Prime Number Theorem with Remainder Term

Shuhao Song and Bowen Yao

February 6, 2026

Abstract

We have formalized the proof of the Prime Number Theorem with remainder term. This is the first formalized version of PNT with an explicit error term.

There are many useful results in this AFP entry.

First, the main result, prime number theorem with remainder:

$$\pi(x) = \mathrm{Li}(x) + O\left(x \exp\left(-\sqrt{\log x}/3653\right)\right)$$

Second, the zero-free region of the Riemann zeta function:

$$\zeta(\beta + i\gamma) \neq 0 \text{ when } \beta \geq 1 - \frac{1}{952320}\left(\log(|\gamma| + 2)\right)^{-1}$$

Moreover, we proved a revised version of Perron's formula, together with the zero-free region we can prove the main result.

Contents

1 Auxiliary library for prime number theorem **2**
- 1.1 Zeta function . . . 2
- 1.2 Logarithm derivatives . . . 2
- 1.3 Lemmas of integration and integrability . . . 4
- 1.4 Lemmas on asymptotics . . . 5
- 1.5 Lemmas of *floor*, *ceil* and *nat_powr* . . . 6
- 1.6 Elementary estimation of *exp* and *ln* . . . 6
- 1.7 Miscellaneous lemmas . . . 6

2 Implication relation of many forms of prime number theorem **7**

3 Some basic theorems in complex analysis **9**
- 3.1 Introduction rules for holomorphic functions and analytic functions . . . 9
- 3.2 Factorization of analytic function on compact region . . . 10
  - 3.2.1 Auxiliary propositions for theorem *analytic_factorization* . . . 11
- 3.3 Schwarz theorem in complex analysis . . . 11
- 3.4 Borel-Carathedory theorem . . . 12
- 3.5 Lemma 3.9 . . . 12

4 Zero-free region of zeta function **13**

5 Perron's formula **21**

6 Estimation of the order of $\frac{\zeta'(s)}{\zeta(s)}$ **24**

theory *PNT_Notation*
imports
Prime_Number_Theorem.Prime_Counting_Functions
begin

definition $PNT_const_C_1 \equiv 1 \,/\, 952320 :: real$

abbreviation *nat_powr*
(**infixr** ‹*nat'_powr*› *80*)
where
$n\ nat_powr\ x \equiv (of_nat\ n)\ powr\ x$

bundle *pnt_syntax*
begin
notation $PNT_const_C_1$ (‹C_1›)
notation *norm* (‹‖_‖›)
notation *Suc* (‹_+› [*101*] *100*)
end

end
theory *PNT_Remainder_Library*
imports
PNT_Notation
begin
unbundle *pnt_syntax*

1 Auxiliary library for prime number theorem

1.1 Zeta function

lemma *pre_zeta_1_bound*:
assumes $0 < Re\ s$
shows $\|pre_zeta\ 1\ s\| \leq \|s\| \,/\, Re\ s$
⟨*proof*⟩

lemma *zeta_pole_eq*:
assumes $s \neq 1$
shows $zeta\ s = pre_zeta\ 1\ s + 1 \,/\, (s - 1)$
⟨*proof*⟩

definition *zeta'* **where** $zeta'\ s \equiv pre_zeta\ 1\ s * (s - 1) + 1$

lemma *zeta'_analytic*:
$zeta'\ analytic_on\ UNIV$
⟨*proof*⟩

lemma *zeta'_analytic_on* [*analytic_intros*]:
$zeta'\ analytic_on\ A$ ⟨*proof*⟩

lemma *zeta'_holomorphic_on* [*holomorphic_intros*]:
$zeta'\ holomorphic_on\ A$ ⟨*proof*⟩

lemma *zeta_eq_zeta'*:
$zeta\ s = zeta'\ s \,/\, (s - 1)$

⟨*proof*⟩

lemma *zeta'_1* [*simp*]: *zeta' 1 = 1* ⟨*proof*⟩

lemma *zeta_eq_zero_iff_zeta'*:
shows *s ≠ 1 ⟹ zeta' s = 0 ⟷ zeta s = 0*
⟨*proof*⟩

lemma *zeta'_eq_zero_iff*:
shows *zeta' s = 0 ⟷ zeta s = 0 ∧ s ≠ 1*
⟨*proof*⟩

lemma *zeta_eq_zero_iff*:
shows *zeta s = 0 ⟷ zeta' s = 0 ∨ s = 1*
⟨*proof*⟩

1.2 Logarithm derivatives

definition *logderiv f x ≡ deriv f x / f x*
definition *log_differentiable*
(**infixr** ‹(*log'_differentiable*)› *50*)
where
f log_differentiable x ≡ (f field_differentiable (at x)) ∧ f x ≠ 0

lemma *logderiv_prod'*:
fixes *f :: 'n ⇒ 'f ⇒ 'f :: real_normed_field*
assumes *fin*: *finite I*
and *lder*: *⋀i. i ∈ I ⟹ f i log_differentiable a*
shows *logderiv (λx. ∏ i∈I. f i x) a = (∑ i∈I. logderiv (f i) a)* (**is** *?P*)
and *(λx. ∏ i∈I. f i x) log_differentiable a* (**is** *?Q*)
⟨*proof*⟩

lemma *logderiv_prod*:
fixes *f :: 'n ⇒ 'f ⇒ 'f :: real_normed_field*
assumes *lder*: *⋀i. i ∈ I ⟹ f i log_differentiable a*
shows *logderiv (λx. ∏ i∈I. f i x) a = (∑ i∈I. logderiv (f i) a)* (**is** *?P*)
and *(λx. ∏ i∈I. f i x) log_differentiable a* (**is** *?Q*)
⟨*proof*⟩

lemma *logderiv_mult*:
assumes *f log_differentiable a*
and *g log_differentiable a*
shows *logderiv (λz. f z * g z) a = logderiv f a + logderiv g a* (**is** *?P*)
and *(λz. f z * g z) log_differentiable a* (**is** *?Q*)
⟨*proof*⟩

lemma *logderiv_cong_ev*:
assumes *∀ᶠ x in nhds x. f x = g x*
and *x = y*
shows *logderiv f x = logderiv g y*
⟨*proof*⟩

lemma *logderiv_linear*:
assumes *z ≠ a*
shows *logderiv (λw. w − a) z = 1 / (z − a)*
and *(λw. w − z) log_differentiable a*

⟨*proof*⟩

lemma *deriv_shift*:
assumes *f field_differentiable at* $(a + x)$
shows *deriv* $(\lambda t.\ f\ (a + t))\ x =$ *deriv f* $(a + x)$
⟨*proof*⟩

lemma *logderiv_shift*:
assumes *f field_differentiable at* $(a + x)$
shows *logderiv* $(\lambda t.\ f\ (a + t))\ x =$ *logderiv f* $(a + x)$
⟨*proof*⟩

lemma *logderiv_inverse*:
assumes $x \neq 0$
shows *logderiv* $(\lambda x.\ 1\ /\ x)\ x = -\ 1\ /\ x$
⟨*proof*⟩

lemma *logderiv_zeta_eq_zeta'*:
assumes $s \neq 1$ *zeta* $s \neq 0$
shows *logderiv zeta* $s =$ *logderiv zeta'* $s - 1\ /\ (s - 1)$
⟨*proof*⟩

lemma *analytic_logderiv* [*analytic_intros*]:
assumes *f analytic_on A* $\bigwedge z.\ z \in A \Longrightarrow f\ z \neq 0$
shows $(\lambda s.$ *logderiv f* $s)$ *analytic_on A*
⟨*proof*⟩

1.3 Lemmas of integration and integrability

lemma *powr_has_integral*:
fixes *a b w* :: *real*
assumes *Hab*: $a \leq b$ **and** *Hw*: $w > 0 \wedge w \neq 1$
shows $((\lambda x.\ w\ powr\ x)$ *has_integral w powr b / ln w − w powr a / ln w*$)\ \{a..b\}$
⟨*proof*⟩

lemma *powr_integrable*:
fixes *a b w* :: *real*
assumes *Hab*: $a \leq b$ **and** *Hw*: $w > 0 \wedge w \neq 1$
shows $(\lambda x.\ w\ powr\ x)$ *integrable_on* $\{a..b\}$
⟨*proof*⟩

lemma *powr_integral_bound_gt_1*:
fixes *a b w* :: *real*
assumes *Hab*: $a \leq b$ **and** *Hw*: $w > 1$
shows *integral* $\{a..b\}$ $(\lambda x.\ w\ powr\ x) \leq w\ powr\ b\ /\ |ln\ w|$
⟨*proof*⟩

lemma *powr_integral_bound_lt_1*:
fixes *a b w* :: *real*
assumes *Hab*: $a \leq b$ **and** *Hw*: $0 < w \wedge w < 1$
shows *integral* $\{a..b\}$ $(\lambda x.\ w\ powr\ x) \leq w\ powr\ a\ /\ |ln\ w|$
⟨*proof*⟩

lemma *set_integrableI_bounded*:
fixes *f* :: *'a* ⇒ *'b*::{*banach*, *second_countable_topology*}
shows *A* ∈ *sets M*

$\Longrightarrow$ $(\lambda x.\ indicator\ A\ x *_R f\ x) \in borel_measurable\ M$
$\Longrightarrow$ $emeasure\ M\ A < \infty$
$\Longrightarrow$ $(AE\ x\ in\ M.\ x \in A \longrightarrow norm\ (f\ x) \leq B)$
$\Longrightarrow$ $set_integrable\ M\ A\ f$
⟨*proof*⟩

lemma *integrable_cut'*:
fixes $a\ b\ c :: real$ **and** $f :: real \Rightarrow real$
assumes $a \leq b\ b \leq c$
and *Hf*: $\bigwedge x.\ a \leq x \Longrightarrow f\ integrable_on\ \{a..x\}$
shows $f\ integrable_on\ \{b..c\}$
⟨*proof*⟩

lemma *integration_by_part'*:
fixes $a\ b :: real$
and $f\ g :: real \Rightarrow 'a :: \{real_normed_field, banach\}$
and $f'\ g' :: real \Rightarrow 'a$
assumes $a \leq b$
and $\bigwedge x.\ x \in \{a..b\} \Longrightarrow (f\ has_vector_derivative\ f'\ x)\ (at\ x)$
and $\bigwedge x.\ x \in \{a..b\} \Longrightarrow (g\ has_vector_derivative\ g'\ x)\ (at\ x)$
and *int*: $(\lambda x.\ f\ x * g'\ x)\ integrable_on\ \{a..b\}$
shows $((\lambda x.\ f'\ x * g\ x)\ has_integral$
$f\ b * g\ b - f\ a * g\ a - integral\{a..b\}\ (\lambda x.\ f\ x * g'\ x))\ \{a..b\}$
⟨*proof*⟩

lemma *integral_bigo*:
fixes $a :: real$ **and** $f\ g :: real \Rightarrow real$
assumes *f_bound*: $f \in O(g)$
and *Hf*: $\bigwedge x.\ a \leq x \Longrightarrow f\ integrable_on\ \{a..x\}$
and *Hf'*: $\bigwedge x.\ a \leq x \Longrightarrow (\lambda x.\ |f\ x|)\ integrable_on\ \{a..x\}$
and *Hg'*: $\bigwedge x.\ a \leq x \Longrightarrow (\lambda x.\ |g\ x|)\ integrable_on\ \{a..x\}$
shows $(\lambda x.\ integral\{a..x\}\ f) \in O(\lambda x.\ 1 + integral\{a..x\}\ (\lambda x.\ |g\ x|))$
⟨*proof*⟩

lemma *integral_linepath_same_Re*:
assumes *Ha*: $Re\ a = Re\ b$
and *Hb*: $Im\ a < Im\ b$
and *Hf*: $(f\ has_contour_integral\ x)\ (linepath\ a\ b)$
shows $((\lambda t.\ f\ (Complex\ (Re\ a)\ t) * \mathrm{i})\ has_integral\ x)\ \{Im\ a..Im\ b\}$
⟨*proof*⟩

