is continuous at $x \notin D\text{-}R$.

theorem *R-isCont-off-countable*: $\exists D. \text{countable } D \wedge (\forall x. 0 < x \longrightarrow$

$x \notin D \longrightarrow \text{isCont } R\text{-}r\ x)$

<proof>

definition *DO* :: *real set* **where** $DO = \{1 / 3, 1 / 2,$

$1\} \cup \text{range } (\lambda n :: \text{nat}. 1 / \text{real } n)$

lemma *DO-countable*: $\text{countable } DO$

<proof>

theorem *outer-integrand-isCont-off-countable*: $\exists D. \text{countable } D \wedge$

$(\forall y. 0 < y \longrightarrow y \notin D \longrightarrow \text{isCont } \text{outer-integrand } y)$

<proof>

theorem *outer-integrand-bounded*: $\exists Bd. \forall y \in$

$\{1 / 3..2 * \text{lam-r}\}. |\text{outer-integrand } y| \leq Bd$

<proof>

end

theory *Zeta5-Asymptotics*

imports *Zeta5-Integral-Representation Prime-Sum-Limits Zeta5-Explicit-Integrals*

Zeta5-Uniform-Asymptotics

begin

27 Normalisation and the asymptotics of $Q_{K,M}$: Propositions 5.1 and 5.2

Section 5 of the paper: the standing hypotheses, Legendre's formula and the uniformity estimates, integrality of $Q_{K,M}$ (Proposition 5.1, *QKM-int-poly*), the small-prime sum, the prime sums through the prime number theorem, and the limit (5.21) of $K^{-2} \ln m_{K,M}$ (Proposition 5.2, *log-mKM-limsup*, *log-mKM-limsup-AM*). Lean theories *Section5*, *Prop51*, *Legendre5*, *PrimeSums*, *PNT*, *Prop52*, *Section5Final*.

27.1 The small-prime sum

lemma *hof-le-lam*: $\text{real } (\text{hof } K) \leq \text{lam-r} * \text{real } K$
 $\langle \text{proof} \rangle$

Small primes $p \leq K/M$: the contribution of $-L-p$ is $6\lambda K^2/M + o(K^2)$.

theorem *small-prime-sum-bound*:

assumes M : $0 < M$ **and** e : $0 < \varepsilon$

shows $\forall_F K$ in at-top.

$(\sum p \in \{p. p \leq K \wedge \text{prime } p \wedge p * M \leq K\}.$

$\text{real } (6 * \text{hof } K * \text{nat-log } p (5 * K) + \text{hof } K * \text{multiplicity } p (24::\text{nat})) * \ln$
 $(\text{real } p))$

$\leq (6 * \text{lam-r} / \text{real } M + \varepsilon) * \text{real } K^2$

$\langle \text{proof} \rangle$

27.2 Standing hypotheses and integrality

The standing hypotheses of Theorem 2.1.

definition *StdHyp* :: $\text{nat} \Rightarrow \text{nat} \Rightarrow \text{bool}$ **where**

$\text{StdHyp } K \ M \longleftrightarrow 40 \leq M \wedge 40 \text{ dvd } K \wedge 0 < K \wedge$

$200 * M^2 \leq K$

lemma *mKM-pos*: $0 < mKM \ K \ M$

$\langle \text{proof} \rangle$

A rational polynomial that is p -integral at every prime has integer coefficients.

lemma *int-of-vge*:

assumes $\bigwedge p. \text{prime } p \implies \text{vge } p \ x \ 0$

shows $\exists n::\text{int}. x = \text{of-int } n$

$\langle \text{proof} \rangle$

lemma *intPoly-of-vge*:

assumes $\bigwedge p. \text{prime } p \implies \text{vpGge } p \ Q \ 0$

shows $\exists P :: \text{int poly}. \text{map-poly of-int } P = Q$

$\langle \text{proof} \rangle$

27.3 Legendre's formula and the uniformity estimates

(5.3), Legendre's formula for $v\text{-}p(S\text{-}K)$ ($K > 0$; false at $K = 0$).

theorem *vpS-legendre*:

assumes *prime* $p \nmid 0 \text{ dvd } K \ 0 < K$

defines $B \equiv 2 * \text{hof } K + K + 1$

shows $vpS \ K \ p = 2 * \text{int } (\text{hof } K) * (\sum_{a=1..B} \text{int } (K \text{ div } p^a))$
 $- 12 * \text{int } (\text{hof } K) * (\sum_{a=1..B} \text{int } (\text{Nof } K \text{ div } p^a))$
 $- 2 * (\sum_{i=1..hof \ K - 1} \sum_{a=1..B} \text{int } (2 * i \text{ div } p^a))$
 $+ (\text{int } (\text{hof } K) - 1) * \text{int } (\text{multiplicity } p \ (4::nat))$

<proof>

27.4 Proposition 5.1

lemma *vp-prime-pow*:

assumes *prime* p *prime* q

shows $vp \ p \ (\text{of-nat } q \ \text{pow } k) = (\text{if } q = p \ \text{then } k \ \text{else } 0)$

<proof>

lemma *vp-mKM*:

assumes *prime* p

shows $vp \ p \ (mKM \ K \ M) = (\text{if } p \leq 2 * \text{hof } K \ \text{then } - \ Lp \ K \ M \ p \ \text{else } 0)$

<proof>

lemma *vpS-eq-0-large*:

assumes *prime* $p \nmid 0 \text{ dvd } K \ 0 < K \ 2 * \text{hof } K < p$

shows $vpS \ K \ p = 0$

<proof>

lemma *QKM-vpGge*:

assumes *StdHyp* $K \ M$ *prime* p

shows $vpGge \ p \ (QKM \ K \ M) \ 0$

<proof>

Proposition 5.1: $Q\text{-}\{K, M\} \in \mathbb{Z}[X]$. At each prime, $L\text{-}p(K, M)$ is covered by (3.12), Proposition 4.1 or Proposition 4.3.

theorem *QKM-int-poly*: *StdHyp* $K \ M \implies$

$\exists P :: \text{int poly. map-poly of-int } P = QKM \ K \ M$

<proof>

(5.7), inner range: $\gamma\text{-}p^{\wedge}in = p\Gamma(K/p) + O\text{-}M(1)$ and $v\text{-}p(S\text{-}K) = pN(K/p) + O\text{-}M(1)$, uniformly over (4.1) (the Lean constant is $1000M^{\wedge}2$).

27.5 The outer range of the uniformity estimate (Lean: Legendre5)

For $n < p^{\wedge}2$ only $a = 1$ contributes to Legendre's sum.

lemma *sum-div-pow-single*:

assumes *prime* p $1 \leq B \ n < (p :: nat) \wedge 2$
shows $(\sum a = 1..B. n \text{ div } p \wedge a) = n \text{ div } p$
 $\langle proof \rangle$

Under (4.9), Legendre's formula collapses to a single term per factorial:
 $v\text{-}p(S\text{-}K) = 2h \lfloor K/p \rfloor - 2 \sum \{-i=1\} \wedge \{h-1\} \lfloor 2i/p \rfloor$.

lemma *vpS-outer*:

assumes p : *prime* p **and** K : $40 \text{ dvd } K$ **and** h : *OuterHyp* K p
shows $vpS \ K \ p = 2 * \text{int } (hof \ K) * \text{int } (K \text{ div } p) - 2 * \text{int } (\sum i = 1..hof \ K - 1. 2 * i \text{ div } p)$
 $\langle proof \rangle$

$\sum \{-i=1\} \wedge \{h-1\} \lfloor 2i/p \rfloor = \sum \{-j=1\} \wedge \{5\} (h - \lceil jp/2 \rceil) \text{--} +$ when $2h < 6p$:
count the $j \geq 1$ with $jp \leq 2i$ and swap the sums.

lemma *sum-if-one-card*: $\text{finite } A \implies (\sum x \in A.$
if $P \ x$ *then* $(1::nat)$ *else* $0) = \text{card } \{x \in A. P \ x\}$
 $\langle proof \rangle$

lemma *half-ceil-le-iff*: $((m + 1) \text{ div } 2 \leq (i::nat)) = (m \leq 2 * i)$
 $\langle proof \rangle$

lemma *suc-pred-sub*: $1 \leq x \implies \text{Suc } (h - 1) - x = h - (x::nat)$
 $\langle proof \rangle$

lemma *half-ceil-ge-1*: $1 \leq (m::nat) \implies 1 \leq (m + 1) \text{ div } 2$
 $\langle proof \rangle$

lemma *sum-floor-eq*:

assumes p : *prime* p **and** hh : $2 * h < 6 * (p :: nat)$
shows $(\sum i = 1..h - 1. 2 * i \text{ div } p) = (\sum j = 1..5. h - (j * p + 1) \text{ div } 2)$
 $\langle proof \rangle$

The integer $K \ (R\text{-}0(p/K) - d(p/K))$, written with $N = \text{Nof } K$.

definition *Eout* :: $nat \Rightarrow nat \Rightarrow int$ **where**

$Eout \ K \ p = (\text{let } N = \text{int } (\text{Nof } K); K' = \text{int } K; p' = \text{int } p \text{ in}$
if $K < 2 * p$
then $7 * (K' - p') - 6 * \min N \ (K' - p') - 6 * \max (K' + N - 2 * p') \ 0$
 $+ \max (K' + 4 * N - 2 * p') \ 0$
else $8 * K' - 9 * p' - 8 * N - 5 * \min N \ (K' - 2 * p') - 5 * \max (K' + N - 3 * p') \ 0$
 $- \max (K' + 4 * N - 3 * p' - \max (K' + N - 3 * p') \ 0) \ 0)$

$p < K$ under (4.9) with $40 \mid K$: $p = K$ would make $40 \mid p$.

lemma *outer-p-less*:

assumes p : *prime* p **and** K : $40 \text{ dvd } K$ **and** h : *OuterHyp* K p
shows $p < K$
 $\langle proof \rangle$

lemma *odd-prime-ge-7*: $\text{prime } p \implies 7 \leq (p :: \text{nat}) \implies$
 $\neg 2 \text{ dvd } p$
 $\langle \text{proof} \rangle$

$|\neg \gamma \cdot p \hat{=} \text{out} - E\text{-out}| \leq 7$: pure integer arithmetic with $K \bmod p = K - p$
resp. $K - 2p$.

lemma *int-nat-sub*: $\text{int } (a - b) = \max (\text{int } a - \text{int } b) 0$
 $\langle \text{proof} \rangle$

lemma *int-min-nat*: $\text{int } (\min a b) = \min (\text{int } a) (\text{int } b)$
 $\langle \text{proof} \rangle$

lemma *gammaOut-sub-Eout*:
assumes p : *prime* p **and** K : $40 \text{ dvd } K$ **and** h : *OuterHyp* K p
shows $|\neg \text{gammaOut } K \ p - E\text{out } K \ p| \leq 7$
 $\langle \text{proof} \rangle$

lemma *hof-real*: $40 \text{ dvd } K \implies \text{real } (\text{hof } K) = \text{lam-r} * \text{real } K$
 $\langle \text{proof} \rangle$

lemma *Nof-real*: $40 \text{ dvd } K \implies \text{real } (\text{Nof } K) = \text{alpha-r} * \text{real } K$
 $\langle \text{proof} \rangle$

lemma *hof-le*: $\text{hof } K \leq K$ **and** *Nof-le*: $\text{Nof } K \leq K$ **and** *Nof-lt-hof*: $2 \leq$
 $K \implies \text{Nof } K < \text{hof } K$
 $\langle \text{proof} \rangle$

The real identity behind *E-out*.

lemma *mult-min-nonneg*:
assumes $0 \leq (c :: \text{real})$ **shows** $c * \min a b = \min (c * a) (c * b)$
 $\langle \text{proof} \rangle$

lemma *mult-pos-r-nonneg*:
assumes $0 \leq (c :: \text{real})$ **shows** $c * \text{pos-r } a = \max (c * a) 0$
 $\langle \text{proof} \rangle$

lemma *K-mul-R0-sub-dfun*:
assumes p : *prime* p **and** K : $40 \text{ dvd } K$ **and** h : *OuterHyp* K p
shows $\text{real } K * (R0\text{-r } (\text{real } p / \text{real } K) - \text{dfun-r } (\text{real } p / \text{real } K)) = \text{of-int } (E\text{out } K \ p)$
 $\langle \text{proof} \rangle$

$-v\text{-p}(S\text{-}K)$ against its limit (5.7, outer): an explicit sum of five bounded terms.

