

Prime Number Theorem with Remainder Term

Shuhao Song and Bowen Yao

May 8, 2024

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:

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

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

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

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 <i>floor</i> , <i>ceil</i> and <i>nat_pow</i>	6
1.6	Elementary estimation of <i>exp</i> and <i>ln</i>	6
1.7	Miscellaneous lemmas	7
2	Implication relation of many forms of prime number theorem	7
3	Some basic theorems in complex analysis	10
3.1	Introduction rules for holomorphic functions and analytic functions	10
3.2	Factorization of analytic function on compact region	10
3.2.1	Auxiliary propositions for theorem <i>analytic_factorization</i>	11
3.3	Schwarz theorem in complex analysis	12
3.4	Borel-Carathedory theorem	12
3.5	Lemma 3.9	13
4	Zero-free region of zeta function	14
5	Perron's formula	21
6	Estimation of the order of $\frac{\zeta'(s)}{\zeta(s)}$	24

7 Deducing prime number theorem using Perron's formula

```

theory PNT_Notation
imports
  Prime_Number_Theorem.Prime_Counting_Functions
begin

definition PNT_const_C1  $\equiv 1 / 952320 :: real$ 

abbreviation nat_powr
  (infixr nat'_powr 80)
where
  n nat_powr x  $\equiv (of\_nat n) powr x$ 

bundle pnt_notation
begin
notation PNT_const_C1 (C1)
notation norm (||_||)
notation Suc ( $\_+ [101] 100$ )
end

bundle no_pnt_notation
begin
no_notation PNT_const_C1 (C1)
no_notation norm (||_||)
no_notation Suc ( $\_+ [101] 100$ )
end

end
theory PNT_Remainder_Library
imports
  PNT_Notation
begin
unbundle pnt_notation

```

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 $s \neq 1 \implies zeta'\ s = 0 \iff zeta\ s = 0$

⟨proof⟩

lemma *zeta'_eq_zero_iff*:

shows $zeta'\ s = 0 \iff zeta\ s = 0 \wedge s \neq 1$

⟨proof⟩

lemma *zeta_eq_zero_iff*:

shows $zeta\ s = 0 \iff zeta'\ s = 0 \vee s = 1$

⟨proof⟩

1.2 Logarithm derivatives

definition *logderiv* $f\ x \equiv deriv\ f\ x / f\ x$

definition *log_differentiable*

(**infixr** (*log'_differentiable*) 50)

where

$f\ log_differentiable\ x \equiv (f\ field_differentiable\ (at\ x)) \wedge f\ x \neq 0$

lemma *logderiv_prod'*:

fixes $f :: 'n \Rightarrow 'f \Rightarrow 'f :: real_normed_field$

assumes *fin*: finite *I*

and *lder*: $\bigwedge i. i \in I \implies f\ i\ log_differentiable\ a$

shows $logderiv\ (\lambda x. \prod_{i \in I}. f\ i\ x)\ a = (\sum_{i \in I}. logderiv\ (f\ i)\ a)$ (**is** ?*P*)

and $(\lambda x. \prod_{i \in I}. f\ i\ x)\ log_differentiable\ a$ (**is** ?*Q*)

⟨proof⟩

lemma *logderiv_prod*:

fixes $f :: 'n \Rightarrow 'f \Rightarrow 'f :: real_normed_field$

assumes *lder*: $\bigwedge i. i \in I \implies f\ i\ log_differentiable\ a$

shows $logderiv\ (\lambda x. \prod_{i \in I}. f\ i\ x)\ a = (\sum_{i \in I}. logderiv\ (f\ i)\ a)$ (**is** ?*P*)

and $(\lambda x. \prod_{i \in I}. f\ i\ x)\ log_differentiable\ a$ (**is** ?*Q*)

⟨proof⟩

lemma *logderiv_mult*:

assumes *f* *log_differentiable* *a*

and *g* *log_differentiable* *a*

shows $logderiv\ (\lambda z. f\ z * g\ z)\ a = logderiv\ f\ a + logderiv\ g\ a$ (**is** ?*P*)

and $(\lambda z. f\ z * g\ z)\ log_differentiable\ a$ (**is** ?*Q*)

⟨proof⟩

lemma *logderiv_cong_ev*:

assumes $\forall_F\ x\ in\ nhds\ x. f\ x = g\ x$

and $x = y$

shows $\text{logderiv } f \ x = \text{logderiv } g \ y$
 $\langle \text{proof} \rangle$

lemma *logderiv_linear*:

assumes $z \neq a$
shows $\text{logderiv } (\lambda w. w - a) \ z = 1 / (z - a)$
and $(\lambda w. w - z) \ \text{log_differentiable } a$
 $\langle \text{proof} \rangle$

lemma *deriv_shift*:

assumes $f \ \text{field_differentiable at } (a + x)$
shows $\text{deriv } (\lambda t. f \ (a + t)) \ x = \text{deriv } f \ (a + x)$
 $\langle \text{proof} \rangle$

lemma *logderiv_shift*:

assumes $f \ \text{field_differentiable at } (a + x)$
shows $\text{logderiv } (\lambda t. f \ (a + t)) \ x = \text{logderiv } f \ (a + x)$
 $\langle \text{proof} \rangle$

lemma *logderiv_inverse*:

assumes $x \neq 0$
shows $\text{logderiv } (\lambda x. 1 / x) \ x = - 1 / x$
 $\langle \text{proof} \rangle$

lemma *logderiv_zeta_eq_zeta'*:

assumes $s \neq 1 \ \text{zeta } s \neq 0$
shows $\text{logderiv } \text{zeta } s = \text{logderiv } \text{zeta}' \ s - 1 / (s - 1)$
 $\langle \text{proof} \rangle$

lemma *analytic_logderiv* [*analytic_intros*]:

assumes $f \ \text{analytic_on } A \ \wedge z. z \in A \implies f \ z \neq 0$
shows $(\lambda s. \text{logderiv } f \ s) \ \text{analytic_on } A$
 $\langle \text{proof} \rangle$