1.4 Lemmas on asymptotics

lemma *eventually_at_top_linorderI'*:
fixes $c :: 'a :: \{no_top, linorder\}$
assumes *h*: $\bigwedge x.\ c < x \Longrightarrow P\ x$
shows $eventually\ P\ at_top$
⟨*proof*⟩

lemma *eventually_le_imp_bigo*:
assumes $\forall_F\ x\ in\ F.\ \|f\ x\| \leq g\ x$
shows $f \in O[F](g)$
⟨*proof*⟩

lemma *eventually_le_imp_bigo'*:
assumes $\forall_F\ x\ in\ F.\ \|f\ x\| \leq g\ x$

shows $(\lambda x.\ \|f\ x\|) \in O[F](g)$
⟨*proof*⟩

lemma *le_imp_bigo*:
assumes $\bigwedge x.\ \|f\ x\| \leq g\ x$
shows $f \in O[F](g)$
⟨*proof*⟩

lemma *le_imp_bigo'*:
assumes $\bigwedge x.\ \|f\ x\| \leq g\ x$
shows $(\lambda x.\ \|f\ x\|) \in O[F](g)$
⟨*proof*⟩

lemma *exp_bigo*:
fixes $f\ g :: real \Rightarrow real$
assumes $\forall_F\ x\ in\ at_top.\ f\ x \leq g\ x$
shows $(\lambda x.\ exp\ (f\ x)) \in O(\lambda x.\ exp\ (g\ x))$
⟨*proof*⟩

lemma *ev_le_imp_exp_bigo*:
fixes $f\ g :: real \Rightarrow real$
assumes *hf*: $\forall_F\ x\ in\ at_top.\ 0 < f\ x$
and *hg*: $\forall_F\ x\ in\ at_top.\ 0 < g\ x$
and *le*: $\forall_F\ x\ in\ at_top.\ ln\ (f\ x) \leq ln\ (g\ x)$
shows $f \in O(g)$
⟨*proof*⟩

lemma *smallo_ln_diverge_1*:
fixes $f :: real \Rightarrow real$
assumes *f_ln*: $f \in o(ln)$
shows $LIM\ x\ at_top.\ x * exp\ (-\ f\ x) :>\ at_top$
⟨*proof*⟩

lemma *ln_ln_asymp_pos*: $\forall_F\ x :: real\ in\ at_top.\ 0 < ln\ (ln\ x)$ ⟨*proof*⟩
lemma *ln_asymp_pos*: $\forall_F\ x :: real\ in\ at_top.\ 0 < ln\ x$ ⟨*proof*⟩
lemma *x_asymp_pos*: $\forall_F\ x :: real\ in\ at_top.\ 0 < x$ ⟨*proof*⟩

1.5 Lemmas of *floor*, *ceil* and *nat_powr*

lemma *nat_le_self*: $0 \leq x \Longrightarrow nat\ (int\ x) \leq x$ ⟨*proof*⟩
lemma *floor_le*: $\bigwedge x :: real.\ \lfloor x \rfloor \leq x$ ⟨*proof*⟩
lemma *ceil_ge*: $\bigwedge x :: real.\ x \leq \lceil x \rceil$ ⟨*proof*⟩

lemma *nat_lt_real_iff*:
$(n :: nat) < (a :: real) = (n < nat\ \lceil a \rceil)$
⟨*proof*⟩

lemma *nat_le_real_iff*:
$(n :: nat) \leq (a :: real) = (n < nat\ (\lfloor a \rfloor + 1))$
⟨*proof*⟩

lemma *of_real_nat_power*: $n\ nat_powr\ (of_real\ x :: complex) = of_real\ (n\ nat_powr\ x)$ **for** $n\ x$
⟨*proof*⟩

lemma *norm_nat_power*: $\|n\ nat_powr\ (s :: complex)\| = n\ powr\ (Re\ s)$
⟨*proof*⟩

1.6 Elementary estimation of *exp* and *ln*

lemma *ln_when_ge_3*:
  $1 < ln\ x$ **if** $3 \leq x$ **for** $x :: real$
⟨*proof*⟩

lemma *exp_lemma_1*:
  fixes $x :: real$
  assumes $1 \leq x$
  shows $1 + exp\ x \leq exp\ (2 * x)$
⟨*proof*⟩

lemma *ln_bound_1*:
  fixes $t :: real$
  assumes *Ht*: $0 \leq t$
  shows $ln\ (14 + 4 * t) \leq 4 * ln\ (t + 2)$
⟨*proof*⟩

1.7 Miscellaneous lemmas

abbreviation *fds_zeta_complex* :: *complex fds* ≡ *fds_zeta*

lemma *powr_mono_lt_1_cancel*:
  fixes $x\ a\ b :: real$
  assumes *Hx*: $0 < x \wedge x < 1$
  shows $(x\ powr\ a \leq x\ powr\ b) = (b \leq a)$
  ⟨*proof*⟩

abbreviation *mangoldt_real* :: _ ⇒ *real* ≡ *mangoldt*
abbreviation *mangoldt_complex* :: _ ⇒ *complex* ≡ *mangoldt*

lemma *norm_fds_mangoldt_complex*:
  $\bigwedge n.\ \|fds_nth\ (fds\ mangoldt_complex)\ n\| = mangoldt_real\ n$ ⟨*proof*⟩

lemma *suminf_norm_bound*:
  fixes $f :: nat \Rightarrow 'a :: banach$
  assumes *summable g*
    and $\bigwedge n.\ \|f\ n\| \leq g\ n$
  shows $\|suminf\ f\| \leq (\sum n.\ g\ n)$
⟨*proof*⟩

lemma C_1*_gt_zero*: $0 < C_1$ ⟨*proof*⟩

unbundle *no pnt_syntax*

end
theory *Relation_of_PNTs*
imports
  PNT_Remainder_Library
begin
unbundle *pnt_syntax*
unbundle *prime_counting_syntax*

2 Implication relation of many forms of prime number theorem

definition *rem_est* :: *real* ⇒ *real* ⇒ *real* ⇒ _ **where**
rem_est c m n ≡ $O(\lambda\ x.\ x * exp\ (-c * ln\ x\ powr\ m * ln\ (ln\ x)\ powr\ n))$

definition *Li* :: *real* ⇒ *real* **where** *Li x* ≡ *integral* {*2*..*x*} (λ*x*. *1* / *ln x*)
definition *PNT_1* **where** *PNT_1 c m n* ≡ ((λ*x*. π *x* − *Li x*) ∈ *rem_est c m n*)
definition *PNT_2* **where** *PNT_2 c m n* ≡ ((λ*x*. ϑ *x* − *x*) ∈ *rem_est c m n*)
definition *PNT_3* **where** *PNT_3 c m n* ≡ ((λ*x*. ψ *x* − *x*) ∈ *rem_est c m n*)

lemma *rem_est_compare_powr*:
fixes *c m n* :: *real*
assumes *h*: *0* < *m m* < *1*
shows (λ*x*. *x powr* (*2* / *3*)) ∈ *rem_est c m n*
⟨*proof*⟩

lemma *PNT_3_imp_PNT_2*:
fixes *c m n* :: *real*
assumes *h*: *0* < *m m* < *1* **and** *PNT_3 c m n*
shows *PNT_2 c m n*
⟨*proof*⟩

definition r_1 **where** $r_1\ x \equiv \pi\ x - Li\ x$ **for** *x*
definition r_2 **where** $r_2\ x \equiv \vartheta\ x - x$ **for** *x*

lemma *pi_represent_by_theta*:
fixes *x* :: *real*
assumes *2* ≤ *x*
shows π *x* = ϑ *x* / (*ln x*) + *integral* {*2*..*x*} (λ*t*. ϑ *t* / (*t* ∗ (*ln t*)²))
⟨*proof*⟩

lemma *Li_integrate_by_part*:
fixes *x* :: *real*
assumes *2* ≤ *x*
shows
(λ*x*. *1* / (*ln x*)²) *integrable_on* {*2*..*x*}
Li x = *x* / (*ln x*) − *2* / (*ln 2*) + *integral* {*2*..*x*} (λ*t*. *1* / (*ln t*)²)
⟨*proof*⟩

lemma *ϑ_integrable*:
fixes *x* :: *real*
assumes *2* ≤ *x*
shows (λ*t*. ϑ *t* / (*t* ∗ (*ln t*)²)) *integrable_on* {*2*..*x*}
⟨*proof*⟩

lemma r_1*_represent_by_*r_2:
fixes *x* :: *real*
assumes *Hx*: *2* ≤ *x*
shows (λ*t*. r_2 *t* / (*t* ∗ (*ln t*)²)) *integrable_on* {*2*..*x*} (**is** *?P*)
$r_1\ x = r_2\ x$ / (*ln x*) + *2* / *ln 2* + *integral* {*2*..*x*} (λ*t*. r_2 *t* / (*t* ∗ (*ln t*)²)) (**is** *?Q*)
⟨*proof*⟩

lemma *exp_integral_asymp*:
fixes *f f'* :: *real* ⇒ *real*

assumes *cf*: *continuous_on* $\{a..\}$ f
and *der*: $\bigwedge x.\ a < x \Longrightarrow DERIV\ f\ x :> f'\ x$
and *td*: $((\lambda x.\ x * f'\ x) \longrightarrow 0)\ at_top$
and *f_ln*: $f \in o(ln)$
shows $(\lambda x.\ integral\ \{a..x\}\ (\lambda t.\ exp\ (-f\ t))) \sim[at_top]\ (\lambda x.\ x * exp(-f\ x))$
⟨*proof*⟩

lemma *x_mul_exp_larger_than_const*:
fixes $c :: real$ **and** $g :: real \Rightarrow real$
assumes *g_ln*: $g \in o(ln)$
shows $(\lambda x.\ c) \in O(\lambda x.\ x * exp(-g\ x))$
⟨*proof*⟩