lemma *vpS-sub-limit*:
assumes p : *prime* p **and** K : $40 \text{ dvd } K$ **and** h : *OuterHyp* K p
shows $-\text{of-int } (vpS \ K \ p) - \text{real } K * (-2 * \text{lam-r} * \text{of-int } (\text{floor } (\text{real } K / \text{real } p))) +$

$$(\sum j = 1..5. \text{pos-r } (2 * \text{lam-r} - \text{real } j * (\text{real } p / \text{real } K))))$$

$$= \text{of-int } (\sum j = 1..5. 2 * \text{int } (\text{hof } K - (j * p + 1) \text{ div } 2) - \max (2 * \text{int } (\text{hof } K) - \text{int } j * \text{int } p) 0)$$

$$\langle \text{proof} \rangle$$

lemma *half-ceil-abs*:

fixes $h \ m :: \text{nat}$

shows $|2 * \text{int } (h - (m + 1) \text{ div } 2) - \max (2 * \text{int } h - \text{int } m) 0| \leq 1$

$\langle \text{proof} \rangle$

lemma *two-sub-half-le*:

fixes $h \ m :: \text{nat}$

shows $2 * \text{real } (h - (m + 1) \text{ div } 2) \leq \max (2 * \text{real } h - \text{real } m) 0$

$\langle \text{proof} \rangle$

lemma *vpS-sub-limit-abs*:

assumes p : *prime* p **and** K : $40 \text{ dvd } K$ **and** h : *OuterHyp* $K \ p$

shows $|- \text{of-int } (\text{vpS } K \ p) - \text{real } K * (- 2 * \text{lam-r} * \text{of-int } (\text{floor } (\text{real } K / \text{real } p))) +$

$(\sum j = 1..5. \text{pos-r } (2 * \text{lam-r} - \text{real } j * (\text{real } p / \text{real } K))))| \leq 5$

$\langle \text{proof} \rangle$

The outer analogue of (5.7) (constant 7).

theorem *uniformity-outer*:

$\exists \text{Cst}. \forall K \ p. \text{prime } p \longrightarrow 40 \text{ dvd } K \longrightarrow$

$\text{OuterHyp } K \ p \longrightarrow$

$|- \text{of-int } (\text{gammaOut } K \ p) - \text{real } K * (R0\text{-r } (\text{real } p / \text{real } K) - \text{dfun-r } (\text{real } p / \text{real } K))| \leq \text{Cst} \wedge$

$|- \text{of-int } (\text{vpS } K \ p) - \text{real } K * (- 2 * \text{lam-r} * \text{of-int } (\text{floor } (\text{real } K / \text{real } p)))$

$+$

$(\sum j = 1..5. \text{pos-r } (2 * \text{lam-r} - \text{real } j * (\text{real } p / \text{real } K))))| \leq \text{Cst}$

$\langle \text{proof} \rangle$

27.6 Exact integrals and tails

$\int -\{1/3\} \sim \{1/2\} \ d(y) \ dy = 9/640.$

theorem *integral-dfun*: *interval-lebesgue-integral lborel* (*ereal* $(1 / 3)$) (*ereal* $(1 / 2)$) *dfun-r* =

$9 / 640$

$\langle \text{proof} \rangle$

(5.12)-(5.14): $R(x) = x F(x) + Q(x)$ with $-1/2 \leq Q(x) \leq 13/8$ (for all $x > 0$).

theorem *R-decomp-bound*:

assumes $3 \leq x$

shows $- 1 / 2 \leq R\text{-r } x - x * (4 * \text{lam-r} + 2 * \text{lam-r} * \text{frac } x - 12 * \text{lam-r} * \text{frac } (\text{alpha-r} * \text{frac } x))$

$$\begin{aligned}
& x)) \wedge \\
& R-r \ x - x * (4 * lam-r + 2 * lam-r * frac \ x - 12 * lam-r * frac \ (alpha-r \\
& * x)) \leq \\
& 13 / 8 \\
& \langle proof \rangle
\end{aligned}$$

The mean of P over a period is $2923/240$.

theorem *Pper-mean: interval-lebesgue-integral lborel (ereal 0) (ereal 40) Pper / 40 = 2923 / 240*
 $\langle proof \rangle$

$R(x)/x^3$ is integrable on $[3, \infty)$.

theorem *R-integrableOn: set-integrable lborel {3..} (λx. R-r x / x ^ 3)*
 $\langle proof \rangle$

27.7 Prime sums via the prime number theorem

The prime number theorem in Chebyshev's form, from the AFP (*Prime-Number-Theorem.ϑ-asymptotic* $\vartheta \sim x$).

lemma *theta-div-tendsto: ((λx. primes-theta x / x) → 1) at-top*
 $\langle proof \rangle$

Chebyshev's bound $\vartheta(n) \leq n \log 4$ (from `Prime_Distribution_Elementary`).

lemma *sum-log-primes-le: (∑ p ∈ {p. p ≤ n ∧ prime p}. ln (real p)) ≤ ln 4 * real n*
 $\langle proof \rangle$

Outer range, variable $y = p/K$: Riemann-sum upper bound for a bounded, almost-everywhere continuous φ (step majorants + the PNT cell estimates).

theorem *outer-prime-sum-limsup:*
assumes $0 < a \leq b \wedge y. y \in \{a..b\} \implies$
 $|\varphi \ y| \leq Bd \text{ countable } D$
and $\bigwedge y. y \in \{a < .. < b\} \implies y \notin D \implies$
 $isCont \ \varphi \ y \ 0 < \varepsilon$
shows $\forall_F \ K \text{ in at-top.}$
 $(\sum p \in \{p. p \leq nat \ (floor \ (b * real \ K)) \} \wedge prime \ p \wedge$
 $a * real \ K < real \ p \wedge real \ p \leq b * real \ K\}.$
 $\varphi \ (real \ p / real \ K) * ln \ (real \ p))$
 $\leq (interval-lebesgue-integral lborel \ (ereal \ a) \ (ereal \ b) \ \varphi + \varepsilon) * real \ K$
 $\langle proof \rangle$

Inner range, variable $x = K/p$.

theorem *inner-prime-sum-limsup:*
assumes $3 < M \wedge x. x \in \{3..real \ M\} \implies$
 $|f \ x| \leq Bd \text{ countable } D$
and $\bigwedge x. x \in \{3 < .. < real \ M\} \implies x \notin D \implies$
 $isCont \ f \ x \ 0 < \varepsilon$

shows $\forall_F K$ in at-top.

$(\sum p \in \{p. p \leq K \wedge \text{prime } p \wedge K < p * M \wedge$
 $3 * p \leq K\}. \text{real } p * f(\text{real } K / \text{real } p) * \ln(\text{real } p))$
 $\leq (\text{interval-lebesgue-integral lborel } (\text{ereal } 3) (\text{ereal } (\text{real } M))) (\lambda x. f x /$
 $x \wedge 3) + \varepsilon) * \text{real } K \wedge 2$

$\langle \text{proof} \rangle$

27.8 Continuity of the limiting functions off a countable set

theorem *R-continuousAt-off*: $\exists D. \text{countable } D \wedge (\forall x. 0 < x \longrightarrow$
 $x \notin D \longrightarrow \text{isCont } R\text{-}r\ x)$

$\langle \text{proof} \rangle$

theorem *outerIntegrand-continuousAt-off*: $\exists D. \text{countable } D \wedge$
 $(\forall y. 0 < y \longrightarrow y \notin D \longrightarrow \text{isCont } \text{outer-integrand } y)$

$\langle \text{proof} \rangle$

theorem *outerIntegrand-bounded*: $\exists B d. \forall y \in$
 $\{1 / 3..2 * \text{lam-r}\}. |\text{outer-integrand } y| \leq B d$

$\langle \text{proof} \rangle$

27.9 Proposition 5.2 and (5.21)

lemma *of-rat-power-int*: $\text{of-rat } (x \text{ powi } k) = (\text{of-rat } x :: 'a :: \text{real-field}) \text{ powi } k$

$\langle \text{proof} \rangle$

lemma *ln-power-int*: $0 < x \implies \ln(x \text{ powi } k) = \text{of-int } k * \ln(x :: \text{real})$

$\langle \text{proof} \rangle$

lemma *log-mKM*:

$\ln(\text{of-rat } (mKM\ K\ M)) = (\sum p \in \{p. p \leq 2 * \text{hof } K \wedge$
 $\text{prime } p\}. - \text{of-int } (Lp\ K\ M\ p) * \ln(\text{real } p))$

$\langle \text{proof} \rangle$

$|R(x)| \leq 18M + 2$ on $[3, M]$, from (5.12)-(5.14).

theorem *R-bounded*: $\exists B d. \forall x \in \{3.. \text{real } M\}. |R\text{-}r\ x| \leq B d$

$\langle \text{proof} \rangle$

For $K < p \leq 2h$: $-v\text{-}p(S\text{-}K) \leq K \cdot \text{outerIntegrand}(p/K)$ (Legendre again, now $K < p$).

lemma *vpS-large*:

assumes p : *prime* p **and** K : $40 \text{ dvd } K$ $40 \leq K$ **and** Kp : $K < p$ **and** $p2h$: $p \leq 2$
 $* \text{hof } K$

shows $- \text{of-int } (vpS\ K\ p) \leq \text{real } K * \text{outer-integrand } (\text{real } p / \text{real } K)$

$\langle \text{proof} \rangle$

The main term of $-L\text{-}p(K, M)$.

definition *mainCoef* :: $\text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{real}$ **where**

$\text{mainCoef } K\ M\ p =$

$(\text{if } p * M \leq K \text{ then } \text{real } (6 * \text{hof } K * \text{nat-log } p (5 * K) + \text{hof } K * \text{multiplicity}$
 $p (24 :: \text{nat}))$

else if $3 * p \leq K$ then $\text{real } p * R\text{-r } (\text{real } K / \text{real } p)$
 else $\text{real } K * \text{outer-integrand } (\text{real } p / \text{real } K)$

Termwise: $-L\text{-}p \leq \text{mainCoef} + (2 \text{ } C\text{-}1 + 1 + 2 \text{ } C\text{-}2)$ for every prime $p \leq 2h$.

lemma *neg-Lp-le*:

assumes M : $40 \leq M$ **and** $C1$: $0 \leq C1$ **and** $C2$: $0 \leq C2$
and hin : $\bigwedge K \text{ p. prime } p \implies \text{InnerHyp } K \text{ } M \text{ } p \implies$
 $|\text{of-rat } (\text{gammaIn } K \text{ } M \text{ } p) - \text{real } p * \text{Gam-r } (\text{real } K / \text{real } p)| \leq C1 \wedge$
 $|\text{of-int } (\text{vpS } K \text{ } p) - \text{real } p * \text{Nfun-r } (\text{real } K / \text{real } p)| \leq C1$
and hout : $\bigwedge K \text{ p. prime } p \implies 40 \text{ dvd } K \implies$
 $\text{OuterHyp } K \text{ } p \implies$
 $|\text{of-int } (\text{gammaOut } K \text{ } p) - \text{real } K * (\text{R0-r } (\text{real } p / \text{real } K) - \text{dfun-r } (\text{real } p /$
 $\text{real } K))| \leq C2 \wedge$
 $|\text{of-int } (\text{vpS } K \text{ } p) - \text{real } K * (-2 * \text{lam-r } * \text{of-int } (\text{floor } (\text{real } K / \text{real } p)) +$
 $(\sum j = 1..5. \text{pos-r } (2 * \text{lam-r } - \text{real } j * (\text{real } p / \text{real } K))))| \leq C2$
and K : $40 \text{ dvd } K \text{ } 200 * M^2 \leq K < K$ **and** p : $\text{prime } p \text{ } p \leq 2 * \text{hof } K$
shows $-\text{of-int } (Lp \text{ } K \text{ } M \text{ } p) \leq \text{mainCoef } K \text{ } M \text{ } p + (2 * C1 + 1 + 2 * C2)$
 $\langle \text{proof} \rangle$

lemma *sum-log-P-le*:

$(\sum p \in \{p. p \leq 2 * \text{hof } K \wedge \text{prime } p\}. \ln (\text{real } p)) \leq 2 * \text{real } K * \ln 4$
 $\langle \text{proof} \rangle$

The primes $p \leq 2h$ split into the three ranges of (5.1) ($40 \mid K$, $K > 0$, $M \geq 3$), and mainCoef takes the corresponding branch on each.