1.3 Lemmas of integration and integrability

lemma *powr_has_integral*:

fixes $a \ b \ w :: \text{real}$
assumes $Hab: a \leq b$ **and** $Hw: w > 0 \ \wedge \ w \neq 1$
shows $((\lambda x. w \ \text{powr } x) \ \text{has_integral } w \ \text{powr } b / \ln \ w - w \ \text{powr } a / \ln \ w) \ \{a..b\}$
 $\langle \text{proof} \rangle$

lemma *powr_integrable*:

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

lemma *powr_integral_bound_gt_1*:

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

lemma *powr_integral_bound_lt_1*:

fixes $a \ b \ w :: \text{real}$

assumes $Hab: a \leq b$ **and** $Hw: 0 < w \wedge w < 1$
shows $\text{integral } \{a..b\} (\lambda x. w \text{ powr } x) \leq w \text{ powr } a / |\ln w|$
 $\langle \text{proof} \rangle$

lemma $\text{set_integrableI_bounded}$:
fixes $f :: 'a \Rightarrow 'b :: \{\text{banach, second_countable_topology}\}$
shows $A \in \text{sets } M$
 $\implies (\lambda x. \text{indicator } A \ x *_{\mathbb{R}} f \ x) \in \text{borel_measurable } M$
 $\implies \text{emeasure } M \ A < \infty$
 $\implies (AE \ x \ \text{in } M. \ x \in A \longrightarrow \text{norm } (f \ x) \leq B)$
 $\implies \text{set_integrable } M \ A \ f$
 $\langle \text{proof} \rangle$

lemma $\text{integrable_cut}'$:
fixes $a \ b \ c :: \text{real}$ **and** $f :: \text{real} \Rightarrow \text{real}$
assumes $a \leq b \ b \leq c$
and $Hf: \bigwedge x. a \leq x \implies f \ \text{integrable_on } \{a..x\}$
shows $f \ \text{integrable_on } \{b..c\}$
 $\langle \text{proof} \rangle$

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

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

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

1.4 Lemmas on asymptotics

lemma $\text{eventually_at_top_linorderI}'$:
fixes $c :: 'a :: \{\text{no_top, linorder}\}$
assumes $h: \bigwedge x. c < x \implies P \ x$
shows $\text{eventually } P \ \text{at_top}$
 $\langle \text{proof} \rangle$

lemma *eventually_le_imp_bigo*:
assumes $\forall_F x \text{ in } F. \|f x\| \leq g x$
shows $f \in O[F](g)$
 $\langle \text{proof} \rangle$

lemma *eventually_le_imp_bigo'*:
assumes $\forall_F x \text{ in } F. \|f x\| \leq g x$
shows $(\lambda x. \|f x\|) \in O[F](g)$
 $\langle \text{proof} \rangle$

lemma *le_imp_bigo*:
assumes $\bigwedge x. \|f x\| \leq g x$
shows $f \in O[F](g)$
 $\langle \text{proof} \rangle$

lemma *le_imp_bigo'*:
assumes $\bigwedge x. \|f x\| \leq g x$
shows $(\lambda x. \|f x\|) \in O[F](g)$
 $\langle \text{proof} \rangle$

lemma *exp_bigo*:
fixes $f g :: \text{real} \Rightarrow \text{real}$
assumes $\forall_F x \text{ in } \text{at_top}. f x \leq g x$
shows $(\lambda x. \text{exp } (f x)) \in O(\lambda x. \text{exp } (g x))$
 $\langle \text{proof} \rangle$

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

lemma *smallo_ln_diverge_1*:
fixes $f :: \text{real} \Rightarrow \text{real}$
assumes $f_ln: f \in o(\ln)$
shows $LIM x \text{ at_top}. x * \text{exp } (- f x) :> \text{at_top}$
 $\langle \text{proof} \rangle$

lemma *ln_ln_asymp_pos*: $\forall_F x :: \text{real in } \text{at_top}. 0 < \ln (\ln x) \langle \text{proof} \rangle$
lemma *ln_asymp_pos*: $\forall_F x :: \text{real in } \text{at_top}. 0 < \ln x \langle \text{proof} \rangle$
lemma *x_asymp_pos*: $\forall_F x :: \text{real in } \text{at_top}. 0 < x \langle \text{proof} \rangle$

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

lemma *nat_le_self*: $0 \leq x \implies \text{nat } (\text{int } x) \leq x \langle \text{proof} \rangle$
lemma *floor_le*: $\bigwedge x :: \text{real}. \lfloor x \rfloor \leq x \langle \text{proof} \rangle$
lemma *ceil_ge*: $\bigwedge x :: \text{real}. x \leq \lceil x \rceil \langle \text{proof} \rangle$

lemma *nat_lt_real_iff*:
 $(n :: \text{nat}) < (a :: \text{real}) = (n < \text{nat } \lceil a \rceil)$
 $\langle \text{proof} \rangle$

lemma *nat_le_real_iff*:
 $(n :: \text{nat}) \leq (a :: \text{real}) = (n < \text{nat } (\lfloor a \rfloor + 1))$

$\langle proof \rangle$

lemma *of_real_nat_power*: $n \text{ nat_powr } (of_real \ x :: complex) = of_real \ (n \text{ nat_powr } x)$ **for** $n \ x$
 $\langle proof \rangle$

lemma *norm_nat_power*: $\|n \text{ nat_powr } (s :: complex)\| = n \text{ powr } (Re \ s)$
 $\langle proof \rangle$