lemma *integral_bigo_exp'*:
fixes $a :: real$ **and** $f\ g\ g' :: real \Rightarrow real$
assumes *f_bound*: $f \in O(\lambda x.\ exp(-g\ x))$
and *Hf*: $\bigwedge x.\ a \le x \Longrightarrow f\ integrable_on\ \{a..x\}$
and *Hf'*: $\bigwedge x.\ a \le x \Longrightarrow (\lambda x.\ |f\ x|)\ integrable_on\ \{a..x\}$
and *Hg*: $continuous_on\ \{a..\}\ g$
and *der*: $\bigwedge x.\ a < x \Longrightarrow DERIV\ g\ x :> g'\ x$
and *td*: $((\lambda x.\ x * g'\ x) \longrightarrow 0)\ at_top$
and *g_ln*: $g \in o(ln)$
shows $(\lambda x.\ integral\{a..x\}\ f) \in O(\lambda x.\ x * exp(-g\ x))$
⟨*proof*⟩

lemma *integral_bigo_exp*:
fixes $a\ b :: real$ **and** $f\ g\ g' :: real \Rightarrow real$
assumes *le*: $a \le b$
and *f_bound*: $f \in O(\lambda x.\ exp(-g\ x))$
and *Hf*: $\bigwedge x.\ a \le x \Longrightarrow f\ integrable_on\ \{a..x\}$
and *Hf'*: $\bigwedge x.\ b \le x \Longrightarrow (\lambda x.\ |f\ x|)\ integrable_on\ \{b..x\}$
and *Hg*: $continuous_on\ \{b..\}\ g$
and *der*: $\bigwedge x.\ b < x \Longrightarrow DERIV\ g\ x :> g'\ x$
and *td*: $((\lambda x.\ x * g'\ x) \longrightarrow 0)\ at_top$
and *g_ln*:$g \in o(ln)$
shows $(\lambda x.\ integral\ \{a..x\}\ f) \in O(\lambda x.\ x * exp(-g\ x))$
⟨*proof*⟩

lemma *integrate_r₂_estimate*:
fixes $c\ m\ n :: real$
assumes *hm*: $0 < m\ m < 1$
and *h*: $r_2 \in rem_est\ c\ m\ n$
shows $(\lambda x.\ integral\ \{2..x\}\ (\lambda t.\ r_2\ t\ /\ (t * (ln\ t)^2))) \in rem_est\ c\ m\ n$
⟨*proof*⟩

lemma *r₂_div_ln_estimate*:
fixes $c\ m\ n :: real$
assumes *hm*: $0 < m\ m < 1$
and *h*: $r_2 \in rem_est\ c\ m\ n$
shows $(\lambda x.\ r_2\ x\ /\ (ln\ x) + 2\ /\ ln\ 2) \in rem_est\ c\ m\ n$
⟨*proof*⟩

lemma *PNT_2_imp_PNT_1*:
fixes $l :: real$
assumes *h*: $0 < m\ m < 1$ **and** $PNT_2\ c\ m\ n$

shows *PNT_1 c m n*
⟨*proof*⟩

theorem *PNT_3_imp_PNT_1*:
fixes *l* :: *real*
assumes *h* : *0* < *m m* < *1* **and** *PNT_3 c m n*
shows *PNT_1 c m n*
⟨*proof*⟩

hide_const (**open**) r_1 r_2
unbundle *no prime_counting_syntax* **and** *no pnt_syntax*

end
theory *PNT_Complex_Analysis_Lemmas*
imports
PNT_Remainder_Library
begin
unbundle *pnt_syntax*

3 Some basic theorems in complex analysis

3.1 Introduction rules for holomorphic functions and analytic functions

lemma *holomorphic_on_shift* [*holomorphic_intros*]:
assumes *f holomorphic_on* ((λ*z*. *s* + *z*) ‘ *A*)
shows (λ*z*. *f* (*s* + *z*)) *holomorphic_on A*
⟨*proof*⟩

lemma *holomorphic_logderiv* [*holomorphic_intros*]:
assumes *f holomorphic_on A open A* ⋀*z*. *z* ∈ *A* ⟹ *f z* ≠ *0*
shows (λ*s*. *logderiv f s*) *holomorphic_on A*
⟨*proof*⟩

lemma *holomorphic_glue_to_analytic*:
assumes *o*: *open S open T*
and *hf*: *f holomorphic_on S*
and *hg*: *g holomorphic_on T*
and *hI*: ⋀*z*. *z* ∈ *S* ⟹ *z* ∈ *T* ⟹ *f z* = *g z*
and *hU*: *U* ⊆ *S* ∪ *T*
obtains *h*
where *h analytic_on U*
⋀*z*. *z* ∈ *S* ⟹ *h z* = *f z*
⋀*z*. *z* ∈ *T* ⟹ *h z* = *g z*
⟨*proof*⟩

lemma *analytic_on_powr_right* [*analytic_intros*]:
assumes *f analytic_on s*
shows (λ*z*. *w powr f z*) *analytic_on s*
⟨*proof*⟩

3.2 Factorization of analytic function on compact region

definition *not_zero_on* (**infixr** ‹*not'_zero'_on*› *46*)
where *f not_zero_on S* ≡ ∃ *z* ∈ *S*. *f z* ≠ *0*

lemma *not_zero_on_obtain*:
assumes *f not_zero_on S* **and** $S \subseteq T$
obtains *t* **where** $f\ t \neq 0$ **and** $t \in T$
⟨*proof*⟩

lemma *analytic_on_holomorphic_connected*:
assumes *hf*: *f analytic_on S*
and *con*: *connected A*
and *ne*: $\xi \in A$ **and** *AS*: $A \subseteq S$
obtains *T T'* **where**
f holomorphic_on T f holomorphic_on T'
open T open T' A ⊆ *T S* ⊆ *T' connected T*
⟨*proof*⟩

lemma *analytic_factor_zero*:
assumes *hf*: *f analytic_on S*
and *KS*: $K \subseteq S$ **and** *con*: *connected K*
and ξK: $\xi \in K$ **and** ξz: $f\ \xi = 0$
and *nz*: *f not_zero_on K*
obtains *g r n*
where $0 < n\ 0 < r$
g analytic_on S g not_zero_on K
$\bigwedge z.\ z \in S \Longrightarrow f\ z = (z - \xi)\hat{}n * g\ z$
$\bigwedge z.\ z \in ball\ \xi\ r \Longrightarrow g\ z \neq 0$
⟨*proof*⟩

lemma *analytic_compact_finite_zeros*:
assumes *af*: *f analytic_on S*
and *KS*: $K \subseteq S$
and *con*: *connected K*
and *cm*: *compact K*
and *nz*: *f not_zero_on K*
shows *finite* $\{z \in K.\ f\ z = 0\}$
⟨*proof*⟩

3.2.1 Auxiliary propositions for theorem *analytic_factorization*

definition *analytic_factor_p'* **where**
‹*analytic_factor_p' f S K* ≡
∃ *g n*. ∃ α :: *nat* ⇒ *complex*.
g analytic_on S
∧ (∀ *z* ∈ *K*. *g z* ≠ 0)
∧ (∀ *z* ∈ *S*. *f z* = *g z* ∗ (∏ *k*<*n*. *z* − α *k*))
∧ α ‘ {..<*n*} ⊆ *K*›

definition *analytic_factor_p* **where**
‹*analytic_factor_p F* ≡
∀ *f S K*. *f analytic_on S*
⟶ *K* ⊆ *S*
⟶ *connected K*
⟶ *compact K*
⟶ *f not_zero_on K*
⟶ {*z* ∈ *K*. *f z* = 0} = *F*
⟶ *analytic_factor_p' f S K*›

lemma *analytic_factorization_E*:

shows *analytic_factor_p* {}
⟨*proof*⟩

lemma *analytic_factorization_I*:
assumes *ind*: *analytic_factor_p F*
and *ξni*: $\xi \notin F$
shows *analytic_factor_p* (*insert ξ F*)
⟨*proof*⟩

A nontrivial analytic function on connected compact region can be factorized as a everywhere-non-zero function and linear terms $z - s_0$ for all zeros s_0. Note that the connected assumption of K may be removed, but we remain it just for simplicity of proof.

theorem *analytic_factorization*:
assumes *af*: *f analytic_on S*
and *KS*: $K \subseteq S$
and *con*: *connected K*
and *compact K*
and *f not_zero_on K*
obtains *g n* **and** $\alpha :: nat \Rightarrow complex$ **where**
g analytic_on S
$\bigwedge z.\ z \in K \Longrightarrow g\ z \neq 0$
$\bigwedge z.\ z \in S \Longrightarrow f\ z = g\ z * (\prod k{<}n.\ (z - \alpha\ k))$
α ' $\{..{<}n\} \subseteq K$
⟨*proof*⟩

3.3 Schwarz theorem in complex analysis

lemma *Schwarz_Lemma1*:
fixes $f :: complex \Rightarrow complex$
and $\xi :: complex$
assumes *f holomorphic_on ball 0 1*
and *f 0 = 0*
and $\bigwedge z.\ \|z\| < 1 \Longrightarrow \|f\ z\| \leq 1$
and $\|\xi\| < 1$
shows $\|f\ \xi\| \leq \|\xi\|$
⟨*proof*⟩

theorem *Schwarz_Lemma2*:
fixes $f :: complex \Rightarrow complex$
and $\xi :: complex$
assumes *holf*: *f holomorphic_on ball 0 R*
and *hR*: *0 < R* **and** *nz*: *f 0 = 0*
and *bn*: $\bigwedge z.\ \|z\| < R \Longrightarrow \|f\ z\| \leq 1$
and *ξR*: $\|\xi\| < R$
shows $\|f\ \xi\| \leq \|\xi\|\ /\ R$
⟨*proof*⟩

3.4 Borel-Carathedory theorem

Borel-Carathedory theorem, from book *Theorem 5.5*, *The Theory of Functions*, *E. C. Titchmarsh*

lemma *Borel_Caratheodory1*:
assumes *hr*: *0 < R 0 < r r < R*
and *f0*: *f 0 = 0*
and *hf*: $\bigwedge z.\ \|z\| < R \Longrightarrow Re\ (f\ z) \leq A$
and *holf*: *f holomorphic_on* (*ball 0 R*)

and *zr*: $\|z\| \leq r$
shows $\|f\ z\| \leq 2{*}r/(R{-}r) * A$
⟨*proof*⟩

lemma *Borel_Caratheodory2*:
assumes *hr*: $0 < R\ 0 < r\ r < R$
and *hf*: $\bigwedge z.\ \|z\| < R \Longrightarrow Re\ (f\ z - f\ 0) \leq A$
and *holf*: f *holomorphic_on* $(ball\ 0\ R)$
and *zr*: $\|z\| \leq r$
shows $\|f\ z - f\ 0\| \leq 2{*}r/(R{-}r) * A$
⟨*proof*⟩

theorem *Borel_Caratheodory3*:
assumes *hr*: $0 < R\ 0 < r\ r < R$
and *hf*: $\bigwedge w.\ w \in ball\ s\ R \Longrightarrow Re\ (f\ w - f\ s) \leq A$
and *holf*: f *holomorphic_on* $(ball\ s\ R)$
and *zr*: $z \in ball\ s\ r$
shows $\|f\ z - f\ s\| \leq 2{*}r/(R{-}r) * A$
⟨*proof*⟩