lemma *three-le-mul*: $3 \leq M \implies 3 * q \leq q * (M::\text{nat})$
 $\langle \text{proof} \rangle$

lemma *not-mul-le-of-lt*: $3 \leq M \implies K < 3 * q \implies$
 $\neg q * M \leq (K::\text{nat})$
 $\langle \text{proof} \rangle$

lemma *le-of-three-mul*: $3 * q \leq K \implies q \leq (K::\text{nat})$
 $\langle \text{proof} \rangle$

lemma *primes-split*:

assumes K : $40 \text{ dvd } K \text{ } 0 < K$ **and** M : $3 \leq M$
shows $\{p. p \leq 2 * \text{hof } K \wedge \text{prime } p\} =$
 $\{p. p \leq K \wedge \text{prime } p \wedge p * M \leq K\} \cup \{p. p \leq K \wedge$
 $\text{prime } p \wedge K < p * M \wedge 3 * p \leq K\}$
 $\cup \{p. p \leq \text{nat } (\text{floor } (2 * \text{lam-r } * \text{real } K)) \wedge \text{prime } p \wedge$
 $1 / 3 * \text{real } K < \text{real } p \wedge \text{real } p \leq 2 * \text{lam-r } * \text{real } K\}$
and $\{p. p \leq K \wedge \text{prime } p \wedge p * M \leq K\} \cap \{p. p \leq K \wedge$
 $\text{prime } p \wedge K < p * M \wedge 3 * p \leq K\} = \{\}$
and $(\{p. p \leq K \wedge \text{prime } p \wedge p * M \leq K\} \cup \{p. p \leq K \wedge$
 $\text{prime } p \wedge K < p * M \wedge 3 * p \leq K\})$

$\cap \{p. p \leq \text{nat } (\text{floor } (2 * \text{lam-r} * \text{real } K)) \wedge \text{prime } p \wedge$
 $1 / 3 * \text{real } K < \text{real } p \wedge \text{real } p \leq 2 * \text{lam-r} * \text{real } K\} = \{\}$
and $\bigwedge p. p \in \{p. p \leq K \wedge \text{prime } p \wedge p * M \leq K\} \implies$
 $\text{mainCoef } K \ M \ p = \text{real } (6 * \text{hof } K * \text{nat-log } p \ (5 * K) + \text{hof } K * \text{multiplicity } p \ (24::\text{nat}))$
and $\bigwedge p. p \in \{p. p \leq K \wedge \text{prime } p \wedge K < p * M \wedge$
 $3 * p \leq K\} \implies \text{mainCoef } K \ M \ p = \text{real } p * R\text{-r } (\text{real } K / \text{real } p)$
and $\bigwedge p. p \in \{p. p \leq \text{nat } (\text{floor } (2 * \text{lam-r} * \text{real } K)) \wedge \text{prime } p \wedge$
 $1 / 3 * \text{real } K < \text{real } p \wedge \text{real } p \leq 2 * \text{lam-r} * \text{real } K\} \implies$
 $\text{mainCoef } K \ M \ p = \text{real } K * \text{outer-integrand } (\text{real } p / \text{real } K)$
 $\langle \text{proof} \rangle$

lemma *filterlim-40*: *filterlim* $(\lambda n :: \text{nat}. 40 * n)$ *at-top at-top*
 $\langle \text{proof} \rangle$

Proposition 5.2 (with $K = 40n$): $\limsup K^{-2} \log m\{K, M\} \leq I\text{-out} + 6\lambda/M + \int -3^M R(x)/x^3 dx$.

theorem *log-mKM-limsup*:
assumes $M: 40 \leq M$ **and** $e: 0 < \varepsilon$
shows $\forall_F n$ *in at-top*.
 $\ln (\text{of-rat } (mKM \ (40 * n) \ M)) / \text{real } (40 * n)^{-2} \leq$
 $\text{of-rat } I\text{out} + 6 * \text{lam-r} / \text{real } M$
 $+ \text{interval-lebesgue-integral lborel } (ereal \ 3) \ (ereal \ (\text{real } M)) \ (\lambda x. R\text{-r } x / x^{-3}) +$
 ε
 $\langle \text{proof} \rangle$

(5.21): $\limsup K^{-2} \log m\{K, M\} \leq A\text{-}M$ for $M \in 40\mathbb{Z}$, $M \geq 40$: split the integral at 20 and at M and use (5.16)-(5.18).

theorem *log-mKM-limsup-AM*:
assumes $M: 40 \leq M$ $40 \text{ dvd } M$ **and** $e: 0 < \varepsilon$
shows $\forall_F n$ *in at-top*. $\ln (\text{of-rat } (mKM \ (40 * n) \ M)) / \text{real } (40 * n)^{-2} \leq$
 $\text{of-rat } (AM \ M) + \varepsilon$
 $\langle \text{proof} \rangle$

end

theory *Zeta5-Equilibrium-Measure*
imports *Zeta5-Asymptotics HOL-Complex-Analysis.Complex-Analysis*
HOL-Decision-Procs.Approximation
begin

28 The comparison measure ϱ and its logarithmic potential

Appendix A of the paper: the measure $\varrho = \sum c_j \omega_{[a_j, b_j]}$ of Table 1 as a single density, its logarithmic potential and energy in closed form ((A.1),

(A.2)), the analytic half of the potential inequality (A.9) (the tail $[2, \infty)$), and the bounds on the mass of short intervals used in Section 6. Lean theories *AppendixA*, *Lemma61*, *Lemma61Pot*.

28.1 Table 1

$\sum c\text{-}j = 37/40 \cdot 10^{\wedge 12}$: the mass of ϱ is λ . Trivial (simp/eval).

lemma *table1-sum-c*: $(\sum e \leftarrow \text{table1}. \text{snd} (\text{snd } e)) = 37 * 10^{\wedge 12} \text{ div } 40$
 $\langle \text{proof} \rangle$

Nesting $0 < a\text{-}1\text{-}6 < \dots < a\text{-}1 < b\text{-}1 < \dots < b\text{-}1\text{-}6 < 2$ and $b\text{-}j - a\text{-}j > 1/225$. Trivial.

lemma *table1-nested*:
 $\text{sorted-wrt } (\lambda x y. y < x) (\text{map fst table1}) \wedge$
 $\text{sorted-wrt } (<) (\text{map } (\text{fst} \circ \text{snd}) \text{ table1}) \wedge$
 $(\forall e \in \text{set table1}. 0 < \text{fst } e \wedge \text{fst } e < \text{fst} (\text{snd } e) \wedge$
 $\text{fst} (\text{snd } e) < 2 * 10^{\wedge 12} \wedge$
 $10^{\wedge 12} < 225 * (\text{fst} (\text{snd } e) - \text{fst } e))$
 $\langle \text{proof} \rangle$

lemma *sum-list-dens-measurable* [*measurable*]:
 $(\lambda t. \sum e \leftarrow xs. tC\ e * \text{arcsine-dens } (tA\ e) (tB\ e) t) \in$
 $\text{borel-measurable borel}$
 $\langle \text{proof} \rangle$

lemma *sum-list-map-zero*: $(\bigwedge e. e \in \text{set } xs \implies f\ e = 0) \implies$
 $(\sum e \leftarrow xs. f\ e) = (0 :: \text{real})$
 $\langle \text{proof} \rangle$

lemma *nn-integral-sum-list-dens*:
assumes $\forall e \in \text{set } xs. 0 \leq tC\ e \wedge tA\ e < tB\ e$
shows $(\int^+ t. \text{ennreal } (\sum e \leftarrow xs. tC\ e * \text{arcsine-dens } (tA\ e) (tB\ e) t) \partial \text{lborel})$
 $= \text{ennreal } (\sum e \leftarrow xs. tC\ e)$
 $\langle \text{proof} \rangle$

lemma *table1-props*: $\forall e \in \text{set table1}. 0 \leq tC\ e \wedge tA\ e < tB\ e \wedge$
 $0 < tA\ e \wedge tB\ e < 2$
 $\langle \text{proof} \rangle$

lemma *table1-sum-tC*: $(\sum e \leftarrow \text{table1}. tC\ e) = \text{lam-r}$
 $\langle \text{proof} \rangle$

theorem *rho-univ*: $\text{emeasure rho UNIV} = \text{ennreal lam-r}$
 $\langle \text{proof} \rangle$

theorem *rho-compl*: $\text{emeasure rho } (- \{0 < .. < 2\}) = 0$

$\langle proof \rangle$

(A.2): $I(\varrho) = \sum -j (S_j^2 - S_{j-1}^2) \log((b_j - a_j)/4)$ (nesting makes the j -th potential constant on every earlier interval).

The sixteen arcsine potentials U_k and their constant values L_k on their intervals.

definition $Uk :: nat \Rightarrow real \Rightarrow real$ **where** $Uk\ k\ t = \logPot\ (\arcsine\ (tA\ (table1\ !\ k))\ (tB\ (table1\ !\ k)))\ t$

definition $Lk :: nat \Rightarrow real$ **where** $Lk\ k = \ln\ ((tB\ (table1\ !\ k) - tA\ (table1\ !\ k)) / 4)$

definition $cK :: nat \Rightarrow real$ **where** $cK\ k = tC\ (table1\ !\ k)$

lemma $table1\text{-}nth$: $k < 16 \implies 0 < tA\ (table1\ !\ k) \wedge tA\ (table1\ !\ k) < tB\ (table1\ !\ k) \wedge tB\ (table1\ !\ k) < 2 \wedge 0 \leq cK\ k$
 $\langle proof \rangle$

lemma $table1\text{-}nested\text{-}nth$: $j \leq k \implies k < 16 \implies tA\ (table1\ !\ k) \leq tA\ (table1\ !\ j) \wedge tB\ (table1\ !\ j) \leq tB\ (table1\ !\ k)$
 $\langle proof \rangle$

lemma $Uk\text{-}eq$: $k < 16 \implies Uk\ k\ t = (if\ tA\ (table1\ !\ k) \leq t \wedge t \leq tB\ (table1\ !\ k)\ then\ Lk\ k\ else\ \ln\ ((|t - (tA\ (table1\ !\ k) + tB\ (table1\ !\ k)) / 2| + \sqrt{(t - tA\ (table1\ !\ k)) * (t - tB\ (table1\ !\ k))}) / 2))$
 $\langle proof \rangle$

lemma $Uk\text{-}const$: $k < 16 \implies tA\ (table1\ !\ k) \leq t \implies t \leq tB\ (table1\ !\ k) \implies Uk\ k\ t = Lk\ k$
 $\langle proof \rangle$

lemma $Uk\text{-}bounds$: $k < 16 \implies 0 < t \implies t < 2 \implies Lk\ k \leq Uk\ k\ t \wedge Uk\ k\ t \leq \ln\ 2$
 $\langle proof \rangle$

lemma $Uk\text{-}measurable\ [measurable]$: $k < 16 \implies Uk\ k \in \text{borel-measurable borel}$
 $\langle proof \rangle$

lemma $Uk\text{-}integrable$: $j < 16 \implies k < 16 \implies integrable\ (\arcsine\ (tA\ (table1\ !\ j))\ (tB\ (table1\ !\ j)))\ (Uk\ k)$
 $\langle proof \rangle$

$\int U_k\ d\omega_j = L_{\{max(j,k)\}}$: by nesting the outer potential is constant on the inner interval; otherwise swap (Fubini).

lemma $Uk\text{-}integral$:
assumes $j < 16\ k < 16$
shows $integral^L\ (\arcsine\ (tA\ (table1\ !\ j))\ (tB\ (table1\ !\ j)))\ (Uk\ k) = Lk\ (max\ j\ k)$
 $\langle proof \rangle$

$U\hat{\varrho}(t) = \sum -k \ c-k \ U-k(t)$ and $I(\varrho) = \sum -\{j,k\} \ c-j \ c-k \ L-\{max(j,k)\}$.

lemma *logPot-rho*: $logPot \ rho \ t = (\sum \ k < 16. \ cK \ k * Uk \ k \ t)$

<proof>

lemma *dens-Uk-integrable*:

assumes $j: j < 16$ **and** $k: k < 16$

shows $integrable \ lborel \ (\lambda t. \ arcsine-dens \ (tA \ (table1 \ ! \ j)) \ (tB \ (table1 \ ! \ j)) \ t * Uk \ k \ t)$

<proof>

lemma *dens-Uk-integral*:

assumes $j: j < 16$ **and** $k: k < 16$

shows $(\int \ t. \ arcsine-dens \ (tA \ (table1 \ ! \ j)) \ (tB \ (table1 \ ! \ j)) \ t * Uk \ k \ t \ \partial lborel) = Lk \ (max \ j \ k)$

<proof>

lemma *logEnergy-rho*: $logEnergy \ rho = (\sum \ j < 16. \ \sum \ k < 16. \ cK \ j * cK \ k * Lk \ (max \ j \ k))$

<proof>

lemma *sum-max-regroup*:

fixes $c \ L :: nat \Rightarrow real$

shows $(\sum \ j < n. \ \sum \ k < n. \ c \ j * c \ k * L \ (max \ j \ k)) = (\sum \ j < n. \ ((\sum \ i \leq j. \ c \ i) \wedge 2 - (\sum \ i < j. \ c \ i) \wedge 2) * L \ j)$

<proof>

lemma *Spart-eq*: $j \leq 16 \implies Spart \ j = (\sum \ i < j. \ cK \ i)$

<proof>

(A.2): $I(\varrho) = \sum -j \ (S-j\hat{2} - S-\{j-1\}\hat{2}) \ log((b-j - a-j)/4)$.

theorem *energy-A2*:

$logEnergy \ rho = (\sum \ j < 16. \ (Spart \ (j + 1) \wedge 2 - Spart \ j \wedge 2) * \ln \ ((tB \ (table1 \ ! \ j) - tA \ (table1 \ ! \ j)) / 4))$

<proof>

28.2 Elementary enclosures

Partial sums of the atanh series.

definition *atS* :: $real \Rightarrow nat \Rightarrow real$ **where**

$atS \ z \ m = (\sum \ k < m. \ 2 * (1 / (2 * real \ k + 1)) * z \wedge (2 * k + 1))$

(A.3): $S-m(z) \leq \log((1+z)/(1-z)) \leq S-m(z) + 2z\wedge\{2m+1\}/((2m+1)(1-z\hat{2}))$

for $0 \leq z < 1$.

lemma *log-series-bounds*:

assumes $0 \leq z \ z < 1$

shows $atS \ z \ m \leq \ln \ ((1 + z) / (1 - z)) \wedge$

$$\ln((1+z)/(1-z)) \leq \text{atS } z \, m + 2 * z^{\wedge}(2 * m + 1) / ((2 * \text{real } m + 1) * (1 - z^{\wedge} 2))$$
 <proof>

(A.10): the enclosures of $I(\varrho)$ and C^* (18 logarithms to 25 digits; in Isabelle either *approximation* or (A.3) evaluated by *simp*). The endpoints combine to exactly $-1366995564511/10^{\wedge}1^{\wedge}2$, so (6.4) rests on the strict enclosures.