1.6 Elementary estimation of exp and ln

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

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

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

1.7 Miscellaneous lemmas

abbreviation *fds_zeta_complex* :: $complex \ fds \equiv fds_zeta$

lemma *powr_mono_lt_1_cancel*:
fixes $x \ a \ b :: real$
assumes $Hx: 0 < x \wedge x < 1$
shows $(x \text{ powr } a \leq x \text{ powr } b) = (b \leq a)$
 $\langle proof \rangle$

abbreviation *mangoldt_real* :: $_ \Rightarrow real \equiv mangoldt$

abbreviation *mangoldt_complex* :: $_ \Rightarrow complex \equiv mangoldt$

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

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

lemma *C1_gt_zero*: $0 < C_1$ $\langle proof \rangle$

unbundle *no_pnt_notation*

end

theory *Relation_of_PNTs*

imports

PNT_Remainder_Library

begin
 unbundle *pnt_notation*
 unbundle *prime_counting_notation*

2 Implication relation of many forms of prime number theorem

definition *rem_est* :: *real* \Rightarrow *real* \Rightarrow *real* \Rightarrow *_* **where**
rem_est *c m n* $\equiv O(\lambda x. x * \exp(-c * \ln x \text{ powr } m * \ln(\ln x) \text{ powr } n))$

definition *Li* :: *real* \Rightarrow *real* **where** *Li* *x* $\equiv \text{integral } \{2..x\} (\lambda x. 1 / \ln x)$
definition *PNT_1* **where** *PNT_1* *c m n* $\equiv ((\lambda x. \pi x - Li x) \in \text{rem_est } c m n)$
definition *PNT_2* **where** *PNT_2* *c m n* $\equiv ((\lambda x. \vartheta x - x) \in \text{rem_est } c m n)$
definition *PNT_3* **where** *PNT_3* *c m n* $\equiv ((\lambda x. \psi x - x) \in \text{rem_est } c m n)$

lemma *rem_est_compare_powr*:
fixes *c m n* :: *real*
assumes *h*: $0 < m$ $m < 1$
shows $(\lambda x. x \text{ powr } (2 / 3)) \in \text{rem_est } c m n$
 $\langle \text{proof} \rangle$

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*
 $\langle \text{proof} \rangle$

definition *r1* **where** *r1* *x* $\equiv \pi x - Li x$ **for** *x*
definition *r2* **where** *r2* *x* $\equiv \vartheta x - x$ **for** *x*

lemma *pi_represent_by_theta*:
fixes *x* :: *real*
assumes $2 \leq x$
shows $\pi x = \vartheta x / (\ln x) + \text{integral } \{2..x\} (\lambda t. \vartheta t / (t * (\ln t)^2))$
 $\langle \text{proof} \rangle$

lemma *Li_integrate_by_part*:
fixes *x* :: *real*
assumes $2 \leq x$
shows
 $(\lambda x. 1 / (\ln x)^2) \text{ integrable_on } \{2..x\}$
 $Li x = x / (\ln x) - 2 / (\ln 2) + \text{integral } \{2..x\} (\lambda t. 1 / (\ln t)^2)$
 $\langle \text{proof} \rangle$

lemma *vartheta_integrable*:
fixes *x* :: *real*
assumes $2 \leq x$
shows $(\lambda t. \vartheta t / (t * (\ln t)^2)) \text{ integrable_on } \{2..x\}$
 $\langle \text{proof} \rangle$

lemma *r1_represent_by_r2*:
fixes *x* :: *real*
assumes *Hx*: $2 \leq x$
shows $(\lambda t. r_2 t / (t * (\ln t)^2)) \text{ integrable_on } \{2..x\}$ **(is ?P)**

$r_1 x = r_2 x / (\ln x) + 2 / \ln 2 + \text{integral } \{2..x\} (\lambda t. r_2 t / (t * (\ln t)^2))$ (is ?Q)
 <proof>

lemma *exp_integral_asymp*:

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

lemma *x_mul_exp_larger_than_const*:

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

lemma *integral_bigo_exp*:

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

lemma *integrate_r2_estimate*:

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

lemma *r2_div_ln_estimate*:

fixes $c m n :: \text{real}$
assumes $hm: 0 < m m < 1$
and $h: r_2 \in \text{rem_est } c m n$
shows $(\lambda x. r_2 x / (\ln x) + 2 / \ln 2) \in \text{rem_est } c m n$

<proof>

lemma *PNT_2_imp_PNT_1*:

fixes $l :: \text{real}$

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 $l :: \text{real}$

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_notation*

unbundle *no_pnt_notation*

end

theory *PNT_Complex_Analysis_Lemmas*

imports

PNT_Remainder_Library

begin

unbundle *pnt_notation*

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* $((\lambda z. s + z) \ ' \ A)$

shows $(\lambda z. f \ (s + z))$ *holomorphic_on* A

<proof>

lemma *holomorphic_logderiv* [*holomorphic_intros*]:

assumes f *holomorphic_on* A *open* $A \ \wedge z. z \in A \implies f \ z \neq 0$

shows $(\lambda s. \text{logderiv } f \ s)$ *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 : $\wedge z. z \in S \implies z \in T \implies f \ z = g \ z$

and hU : $U \subseteq S \cup T$

obtains h

where h *analytic_on* U

$\wedge z. z \in S \implies h \ z = f \ z$

$\wedge z. z \in T \implies h \ z = g \ z$

<proof>

lemma *analytic_on_pour_right* [*analytic_intros*]:

assumes f *analytic_on* s

shows $(\lambda z. w \ \text{pour } f \ z)$ *analytic_on* s

<proof>

3.2 Factorization of analytic function on compact region

definition *not_zero_on* (**infixr** *not'_zero'_on* 46)
where $f \text{ not_zero_on } S \equiv \exists z \in S. f z \neq 0$

lemma *not_zero_on_obtain*:
assumes $f \text{ not_zero_on } S$ **and** $S \subseteq T$
obtains t **where** $f t \neq 0$ **and** $t \in T$
<proof>

lemma *analytic_on_holomorphic_connected*:
assumes $hf: f \text{ analytic_on } S$
and $con: \text{connected } A$
and $ne: \xi \in A$ **and** $AS: A \subseteq S$
obtains $T T'$ **where**
 $f \text{ holomorphic_on } T$ $f \text{ holomorphic_on } T'$
 $\text{open } T$ $\text{open } T'$ $A \subseteq T$ $S \subseteq T'$ $\text{connected } T$
<proof>