3.5 Lemma 3.9

These lemmas is referred to the following material: Theorem 3.9, *The Theory of the Riemann Zeta−Function*, *E. C. Titchmarsh*, *D. R. Heath−Brown.*

lemma *lemma_3_9_beta1*:
fixes $f\ M\ r\ s_0$
assumes *zl*: $0 < r\ 0 \leq M$
and *hf*: f *holomorphic_on ball 0 r*
and *ne*: $\bigwedge z.\ z \in ball\ 0\ r \Longrightarrow f\ z \neq 0$
and *bn*: $\bigwedge z.\ z \in ball\ 0\ r \Longrightarrow \|f\ z\ /\ f\ 0\| \leq exp\ M$
shows $\|logderiv\ f\ 0\| \leq 4 * M\ /\ r$
and $\forall\, s{\in}cball\ 0\ (r\ /\ 4).\ \|logderiv\ f\ s\| \leq 8 * M\ /\ r$
⟨*proof*⟩

lemma *lemma_3_9_beta1'*:
fixes $f\ M\ r\ s_0$
assumes *zl*: $0 < r\ 0 \leq M$
and *hf*: f *holomorphic_on ball s r*
and *ne*: $\bigwedge z.\ z \in ball\ s\ r \Longrightarrow f\ z \neq 0$
and *bn*: $\bigwedge z.\ z \in ball\ s\ r \Longrightarrow \|f\ z\ /\ f\ s\| \leq exp\ M$
and *hs*: $z \in cball\ s\ (r\ /\ 4)$
shows $\|logderiv\ f\ z\| \leq 8 * M\ /\ r$
⟨*proof*⟩

lemma *lemma_3_9_beta2*:
fixes $f\ M\ r$
assumes *zl*: $0 < r\ 0 \leq M$
and *af*: f *analytic_on cball 0 r*
and *f0*: $f\ 0 \neq 0$
and *rz*: $\bigwedge z.\ z \in cball\ 0\ r \Longrightarrow Re\ z > 0 \Longrightarrow f\ z \neq 0$
and *bn*: $\bigwedge z.\ z \in cball\ 0\ r \Longrightarrow \|f\ z\ /\ f\ 0\| \leq exp\ M$
and *hg*: $\Gamma \subseteq \{z \in cball\ 0\ (r\ /\ 2).\ f\ z = 0\}$
shows $-\ Re\ (logderiv\ f\ 0) \leq 8 * M\ /\ r + Re\ (\sum z{\in}\Gamma.\ 1\ /\ z)$
⟨*proof*⟩

theorem *lemma_3_9_beta3*:
fixes f M r **and** s :: *complex*
assumes *zl*: $0 < r$ $0 \leq M$
and *af*: f *analytic_on cball* s r
and *f0*: $f\ s \neq 0$
and *rz*: $\bigwedge z.\ z \in cball\ s\ r \Longrightarrow Re\ z > Re\ s \Longrightarrow f\ z \neq 0$
and *bn*: $\bigwedge z.\ z \in cball\ s\ r \Longrightarrow \|f\ z\ /\ f\ s\| \leq exp\ M$
and *hg*: $\Gamma \subseteq \{z \in cball\ s\ (r\ /\ 2).\ f\ z = 0\}$
shows $-\ Re\ (logderiv\ f\ s) \leq 8 * M\ /\ r + Re\ (\sum z{\in}\Gamma.\ 1\ /\ (z - s))$
⟨*proof*⟩

unbundle *no pnt_syntax*

end
theory *Zeta_Zerofree*
imports
PNT_Complex_Analysis_Lemmas
begin
unbundle *pnt_syntax*

4 Zero-free region of zeta function

lemma *cos_inequality_1*:
fixes x :: *real*
shows $3 + 4 * cos\ x + cos\ (2 * x) \geq 0$
⟨*proof*⟩

lemma *multiplicative_fds_zeta*:
completely_multiplicative_function (*fds_nth fds_zeta_complex*)
⟨*proof*⟩

lemma *fds_mangoldt_eq*:
fds mangoldt_complex $= -$(*fds_deriv fds_zeta / fds_zeta*)
⟨*proof*⟩

lemma *abs_conv_abscissa_log_deriv*:
abs_conv_abscissa (*fds_deriv fds_zeta_complex / fds_zeta*) ≤ 1
⟨*proof*⟩

lemma *abs_conv_abscissa_mangoldt*:
abs_conv_abscissa (*fds mangoldt_complex*) ≤ 1
⟨*proof*⟩

lemma
assumes *s*: $Re\ s > 1$
shows *eval_fds_mangoldt*: *eval_fds* (*fds mangoldt*) $s = -\ deriv\ zeta\ s\ /\ zeta\ s$
and *abs_conv_mangoldt*: *fds_abs_converges* (*fds mangoldt*) s
⟨*proof*⟩

lemma *sums_mangoldt*:
fixes s :: *complex*
assumes *s*: $Re\ s > 1$
shows $((\lambda n.\ mangoldt\ n\ /\ n\ nat_powr\ s)\ has_sum\ -\ deriv\ zeta\ s\ /\ zeta\ s)\ \{1..\}$
⟨*proof*⟩

lemma *sums_Re_logderiv_zeta*:
fixes $\sigma\ t :: real$
assumes *s*: $\sigma > 1$
shows $((\lambda n.\ mangoldt_real\ n * n\ nat_powr\ (-\sigma) * cos\ (t * ln\ n))$
$has_sum\ Re\ (-\ deriv\ zeta\ (Complex\ \sigma\ t)\ /\ zeta\ (Complex\ \sigma\ t)))\ \{1..\}$
⟨*proof*⟩

lemma *logderiv_zeta_ineq*:
fixes $\sigma\ t :: real$
assumes *s*: $\sigma > 1$
shows $3 * Re\ (logderiv\ zeta\ (Complex\ \sigma\ 0)) + 4 * Re\ (logderiv\ zeta\ (Complex\ \sigma\ t))$
$+ Re\ (logderiv\ zeta\ (Complex\ \sigma\ (2*t))) \leq 0$ (**is** $?x \leq 0$)
⟨*proof*⟩

lemma *sums_zeta_real*:
fixes $r :: real$
assumes $1 < r$
shows $(\sum n.\ (n_+)\ powr\ -r) = Re\ (zeta\ r)$
⟨*proof*⟩

lemma *inverse_zeta_bound'*:
assumes $1 < Re\ s$
shows $\|inverse\ (zeta\ s)\| \leq Re\ (zeta\ (Re\ s))$
⟨*proof*⟩

lemma *zeta_bound'*:
assumes $1 < Re\ s$
shows $\|zeta\ s\| \leq Re\ (zeta\ (Re\ s))$
⟨*proof*⟩

lemma *zeta_bound_trivial'*:
assumes $1\ /\ 2 \leq Re\ s \wedge Re\ s \leq 2$
and $|Im\ s| \geq 1\ /\ 11$
shows $\|zeta\ s\| \leq 12 + 2 * |Im\ s|$
⟨*proof*⟩

lemma *zeta_bound_gt_1*:
assumes $1 < Re\ s$
shows $\|zeta\ s\| \leq Re\ s\ /\ (Re\ s - 1)$
⟨*proof*⟩

lemma *zeta_bound_trivial*:
assumes $1\ /\ 2 \leq Re\ s$ **and** $|Im\ s| \geq 1\ /\ 11$
shows $\|zeta\ s\| \leq 12 + 2 * |Im\ s|$
⟨*proof*⟩

lemma *zeta_nonzero_small_imag'*:
assumes $|Im\ s| \leq 13\ /\ 22$ **and** $Re\ s \geq 1\ /\ 2$ **and** $Re\ s < 1$
shows $zeta\ s \neq 0$
⟨*proof*⟩

lemma *zeta_nonzero_small_imag*:
assumes $|Im\ s| \leq 13\ /\ 22$ **and** $Re\ s > 0$ **and** $s \neq 1$
shows $zeta\ s \neq 0$
⟨*proof*⟩

lemma *inverse_zeta_bound*:
assumes $1 < Re\ s$
shows $\|inverse\ (zeta\ s)\| \leq Re\ s\ /\ (Re\ s - 1)$
⟨*proof*⟩

lemma *deriv_zeta_bound*:
fixes $s :: complex$
assumes *Hr*: $0 < r$ **and** *Hs*: $s \neq 1$
and *hB*: $\bigwedge w.\ \|s - w\| = r \Longrightarrow \|pre_zeta\ 1\ w\| \leq B$
shows $\|deriv\ zeta\ s\| \leq B\ /\ r + 1\ /\ \|s - 1\|^2$
⟨*proof*⟩

lemma *zeta_lower_bound*:
assumes $0 < Re\ s\ s \neq 1$
shows $1\ /\ \|s - 1\| - \|s\|\ /\ Re\ s \leq \|zeta\ s\|$
⟨*proof*⟩

lemma *logderiv_zeta_bound*:
fixes $\sigma :: real$
assumes $1 < \sigma\ \sigma \leq 23\ /\ 20$
shows $\|logderiv\ zeta\ \sigma\| \leq 5\ /\ 4 * (1\ /\ (\sigma - 1))$
⟨*proof*⟩

lemma *Re_logderiv_zeta_bound*:
fixes $\sigma :: real$
assumes $1 < \sigma\ \sigma \leq 23\ /\ 20$
shows $Re\ (logderiv\ zeta\ \sigma) \geq -\ 5\ /\ 4 * (1\ /\ (\sigma - 1))$
⟨*proof*⟩

locale *zeta_bound_param* =
fixes $\vartheta\ \varphi :: real \Rightarrow real$
assumes *zeta_bn'*: $\bigwedge z.\ 1 - \vartheta\ (Im\ z) \leq Re\ z \Longrightarrow Im\ z \geq 1\ /\ 11 \Longrightarrow \|zeta\ z\| \leq exp\ (\varphi\ (Im\ z))$
and ϑ*_pos*: $\bigwedge t.\ 0 < \vartheta\ t \wedge \vartheta\ t \leq 1\ /\ 2$
and φ*_pos*: $\bigwedge t.\ 1 \leq \varphi\ t$
and *inv_*ϑ: $\bigwedge t.\ \varphi\ t\ /\ \vartheta\ t \leq 1\ /\ 960 * exp\ (\varphi\ t)$
and *mo*ϑ: *antimono* ϑ **and** *mo*φ: *mono* φ
begin
definition *region* $\equiv \{z.\ 1 - \vartheta\ (Im\ z) \leq Re\ z \wedge Im\ z \geq 1\ /\ 11\}$
lemma *zeta_bn*: $\bigwedge z.\ z \in region \Longrightarrow \|zeta\ z\| \leq exp\ (\varphi\ (Im\ z))$
⟨*proof*⟩
lemma ϑ*_pos'*: $\bigwedge t.\ 0 < \vartheta\ t \wedge \vartheta\ t \leq 1$
⟨*proof*⟩
lemma φ*_pos'*: $\bigwedge t.\ 0 < \varphi\ t$ ⟨*proof*⟩
end