The explicit value of $I(\varrho)$ as a combination of sixteen logarithms of rationals.

lemma *logEnergy-explicit*:

$$\text{logEnergy } \rho = (\sum j < 16. (\text{Spart } (j + 1)^{\wedge} 2 - \text{Spart } j^{\wedge} 2) * \ln((\text{tB } (\text{table1 } ! j) - \text{tA } (\text{table1 } ! j)) / 4))$$
 <proof>

A finite sum over sixteen indices, unfolded.

lemma *sum16*: $(\sum j < 16. f \, j) = f \, 0 + f \, 1 + f \, 2 + f \, 3 + f \, 4 + f \, 5 + f \, 6 + f \, 7 + f \, 8 + f \, 9 + f \, 10 + f \, 11 + f \, 12 + f \, 13 + f \, 14 + f \, 15$
 for $f :: \text{nat} \Rightarrow \text{real}$
 <proof>

28.3 (A.9): the potential inequality on the half-line

The certified-checker part. Lean defines computable rational upper/lower bounds for $\sqrt{\cdot}$, $\log$, $\arctan$ (soundness lemmas), a checker $\text{chk } l \, r = (2 \cdot \text{Ubnd } l \, r - \text{VL } l \, r \leq \text{Bd})$ with $\text{Bd} = -66451/10^{\wedge}4$, and checks a chain of 1,052 intervals covering $[0, 2]$ by kernel evaluation. In Isabelle the bound functions can be *lb-ln/ub-ln*, *lb-sqrt/ub-sqrt*, *lb-arctan/ub-arctan* from HOL-Decision_Procs.Approximation_Bounds (soundness: *bnds-ln*, *bnds-sqrt*, *bnds-arctan*); the evaluation is by *eval* (oracle) or *code-simp* (kernel).

Closed forms: $\int -0^{\wedge}c \log(t + u^{\wedge}2) \, du = c \log(t + c^{\wedge}2) - 2c + 2\sqrt{t} \arctan(c/\sqrt{t})$ for $t > 0$, and $2(c \log c - c)$ at $t = 0$.

lemma *Ic-closed*:

assumes $0 < t < c$
 shows $\text{integral } \{0..c\} (\lambda u. \ln(t + u^{\wedge}2)) = c * \ln(t + c^{\wedge}2) - 2 * c + 2 * \text{sqrt } t * \arctan(c / \text{sqrt } t)$
 <proof>

lemma *Ic-zero*:

assumes $0 < c$
 shows $\text{integral } \{0..c\} (\lambda(u::\text{real}). \ln(0 + u^{\wedge}2)) = 2 * (c * \ln c - c)$
 <proof>

lemma *Vf-closed*:

assumes $0 < t$

shows $Vf\ t = 2 * pi * sqrt\ t + (ln\ (t + 1) - 2 + 2 * sqrt\ t * arctan\ (1 / sqrt\ t))$
 $- 6 * (3 / 40 * ln\ (t + (3 / 40) ^ 2) - 2 * (3 / 40) + 2 * sqrt\ t * arctan\ (3 / 40 / sqrt\ t))$
 $\langle proof \rangle$

lemma *Vf-zero*: $Vf\ 0 = - 2 - 6 * (2 * (3 / 40 * ln\ (3 / 40) - 3 / 40))$
 $\langle proof \rangle$

(6.8) on $[2, \infty)$, by hand: $2U^{\varrho}(t) - V(t) \leq (13/10) \log t + 6\alpha^3/t - 2\pi\sqrt{t}$.

lemma *Uk-le-log*: $k < 16 \implies 2 \leq t \implies Uk\ k\ t \leq ln\ t$
 $\langle proof \rangle$

lemma *sum-cK*: $(\sum\ k < 16. cK\ k) = lam-r$
 $\langle proof \rangle$

lemma *logPot-le-of-two-le*: $2 \leq t \implies logPot\ rho\ t \leq lam-r * ln\ t$
 $\langle proof \rangle$

lemma *Ic1-ge*: $0 < t \implies ln\ t \leq$
 $integral\ \{0..1\}\ (\lambda(u::real). ln\ (t + u ^ 2))$
 $\langle proof \rangle$

lemma *Icalpha-le*: $0 < (t::real) \implies$
 $integral\ \{0..3 / 40\}\ (\lambda u. ln\ (t + u ^ 2)) \leq 3 / 40 * ln\ (t + (3 / 40) ^ 2)$
 $\langle proof \rangle$

(6.8) on $[2, \infty)$, by hand.

lemma *tail-bound*: $2 \leq t \implies 2 * logPot\ rho\ t - Vf\ t < - 6645002 / 10 ^ 6$
 $\langle proof \rangle$

28.4 Ingredients of (6.9) that live here

The circle average of $\log|z - a|$ (*circ-log*) is proved in the circle-average section above (a second copy of the statement here was a duplicate fact declaration).

The mass bound for ϱ : $\varrho([x - r, x + r]) \leq 40\sqrt{r}$ (from the density).

lemma *table1-gap*: $\forall e \in set\ table1. 1 / 225 < tB\ e - tA\ e$
 $\langle proof \rangle$

lemma *rho-Icc-aux*:

assumes $\forall e \in set\ xs. 0 \leq tC\ e \wedge tA\ e < tB\ e \wedge$

```

1 / 225 < tB e - tA e and r: 0 ≤ r
shows (∫+ t. ennreal (∑ e ← xs. tC e *
  arcsine-dens (tA e) (tB e) t) * indicator {x - r..x + r} t ∂lborel)
  ≤ ennreal ((∑ e ← xs. tC e) * (40 * sqrt r))
⟨proof⟩

lemma rho-Icc-le: 0 ≤ r ⇒
  emeasure rho {x - r..x + r} ≤ ennreal (40 * sqrt r)
⟨proof⟩

(6.7): 2U∧ρ(t) - V(t) + √t/K ≤ M-0 + √2/K for t ≥ 0, K ≥ 40.

lemma V-lower: 2 ≤ t ⇒
  2 * pi * sqrt t + (1 - 6 * alpha-r) * ln t - 2 * alpha-r∧3 / t ≤ V t
⟨proof⟩

end

theory Zeta5-Numeric-Enclosures
imports Zeta5-Equilibrium-Measure HOL-Decision-Procs.Approximation
begin

```

29 Numeric enclosures: (A.9), (A.10) and Lemma 6.1

The explicit numeric inequalities of Appendix A: the sixteen-term enclosures (A.10) of the energy of ρ and the region check (A.9) of the potential inequality on $[0, 2]$, followed by the statements that depend on them (Lemma 6.1, (6.4), (6.7)). Every numeric fact is marked (** numeric **) and is proved by the *approximation* method of HOL-Decision_Procs, whose certified interval arithmetic runs through the *holds* oracle of code evaluation; these 72 facts are the only source of the oracle in the final theorem (*thm-oracles zeta5-irrational* lists only *holds*). The Lean formalisation performs the same checks by kernel computation on 1052 dyadic intervals (Lean theories *Lemma61Check*, *Lemma61Final*).

29.1 Elementary enclosures (A.10)

```

definition eterm :: nat ⇒ real where
  eterm j = (Spart (j + 1)∧2 - Spart j∧2) * ln ((tB (table1 ! j) - tA (table1
! j)) / 4)

lemma eterm-0: - 737284788112975 / 1000000000000000000 < eterm 0 ∧
  eterm 0 < - 737284788112774 / 1000000000000000000
⟨proof⟩

```

lemma *eterm-1*: $- 8523957090042450 / 10000000000000000 < \text{eterm } 1 \wedge$
 $\text{eterm } 1 < - 8523957090042249 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *eterm-2*: $- 26925610911599487 / 10000000000000000 < \text{eterm } 2 \wedge$
 $\text{eterm } 2 < - 26925610911599286 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *eterm-3*: $- 59722954555535072 / 10000000000000000 < \text{eterm } 3 \wedge$
 $\text{eterm } 3 < - 59722954555534871 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *ln-split-4*: $\ln (65272891657 / 400000000000 :: \text{real}) =$
 $\ln (65272891657 / 62500000000) - 6 * \ln 2$
 $\langle \text{proof} \rangle$

lemma *eterm-4*: $- 99809230236437933 / 10000000000000000 < \text{eterm } 4 \wedge$
 $\text{eterm } 4 < - 99809230236429932 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *eterm-5*: $- 145606013686162115 / 10000000000000000 < \text{eterm } 5 \wedge$
 $\text{eterm } 5 < - 145606013686161914 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *ln-split-6*: $\ln (144041816267 / 400000000000 :: \text{real}) =$
 $\ln (144041816267 / 125000000000) - 5 * \ln 2$
 $\langle \text{proof} \rangle$

lemma *eterm-6*: $- 186983992097036267 / 10000000000000000 < \text{eterm } 6 \wedge$
 $\text{eterm } 6 < - 186983992097028266 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *eterm-7*: $- 221100588014681656 / 10000000000000000 < \text{eterm } 7 \wedge$
 $\text{eterm } 7 < - 221100588014681455 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *ln-split-8*: $\ln (269180899217 / 400000000000 :: \text{real}) =$
 $\ln (269180899217 / 250000000000) - 4 * \ln 2$
 $\langle \text{proof} \rangle$

lemma *eterm-8*: $- 241370916063655491 / 10000000000000000 < \text{eterm } 8 \wedge$
 $\text{eterm } 8 < - 241370916063647490 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *eterm-9*: $- 247972224603869700 / 10000000000000000 < \text{eterm } 9 \wedge$
 $\text{eterm } 9 < - 247972224603869499 / 10000000000000000$
 $\langle \text{proof} \rangle$

lemma *eterm-10*: $- 237562912254961608 / 10000000000000000 < \text{eterm } 10 \wedge$

$eterm\ 10 < -\ 237562912254961407 / 1000000000000000000$
 $\langle proof \rangle$

lemma *ln-split-11*: $\ln (128866386789 / 1000000000000 :: real) =$
 $\ln (128866386789 / 125000000000) - 3 * \ln 2$
 $\langle proof \rangle$

lemma *eterm-11*: $- 216269698612393279 / 1000000000000000000 < eterm\ 11 \wedge$
 $eterm\ 11 < - 216269698612385278 / 1000000000000000000$
 $\langle proof \rangle$

lemma *eterm-12*: $- 182633164362425959 / 1000000000000000000 < eterm\ 12 \wedge$
 $eterm\ 12 < - 182633164362425758 / 1000000000000000000$
 $\langle proof \rangle$

lemma *eterm-13*: $- 138201939148464454 / 1000000000000000000 < eterm\ 13 \wedge$
 $eterm\ 13 < - 138201939148464253 / 1000000000000000000$
 $\langle proof \rangle$

lemma *eterm-14*: $- 94725877510899352 / 1000000000000000000 < eterm\ 14 \wedge$
 $eterm\ 14 < - 94725877510899151 / 1000000000000000000$
 $\langle proof \rangle$

lemma *eterm-15*: $- 18447081210789815 / 1000000000000000000 < eterm\ 15 \wedge$
 $eterm\ 15 < - 18447081210789614 / 1000000000000000000$
 $\langle proof \rangle$

lemma *logEnergy-eterm*: $\logEnergy\ rho = (\sum\ j < 16.\ eterm\ j)$
 $\langle proof \rangle$

theorem *enclosures-A10*:
 $- 2126593445148 / 10 \wedge 12 < \logEnergy\ rho \wedge \logEnergy\ rho < - 2126593445147$
 $/ 10 \wedge 12 \wedge$
 $2653035990340 / 10 \wedge 12 < Cstar \wedge Cstar < 2653035990341 / 10 \wedge 12$
 $\langle proof \rangle$