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

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

3.2.1 Auxiliary propositions for theorem *analytic_factorization*

definition *analytic_factor_p'* **where**
<analytic_factor_p' f S K \equiv
 $\exists g n. \exists \alpha :: \text{nat} \Rightarrow \text{complex}.$
 $g \text{ analytic_on } S$
 $\bigwedge (\forall z \in K. g z \neq 0)$
 $\bigwedge (\forall z \in S. f z = g z * (\prod_{k < n. z - \alpha k})$
 $\bigwedge \alpha ' \{..<n\} \subseteq K$

definition *analytic_factor_p* **where**
<analytic_factor_p F \equiv
 $\forall f S K. f \text{ analytic_on } S$
 $\longrightarrow K \subseteq S$
 $\longrightarrow \text{connected } K$
 $\longrightarrow \text{compact } K$

$\longrightarrow f \text{ not_zero_on } K$
 $\longrightarrow \{z \in K. f z = 0\} = F$
 $\longrightarrow \text{analytic_factor_p}' f S K$

lemma *analytic_factorization_E*:

shows *analytic_factor_p* { }
 $\langle \text{proof} \rangle$

lemma *analytic_factorization_I*:

assumes *ind*: *analytic_factor_p* F
and $\xi \notin F$
shows *analytic_factor_p* (*insert* ξF)
 $\langle \text{proof} \rangle$

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 $f \text{ not_zero_on } K$
obtains g n **and** $\alpha :: \text{nat} \Rightarrow \text{complex}$ **where**
 g *analytic_on* S
 $\bigwedge z. z \in K \implies g z \neq 0$
 $\bigwedge z. z \in S \implies f z = g z * (\prod_{k < n. (z - \alpha k)}$
 $\alpha \cdot \{.. < n\} \subseteq K$
 $\langle \text{proof} \rangle$

3.3 Schwarz theorem in complex analysis

lemma *Schwarz_Lemma1*:

fixes $f :: \text{complex} \Rightarrow \text{complex}$
and $\xi :: \text{complex}$
assumes f *holomorphic_on* *ball* $0 1$
and $f 0 = 0$
and $\bigwedge z. \|z\| < 1 \implies \|f z\| \leq 1$
and $\|\xi\| < 1$
shows $\|f \xi\| \leq \|\xi\|$
 $\langle \text{proof} \rangle$

theorem *Schwarz_Lemma2*:

fixes $f :: \text{complex} \Rightarrow \text{complex}$
and $\xi :: \text{complex}$
assumes *hol*: f *holomorphic_on* *ball* $0 R$
and *hR*: $0 < R$ **and** *nz*: $f 0 = 0$
and *bn*: $\bigwedge z. \|z\| < R \implies \|f z\| \leq 1$
and *ξR*: $\|\xi\| < R$
shows $\|f \xi\| \leq \|\xi\| / R$
 $\langle \text{proof} \rangle$

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 $hf: \bigwedge z. \|z\| < R \implies \operatorname{Re} (f \ z) \leq A$
and $holf: f \ \text{holomorphic_on} \ (\text{ball } 0 \ R)$
and $zr: \|z\| \leq r$
shows $\|f \ z\| \leq 2*r/(R-r) * A$
 $\langle \text{proof} \rangle$

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

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

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 $hf: f \ \text{holomorphic_on} \ \text{ball } 0 \ r$
and $ne: \bigwedge z. z \in \text{ball } 0 \ r \implies f \ z \neq 0$
and $bn: \bigwedge z. z \in \text{ball } 0 \ r \implies \|f \ z / f \ 0\| \leq \exp M$
shows $\|\logderiv \ f \ 0\| \leq 4 * M / r$
and $\forall s \in \text{cball } 0 \ (r / 4). \|\logderiv \ f \ s\| \leq 8 * M / r$
 $\langle \text{proof} \rangle$

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

lemma *lemma_3_9_beta2*:
fixes $f \ M \ r$
assumes $zl: 0 < r \ 0 \leq M$
and $af: f \ \text{analytic_on} \ \text{cball } 0 \ r$
and $f0: f \ 0 \neq 0$
and $rz: \bigwedge z. z \in \text{cball } 0 \ r \implies \operatorname{Re} z > 0 \implies f \ z \neq 0$

and bn : $\bigwedge z. z \in \text{cball } 0 \ r \implies \|f z / f 0\| \leq \text{exp } M$
and hg : $\Gamma \subseteq \{z \in \text{cball } 0 \ (r / 2). f z = 0 \wedge \text{Re } z \leq 0\}$
shows $- \text{Re } (\text{logderiv } f 0) \leq 8 * M / r + \text{Re } (\sum_{z \in \Gamma}. 1 / z)$
 $\langle \text{proof} \rangle$

theorem *lemma_3_9_beta3*:

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

unbundle *no_pnt_notation*

end

theory *Zeta_Zerofree*

imports

PNT_Complex_Analysis_Lemmas

begin

unbundle *pnt_notation*

4 Zero-free region of zeta function

lemma *cos_inequality_1*:

fixes $x :: \text{real}$
shows $3 + 4 * \cos x + \cos (2 * x) \geq 0$
 $\langle \text{proof} \rangle$

lemma *multiplicative_fds_zeta*:

completely_multiplicative_function ($\text{fds_nth } \text{fds_zeta_complex}$)
 $\langle \text{proof} \rangle$

lemma *fds_mangoldt_eq*:

$\text{fds_mangoldt_complex} = -(\text{fds_deriv } \text{fds_zeta} / \text{fds_zeta})$
 $\langle \text{proof} \rangle$

lemma *abs_conv_abscissa_log_deriv*:

$\text{abs_conv_abscissa } (\text{fds_deriv } \text{fds_zeta_complex} / \text{fds_zeta}) \leq 1$
 $\langle \text{proof} \rangle$

lemma *abs_conv_abscissa_mangoldt*:

$\text{abs_conv_abscissa } (\text{fds_mangoldt_complex}) \leq 1$
 $\langle \text{proof} \rangle$

lemma

assumes s : $\text{Re } s > 1$
shows eval_fds_mangoldt : $\text{eval_fds } (\text{fds_mangoldt}) \ s = - \text{deriv } \text{zeta } s / \text{zeta } s$
and abs_conv_mangoldt : $\text{fds_abs_converges } (\text{fds_mangoldt}) \ s$
 $\langle \text{proof} \rangle$

lemma *sums_mangoldt*:

fixes $s :: \text{complex}$

assumes $s: \text{Re } s > 1$
shows $((\lambda n. \text{mangoldt } n / n \text{ nat_powr } s) \text{ has_sum } - \text{deriv zeta } s / \text{zeta } s) \{1..\}$
 $\langle \text{proof} \rangle$

lemma *sums_Re_logderiv_zeta*:

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

lemma *logderiv_zeta_ineq*:

fixes $\sigma t :: \text{real}$
assumes $s: \sigma > 1$
shows $3 * \text{Re } (\text{logderiv zeta } (\text{Complex } \sigma 0)) + 4 * \text{Re } (\text{logderiv zeta } (\text{Complex } \sigma t)) + \text{Re } (\text{logderiv zeta } (\text{Complex } \sigma (2*t))) \leq 0$ (**is** $?x \leq 0$)
 $\langle \text{proof} \rangle$

lemma *sums_zeta_real*:

fixes $r :: \text{real}$
assumes $1 < r$
shows $(\sum n. (n_+) \text{ powr } -r) = \text{Re } (\text{zeta } r)$
 $\langle \text{proof} \rangle$

lemma *inverse_zeta_bound'*:

assumes $1 < \text{Re } s$
shows $\|\text{inverse } (\text{zeta } s)\| \leq \text{Re } (\text{zeta } (\text{Re } s))$
 $\langle \text{proof} \rangle$

lemma *zeta_bound'*:

assumes $1 < \text{Re } s$
shows $\|\text{zeta } s\| \leq \text{Re } (\text{zeta } (\text{Re } s))$
 $\langle \text{proof} \rangle$

lemma *zeta_bound_trivial'*:

assumes $1 / 2 \leq \text{Re } s \wedge \text{Re } s \leq 2$
and $|\text{Im } s| \geq 1 / 11$
shows $\|\text{zeta } s\| \leq 12 + 2 * |\text{Im } s|$
 $\langle \text{proof} \rangle$

lemma *zeta_bound_gt_1*:

assumes $1 < \text{Re } s$
shows $\|\text{zeta } s\| \leq \text{Re } s / (\text{Re } s - 1)$
 $\langle \text{proof} \rangle$

lemma *zeta_bound_trivial*:

assumes $1 / 2 \leq \text{Re } s$ **and** $|\text{Im } s| \geq 1 / 11$
shows $\|\text{zeta } s\| \leq 12 + 2 * |\text{Im } s|$
 $\langle \text{proof} \rangle$

lemma *zeta_nonzero_small_imag'*:

assumes $|\text{Im } s| \leq 13 / 22$ **and** $\text{Re } s \geq 1 / 2$ **and** $\text{Re } s < 1$
shows $\text{zeta } s \neq 0$
 $\langle \text{proof} \rangle$

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 $hB: \bigwedge w. \|s - w\| = r \implies \|pre_zeta\ 1\ w\| \leq B$
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 $\vartheta\ \varphi :: real \implies real$
assumes $zeta_bn'$: $\bigwedge z. 1 - \vartheta\ (Im\ z) \leq Re\ z \implies Im\ z \geq 1 / 11 \implies \|zeta\ z\| \leq exp\ (\varphi\ (Im\ z))$
and ϑ_pos : $\bigwedge t. 0 < \vartheta\ t \wedge \vartheta\ t \leq 1 / 2$
and φ_pos : $\bigwedge t. 1 \leq \varphi\ t$
and $inv_vartheta$: $\bigwedge t. \varphi\ t / \vartheta\ t \leq 1 / 960 * exp\ (\varphi\ t)$
and $mo\vartheta$: *antimono* ϑ **and** $mo\varphi$: *mono* φ

begin

definition *region* $\equiv \{z. 1 - \vartheta\ (Im\ z) \leq Re\ z \wedge Im\ z \geq 1 / 11\}$

lemma $zeta_bn$: $\bigwedge z. z \in region \implies \|zeta\ z\| \leq exp\ (\varphi\ (Im\ z))$

<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 $\sigma \delta :: \text{real}$

assumes $\sigma_cnd: \sigma \geq 1 + \exp(-\varphi(2 * \gamma + 1))$

and $\delta_cnd: \delta = \gamma \vee \delta = 2 * \gamma$

begin

definition s where $s \equiv \text{Complex } \sigma \delta$

end

context zeta_bound_param_2 begin

declare dist_complex_def [simp] $\text{norm_minus_commute}$ [simp]

declare $\text{legacy_Complex_simps}$ [simp]

lemma cball_lm :

assumes $z \in \text{cball } s \ r$

shows $r \leq 1 \ | \ \text{Re } z - \sigma| \leq r \ | \ \text{Im } z - \delta| \leq r$