locale *zeta_bound_param_1* = *zeta_bound_param* +
fixes $\gamma :: real$
assumes γ*_cnd*: $\gamma \geq 13\ /\ 22$
begin
definition r **where** $r \equiv \vartheta\ (2 * \gamma + 1)$
end

locale *zeta_bound_param_2* = *zeta_bound_param_1* +
fixes $\sigma\ \delta :: real$

assumes σ_cnd: $\sigma \geq 1 + exp\ (-\ \varphi(2 * \gamma + 1))$
and δ_cnd: $\delta = \gamma \vee \delta = 2 * \gamma$
begin
definition s **where** $s \equiv Complex\ \sigma\ \delta$
end

context *zeta_bound_param_2* **begin**
declare *dist_complex_def* [*simp*] *norm_minus_commute* [*simp*]
declare *Complex_simps* [*simp*]

lemma *cball_lm*:
assumes $z \in cball\ s\ r$
shows $r \leq 1\ |Re\ z - \sigma| \leq r\ |Im\ z - \delta| \leq r$
$1\ /\ 11 \leq Im\ z\ Im\ z \leq 2 * \gamma + r$
⟨*proof*⟩

lemma *cball_in_region*:
shows $cball\ s\ r \subseteq region$
⟨*proof*⟩

lemma *Re_s_gt_1*:
shows $1 < Re\ s$
⟨*proof*⟩

lemma *zeta_analytic_on_region*:
shows *zeta analytic_on region*
⟨*proof*⟩

lemma *zeta_div_bound*:
assumes $z \in cball\ s\ r$
shows $\|zeta\ z\ /\ zeta\ s\| \leq exp\ (3 * \varphi\ (2 * \gamma + 1))$
⟨*proof*⟩

lemma *logderiv_zeta_bound*:
shows $Re\ (logderiv\ zeta\ s) \geq -\ 24 * \varphi\ (2 * \gamma + 1)\ /\ r$
and $\bigwedge\beta.\ \sigma - r\ /\ 2 \leq \beta \Longrightarrow zeta\ (Complex\ \beta\ \delta) = 0 \Longrightarrow$
$Re\ (logderiv\ zeta\ s) \geq -\ 24 * \varphi\ (2 * \gamma + 1)\ /\ r + 1\ /\ (\sigma - \beta)$
⟨*proof*⟩
end

context *zeta_bound_param_1* **begin**
lemma *zeta_nonzero_region'*:
assumes $1 + 1\ /\ 960 * (r\ /\ \varphi\ (2 * \gamma + 1)) - r\ /\ 2 \leq \beta$
and $zeta\ (Complex\ \beta\ \gamma) = 0$
shows $1 - \beta \geq 1\ /\ 29760 * (r\ /\ \varphi\ (2 * \gamma + 1))$
⟨*proof*⟩

lemma *zeta_nonzero_region*:
assumes $zeta\ (Complex\ \beta\ \gamma) = 0$
shows $1 - \beta \geq 1\ /\ 29760 * (r\ /\ \varphi\ (2 * \gamma + 1))$
⟨*proof*⟩
end

context *zeta_bound_param* **begin**
theorem *zeta_nonzero_region*:

assumes *zeta* (*Complex* β γ) = *0* **and** *Complex* β $\gamma \neq$ *1*
shows *1* − $\beta \geq$ *1* / *29760* ∗ (ϑ (*2* ∗ |γ| + *1*) / φ (*2* ∗ |γ| + *1*))
⟨*proof*⟩
end

lemma *zeta_bound_param_nonneg*:
fixes ϑ φ :: *real* ⇒ *real*
assumes *zeta_bn'*: ⋀*z*. *1* − ϑ (*Im z*) ≤ *Re z* ⟹ *Im z* ≥ *1* / *11* ⟹ ‖*zeta z*‖ ≤ *exp* (φ (*Im z*))
and ϑ*_pos*: ⋀*t*. *0* ≤ *t* ⟹ *0* < ϑ *t* ∧ ϑ *t* ≤ *1* / *2*
and φ*_pos*: ⋀*t*. *0* ≤ *t* ⟹ *1* ≤ φ *t*
and *inv_*ϑ: ⋀*t*. *0* ≤ *t* ⟹ φ *t* / ϑ *t* ≤ *1* / *960* ∗ *exp* (φ *t*)
and *mo*ϑ: ⋀*x y*. *0* ≤ *x* ⟹ *x* ≤ *y* ⟹ ϑ *y* ≤ ϑ *x*
and *mo*φ: ⋀*x y*. *0* ≤ *x* ⟹ *x* ≤ *y* ⟹ φ *x* ≤ φ *y*
shows *zeta_bound_param* (λ*t*. ϑ (*max 0 t*)) (λ*t*. φ (*max 0 t*))
⟨*proof*⟩

interpretation *classical_zeta_bound*:
zeta_bound_param λ*t*. *1* / *2* λ*t*. *4* ∗ *ln* (*12* + *2* ∗ *max 0 t*)
⟨*proof*⟩

theorem *zeta_nonzero_region*:
assumes *zeta* (*Complex* β γ) = *0* **and** *Complex* β $\gamma \neq$ *1*
shows *1* − $\beta \geq C_1$ / *ln* (|γ| + *2*)
⟨*proof*⟩

unbundle *no pnt_syntax*

end
theory *PNT_Subsummable*
imports
PNT_Remainder_Library
begin
unbundle *pnt_syntax*

definition *has_subsum* **where** *has_subsum f S x* ≡ (λ*n*. *if n* ∈ *S then f n else 0*) *sums x*
definition *subsum* **where** *subsum f S* ≡ ∑ *n*. *if n* ∈ *S then f n else 0*
definition *subsummable* (**infix** ‹*subsummable*› *50*)
where *f subsummable S* ≡ *summable* (λ*n*. *if n* ∈ *S then f n else 0*)

syntax *_subsum* :: *pttrn* ⇒ *nat set* ⇒ *'a* ⇒ *'a*
(‹(*2*∑ ‘_ ∈ (_)./ _)› [*0*, *0*, *10*] *10*)
syntax_consts *_subsum* == *subsum*
translations
∑ ‘ *x*∈*S*. *t* => *CONST subsum* (λ*x*. *t*) *S*

syntax *_subsum_prop* :: *pttrn* ⇒ *bool* ⇒ *'a* ⇒ *'a*
(‹(*2*∑ ‘_ | (_)./ _)› [*0*, *0*, *10*] *10*)
syntax_consts *_subsum_prop* == *subsum*
translations
∑ ‘ *x*|*P*. *t* => *CONST subsum* (λ*x*. *t*) {*x*. *P*}

syntax *_subsum_ge* :: *pttrn* ⇒ *nat* ⇒ *'a* ⇒ *'a*
(‹(*2*∑ ‘_ ≥ _./ _)› [*0*, *0*, *10*] *10*)
syntax_consts *_subsum_ge* == *subsum*
translations

$\sum$ ‘ $x{\geq}n.\ t$ => $CONST\ subsum\ (\lambda x.\ t)\ \{n..\}$

lemma *has_subsum_finite*:
finite $F \Longrightarrow$ *has_subsum* $f\ F\ (sum\ f\ F)$
⟨*proof*⟩

lemma *has_subsum_If_finite_set*:
assumes *finite* F
shows *has_subsum* $(\lambda n.\ if\ n \in F\ then\ f\ n\ else\ 0)\ A\ (sum\ f\ (F \cap A))$
⟨*proof*⟩

lemma *has_subsum_If_finite*:
assumes *finite* $\{n \in A.\ p\ n\}$
shows *has_subsum* $(\lambda n.\ if\ p\ n\ then\ f\ n\ else\ 0)\ A\ (sum\ f\ \{n \in A.\ p\ n\})$
⟨*proof*⟩

lemma *has_subsum_univ*:
$f\ sums\ v \Longrightarrow$ *has_subsum* $f\ UNIV\ v$
⟨*proof*⟩

lemma *subsumI*:
fixes $f :: nat \Rightarrow 'a :: \{t2_space, comm_monoid_add\}$
shows *has_subsum* $f\ A\ x \Longrightarrow x = subsum\ f\ A$
⟨*proof*⟩

lemma *has_subsum_summable*:
has_subsum $f\ A\ x \Longrightarrow f$ *subsummable* A
⟨*proof*⟩

lemma *subsummable_sums*:
fixes $f :: nat \Rightarrow 'a :: \{comm_monoid_add, t2_space\}$
shows f *subsummable* $S \Longrightarrow$ *has_subsum* $f\ S\ (subsum\ f\ S)$
⟨*proof*⟩

lemma *has_subsum_diff_finite*:
fixes $S :: 'a :: \{topological_ab_group_add, t2_space\}$
assumes *finite* F *has_subsum* $f\ A\ S\ F \subseteq A$
shows *has_subsum* $f\ (A - F)\ (S - sum\ f\ F)$
⟨*proof*⟩

lemma *subsum_split*:
fixes $f :: nat \Rightarrow 'a :: \{topological_ab_group_add, t2_space\}$
assumes f *subsummable* A *finite* F $F \subseteq A$
shows $subsum\ f\ A = sum\ f\ F + subsum\ f\ (A - F)$
⟨*proof*⟩

lemma *has_subsum_zero* [*simp*]: *has_subsum* $(\lambda n.\ 0)\ A\ 0$ ⟨*proof*⟩
lemma *zero_subsummable* [*simp*]: $(\lambda n.\ 0)$ *subsummable* A ⟨*proof*⟩
lemma *zero_subsum* [*simp*]: $(\sum$ ‘$n{\in}A.\ 0 :: 'a :: \{comm_monoid_add, t2_space\}) = 0$ ⟨*proof*⟩

lemma *has_subsum_minus*:
fixes $f :: nat \Rightarrow 'a :: real_normed_vector$
assumes *has_subsum* $f\ A\ a$ *has_subsum* $g\ A\ b$
shows *has_subsum* $(\lambda n.\ f\ n - g\ n)\ A\ (a - b)$
⟨*proof*⟩

lemma *subsum_minus*:
assumes *f subsummable A g subsummable A*
shows *subsum f A − subsum g A* = (∑ ‘*n*∈*A*. *f n − g n* :: ′*a* :: *real_normed_vector*)
⟨*proof*⟩

lemma *subsummable_minus*:
assumes *f subsummable A g subsummable A*
shows (λ*n*. *f n − g n* :: ′*a* :: *real_normed_vector*) *subsummable A*
⟨*proof*⟩