29.2 (A.9): the region check on $[0, 2]$

(A.9) on $[0, 2]$. Lean checks 1052 dyadic intervals with certified rational bounds for $\sqrt{\cdot}$, $\log$, $\arctan$ (*decide + kernel*). Isabelle route: $2\ U^{\wedge}_{\varrho}(t) - V(t)$ is an explicit expression in $\ln$, $\sqrt{\cdot}$, $\arctan$ of t on each of the 33 regions cut out by the table endpoints $a-16 < \dots < a-1 < b-1 < \dots < b-16$ (*Uk-eq*, *Vf-closed*); on each region the inequality $\forall t \in [l, r].\ expr(t) \leq Bd$ is proved by *approximation N* (*splitting: t = k*) (* numeric *).

lemma *Uk-max*:

assumes *k*: $k < 16$

shows $Uk\ k\ t = \ln (max ((tB (table1 ! k) - tA (table1 ! k)) / 4)$
 $((|t - (tA (table1 ! k) + tB (table1 ! k)) / 2| + \sqrt{\max 0 ((t -$

$tA \text{ (table1 ! } k)) * (t - tB \text{ (table1 ! } k)))) / 2))$
 $\langle proof \rangle$

definition $Vc :: real \Rightarrow real$ **where**

$Vc \ t = 2 * pi * sqrt \ t + (ln \ (t + 1) - 2 + 2 * sqrt \ t * (pi / 2 - arctan \ (sqrt$
 $t)))$
 $- 6 * (3 / 40 * ln \ (t + (3 / 40) ^ 2) - 2 * (3 / 40) + 2 * sqrt \ t * (pi$
 $/ 2 -$
 $arctan \ (sqrt \ t / (3 / 40))))$

lemma $Vf \text{--} Vc$: **assumes** $0 \leq t$ **shows** $Vf \ t = Vc \ t$

$\langle proof \rangle$

definition $Eb :: real \Rightarrow real$ **where**

$Eb \ t = 2 * (10515596180 / 1000000000000 * ln \ (max \ (5085947445 / 4000000000000)$
 $((|t -$
 $12899443617 / 2000000000000| + sqrt \ (max \ 0 \ ((t - 3906748086 / 1000000000000)$
 $* (t -$
 $8992695531 / 1000000000000)))) / 2)) +$
 $29471737793 / 1000000000000 * ln \ (max \ (13028749591 / 4000000000000)$
 $((|t - 17653246119 /$
 $2000000000000| + sqrt \ (max \ 0 \ ((t - 2312248264 / 1000000000000) * (t -$
 $15340997855 /$
 $1000000000000)))) / 2)) +$
 $42934365099 / 1000000000000 * ln \ (max \ (24327894059 / 4000000000000)$
 $((|t - 27132467389 /$
 $2000000000000| + sqrt \ (max \ 0 \ ((t - 1402286665 / 1000000000000) * (t -$
 $25730180724 /$
 $1000000000000)))) / 2)) +$
 $58204231966 / 1000000000000 * ln \ (max \ (41027852890 / 4000000000000)$
 $((|t - 42791303602 /$
 $2000000000000| + sqrt \ (max \ 0 \ ((t - 881725356 / 1000000000000) * (t -$
 $41909578246 /$
 $1000000000000)))) / 2)) +$
 $69037621310 / 1000000000000 * ln \ (max \ (65272891657 / 4000000000000)$
 $((|t - 66429287469 /$
 $2000000000000| + sqrt \ (max \ 0 \ ((t - 578197906 / 1000000000000) * (t -$
 $65851089563 /$
 $1000000000000)))) / 2)) +$
 $78873099189 / 1000000000000 * ln \ (max \ (99084713271 / 4000000000000)$
 $((|t - 99877362497 /$
 $2000000000000| + sqrt \ (max \ 0 \ ((t - 396324613 / 1000000000000) * (t -$
 $99481037884 /$
 $1000000000000)))) / 2)) +$
 $84856120711 / 1000000000000 * ln \ (max \ (144041816267 / 4000000000000)$
 $((|t -$
 $144609638649 / 2000000000000| + sqrt \ (max \ 0 \ ((t - 283911191 /$
 $1000000000000) * (t -$
 $144325727458 / 1000000000000)))) / 2)) +$

$$\begin{aligned}
& 88396082127 / 100000000000 * \ln (\max (200893556541 / 400000000000) \\
& ((|t - \\
& \quad 201317968917 / 200000000000| + \sqrt{\max 0 ((t - 212206188 / \\
& 100000000000) * (t - \\
& \quad 201105762729 / 100000000000))}) / 2)) + \\
& 88303382125 / 100000000000 * \ln (\max (269180899217 / 400000000000) \\
& ((|t - \\
& \quad 269511094589 / 200000000000| + \sqrt{\max 0 ((t - 165097686 / \\
& 100000000000) * (t - \\
& \quad 269345996903 / 100000000000))}) / 2)) + \\
& 85472321255 / 100000000000 * \ln (\max (346956207024 / 400000000000) \\
& ((|t - \\
& \quad 347222901288 / 200000000000| + \sqrt{\max 0 ((t - 133347132 / \\
& 100000000000) * (t - \\
& \quad 347089554156 / 100000000000))}) / 2)) + \\
& 78899184238 / 100000000000 * \ln (\max (430695182301 / 400000000000) \\
& ((|t - \\
& \quad 430918226529 / 200000000000| + \sqrt{\max 0 ((t - 111522114 / \\
& 100000000000) * (t - \\
& \quad 430806704415 / 100000000000))}) / 2)) + \\
& 70353471918 / 100000000000 * \ln (\max (515465547156 / 400000000000) \\
& ((|t - \\
& \quad 515658245866 / 200000000000| + \sqrt{\max 0 ((t - 96349355 / 100000000000) \\
& * (t - \\
& \quad 515561896511 / 100000000000))}) / 2)) + \\
& 58838976615 / 100000000000 * \ln (\max (595362962907 / 400000000000) \\
& ((|t - \\
& \quad 595534594185 / 200000000000| + \sqrt{\max 0 ((t - 85815639 / 100000000000) \\
& * (t - \\
& \quad 595448778546 / 100000000000))}) / 2)) + \\
& 44421321106 / 100000000000 * \ln (\max (664162715772 / 400000000000) \\
& ((|t - \\
& \quad 664320051194 / 200000000000| + \sqrt{\max 0 ((t - 78667711 / 100000000000) \\
& * (t - \\
& \quad 664241383483 / 100000000000))}) / 2)) + \\
& 30462865791 / 100000000000 * \ln (\max (716086447547 / 400000000000) \\
& ((|t - \\
& \quad 716234706677 / 200000000000| + \sqrt{\max 0 ((t - 74129565 / 100000000000) \\
& * (t - \\
& \quad 716160577112 / 100000000000))}) / 2)) + \\
& 5959622577 / 100000000000 * \ln (\max (746565554359 / 400000000000) \\
& ((|t - 746709036979 / \\
& \quad 200000000000| + \sqrt{\max 0 ((t - 71741310 / 100000000000) * (t - \\
& 746637295669 / \\
& \quad 100000000000))}) / 2))) - V_c t
\end{aligned}$$

lemma *Eb-eq*: assumes $0 \leq t$ shows $2 * \log \text{Pot } \rho h o \ t - \text{Vf } t = \text{Eb } t$
<proof>

lemma *Eb-R29*: $595448778546 / 100000000000 \leq t \wedge$
 $t \leq 664241383483 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R28*: $515561896511 / 100000000000 \leq t \wedge$
 $t \leq 595448778546 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R30*: $664241383483 / 100000000000 \leq t \wedge$
 $t \leq 716160577112 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R23*: $144325727458 / 100000000000 \leq t \wedge$
 $t \leq 201105762729 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R24*: $201105762729 / 100000000000 \leq t \wedge$
 $t \leq 269345996903 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R25*: $269345996903 / 100000000000 \leq t \wedge$
 $t \leq 347089554156 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R26*: $347089554156 / 100000000000 \leq t \wedge$
 $t \leq 430806704415 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R27*: $430806704415 / 100000000000 \leq t \wedge$
 $t \leq 515561896511 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R31*: $716160577112 / 100000000000 \leq t \wedge$
 $t \leq 746637295669 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R16*: $3906748086 / 100000000000 \leq t \wedge$
 $t \leq 8992695531 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R18*: $15340997855 / 100000000000 \leq t \wedge$
 $t \leq 25730180724 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R19*: $25730180724 / 100000000000 \leq t \wedge$
 $t \leq 41909578246 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
<proof>

lemma *Eb-R20*: $41909578246 / 100000000000 \leq t \wedge$

$t \leq 65851089563 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R21*: $65851089563 / 100000000000 \leq t \wedge$
 $t \leq 99481037884 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R22*: $99481037884 / 100000000000 \leq t \wedge$
 $t \leq 144325727458 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-Q0*: $8992695531 / 100000000000 \leq t \wedge$
 $t \leq 9786233321 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-Q2*: $10579771112 / 100000000000 \leq t \wedge$
 $t \leq 11373308902 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-Q3*: $11373308902 / 100000000000 \leq t \wedge$
 $t \leq 12166846693 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-P0*: $9786233321 / 100000000000 \leq t \wedge$
 $t \leq 9984617768 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-P2*: $10183002216 / 100000000000 \leq t \wedge$
 $t \leq 10381386664 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-P3*: $10381386664 / 100000000000 \leq t \wedge$
 $t \leq 10579771112 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *ln-shift64*: **assumes** $0 \leq t$ **shows** $\ln(t + (3 / 40)^2) =$
 $\ln(64 * (t + (3 / 40)^2)) - 6 * \ln(2 :: real)$
 $\langle proof \rangle$

lemma *Eb-P1*: $9984617768 / 100000000000 \leq t \wedge$
 $t \leq 10183002216 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-T17b*: $12166846693 / 100000000000 \leq t \wedge$
 $t \leq 15340997855 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R11*: $396324613 / 100000000000 \leq t \wedge$
 $t \leq 578197906 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$

$\langle proof \rangle$

lemma *Eb-R12*: $578197906 / 1000000000000 \leq t \wedge$
 $t \leq 881725356 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R13*: $881725356 / 1000000000000 \leq t \wedge$
 $t \leq 1402286665 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R14*: $1402286665 / 1000000000000 \leq t \wedge$
 $t \leq 2312248264 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R15*: $2312248264 / 1000000000000 \leq t \wedge$
 $t \leq 3906748086 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R0*: $0 \leq t \wedge t \leq 71741310 / 1000000000000 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R1*: $71741310 / 1000000000000 \leq t \wedge$
 $t \leq 74129565 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R2*: $74129565 / 1000000000000 \leq t \wedge$
 $t \leq 78667711 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R3*: $78667711 / 1000000000000 \leq t \wedge$
 $t \leq 85815639 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R4*: $85815639 / 1000000000000 \leq t \wedge$
 $t \leq 96349355 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R5*: $96349355 / 1000000000000 \leq t \wedge$
 $t \leq 111522114 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R6*: $111522114 / 1000000000000 \leq t \wedge$
 $t \leq 133347132 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-R7*: $133347132 / 1000000000000 \leq t \wedge$
 $t \leq 165097686 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-R8: $165097686 / 100000000000 \leq t \wedge$
 $t \leq 212206188 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-R9: $212206188 / 100000000000 \leq t \wedge$
 $t \leq 283911191 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-R10: $283911191 / 100000000000 \leq t \wedge$
 $t \leq 396324613 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S0: $746637295669 / 100000000000 \leq t \wedge$
 $t \leq 800000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S1: $800000000000 / 100000000000 \leq t \wedge$
 $t \leq 900000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S2: $900000000000 / 100000000000 \leq t \wedge$
 $t \leq 1000000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S3: $1000000000000 / 100000000000 \leq t \wedge$
 $t \leq 1100000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S4: $1100000000000 / 100000000000 \leq t \wedge$
 $t \leq 1200000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S5: $1200000000000 / 100000000000 \leq t \wedge$
 $t \leq 1300000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S6: $1300000000000 / 100000000000 \leq t \wedge$
 $t \leq 1400000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S7: $1400000000000 / 100000000000 \leq t \wedge$
 $t \leq 1500000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma Eb-S8: $1500000000000 / 100000000000 \leq t \wedge$
 $t \leq 1600000000000 / 100000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-S9*: $1600000000000 / 1000000000000 \leq t \wedge$
 $t \leq 1700000000000 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-S10*: $1700000000000 / 1000000000000 \leq t \wedge$
 $t \leq 1800000000000 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-S11*: $1800000000000 / 1000000000000 \leq t \wedge$
 $t \leq 1900000000000 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-S12*: $1900000000000 / 1000000000000 \leq t \wedge$
 $t \leq 2000000000000 / 1000000000000 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-51*: $1900000000000 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-50*: $1800000000000 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-49*: $1700000000000 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-48*: $1600000000000 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-47*: $1500000000000 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-46*: $1400000000000 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-45*: $1300000000000 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-44*: $1200000000000 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-43*: $1100000000000 / 1000000000000 \leq t \implies$