$1 / 11 \leq \text{Im } z \ \text{Im } z \leq 2 * \gamma + r$

$\langle \text{proof} \rangle$

lemma cball_in_region :

shows $\text{cball } s \ r \subseteq \text{region}$

$\langle \text{proof} \rangle$

lemma Re_s_gt_1 :

shows $1 < \text{Re } s$

$\langle \text{proof} \rangle$

lemma $\text{zeta_analytic_on_region}$:

shows $\text{zeta analytic_on region}$

$\langle \text{proof} \rangle$

lemma zeta_div_bound :

assumes $z \in \text{cball } s \ r$

shows $\|\text{zeta } z / \text{zeta } s\| \leq \exp(3 * \varphi(2 * \gamma + 1))$

$\langle \text{proof} \rangle$

lemma $\text{logderiv_zeta_bound}$:

shows $\text{Re } (\text{logderiv } \text{zeta } s) \geq -24 * \varphi(2 * \gamma + 1) / r$

and $\bigwedge \beta. \sigma - r / 2 \leq \beta \implies \text{zeta } (\text{Complex } \beta \delta) = 0 \implies$

$\text{Re } (\text{logderiv } \text{zeta } s) \geq -24 * \varphi(2 * \gamma + 1) / r + 1 / (\sigma - \beta)$

$\langle \text{proof} \rangle$

end

context zeta_bound_param_1 begin

lemma $\text{zeta_nonzero_region}'$:

assumes $1 + 1 / 960 * (r / \varphi(2 * \gamma + 1)) - r / 2 \leq \beta$

and $\text{zeta } (\text{Complex } \beta \gamma) = 0$

shows $1 - \beta \geq 1 / 29760 * (r / \varphi(2 * \gamma + 1))$

$\langle \text{proof} \rangle$

lemma $\text{zeta_nonzero_region}$:

assumes $\text{zeta } (\text{Complex } \beta \gamma) = 0$

shows $1 - \beta \geq 1 / 29760 * (r / \varphi(2 * \gamma + 1))$

$\langle \text{proof} \rangle$

end

context *zeta_bound_param* **begin**

theorem *zeta_nonzero_region*:

assumes *zeta* (Complex $\beta \gamma$) = 0 **and** Complex $\beta \gamma \neq 1$

shows $1 - \beta \geq 1 / 29760 * (\vartheta (2 * |\gamma| + 1) / \varphi (2 * |\gamma| + 1))$

<proof>

end

lemma *zeta_bound_param_nonneg*:

fixes $\vartheta \varphi :: \text{real} \Rightarrow \text{real}$

assumes *zeta_bn'*: $\bigwedge z. 1 - \vartheta (\text{Im } z) \leq \text{Re } z \implies \text{Im } z \geq 1 / 11 \implies \|zeta\ z\| \leq \exp (\varphi (\text{Im } z))$

and *var_pos*: $\bigwedge t. 0 \leq t \implies 0 < \vartheta t \wedge \vartheta t \leq 1 / 2$

and *var_pos*: $\bigwedge t. 0 \leq t \implies 1 \leq \varphi t$

and *inv_var*: $\bigwedge t. 0 \leq t \implies \varphi t / \vartheta t \leq 1 / 960 * \exp (\varphi t)$

and *mod*: $\bigwedge x y. 0 \leq x \implies x \leq y \implies \vartheta y \leq \vartheta x$

and *mo*: $\bigwedge x y. 0 \leq x \implies x \leq y \implies \varphi x \leq \varphi y$

shows *zeta_bound_param* ($\lambda t. \vartheta (\max 0 t)$) ($\lambda t. \varphi (\max 0 t)$)

<proof>

interpretation *classical_zeta_bound*:

zeta_bound_param $\lambda t. 1 / 2$ $\lambda t. 4 * \ln (12 + 2 * \max 0 t)$

<proof>

theorem *zeta_nonzero_region*:

assumes *zeta* (Complex $\beta \gamma$) = 0 **and** Complex $\beta \gamma \neq 1$

shows $1 - \beta \geq C_1 / \ln (|\gamma| + 2)$

<proof>

unbundle *no_pnt_notation*

end

theory *PNT_Subsummable*

imports

PNT_Remainder_Library

begin

unbundle *pnt_notation*

definition *has_subsum* **where** *has_subsum* $f S x \equiv (\lambda n. \text{if } n \in S \text{ then } f n \text{ else } 0)$ *sums* x

definition *subsum* **where** *subsum* $f S \equiv \sum n. \text{if } n \in S \text{ then } f n \text{ else } 0$

definition *subsummable* (**infix** *subsummable* 50)

where *f subsummable* $S \equiv \text{summable } (\lambda n. \text{if } n \in S \text{ then } f n \text{ else } 0)$

syntax *_subsum* :: *pttrn* \Rightarrow *nat set* \Rightarrow 'a \Rightarrow 'a

(($2 \sum ' _ \in _ / _$) [0, 0, 10] 10)

translations

$\sum ' x \in S. t \Rightarrow \text{CONST } \text{subsum } (\lambda x. t) S$

syntax *_subsum_prop* :: *pttrn* \Rightarrow *bool* \Rightarrow 'a \Rightarrow 'a

(($2 \sum ' _ | _ / _$) [0, 0, 10] 10)

translations

$\sum ' x | P. t \Rightarrow \text{CONST } \text{subsum } (\lambda x. t) \{x. P\}$

syntax *_subsum_ge* :: *pttrn* \Rightarrow *nat* \Rightarrow 'a \Rightarrow 'a

(($2 \sum ' _ \geq _ / _$) [0, 0, 10] 10)

translations

$\sum 'x \geq n. t \Rightarrow \text{CONST subsum } (\lambda x. t) \{n..\}$

lemma *has_subsum_finite*:

finite F \Rightarrow *has_subsum f F (sum f F)*
<proof>

lemma *has_subsum_If_finite_set*:

assumes finite F
shows has_subsum $(\lambda n. \text{if } n \in F \text{ then } f \ n \text{ else } 0) \ A \ (\text{sum } f \ (F \cap \ A))$
<proof>