lemma *has_subsum_uminus*:
assumes *has_subsum f A a*
shows *has_subsum* (λ*n*. − *f n* :: ′*a* :: *real_normed_vector*) *A* (− *a*)
⟨*proof*⟩

lemma *subsum_uminus*:
f subsummable A ⟹ − *subsum f A* = (∑ ‘*n*∈*A*. − *f n* :: ′*a* :: *real_normed_vector*)
⟨*proof*⟩

lemma *subsummable_uminus*:
f subsummable A ⟹ (λ*n*. − *f n* :: ′*a* :: *real_normed_vector*) *subsummable A*
⟨*proof*⟩

lemma *has_subsum_add*:
fixes *f* :: *nat* ⇒ ′*a* :: *real_normed_vector*
assumes *has_subsum f A a has_subsum g A b*
shows *has_subsum* (λ*n*. *f n* + *g n*) *A* (*a* + *b*)
⟨*proof*⟩

lemma *subsum_add*:
assumes *f subsummable A g subsummable A*
shows *subsum f A* + *subsum g A* = (∑ ‘*n*∈*A*. *f n* + *g n* :: ′*a* :: *real_normed_vector*)
⟨*proof*⟩

lemma *subsummable_add*:
assumes *f subsummable A g subsummable A*
shows (λ*n*. *f n* + *g n* :: ′*a* :: *real_normed_vector*) *subsummable A*
⟨*proof*⟩

lemma *subsum_cong*:
(⋀*x*. *x* ∈ *A* ⟹ *f x* = *g x*) ⟹ *subsum f A* = *subsum g A*
⟨*proof*⟩

lemma *subsummable_cong*:
fixes *f* :: *nat* ⇒ ′*a* :: *real_normed_vector*
shows (⋀*x*. *x* ∈ *A* ⟹ *f x* = *g x*) ⟹ (*f subsummable A*) = (*g subsummable A*)
⟨*proof*⟩

lemma *subsum_norm_bound*:
fixes *f* :: *nat* ⇒ ′*a* :: *banach*
assumes *g subsummable A* ⋀*n*. *n* ∈ *A* ⟹ ‖*f n*‖ ≤ *g n*
shows ‖*subsum f A*‖ ≤ *subsum g A*
⟨*proof*⟩

lemma *eval_fds_subsum*:
fixes $f :: 'a :: \{nat_power, banach, real_normed_field\}$ *fds*
assumes *fds_converges f s*
shows *has_subsum* $(\lambda n.$ *fds_nth f n / nat_power n s*$)$ $\{1..\}$ $($*eval_fds f s*$)$
⟨*proof*⟩

lemma *fds_abs_subsummable*:
fixes $f :: 'a :: \{nat_power, banach, real_normed_field\}$ *fds*
assumes *fds_abs_converges f s*
shows $(\lambda n.$ $\|$*fds_nth f n / nat_power n s*$\|)$ *subsummable* $\{1..\}$
⟨*proof*⟩

lemma *subsum_mult2*:
fixes $f :: nat \Rightarrow 'a ::$ *real_normed_algebra*
shows *f subsummable A* $\Longrightarrow$ $(\sum$ ‘$x \in A.$ *f x* $*$ *c*$) =$ *subsum f A* $*$ *c*
⟨*proof*⟩

lemma *subsummable_mult2*:
fixes $f :: nat \Rightarrow 'a ::$ *real_normed_algebra*
assumes *f subsummable A*
shows $(\lambda x.$ *f x* $*$ *c*$)$ *subsummable A*
⟨*proof*⟩

lemma *subsum_ge_limit*:
lim $(\lambda N. \sum n = m..N.$ *f n*$) = (\sum$ ‘$n \geq m.$ *f n*$)$
⟨*proof*⟩

lemma *has_subsum_ge_limit*:
fixes $f :: nat \Rightarrow 'a :: \{t2_space, comm_monoid_add, topological_space\}$
assumes $((\lambda N. \sum n = m..N.$ *f n*$) \longrightarrow l)$ *at_top*
shows *has_subsum f* $\{m..\}$ *l*
⟨*proof*⟩

lemma *eval_fds_complex*:
fixes $f ::$ *complex fds*
assumes *fds_converges f s*
shows *has_subsum* $(\lambda n.$ *fds_nth f n / n nat_powr s*$)$ $\{1..\}$ $($*eval_fds f s*$)$
⟨*proof*⟩

lemma *eval_fds_complex_subsum*:
fixes $f ::$ *complex fds*
assumes *fds_converges f s*
shows *eval_fds f s* $= (\sum$ ‘$n \geq 1.$ *fds_nth f n / n nat_powr s*$)$
$(\lambda n.$ *fds_nth f n / n nat_powr s*$)$ *subsummable* $\{1..\}$
⟨*proof*⟩

lemma *has_sum_imp_has_subsum*:
fixes $x :: 'a :: \{comm_monoid_add, t2_space\}$
assumes $(f$ *has_sum x*$)$ *A*
shows *has_subsum f A x*
⟨*proof*⟩

unbundle *no pnt_syntax*

end

theory *Perron_Formula*
imports
PNT_Remainder_Library
PNT_Subsummable
begin
unbundle *pnt_syntax*

5 Perron's formula

This version of Perron's theorem is referenced to: *Perron′s Formula and the Prime Number Theorem for Automorphic L−Functions*, *Jianya Liu*, *Y. Ye*

A contour integral estimation lemma that will be used both in proof of Perron's formula and the prime number theorem.

lemma *perron_aux_3′*:
fixes $f :: complex \Rightarrow complex$ **and** $a\ b\ B\ T :: real$
assumes *Ha*: $0 < a$ **and** *Hb*: $0 < b$ **and** *hT*: $0 < T$
and *Hf*: $\bigwedge t.\ t \in \{-T..T\} \Longrightarrow \|f\ (Complex\ b\ t)\| \leq B$
and *Hf′*: $(\lambda s.\ f\ s * a\ powr\ s\ /\ s)\ contour_integrable_on\ (linepath\ (Complex\ b\ (-T))\ (Complex\ b\ T))$
shows $\|1\ /\ (2 * pi * \mathrm{i}) * contour_integral\ (linepath\ (Complex\ b\ (-T))\ (Complex\ b\ T))\ (\lambda s.\ f\ s * a\ powr\ s\ /\ s)\|$
$\leq B * a\ powr\ b * ln\ (1 + T\ /\ b)$
⟨*proof*⟩

locale *perron_locale* =
fixes $b\ B\ H\ T\ x :: real$ **and** $f :: complex\ fds$
assumes *Hb*: $0 < b$ **and** *hT*: $b \leq T$
and *Hb′*: $abs_conv_abscissa\ f < b$
and *hH*: $1 < H$ **and** *hH′*: $b + 1 \leq H$ **and** *Hx*: $0 < x$
and *hB*: $(\sum\ 'n \geq 1.\ \|fds_nth\ f\ n\|\ /\ n\ nat_powr\ b) \leq B$
begin
definition *r* **where** $r\ a \equiv$
if $a \neq 1$ *then* $min\ (1\ /\ (2 * T * |ln\ a|))\ (2 + ln\ (T\ /\ b))$
else $(2 + ln\ (T\ /\ b))$
definition *path* **where** $path \equiv linepath\ (Complex\ b\ (-T))\ (Complex\ b\ T)$
definition *img_path* **where** $img_path \equiv path_image\ path$
definition σ_a **where** $\sigma_a \equiv abs_conv_abscissa\ f$
definition *region* **where** $region = \{n :: nat.\ x - x\ /\ H \leq n \wedge n \leq x + x\ /\ H\}$
definition *F* **where** $F\ (a :: real) \equiv$
$1\ /\ (2 * pi * \mathrm{i}) * contour_integral\ path\ (\lambda s.\ a\ powr\ s\ /\ s) - (if\ 1 \leq a\ then\ 1\ else\ 0)$
definition F' **where** $F'\ (n :: nat) \equiv F\ (x\ /\ n)$

lemma *hT′*: $0 < T$ ⟨*proof*⟩
lemma *cond*: $0 < b\ b \leq T\ 0 < T$ ⟨*proof*⟩

lemma *perron_integrable*:
assumes $(0 :: real) < a$
shows $(\lambda s.\ a\ powr\ s\ /\ s)\ contour_integrable_on\ (linepath\ (Complex\ b\ (-T))\ (Complex\ b\ T))$
⟨*proof*⟩

lemma *perron_aux_1′*:
fixes $U :: real$
assumes *hU*: $0 < U$ **and** *Ha*: $1 < a$
shows $\|F\ a\| \leq 1\ /\ pi * a\ powr\ b\ /\ (T * |ln\ a|) + a\ powr\ -U * T\ /\ (pi * U)$
⟨*proof*⟩

lemma *perron_aux_1*:
assumes *Ha*: $1 < a$
shows $\|F\ a\| \leq 1\ /\ pi * a\ powr\ b\ /\ (T * |ln\ a|)$ (**is** $_ \leq ?x$)
⟨*proof*⟩

lemma *perron_aux_2′*:
fixes $U :: real$
assumes *hU*: $0 < U\ b < U$ **and** *Ha*: $0 < a \wedge a < 1$
shows $\|F\ a\| \leq 1\ /\ pi * a\ powr\ b\ /\ (T * |ln\ a|) + a\ powr\ U * T\ /\ (pi * U)$
⟨*proof*⟩

lemma *perron_aux_2*:
assumes *Ha*: $0 < a \wedge a < 1$
shows $\|F\ a\| \leq 1\ /\ pi * a\ powr\ b\ /\ (T * |ln\ a|)$ (**is** $_ \leq ?x$)
⟨*proof*⟩

lemma *perron_aux_3*:
assumes *Ha*: $0 < a$
shows $\|1\ /\ (2 * pi * \mathrm{i}) * contour_integral\ path\ (\lambda s.\ a\ powr\ s\ /\ s)\| \leq a\ powr\ b * ln\ (1 + T\ /\ b)$
⟨*proof*⟩

lemma *perron_aux′*:
assumes *Ha*: $0 < a$
shows $\|F\ a\| \leq a\ powr\ b * r\ a$
⟨*proof*⟩

lemma *r_bound*:
assumes *Hn*: $1 \leq n$
shows $r\ (x\ /\ n) \leq H\ /\ T + (if\ n \in region\ then\ 2 + ln\ (T\ /\ b)\ else\ 0)$
⟨*proof*⟩

lemma *perron_aux*:
assumes *Hn*: $0 < n$
shows $\|F'\ n\| \leq 1\ /\ n\ nat_powr\ b * (x\ powr\ b * H\ /\ T)$
$+ (if\ n \in region\ then\ 3 * (2 + ln\ (T\ /\ b))\ else\ 0)$ (**is** $?P \leq ?Q$)
⟨*proof*⟩

definition *a* **where** $a\ n \equiv fds_nth\ f\ n$

lemma *finite_region*: *finite region*
⟨*proof*⟩

lemma *zero_notin_region*: $0 \notin region$
⟨*proof*⟩

lemma *path_image_conv*:
assumes $s \in img_path$
shows $conv_abscissa\ f < s \cdot 1$
⟨*proof*⟩