$t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-42*: $100000000000 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-41*: $900000000000 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-40*: $800000000000 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-39*: $746637295669 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-38*: $716160577112 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-37*: $664241383483 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-36*: $595448778546 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-35*: $515561896511 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-34*: $430806704415 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-33*: $347089554156 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-32*: $269345996903 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-31*: $201105762729 / 100000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$

$\langle proof \rangle$

lemma *Eb-from-30*: $144325727458 / 1000000000000 \leq t \implies$
 $t \leq 2 \implies Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-29*: $99481037884 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-28*: $65851089563 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-27*: $41909578246 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-26*: $25730180724 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-25*: $15340997855 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-24*: $12166846693 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-23*: $11373308902 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-22*: $10579771112 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-21*: $10381386664 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-20*: $10183002216 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-19*: $9984617768 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-18*: $9786233321 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-17*: $8992695531 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-16*: $3906748086 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-15*: $2312248264 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-14*: $1402286665 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-13*: $881725356 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-12*: $578197906 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-11*: $396324613 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-10*: $283911191 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-9*: $212206188 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-8*: $165097686 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-7*: $133347132 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-6*: $111522114 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-5*: $96349355 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-4*: $85815639 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-3*: $78667711 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-2*: $74129565 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-1*: $71741310 / 1000000000000 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *Eb-from-0*: $0 \leq t \implies t \leq 2 \implies$
 $Eb\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

lemma *potential-bound-0-2*: $0 \leq t \implies t \leq 2 \implies$
 $2 * \logPot\ rho\ t - \forall f\ t \leq -66451 / 10^4$
 $\langle proof \rangle$

(A.9) with (6.8): $2U^{\varrho}(t) - V(t) < -6645002/10^6 < M-0$ for $t \geq 0$.

theorem *potential-A9*: $0 \leq t \implies 2 * \logPot\ rho\ t - \forall f\ t < -6645002 / 10^6$
 $\langle proof \rangle$

(6.4).

theorem *rho-energy-bound*: $lam-r * of-rat\ M0c - \logEnergy\ rho + Cstar \leq of-rat\ Ubar$
 $\langle proof \rangle$

Lemma 6.1: ϱ has mass λ , is supported in $(0, 2)$, satisfies (6.2) and (6.4).

theorem *rho-properties*:
 $emeasure\ rho\ UNIV = ennreal\ lam-r \wedge emeasure\ rho\ (-\{0 <..<2\}) = 0 \wedge$
 $(\forall t. 0 \leq t \implies 2 * \logPot\ rho\ t - \forall f\ t \leq of-rat\ M0c) \wedge$
 $lam-r * of-rat\ M0c - \logEnergy\ rho + Cstar \leq of-rat\ Ubar$
 $\langle proof \rangle$

29.3 (6.9) ingredient

(6.7): $2U^{\varrho}(t) - V(t) + \sqrt{t}/K \leq M - 0 + \sqrt{2}/K$ for $t \geq 0$, $K \geq 40$.

lemma *field-bound*: $40 \leq K \implies 0 \leq t \implies$

$2 * \log \text{Pot } \rho t - V f t + \text{sqrt } t / K \leq \text{of-rat } M0c + \text{sqrt } 2 / K$

<proof>

end

theory *Zeta5-Archimedean-Bound*

imports *Zeta5-Numeric-Enclosures Andreief-Identity*

begin

30 The archimedean bound: Proposition 6.3

Section 6 of the paper: the bound (6.11) on the weight, (6.10) by Andreief's identity, the one-coordinate bound (6.12), the bound (6.9) for every configuration through the logarithmic energy of ϱ and the zero-mass energy inequality, and the estimates (6.14), (6.15) leading to Proposition 6.3 (*log-FK-zeta5-bound*): $\ln F_K(\zeta(5)) \leq \text{@\{text Ubar\}} \cdot K^2 + O(K \ln K)$. Lean theories *Section6*, *Energy6*, *Section6b*, *Section6c*, *Config69*.

30.1 (6.11) and Lemma 6.2

(6.11): $w(y) \leq 8192(1+y)^5 e^{-2\pi y}$.

lemma *binomial-term-le*:

fixes $t :: \text{real}$

assumes $0 \leq t$

shows $\text{real } (n \text{ choose } k) * t^k \leq (1 + t)^n$

<proof>

lemma *pow4-exp-bound*:

fixes $x :: \text{real}$

assumes $0 \leq x$

shows $x^4 * \exp(-x) \leq 4^2$

<proof>

theorem *weight-le*: $0 < y \implies \text{weight } y \leq 8192 * (1 + y)^5 * \exp(-2 * \pi * y)$

<proof>

theorem *DeltaK-zeta5-integral*:

assumes $40 \text{ dvd } K$
shows $\text{real-eval } (\text{DeltaK } K) \text{ zeta5} = 1 / \text{fact } (\text{hof } K) *$
 $\text{set-lebesgue-integral } (\text{PiM } \{..<\text{hof } K\} (\lambda-. \text{lborel})) \{y. \forall i < \text{hof } K. 0 < y \ i\}$
 $(\lambda y. (\prod i < \text{hof } K. \prod j \in \{j. i < j \wedge$
 $j < \text{hof } K\}. (y \ i \wedge^2 - y \ j \wedge^2) \wedge^2) *$
 $(\prod i < \text{hof } K. \text{real-eval } (\text{Dm } (\text{Nof } K)) (y \ i \wedge^2) \wedge^6 / \text{real-eval } (\text{Dm } K)$
 $(y \ i \wedge^2) *$
 $\text{weight } (y \ i)))$
 $\langle \text{proof} \rangle$

30.2 (6.12) and the one-coordinate bound

(6.12): $0 \leq \sum_{j \leq m} \log(t + (j/K) \wedge^2) - K \int_{-0}^{\{m/K\}} \log(t + u \wedge^2) du \leq 2 \log m + 2.$

lemma *sum-ge-int*:

$0 < t \implies 0 < \kappa \implies$
 $\kappa * \text{integral } \{0.. \text{real } m / \kappa\} (\lambda u. \ln (t + u \wedge^2)) \leq (\sum j =$
 $1..m. \ln (t + (\text{real } j / \kappa) \wedge^2))$
 $\langle \text{proof} \rangle$

lemma *sum-log-le*: $1 \leq m \implies$

$(\sum k = 1..m. \ln (\text{real } k)) \leq \text{real } m * \ln (\text{real } m) - \text{real } m + \ln (\text{real } m) + 1$
 $\langle \text{proof} \rangle$

lemma *ln-int0*: $0 < (c :: \text{real}) \implies \ln \text{ integrable-on } \{0..c\}$

$\langle \text{proof} \rangle$

lemma *integral-ln-0*: $0 < (b :: \text{real}) \implies$

$\text{integral } \{0..b\} (\lambda u. \ln u) = b * \ln b - b$
 $\langle \text{proof} \rangle$

Telescoping a sum of integrals over the cells $[(j-1)/\kappa, j/\kappa]$.

lemma *tele-gen*:

fixes $g :: \text{real} \Rightarrow \text{real}$ **and** $\kappa :: \text{real}$
assumes $k: 0 < \kappa$ **and** $gi: \bigwedge c. 0 < c \implies g \text{ integrable-on } \{0..c\}$
shows $(\sum j = 1..n. \text{integral } \{\text{real } (j-1) / \kappa.. \text{real } j / \kappa\} g) =$
 $\text{integral } \{0.. \text{real } n / \kappa\} g$
 $\langle \text{proof} \rangle$

(6.12): $\sum_{j \leq m} \log(t + (j/\kappa) \wedge^2) - \kappa \int_{-0}^{\{m/\kappa\}} \log(t + u \wedge^2) du \leq 2 \log m + 2$: on each cell $[(j-1)/\kappa, j/\kappa]$, $\log(t + b \wedge^2) - \log(t + u \wedge^2) \leq 2 \log b - 2 \log u.$

lemma *sum-le-int*:

$0 < t \implies 0 < \kappa \implies 1 \leq m \implies$
 $(\sum j = 1..m. \ln (t + (\text{real } j / \kappa) \wedge^2)) \leq$
 $\kappa * \text{integral } \{0.. \text{real } m / \kappa\} (\lambda u. \ln (t + u \wedge^2)) + 2 * \ln (\text{real } m) +$

2
 <proof>

The one-coordinate bound: (6.11) and (6.12) give $D-N(y^2)^6/D-K(y^2)$
 $w(y) \leq 8192 e^{1/2} K^{12N+12}/K^{2K} (1+y)^5 e^{-K V((y/K)^2)}$.

lemma *g-le*:

assumes $1 \leq N \leq K$ *real* $N / \text{real } K = 3 / 40$ $0 < y$

shows *real-eval* $(Dm\ N) (y^2)^6 / \text{real-eval } (Dm\ K) (y^2) * \text{weight } y \leq$

$8192 * \exp 12 * \text{real } K^{(12 * N + 12)} / \text{real } K^{(2 * K)} *$

$((1 + y)^5 * \exp (- \text{real } K * V((y / \text{real } K)^2)))$

<proof>

30.3 (6.9) The bound for every configuration

(6.9): for every configuration $0 \leq t-1, \dots, t-h$ of distinct points, $2 \sum_{- \{i < j\}} \log|t-i - t-j| - K \sum V(t-i) + \sum \sqrt{t-i} \leq (\lambda M - 0 - I(\varrho)) K^2 + (120 + \sqrt{2})h + 2h \log K$. Proof: regularise by circle measures of radius $\varepsilon = 1/(4K^2)$, apply Lemma 6.2 to $\sigma = K^{-1} \sum \omega_i$ and ϱ , the circle average of $\log|z-a|$, the arcsine mass bound $\varrho([x-r, x+r]) \leq 40\sqrt{r}$, and (6.7) (Lean: *Config69*).

lemma *rho-singleton*: *emeasure* $\rho \{a\} = 0$

<proof>

The cross bound: $\int \ln^+(\varepsilon/|x - u|) d\varrho(u) \leq 80 \sqrt{\varepsilon}$, by the layer cake over *rho-Icc-le*.

lemma *cross-bound*:

fixes $x\ e :: \text{real}$

assumes $e: 0 < e$

shows $(\int^+ u. \text{ennreal } (\max 0 (\ln (e / |x - u|))) \partial \rho) \leq$

$\text{ennreal } (80 * \sqrt{e})$

<proof>

Helpers for (6.9): the normalised arclength density on $[0, 2\pi]$ and the circle measures.

abbreviation *cden* :: *real measure* **where**

$\text{cden} \equiv \text{density lborel } (\lambda \vartheta. \text{ennreal } (\text{indicator } \{0..2 * \pi\} \vartheta / (2 * \pi)))$

lemma *cden-univ*: *emeasure* *cden* *UNIV* = 1

<proof>

lemma *cden-finite*: *finite-measure* *cden*

<proof>

lemma *circ-meas*: $(\lambda \vartheta :: \text{real}. c + \text{of-real } \varepsilon * \text{cis } \vartheta) \in$

borel-measurable borel

<proof>

lemma *circ-meas'*: $(\lambda \vartheta :: \text{real. } c + \text{of-real } \varepsilon * \text{cis } \vartheta) \in$
measurable cden borel
<proof>

lemma *sets-circ*: $\text{sets } (\text{circ } c \ \varepsilon) = \text{sets borel}$
<proof>

lemma *space-circ*: $\text{space } (\text{circ } c \ \varepsilon) = \text{UNIV}$
<proof>

lemma *circ-univ*: $\text{emeasure } (\text{circ } c \ \varepsilon) \ \text{UNIV} = 1$
<proof>

lemma *circ-finite*: $\text{finite-measure } (\text{circ } c \ \varepsilon)$
<proof>

lemma *circ-AE*: $\text{AE } z \text{ in } \text{circ } c \ \varepsilon. \ \text{norm } (z - c) = |\varepsilon|$
<proof>

lemma *circ-integrable-bound*:
fixes $f :: \text{complex} \Rightarrow \text{real}$ **and** $B :: \text{real}$
assumes $m: f \in \text{borel-measurable borel}$ **and** $b: \bigwedge z. \text{norm } (z - c) =$
 $|\varepsilon| \implies |f \ z| \leq B$
shows $\text{integrable } (\text{circ } c \ \varepsilon) \ f$
<proof>

lemma *cis-eq-null*: $\{\vartheta :: \text{real. } \text{cis } \vartheta = w\} \in \text{null-sets lborel}$
<proof>

lemma *circ-log-integrable*:
assumes $e: 0 < \varepsilon$
shows $\text{integrable } (\text{circ } c \ \varepsilon) \ (\lambda z. \ln (\text{norm } (z - a)))$
<proof>

lemma *circ-singleton*:
assumes $e: 0 < \varepsilon$
shows $\text{emeasure } (\text{circ } c \ \varepsilon) \ \{a\} = 0$
<proof>

lemma *circ-neg-log*:
fixes $c \ z :: \text{complex}$ **and** $\varepsilon \ R :: \text{real}$
assumes $e: 0 < \varepsilon$ **and** $hc: \text{norm } c + \varepsilon \leq R$ **and** $hz: \text{norm } z \leq R$
shows $(\int^+ w. \text{ennreal } (- \ln (\text{norm } (z - w)))) \ \partial \text{circ } c \ \varepsilon \leq$
 $\text{ennreal } (2 * R - \ln \varepsilon)$
<proof>