lemma *has_subsum_If_finite*:

assumes finite $\{n \in A. p \ n\}$
shows has_subsum $(\lambda n. \text{if } p \ n \text{ then } f \ n \text{ else } 0) \ A \ (\text{sum } f \ \{n \in A. p \ n\})$
<proof>

lemma *has_subsum_univ*:

f sums v \Rightarrow *has_subsum f UNIV v*
<proof>

lemma *subsumI*:

fixes f :: nat \Rightarrow *'a ::* $\{t2_space, comm_monoid_add\}$
shows has_subsum f A x \Rightarrow $x = \text{subsum } f \ A$
<proof>

lemma *has_subsum_summable*:

has_subsum f A x \Rightarrow *f summable A*
<proof>

lemma *summable_sums*:

fixes f :: nat \Rightarrow *'a ::* $\{comm_monoid_add, t2_space\}$
shows f summable S \Rightarrow *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 summable 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_summable [simp]*: $(\lambda n. 0)$ *summable 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 $\text{subsum } f A - \text{subsum } g A = (\sum 'n \in A. f n - g n :: 'a :: \text{real_normed_vector})$

$\langle \text{proof} \rangle$

lemma *subsummable_minus*:

assumes f *subsummable* A g *subsummable* A

shows $(\lambda n. f n - g n :: 'a :: \text{real_normed_vector})$ *subsummable* A

$\langle \text{proof} \rangle$

lemma *has_subsum_uminus*:

assumes *has_subsum* $f A a$

shows *has_subsum* $(\lambda n. - f n :: 'a :: \text{real_normed_vector}) A (- a)$

$\langle \text{proof} \rangle$

lemma *subsum_uminus*:

f *subsummable* $A \implies - \text{subsum } f A = (\sum 'n \in A. - f n :: 'a :: \text{real_normed_vector})$

$\langle \text{proof} \rangle$

lemma *subsummable_uminus*:

f *subsummable* $A \implies (\lambda n. - f n :: 'a :: \text{real_normed_vector})$ *subsummable* A

$\langle \text{proof} \rangle$

lemma *has_subsum_add*:

fixes $f :: \text{nat} \Rightarrow 'a :: \text{real_normed_vector}$

assumes *has_subsum* $f A a$ *has_subsum* $g A b$

shows *has_subsum* $(\lambda n. f n + g n) A (a + b)$

$\langle \text{proof} \rangle$

lemma *subsum_add*:

assumes f *subsummable* A g *subsummable* A

shows $\text{subsum } f A + \text{subsum } g A = (\sum 'n \in A. f n + g n :: 'a :: \text{real_normed_vector})$

$\langle \text{proof} \rangle$

lemma *subsummable_add*:

assumes f *subsummable* A g *subsummable* A

shows $(\lambda n. f n + g n :: 'a :: \text{real_normed_vector})$ *subsummable* A

$\langle \text{proof} \rangle$

lemma *subsum_cong*:

$(\bigwedge x. x \in A \implies f x = g x) \implies \text{subsum } f A = \text{subsum } g A$

$\langle \text{proof} \rangle$

lemma *subsummable_cong*:

fixes $f :: \text{nat} \Rightarrow 'a :: \text{real_normed_vector}$

shows $(\bigwedge x. x \in A \implies f x = g x) \implies (f \text{ subsummable } A) = (g \text{ subsummable } A)$

$\langle \text{proof} \rangle$

lemma *subsum_norm_bound*:

fixes $f :: \text{nat} \Rightarrow 'a :: \text{banach}$

assumes g *subsummable* A $\bigwedge n. n \in A \implies \|f n\| \leq g n$

shows $\|\text{subsum } f A\| \leq \text{subsum } g A$

$\langle \text{proof} \rangle$

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

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

lemma *subsum_mult2*:
fixes $f :: \text{nat} \Rightarrow 'a :: \text{real_normed_algebra}$
shows $f\ subsummable\ A \implies (\sum 'x \in A. f\ x * c) = subsum\ f\ A * c$
 $\langle proof \rangle$

lemma *subsummable_mult2*:
fixes $f :: \text{nat} \Rightarrow 'a :: \text{real_normed_algebra}$
assumes $f\ subsummable\ A$
shows $(\lambda x. f\ x * c)\ subsummable\ A$
 $\langle proof \rangle$

lemma *subsum_ge_limit*:
 $\lim (\lambda N. \sum n = m..N. f\ n) = (\sum 'n \geq m. f\ n)$
 $\langle proof \rangle$

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

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

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

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

unbundle *no_pnt_notation*
end
theory *Perron_Formula*

```

imports
  PNT_Remainder_Library
  PNT_Subsummable
begin
unbundle pnt_notation

```

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:  $\bigwedge t. t \in \{-T..T\} \implies \|f (\text{Complex } b \ t)\| \leq B$ 
and Hf':  $(\lambda s. f \ s * a \ \text{powr } s / s) \text{ contour\_integrable\_on } (\text{linepath } (\text{Complex } b \ (-T)) (\text{Complex } b \ T))$ 
shows  $\|1 / (2 * \pi * i) * \text{contour\_integral } (\text{linepath } (\text{Complex } b \ (-T)) (\text{Complex } b \ T)) (\lambda s. f \ s * a \ \text{powr } s / s)\|$ 
   $\leq B * a \ \text{powr } b * \ln (1 + T / b)$ 
<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:  $2 \leq H$  and hH':  $b + 1 \leq H$  and Hx:  $0 < x$ 
and hB:  $(\sum 'n \geq 1. \|fds\_nth \ f \ n\| / n \ \text{nat\_powr } b) \leq B$ 

```

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** $path \equiv \text{linepath } (\text{Complex } b \ (-T)) (\text{Complex } b \ T)$

definition *img_path* **where** $\text{img_path} \equiv \text{path_image } path$

definition σ_a **where** $\sigma_a \equiv \text{abs_conv_abscissa } f$

definition *region* **where** $region = \{n :: \text{nat}. x - x / H \leq n \wedge n \leq x + x / H\}$

definition *F* **where** $F (a :: \text{real}) \equiv$