lemma *converge_on_path*:
assumes $s \in img_path$
shows *fds_converges f s*
⟨*proof*⟩

lemma *summable_on_path*:
assumes $s \in img_path$
shows $(\lambda n.\ a\ n\ /\ n\ nat_powr\ s)$ *subsummable* $\{1..\}$
⟨*proof*⟩

lemma *zero_notin_path*:
shows $0 \notin closed_segment\ (Complex\ b\ (-\ T))\ (Complex\ b\ T)$
⟨*proof*⟩

lemma *perron_bound*:
$\|\sum\ 'n \geq 1.\ a\ n * F'\ n\| \leq x\ powr\ b * H * B\ /\ T$
$+\ 3 * (2 + ln\ (T\ /\ b)) * (\sum n{\in}region.\ \|a\ n\|)$
⟨*proof*⟩

lemma *perron*:
$(\lambda s.\ eval_fds\ f\ s * x\ powr\ s\ /\ s)\ contour_integrable_on\ path$
$\|sum_upto\ a\ x - 1\ /\ (2 * pi * \mathrm{i}) * contour_integral\ path\ (\lambda s.\ eval_fds\ f\ s * x\ powr\ s\ /\ s)\|$
$\leq x\ powr\ b * H * B\ /\ T + 3 * (2 + ln\ (T\ /\ b)) * (\sum n{\in}region.\ \|a\ n\|)$
⟨*proof*⟩
end

theorem *perron_formula*:
fixes $b\ B\ H\ T\ x :: real$ **and** $f :: complex\ fds$
assumes *Hb*: $0 < b$ **and** *hT*: $b \leq T$
and *Hb'*: $abs_conv_abscissa\ f < b$
and *hH*: $1 < H$ **and** *hH'*: $b + 1 \leq H$ **and** *Hx*: $0 < x$
and *hB*: $(\sum\ 'n \geq 1.\ \|fds_nth\ f\ n\|\ /\ n\ nat_powr\ b) \leq B$
shows $(\lambda s.\ eval_fds\ f\ s * x\ powr\ s\ /\ s)\ contour_integrable_on\ (linepath\ (Complex\ b\ (-T))\ (Complex\ b\ T))$
$\|sum_upto\ (fds_nth\ f)\ x - 1\ /\ (2 * pi * \mathrm{i}) *$
$contour_integral\ (linepath\ (Complex\ b\ (-T))\ (Complex\ b\ T))\ (\lambda s.\ eval_fds\ f\ s * x\ powr\ s\ /\ s)\|$
$\leq x\ powr\ b * H * B\ /\ T + 3 * (2 + ln\ (T\ /\ b)) * (\sum n \mid x - x\ /\ H \leq n \wedge n \leq x + x\ /\ H.\ \|fds_nth\ f\ n\|)$
⟨*proof*⟩

theorem *perron_asymp*:
fixes $b\ x :: real$
assumes *b*: $b > 0\ ereal\ b > abs_conv_abscissa\ f$
assumes *x*: $0 < x\ x \notin \mathbb{N}$
defines $L \equiv (\lambda T.\ linepath\ (Complex\ b\ (-T))\ (Complex\ b\ T))$
shows $((\lambda T.\ contour_integral\ (L\ T)\ (\lambda s.\ eval_fds\ f\ s * of_real\ x\ powr\ s\ /\ s)) \longrightarrow 2 * pi * \mathrm{i} * sum_upto\ (\lambda n.\ fds_nth\ f\ n)\ x)\ at_top$
⟨*proof*⟩

unbundle *no pnt_syntax*

end
theory *PNT_with_Remainder*
imports
Relation_of_PNTs
Zeta_Zerofree
Perron_Formula
begin
unbundle *pnt_syntax*

6 Estimation of the order of $\frac{\zeta'(s)}{\zeta(s)}$

notation *primes_psi* (‹ψ›)

lemma *zeta_div_bound'*:
  assumes *1 + exp (− 4 * ln (14 + 4 * t)) ≤ σ*
    and *13 / 22 ≤ t*
    and *z ∈ cball (Complex σ t) (1 / 2)*
  shows *‖zeta z / zeta (Complex σ t)‖ ≤ exp (12 * ln (14 + 4 * t))*
⟨*proof*⟩

lemma *zeta_div_bound*:
  assumes *1 + exp (− 4 * ln (14 + 4 * |t|)) ≤ σ*
    and *13 / 22 ≤ |t|*
    and *z ∈ cball (Complex σ t) (1 / 2)*
  shows *‖zeta z / zeta (Complex σ t)‖ ≤ exp (12 * ln (14 + 4 * |t|))*
⟨*proof*⟩

definition C_2 **where** $C_2 \equiv 319979520 :: real$

lemma $C_2_gt_zero$: $0 < C_2$ ⟨*proof*⟩

lemma *logderiv_zeta_order_estimate'*:
∀F t in (abs going_to at_top).
  *∀σ. 1 − 1 / 7 * C₁ / ln (|t| + 3) ≤ σ*
  *⟶ ‖logderiv zeta (Complex σ t)‖ ≤ C₂ * (ln (|t| + 3))²*
⟨*proof*⟩

definition C_3 **where**
$C_3 \equiv SOME\ T.\ 0 < T \wedge$
  $(\forall t.\ T \le |t| \longrightarrow$
    $(\forall \sigma.\ 1 - 1 / 7 * C_1 / ln\ (|t| + 3) \le \sigma$
     $\longrightarrow \|logderiv\ zeta\ (Complex\ \sigma\ t)\| \le C_2 * (ln\ (|t| + 3))^2))$

lemma C_3_prop:
  $0 < C_3 \wedge$
  $(\forall t.\ C_3 \le |t| \longrightarrow$
    $(\forall \sigma.\ 1 - 1 / 7 * C_1 / ln\ (|t| + 3) \le \sigma$
    $\longrightarrow \|logderiv\ zeta\ (Complex\ \sigma\ t)\| \le C_2 * (ln\ (|t| + 3))^2))$
⟨*proof*⟩

lemma $C_3_gt_zero$: $0 < C_3$ ⟨*proof*⟩

lemma *logderiv_zeta_order_estimate*:
  assumes *1 − 1 / 7 * C₁ / ln (|t| + 3) ≤ σ C₃ ≤ |t|*
  shows *‖logderiv zeta (Complex σ t)‖ ≤ C₂ * (ln (|t| + 3))²*
  ⟨*proof*⟩

definition *zeta_zerofree_region*
  where *zeta_zerofree_region ≡ {s. s ≠ 1 ∧ 1 − C₁ / ln (|Im s| + 2) < Re s}*
definition *logderiv_zeta_region*
  where *logderiv_zeta_region ≡ {s. C₃ ≤ |Im s| ∧ 1 − 1 / 7 * C₁ / ln (|Im s| + 3) ≤ Re s}*
definition *zeta_strip_region*
  where *zeta_strip_region σ T ≡ {s. s ≠ 1 ∧ σ ≤ Re s ∧ |Im s| ≤ T}*
definition *zeta_strip_region'*

where *zeta_strip_region'* $\sigma\ T \equiv \{s.\ s \neq 1 \wedge \sigma \leq Re\ s \wedge C_3 \leq |Im\ s| \wedge |Im\ s| \leq T\}$

lemma *strip_in_zerofree_region*:
assumes $1 - C_1\ /\ ln\ (T + 2) < \sigma$
shows *zeta_strip_region* $\sigma\ T \subseteq$ *zeta_zerofree_region*
⟨*proof*⟩

lemma *strip_in_logderiv_zeta_region*:
assumes $1 - 1\ /\ 7 * C_1\ /\ ln\ (T + 3) \leq \sigma$
shows *zeta_strip_region'* $\sigma\ T \subseteq$ *logderiv_zeta_region*
⟨*proof*⟩

lemma *strip_condition_imp*:
assumes $0 \leq T\ 1 - 1\ /\ 7 * C_1\ /\ ln\ (T + 3) \leq \sigma$
shows $1 - C_1\ /\ ln\ (T + 2) < \sigma$
⟨*proof*⟩

lemma *zeta_zerofree_region*:
assumes $s \in$ *zeta_zerofree_region*
shows *zeta* $s \neq 0$
⟨*proof*⟩

lemma *logderiv_zeta_region_estimate*:
assumes $s \in$ *logderiv_zeta_region*
shows $\|$*logderiv zeta* $s\| \leq C_2 * (ln\ (|Im\ s| + 3))^2$
⟨*proof*⟩

definition C_4 :: *real* **where** $C_4 \equiv 1\ /\ 6666241$

lemma C_4*_prop*:
$\forall_F\ x$ *in at_top.* $C_4\ /\ ln\ x \leq C_1\ /\ (7 * ln\ (x + 3))$
⟨*proof*⟩

lemma C_4*_gt_zero*: $0 < C_4$ ⟨*proof*⟩

definition C_5*_prop* **where**
C_5*_prop* $C_5 \equiv$
$0 < C_5 \wedge (\forall_F\ x$ *in at_top.* $(\forall\, t.\ |t| \leq x$
$\longrightarrow \|$*logderiv zeta* (*Complex* $(1 - C_4\ /\ ln\ x)\ t)\| \leq C_5 * (ln\ x)^2))$

lemma *logderiv_zeta_bound_vertical'*:
$\exists\, C_5.\ C_5$*_prop* C_5
⟨*proof*⟩

definition C_5 **where** $C_5 \equiv$ *SOME* $C_5.\ C_5$*_prop* C_5

lemma
C_5*_gt_zero*: $0 < C_5$ (**is** *?prop_1*) **and**
logderiv_zeta_bound_vertical:
$\forall_F\ x$ *in at_top.* $\forall\, t.\ |t| \leq x$
$\longrightarrow \|$*logderiv zeta* (*Complex* $(1 - C_4\ /\ ln\ x)\ t)\| \leq C_5 * (ln\ x)^2$ (**is** *?prop_2*)
⟨*proof*⟩