Finite sums of circle measures, realised as a push-forward of *count-space I*
 $\otimes$ *cden*.

lemma *csum-meas*:

fixes $c :: \text{nat} \Rightarrow \text{complex}$ **and** $I :: \text{nat set}$
assumes $I: \text{countable } I$
shows $(\lambda(i, \vartheta). c \ i + \text{of-real } \varepsilon * \text{cis } \vartheta) \in$
 $\text{measurable } (\text{count-space } I \otimes_M \text{cden}) \text{ borel}$
 $\langle \text{proof} \rangle$

lemma *csum-nn*:

fixes $c :: \text{nat} \Rightarrow \text{complex}$ **and** $I :: \text{nat set}$ **and** $f :: \text{complex} \Rightarrow \text{ennreal}$
assumes $I: \text{finite } I$ **and** $f: f \in \text{borel-measurable borel}$
shows $(\int^+ z. f \ z \ \partial \text{distr } (\text{count-space } I \otimes_M \text{cden}) \text{ borel}$
 $(\lambda(i, \vartheta). c \ i + \text{of-real } \varepsilon * \text{cis } \vartheta))$
 $= (\sum i \in I. \int^+ z. f \ z \ \partial \text{circ } (c \ i) \ \varepsilon)$
 $\langle \text{proof} \rangle$

lemma *csum-emeasure*:

fixes $c :: \text{nat} \Rightarrow \text{complex}$ **and** $I :: \text{nat set}$
assumes $I: \text{finite } I$ **and** $A: A \in \text{sets borel}$
shows $\text{emeasure } (\text{distr } (\text{count-space } I \otimes_M \text{cden}) \text{ borel } (\lambda(i,$
 $\vartheta). c \ i + \text{of-real } \varepsilon * \text{cis } \vartheta)) \ A = (\sum i \in$
 $I. \text{emeasure } (\text{circ } (c \ i) \ \varepsilon) \ A)$
 $\langle \text{proof} \rangle$

lemma *csum-integral*:

fixes $c :: \text{nat} \Rightarrow \text{complex}$ **and** $I :: \text{nat set}$ **and** $f :: \text{complex} \Rightarrow \text{real}$
assumes $I: \text{finite } I$ **and** $f: f \in \text{borel-measurable borel}$ **and** $f_i: \bigwedge i. i \in$
 $I \implies \text{integrable } (\text{circ } (c \ i) \ \varepsilon) \ f$
shows $\text{integrable } (\text{distr } (\text{count-space } I \otimes_M \text{cden}) \text{ borel } (\lambda(i,$
 $\vartheta). c \ i + \text{of-real } \varepsilon * \text{cis } \vartheta)) \ f$
and $\text{integral}^L (\text{distr } (\text{count-space } I \otimes_M \text{cden}) \text{ borel } (\lambda(i,$
 $\vartheta). c \ i + \text{of-real } \varepsilon * \text{cis } \vartheta)) \ f = (\sum i \in$
 $I. \text{integral}^L (\text{circ } (c \ i) \ \varepsilon) \ f)$
 $\langle \text{proof} \rangle$

A scaled measure is a density with a constant; the Bochner integral scales.

lemma *scale-density*:

fixes $M :: 'a \text{ measure}$ **and** $r :: \text{real}$
shows $\text{scale-measure } (\text{ennreal } r) \ M = \text{density } M \ (\lambda-. \text{ennreal } r)$
 $\langle \text{proof} \rangle$

lemma *scale-integral*:

fixes $M :: 'a \text{ measure}$ **and** $f :: 'a \Rightarrow \text{real}$ **and** $r :: \text{real}$
assumes $r: 0 \leq r$ **and** $f: f \in \text{borel-measurable } M$
shows $\text{integral}^L (\text{scale-measure } (\text{ennreal } r) \ M) \ f = r * \text{integral}^L \ M \ f$
and $\text{integrable } M \ f \implies \text{integrable } (\text{scale-measure } (\text{ennreal } r) \ M) \ f$
 $\langle \text{proof} \rangle$

Facts about ϱ and its image on $\mathbb{C}$.

lemma *rho-finite*: *finite-measure rho*
 $\langle \text{proof} \rangle$

lemma *rhoC-meas*: $(\text{of-real} :: \text{real} \Rightarrow \text{complex}) \in \text{measurable rho borel}$
 $\langle \text{proof} \rangle$

lemma *sets-rhoC*: $\text{sets} (\text{distr rho borel} (\text{of-real} :: \text{real} \Rightarrow \text{complex})) = \text{sets borel}$
 $\langle \text{proof} \rangle$

lemma *rhoC-finite*: $\text{finite-measure} (\text{distr rho borel} (\text{of-real} :: \text{real} \Rightarrow \text{complex}))$
 $\langle \text{proof} \rangle$

lemma *rhoC-singleton*: $\text{emeasure} (\text{distr rho borel} (\text{of-real} :: \text{real} \Rightarrow \text{complex})) \{a\} = 0$
 $\langle \text{proof} \rangle$

lemma *rhoC-AE*: $\text{AE } w \text{ in } \text{distr rho borel} (\text{of-real} :: \text{real} \Rightarrow \text{complex}). \text{norm } w \leq 2$
 $\langle \text{proof} \rangle$

lemma *rhoC-neg-log*: $(\int^+ w. \text{ennreal} (- \ln (\text{norm} (z - w)))) \partial \text{distr rho borel} (\text{of-real} :: \text{real} \Rightarrow \text{complex}) \leq \text{ennreal } 80$
 $\langle \text{proof} \rangle$

Integrability of $\log|z - w|$ against a product of finite measures carried by a ball.

lemma *ennreal-abs-ln-le*:
fixes $y :: \text{real}$
assumes $y: 0 \leq y$
shows $\text{ennreal } |\ln y| \leq \text{ennreal } y + \text{ennreal} (- \ln y)$
 $\langle \text{proof} \rangle$

lemma *integrable-log-prod*:
fixes $\mu \nu :: \text{complex measure}$ **and** $R C :: \text{real}$
assumes *fm*: $\text{finite-measure } \mu$ **and** *fn*: $\text{finite-measure } \nu$ **and** *sm*: $\text{sets } \mu = \text{sets borel}$ **and** *sn*: $\text{sets } \nu = \text{sets borel}$
and *aem*: $\text{AE } z \text{ in } \mu. \text{norm } z \leq R$ **and** *aen*: $\text{AE } w \text{ in } \nu. \text{norm } w \leq R$
and *lg*: $\bigwedge z. \text{norm } z \leq R \implies (\int^+ w. \text{ennreal} (- \ln (\text{norm} (z - w)))) \partial \nu \leq \text{ennreal } C$
shows $\text{integrable} (\mu \otimes_M \nu) (\lambda p. \ln (\text{norm} (\text{fst } p - \text{snd } p)))$
 $\langle \text{proof} \rangle$

The sum of two measures with the Borel sets, as *measure-of*.

lemma *summ-sets*:
fixes $\mu \nu :: 'a::\text{topological-space measure}$
shows $\text{sets} (\text{measure-of UNIV} (\text{sets borel}) (\lambda A. \text{emeasure } \mu A + \text{emeasure } \nu A)) = \text{sets} (\text{borel} :: 'a \text{ measure})$
 $\langle \text{proof} \rangle$

lemma *summ-emeasure*:

fixes $\mu \nu :: 'a::\text{topological-space measure}$
assumes $s1: \text{sets } \mu = \text{sets borel}$ **and** $s2: \text{sets } \nu = \text{sets borel}$ **and** $A: A \in \text{sets borel}$
shows $\text{emeasure } (\text{measure-of UNIV } (\text{sets borel}) (\lambda A. \text{emeasure } \mu A + \text{emeasure } \nu A)) A = \text{emeasure } \mu A + \text{emeasure } \nu A$
 $\langle \text{proof} \rangle$

lemma *summ-nn*:
fixes $\mu \nu :: 'a::\text{topological-space measure}$ **and** $f :: 'a \Rightarrow \text{ennreal}$
assumes $s1: \text{sets } \mu = \text{sets borel}$ **and** $s2: \text{sets } \nu = \text{sets borel}$ **and** $f: f \in \text{borel-measurable borel}$
shows $(\int^+ z. f z \partial \text{measure-of UNIV } (\text{sets borel}) (\lambda A. \text{emeasure } \mu A + \text{emeasure } \nu A)) = (\int^+ z. f z \partial \mu) + (\int^+ z. f z \partial \nu)$
 $\langle \text{proof} \rangle$

Logarithmic integrals against ρ .

lemma *abs-ln-max-le*:
fixes $e x :: \text{real}$
assumes $e: 0 < e$ **and** $x: 0 \leq x$
shows $|\ln (\max e x)| \leq |\ln e| + x$
 $\langle \text{proof} \rangle$

lemma *rho-AE-Ioo*: $AE u \text{ in } \rho. 0 < u \wedge u < 2$
 $\langle \text{proof} \rangle$

lemma *rho-neg-log-le*: $(\int^+ u. \text{ennreal } (-\ln |x - u|) \partial \rho) \leq \text{ennreal } 80$
 $\langle \text{proof} \rangle$

lemma *rho-log-integrable*: $\text{integrable } \rho (\lambda u. \ln |x - u|)$
 $\langle \text{proof} \rangle$

lemma *rho-logmax-integrable*:
assumes $e: 0 < \varepsilon$
shows $\text{integrable } \rho (\lambda u. \ln (\max \varepsilon |x - u|))$
 $\langle \text{proof} \rangle$

lemma *rho-logmax-le*:
assumes $e: 0 < \varepsilon$
shows $\text{integral}^L \rho (\lambda u. \ln (\max \varepsilon |x - u|)) \leq \log \text{Pot } \rho x + 80 * \text{sqr } \varepsilon$
 $\langle \text{proof} \rangle$

The energies of a scaled sum of circle measures.

lemma *csum-scale-integral*:
fixes $t :: \text{nat} \Rightarrow \text{real}$ **and** $h :: \text{nat}$ **and** $\varepsilon r :: \text{real}$ **and** $f :: \text{complex} \Rightarrow \text{real}$
assumes $r: 0 \leq r$ **and** $f: f \in \text{borel-measurable borel}$ **and** $f_i: \bigwedge i. i <$