7 Deducing prime number theorem using Perron's formula

locale *prime_number_theorem* =
  fixes $c\ \varepsilon$ :: *real*
  assumes *Hc*: $0 < c$ **and** *Hc'*: $c * c < 2 * C_4$ **and** *Hε*: $0 < \varepsilon\ 2 * \varepsilon < c$
begin
notation *primes_psi* ($\langle\psi\rangle$)
definition H **where** $H\ x \equiv exp\ (c\ /\ 2 * (ln\ x)\ powr\ (1\ /\ 2))$ **for** x :: *real*
definition T **where** $T\ x \equiv exp\ (c * (ln\ x)\ powr\ (1\ /\ 2))$ **for** x :: *real*
definition a **where** $a\ x \equiv 1 - C_4\ /\ (c * (ln\ x)\ powr\ (1\ /\ 2))$ **for** x :: *real*
definition b **where** $b\ x \equiv 1 + 1\ /\ (ln\ x)$ **for** x :: *real*
definition B **where** $B\ x \equiv 5\ /\ 4 * ln\ x$ **for** x :: *real*
definition f **where** $f\ x\ s \equiv x\ powr\ s\ /\ s * logderiv\ zeta\ s$ **for** x :: *real* **and** s :: *complex*
definition R **where** $R\ x \equiv$
  $x\ powr\ (b\ x) * H\ x * B\ x\ /\ T\ x + 3 * (2 + ln\ (T\ x\ /\ b\ x))$
  $* (\sum n \mid x - x\ /\ H\ x \le n \wedge n \le x + x\ /\ H\ x.\ \|fds_nth\ (fds\ mangoldt_complex)\ n\|)$ **for** x :: *real*
definition Rc' **where** $Rc' \equiv O(\lambda x.\ x * exp\ (-\ (c\ /\ 2 - \varepsilon) * ln\ x\ powr\ (1\ /\ 2)))$
definition Rc **where** $Rc \equiv O(\lambda x.\ x * exp\ (-\ (c\ /\ 2 - 2 * \varepsilon) * ln\ x\ powr\ (1\ /\ 2)))$
definition z_1 **where** $z_1\ x \equiv Complex\ (a\ x)\ (-\ T\ x)$ **for** x
definition z_2 **where** $z_2\ x \equiv Complex\ (b\ x)\ (-\ T\ x)$ **for** x
definition z_3 **where** $z_3\ x \equiv Complex\ (b\ x)\ (T\ x)$ **for** x
definition z_4 **where** $z_4\ x \equiv Complex\ (a\ x)\ (T\ x)$ **for** x
definition *rect* **where** $rect\ x \equiv cbox\ (z_1\ x)\ (z_3\ x)$ **for** x
definition *rect'* **where** $rect'\ x \equiv rect\ x - \{1\}$ **for** x
definition P_t **where** $P_t\ x\ t \equiv linepath\ (Complex\ (a\ x)\ t)\ (Complex\ (b\ x)\ t)$ **for** $x\ t$
definition P_1 **where** $P_1\ x \equiv linepath\ (z_1\ x)\ (z_4\ x)$ **for** x
definition P_2 **where** $P_2\ x \equiv linepath\ (z_2\ x)\ (z_3\ x)$ **for** x
definition P_3 **where** $P_3\ x \equiv P_t\ x\ (-\ T\ x)$ **for** x
definition P_4 **where** $P_4\ x \equiv P_t\ x\ (T\ x)$ **for** x
definition P_r **where** $P_r\ x \equiv rectpath\ (z_1\ x)\ (z_3\ x)$ **for** x

lemma *Rc_eq_rem_est*:
  $Rc = rem_est\ (c\ /\ 2 - 2 * \varepsilon)\ (1\ /\ 2)\ 0$
⟨*proof*⟩

lemma *residue_f*:
  $residue\ (f\ x)\ 1 = -\ x$
⟨*proof*⟩

lemma *rect_in_strip*:
  $rect\ x - \{1\} \subseteq zeta_strip_region\ (a\ x)\ (T\ x)$
  ⟨*proof*⟩

lemma *rect_in_strip'*:
  $\{s \in rect\ x.\ C_3 \le |Im\ s|\} \subseteq zeta_strip_region'\ (a\ x)\ (T\ x)$
  ⟨*proof*⟩

lemma
  rect'_in_zerofree: $\forall_F\ x\ in\ at_top.\ rect'\ x \subseteq zeta_zerofree_region$ **and**
  rect_in_logderiv_zeta: $\forall_F\ x\ in\ at_top.\ \{s \in rect\ x.\ C_3 \le |Im\ s|\} \subseteq logderiv_zeta_region$
⟨*proof*⟩

lemma *zeta_nonzero_in_rect*:
  $\forall_F\ x\ in\ at_top.\ \forall s.\ s \in rect'\ x \longrightarrow zeta\ s \neq 0$
  ⟨*proof*⟩

lemma *zero_notin_rect*: $\forall_F\ x\ in\ at_top.\ 0 \notin rect'\ x$
⟨*proof*⟩

lemma *f_analytic*:
$\forall_F\ x\ in\ at_top.\ f\ x\ analytic_on\ rect'\ x$
⟨*proof*⟩

lemma *path_image_in_rect_1*:
assumes $0 \le T\ x \wedge a\ x \le b\ x$
shows $path_image\ (P_1\ x) \subseteq rect\ x \wedge path_image\ (P_2\ x) \subseteq rect\ x$
⟨*proof*⟩

lemma *path_image_in_rect_2*:
assumes $0 \le T\ x \wedge a\ x \le b\ x \wedge t \in \{-T\ x..T\ x\}$
shows $path_image\ (P_t\ x\ t) \subseteq rect\ x$
⟨*proof*⟩

definition *path_in_rect'* **where**
$path_in_rect'\ x \equiv$
$path_image\ (P_1\ x) \subseteq rect'\ x \wedge path_image\ (P_2\ x) \subseteq rect'\ x \wedge$
$path_image\ (P_3\ x) \subseteq rect'\ x \wedge path_image\ (P_4\ x) \subseteq rect'\ x$

lemma *path_image_in_rect'*:
assumes $0 < T\ x \wedge a\ x < 1 \wedge 1 < b\ x$
shows $path_in_rect'\ x$
⟨*proof*⟩

lemma *asymp_1*:
$\forall_F\ x\ in\ at_top.\ 0 < T\ x \wedge a\ x < 1 \wedge 1 < b\ x$
⟨*proof*⟩

lemma *f_continuous_on*:
$\forall_F\ x\ in\ at_top.\ \forall\ A \subseteq rect'\ x.\ continuous_on\ A\ (f\ x)$
⟨*proof*⟩

lemma *contour_integrability*:
$\forall_F\ x\ in\ at_top.$
$f\ x\ contour_integrable_on\ P_1\ x \wedge f\ x\ contour_integrable_on\ P_2\ x \wedge$
$f\ x\ contour_integrable_on\ P_3\ x \wedge f\ x\ contour_integrable_on\ P_4\ x$
⟨*proof*⟩

lemma *contour_integral_rectpath'*:
assumes $f\ x\ analytic_on\ (rect'\ x)\ 0 < T\ x \wedge a\ x < 1 \wedge 1 < b\ x$
shows $contour_integral\ (P_r\ x)\ (f\ x) = -\ 2 * pi * \mathrm{i} * x$
⟨*proof*⟩

lemma *contour_integral_rectpath*:
$\forall_F\ x\ in\ at_top.\ contour_integral\ (P_r\ x)\ (f\ x) = -\ 2 * pi * \mathrm{i} * x$
⟨*proof*⟩

lemma *valid_paths*:
$valid_path\ (P_1\ x)\ valid_path\ (P_2\ x)\ valid_path\ (P_3\ x)\ valid_path\ (P_4\ x)$
⟨*proof*⟩

lemma *integral_rectpath_split*:

assumes $f\ x$ *contour_integrable_on* $P_1\ x \wedge f\ x$ *contour_integrable_on* $P_2\ x \wedge$
$f\ x$ *contour_integrable_on* $P_3\ x \wedge f\ x$ *contour_integrable_on* $P_4\ x$
shows *contour_integral* $(P_3\ x)\ (f\ x)$ + *contour_integral* $(P_2\ x)\ (f\ x)$
$-$ *contour_integral* $(P_4\ x)\ (f\ x)$ $-$ *contour_integral* $(P_1\ x)\ (f\ x) =$ *contour_integral* $(P_r\ x)\ (f\ x)$
⟨*proof*⟩

lemma P_2*_eq*:
$\forall_F\ x$ *in at_top. contour_integral* $(P_2\ x)\ (f\ x) + 2 * pi * \mathrm{i} * x$
$=$ *contour_integral* $(P_1\ x)\ (f\ x)$ $-$ *contour_integral* $(P_3\ x)\ (f\ x)$ + *contour_integral* $(P_4\ x)\ (f\ x)$
⟨*proof*⟩

lemma *estimation_*P_1:
$(\lambda x.\ \|$*contour_integral* $(P_1\ x)\ (f\ x)\|) \in Rc$
⟨*proof*⟩

lemma *estimation_*$P_t{}'$:
assumes h:
$1 < x \wedge max\ 1\ C_3 \leq T\ x\ a\ x < 1 \wedge 1 < b\ x$
$\{s \in rect\ x.\ C_3 \leq |Im\ s|\} \subseteq logderiv_zeta_region$
$f\ x$ *contour_integrable_on* $P_3\ x \wedge f\ x$ *contour_integrable_on* $P_4\ x$
and Ht: $|t| = T\ x$
shows $\|$*contour_integral* $(P_t\ x\ t)\ (f\ x)\| \leq C_2 * exp\ 1 * x\ /\ T\ x * (ln\ (T\ x + 3))^2 * (b\ x - a\ x)$
⟨*proof*⟩

lemma *estimation_*P_t:
$(\lambda x.\ \|$*contour_integral* $(P_3\ x)\ (f\ x)\|) \in Rc \wedge$
$(\lambda x.\ \|$*contour_integral* $(P_4\ x)\ (f\ x)\|) \in Rc$
⟨*proof*⟩

lemma *Re_path_*P_2:
$\bigwedge z.\ z \in$ *path_image* $(P_2\ x) \Longrightarrow Re\ z = b\ x$
⟨*proof*⟩

lemma *estimation_*P_2:
$(\lambda x.\ \|1\ /\ (2 * pi * \mathrm{i}) *$ *contour_integral* $(P_2\ x)\ (f\ x) + x\|) \in Rc$
⟨*proof*⟩

lemma *estimation_R*:
$R \in Rc$
⟨*proof*⟩

lemma *perron_psi*:
$\forall_F\ x$ *in at_top.* $\|\psi\ x + 1\ /\ (2 * pi * \mathrm{i}) *$ *contour_integral* $(P_2\ x)\ (f\ x)\| \leq R\ x$
⟨*proof*⟩

lemma *estimation_perron_psi*:
$(\lambda x.\ \|\psi\ x + 1\ /\ (2 * pi * \mathrm{i}) *$ *contour_integral* $(P_2\ x)\ (f\ x)\|) \in Rc$
⟨*proof*⟩

theorem *prime_number_theorem*:
PNT_3 $(c\ /\ 2 - 2 * \varepsilon)\ (1\ /\ 2)\ 0$
⟨*proof*⟩

no_notation *primes_psi* (‹ψ›)
end

unbundle *prime_counting_syntax*

theorem *prime_number_theorem*:
  shows $(\lambda x.\ \pi\ x - Li\ x) \in O(\lambda x.\ x * exp\ (-\ 1\ /\ 3653 * (ln\ x)\ powr\ (1\ /\ 2)))$
⟨*proof*⟩

hide_const (**open**) C_3 C_4 C_5
unbundle *no prime_counting_syntax* **and** *no pnt_syntax*

end