$h \implies \text{integrable } (\text{circ } (\text{of-real } (t \ i)) \ \varepsilon) \ f$
shows $\text{integral}^L (\text{scale-measure } (\text{ennreal } r) (\text{distr } (\text{count-space } \{..<h\} \otimes_M \text{cden}) \text{ borel } (\lambda(i, \vartheta). \text{of-real } (t \ i) + \text{of-real } \varepsilon * \text{cis } \vartheta))) \ f$
 $= r * (\sum \ i < h. \text{integral}^L (\text{circ } (\text{of-real } (t \ i)) \ \varepsilon) \ f)$
 $\langle \text{proof} \rangle$

lemma *csum-energy-ge*:

fixes $t :: \text{nat} \Rightarrow \text{real}$ **and** $h :: \text{nat}$ **and** $\varepsilon \ r :: \text{real}$ **and** $S :: \text{complex measure}$
assumes $e: 0 < \varepsilon$ **and** $\text{inj: inj-on } t \ \{..<h\}$ **and** $r: 0 \leq r$
and $S: S = \text{scale-measure } (\text{ennreal } r) (\text{distr } (\text{count-space } \{..<h\} \otimes_M \text{cden}) \text{ borel } (\lambda(i, \vartheta). \text{of-real } (t \ i) + \text{of-real } \varepsilon * \text{cis } \vartheta))$
shows $r \wedge 2 * (\sum \ i < h. \sum \ j < h. (\text{if } i = j \text{ then } \ln \varepsilon \text{ else } \ln |t \ i - t \ j|)) \leq \text{logEnergyC } S \ S$
 $\langle \text{proof} \rangle$

lemma *csum-cross-le*:

fixes $t :: \text{nat} \Rightarrow \text{real}$ **and** $h :: \text{nat}$ **and** $\varepsilon \ r :: \text{real}$ **and** $S :: \text{complex measure}$
assumes $e: 0 < \varepsilon$ **and** $e1: \varepsilon \leq 1$ **and** $\text{tnn: } \bigwedge i. i < h \implies 0 \leq t \ i$ **and** $r: 0 \leq r$
and $S: S = \text{scale-measure } (\text{ennreal } r) (\text{distr } (\text{count-space } \{..<h\} \otimes_M \text{cden}) \text{ borel } (\lambda(i, \vartheta). \text{of-real } (t \ i) + \text{of-real } \varepsilon * \text{cis } \vartheta))$
shows $\text{logEnergyC } S (\text{distr } \rho \text{ borel of-real}) \leq r * (\sum \ i < h. (\text{logPot } \rho (t \ i) + 80 * \text{sqrt } \varepsilon))$
 $\langle \text{proof} \rangle$

theorem *configuration-bound*:

fixes $t :: \text{nat} \Rightarrow \text{real}$
assumes $40 \text{ dvd } K$ $0 < K$ $\bigwedge i. i < \text{hof } K \implies 0 \leq t \ i$ $\text{inj-on } t \ \{..<\text{hof } K\}$
shows $2 * (\sum \ i < \text{hof } K. \sum \ j \in \{j. i < j \wedge j < \text{hof } K\}. \ln |t \ i - t \ j|)$
 $- \text{real } K * (\sum \ i < \text{hof } K. \text{Vf } (t \ i)) + (\sum \ i < \text{hof } K. \text{sqrt } (t \ i))$
 $\leq (\text{lam-r} * \text{of-rat } M0c - \text{logEnergy } \rho) * \text{real } K \wedge 2$
 $+ (120 + \text{sqrt } 2) * \text{real } (\text{hof } K) + 2 * \text{real } (\text{hof } K) * \ln (\text{real } K)$
 $\langle \text{proof} \rangle$

30.4 (6.14), (6.15) and Proposition 6.3

$\int -0^\infty (1+y)^\wedge 5 \ e^\wedge \{-y/\kappa\} \ dy \leq 3872 \ \kappa^\wedge 6$ (Lean: *phi-bound*).

lemma *phi-aux*:

fixes $\kappa :: \text{real}$
assumes $1 \leq \kappa$
shows $\text{set-integrable lborel } \{0 < ..\} (\lambda y. (1 + y)^\wedge 5 * \exp (- y / \kappa))$
and $\text{set-lebesgue-integral lborel } \{0 < ..\} (\lambda y. (1 + y)^\wedge 5 * \exp (- y / \kappa)) \leq 3872 * \kappa^\wedge 6$

<proof>

$$(6.14): \log \Delta\text{-}K(\zeta(5)) \leq 2h(h + 6N - K) \log K + (\lambda M - 0 - I(\varrho))K^2 + 18h \log K + 160h.$$

theorem *log-DeltaK-zeta5-bound:*

assumes $40 \text{ dvd } K$ $0 < K$

shows $\ln (\text{real-eval } (\text{DeltaK } K) \text{ zeta5}) \leq$
 $2 * \text{real } (\text{hof } K) * (\text{real } (\text{hof } K) + 6 * \text{real } (\text{Nof } K) - \text{real } K) * \ln (\text{real } K)$
 $+ (\text{lam-r} * \text{of-rat } M0c - \text{logEnergy } \rho) * \text{real } K^2$
 $+ 18 * \text{real } (\text{hof } K) * \ln (\text{real } K) + 160 * \text{real } (\text{hof } K)$

<proof>

$$(6.15): \log S\text{-}K \leq (2\lambda - 12\alpha\lambda - 2\lambda^2)K^2 \log K + C * K^2 + 6h \log K + 6h \text{ (factorial bounds; } \textit{Stirling-Formula.ln-fact-bounds} \text{ is available).}$$

theorem *log-SK-bound:*

assumes $40 \text{ dvd } K$ $0 < K$

shows $\ln (\text{of-rat } (SK \ K)) \leq$
 $(2 * \text{lam-r} - 12 * \alpha\text{-r} * \text{lam-r} - 2 * \text{lam-r}^2) * \text{real } K^2 * \ln (\text{real } K)$
 $+ Cstar * \text{real } K^2 + 6 * \text{real } (\text{hof } K) * \ln (\text{real } K) + 6 * \text{real } (\text{hof } K)$

<proof>

Proposition 6.3 is at the end of this theory (it needs (6.4) from Appendix A).

lemma *real-eval-FK-eq:* $\text{real-eval } (FK \ K) \text{ zeta5} = \text{of-rat } (SK \ K) * \text{real-eval } (\text{DeltaK } K) \text{ zeta5}$

<proof>

Proposition 6.3: $0 < F\text{-}K(\zeta(5))$ and $\log F\text{-}K(\zeta(5)) \leq UbarK^2 + 24K \log K + 200K$. (Needs (6.4) from Appendix A, which is therefore imported.)

theorem *log-FK-zeta5-bound:*

assumes $40 \text{ dvd } K$ $0 < K$

shows $0 < \text{real-eval } (FK \ K) \text{ zeta5} \wedge$
 $\ln (\text{real-eval } (FK \ K) \text{ zeta5}) \leq$
 $\text{of-rat } Ubar * \text{real } K^2 + 24 * \text{real } K * \ln (\text{real } K) + 200 * \text{real } K$

<proof>

end

theory *Zeta-5-Irrational*

imports *Zeta5-Archimedean-Bound Zeta5-Exact-Constants HOL-Real-Asymp.Real-Asymp*
Liouville-Numbers.Liouville-Numbers-Misc

begin

31 The main theorem: $\zeta(5)$ is irrational

Section 7 of the paper: Theorem 2.1 ($Q_{K,M} \in \mathbb{Z}[X]$ of degree h with $Q_{K,M}(\zeta(5)) > 0$), the limit (7.1), the decay (2.7) for $M = 200$, the elementary irrationality criterion (*irrational-of-int-poly-approx*: integer polynomials Q_n of degree $\leq d n$ with $0 < Q_n(x) < \exp(-c n^2)$ force $x \notin \mathbb{Q}$), and the main theorem *zeta5-irrational*. Lean theories *Section7*, *Main*, *Claim*.

lemma *real-eval-smult*: *real-eval* (*Polynomial.smult* c P) x = *of-rat* c * *real-eval* P x
 $\langle \text{proof} \rangle$

lemma *real-eval-QKM*: *real-eval* (*QKM* K M) *zeta5* = *of-rat* (*mKM* K M) * *real-eval* (*FK* K) *zeta5*
 $\langle \text{proof} \rangle$

lemma *real-eval-FK*: *real-eval* (*FK* K) *zeta5* = *of-rat* (*SK* K) * *real-eval* (*DeltaK* K) *zeta5*
 $\langle \text{proof} \rangle$

Theorem 2.1, first part: $Q_{\{K,M\}} \in \mathbb{Z}[X]$, $\deg Q_{\{K,M\}} = h$, $Q_{\{K,M\}}(\zeta(5)) > 0$.

theorem *QKM-int-degree-pos*:

assumes *StdHyp* K M

shows $(\exists P :: \text{int poly. map-poly of-int } P = \text{QKM } K \text{ } M) \wedge$

$\text{degree } (\text{QKM } K \text{ } M) = \text{hof } K \wedge$

$0 < \text{real-eval } (\text{QKM } K \text{ } M) \text{ zeta5}$

$\langle \text{proof} \rangle$

$(24 K \log K + 200 K)/K^2 \rightarrow 0$ along $K = 40n$ (*real-asymp*).

lemma *error-term-small*:

assumes $0 < \varepsilon$

shows $\forall_F n$ in *at-top*.

$(24 * \text{real } (40 * n) * \ln (\text{real } (40 * n)) + 200 * \text{real } (40 * n)) / \text{real } (40 * n)^2 \leq$

ε

$\langle \text{proof} \rangle$

(7.1): $\limsup K^{-2} \log Q_{\{K,M\}}(\zeta(5)) \leq A - M + \text{Ubar}$ for $M \in 40\mathbb{Z}$, $M \geq 40$.

theorem *log-QKM-zeta5-limsup*:

assumes $40 \leq M$ $40 \text{ dvd } M$ $0 < \varepsilon$

shows $\forall_F n$ in *at-top*.

$\ln (\text{real-eval } (\text{QKM } (40 * n) \text{ } M) \text{ zeta5}) / \text{real } (40 * n)^2 \leq$

$\text{of-rat } (A M \text{ } M) + \text{of-rat } \text{Ubar} + \varepsilon$

$\langle \text{proof} \rangle$

(2.7): $0 < Q_{\{40n, 200\}}(\zeta(5)) < \exp(-139n^2/5)$ for all large n .

theorem *QKM-zeta5-decay*:

$\forall_F n$ in at-top.
 $0 < \text{real-eval } (QKM \ (40 * n) \ 200) \ \text{zeta5} \wedge$
 $\text{real-eval } (QKM \ (40 * n) \ 200) \ \text{zeta5} < \exp \ (- \ (139 / 5 * \text{real } n \wedge 2))$
 <proof>

The abstract top-level argument: if integer polynomials $Q\text{-}n$ of degree at most dn satisfy $0 < Q\text{-}n(x) < \exp(-cn \wedge 2)$ for large n , then x is irrational ($b \wedge \{dn\}$ $Q\text{-}n(a/b)$ is a positive integer that is eventually < 1).

theorem *irrational-of-int-poly-approx*:

fixes $x \ c :: \text{real}$ **and** $Qs :: \text{nat} \Rightarrow \text{int poly}$
assumes $c: 0 < c$ **and** $\text{deg}: \bigwedge n. \text{degree } (Qs \ n) \leq d * n$
and $\text{ev}: \forall_F n$ in at-top. $0 < \text{poly } (\text{map-poly of-int } (Qs \ n)) \ x \wedge$
 $\text{poly } (\text{map-poly of-int } (Qs \ n)) \ x < \exp \ (- \ (c * \text{real } n \wedge 2))$
shows $x \notin \mathbb{Q}$
 <proof>

$\zeta(5)$ is real: its Dirichlet series has real terms (*Zeta-Function.sums-zeta-nat*).

lemma *zeta5-real*: $\text{zeta } 5 \in \mathbb{R}$

<proof>

lemma *zeta5-eq*: $\text{zeta } 5 = \text{of-real } \text{zeta5}$

<proof>

The integer polynomials $Q\text{-}\{40n, 200\}$ (and 0 for small n).

definition $Qint :: \text{nat} \Rightarrow \text{int poly}$ **where**

$Qint \ n = (\text{if } \text{StdHyp } (40 * n) \ 200 \text{ then } (\text{SOME } P. \text{map-poly of-int } P = QKM \ (40 * n) \ 200) \text{ else } 0)$

lemma *Qint-spec*:

assumes $\text{StdHyp } (40 * n) \ 200$
shows $\text{map-poly of-int } (Qint \ n) = QKM \ (40 * n) \ 200$
 <proof>

Theorem 1.1 for the real number zeta5 .

theorem *zeta5-irrational-real*: $\text{zeta5} \notin \mathbb{Q}$

<proof>

Theorem 1.1, stated for the AFP's zeta : $\zeta(5) \notin \mathbb{Q}$.

theorem *zeta5-irrational*: $\text{zeta } 5 \notin \mathbb{Q}$

<proof>

corollary *Re-zeta5-irrational*: $\text{Re } (\text{zeta } 5) \notin \mathbb{Q}$

<proof>

Sanity check of the statement: $\text{zeta } 5$ is the familiar series $\sum_{n \geq 1} n \wedge -5$.

lemma *zeta5-series*: $\text{zeta } 5 = (\sum n. 1 / \text{of-nat } (\text{Suc } n) \wedge 5)$

$\langle proof \rangle$

end

References

- [1] domino14. zeta5: a Lean 4 formalisation of “ $\zeta(5)$ is irrational”. <https://github.com/domino14/zeta5>, 2026.
- [2] A. Fauzan. $\zeta(5)$ is irrational. Zenodo preprint, Sept. 2026. <https://zenodo.org/records/22826419>, doi:10.5281/zenodo.22826419.