```

   $1 / (2 * \pi * i) * \text{contour\_integral } path (\lambda s. a \ \text{powr } s / s) - (\text{if } 1 \leq a \text{ then } 1 \text{ else } 0)$ 

```

definition *F'* **where** $F' (n :: \text{nat}) \equiv F (x / n)$

lemma hT' : $0 < T$ <proof>

lemma *cond*: $0 < b \ b \leq T \ 0 < T$ <proof>

lemma *perron_integrable*:

```

assumes  $(0 :: \text{real}) < a$ 
shows  $(\lambda s. a \ \text{powr } s / s) \text{ contour\_integrable\_on } (\text{linepath } (\text{Complex } b \ (-T)) (\text{Complex } b \ T))$ 
<proof>

```

lemma *perron_aux_1'*:

```

fixes U :: real
assumes hU:  $0 < U$  and Ha:  $1 < a$ 
shows  $\|F' \ a\| \leq 1 / \pi * a \ \text{powr } b / (T * |\ln a|) + a \ \text{powr } -U * T / (\pi * U)$ 
<proof>

```

lemma *perron_aux_1*:

assumes *Ha*: $1 < a$

shows $\|F a\| \leq 1 / \pi * a^{\text{powr } b} / (T * |\ln a|)$ (**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 $\|F a\| \leq 1 / \pi * a^{\text{powr } b} / (T * |\ln a|) + a^{\text{powr } U} * T / (\pi * U)$

<proof>

lemma *perron_aux_2*:

assumes *Ha*: $0 < a \wedge a < 1$

shows $\|F a\| \leq 1 / \pi * a^{\text{powr } b} / (T * |\ln a|)$ (**is** $_ \leq ?x$)

<proof>

lemma *perron_aux_3*:

assumes *Ha*: $0 < a$

shows $\|1 / (2 * \pi * i) * \text{contour_integral path } (\lambda s. a^{\text{powr } s} / s)\| \leq a^{\text{powr } b} * \ln (1 + T / b)$

<proof>

lemma *perron_aux'*:

assumes *Ha*: $0 < a$

shows $\|F a\| \leq a^{\text{powr } b} * r a$

<proof>

lemma *r_bound*:

assumes *Hn*: $1 \leq n$

shows $r (x / n) \leq H / T + (\text{if } n \in \text{region then } 2 + \ln (T / b) \text{ else } 0)$

<proof>

lemma *perron_aux*:

assumes *Hn*: $0 < n$

shows $\|F' n\| \leq 1 / n \text{ nat_powr } b * (x^{\text{powr } b} * H / T)$

+ (*if* $n \in \text{region then } 3 * (2 + \ln (T / b)) \text{ else } 0)$ (**is** $?P \leq ?Q$)

<proof>

definition *a where* $a n \equiv \text{fds_nth } f n$

lemma *finite_region*: *finite region*

<proof>

lemma *zero_notin_region*: $0 \notin \text{region}$

<proof>

lemma *path_image_conv*:

assumes *s* $\in \text{img_path}$

shows $\text{conv_abscissa } f < s * 1$

<proof>

lemma *converge_on_path*:

assumes *s* $\in \text{img_path}$

shows $\text{fds_converges } f s$

<proof>

lemma *summable_on_path*:

assumes $s \in \text{img_path}$

shows $(\lambda n. a\ n / n\ \text{nat_powr}\ s)$ *subsummable* $\{1..\}$

$\langle \text{proof} \rangle$

lemma *zero_notin_path*:

shows $0 \notin \text{closed_segment}\ (\text{Complex}\ b\ (-\ T))\ (\text{Complex}\ b\ T)$

$\langle \text{proof} \rangle$

lemma *perron_bound*:

$\|\sum 'n \geq 1. a\ n * F'\ n\| \leq x\ \text{powr}\ b * H * B / T$
 $+ 3 * (2 + \ln\ (T / b)) * (\sum_{n \in \text{region.}} \|a\ n\|)$

$\langle \text{proof} \rangle$

lemma *perron*:

$(\lambda s. \text{eval_fds}\ f\ s * x\ \text{powr}\ s / s)$ *contour_integrable_on path*

$\|\text{sum_upto}\ a\ x - 1 / (2 * \text{pi} * i) * \text{contour_integral}\ \text{path}\ (\lambda s. \text{eval_fds}\ f\ s * x\ \text{powr}\ s / s)\|$
 $\leq x\ \text{powr}\ b * H * B / T + 3 * (2 + \ln\ (T / b)) * (\sum_{n \in \text{region.}} \|a\ n\|)$

$\langle \text{proof} \rangle$

end

theorem *perron_formula*:

fixes $b\ B\ H\ T\ x :: \text{real}$ **and** $f :: \text{complex}\ \text{fds}$

assumes $Hb: 0 < b$ **and** $hT: b \leq T$

and $Hb': \text{abs_conv_abscissa}\ f < b$

and $hH: 2 \leq H$ **and** $hH': b + 1 \leq H$ **and** $Hx: 2 \leq x$

and $hB: (\sum 'n \geq 1. \| \text{fds_nth}\ f\ n \| / n\ \text{nat_powr}\ b) \leq B$

shows $(\lambda s. \text{eval_fds}\ f\ s * x\ \text{powr}\ s / s)$ *contour_integrable_on* $(\text{linepath}\ (\text{Complex}\ b\ (-T))\ (\text{Complex}\ b\ T))$

$\|\text{sum_upto}\ (\text{fds_nth}\ f)\ x - 1 / (2 * \text{pi} * i) * \text{contour_integral}\ (\text{linepath}\ (\text{Complex}\ b\ (-T))\ (\text{Complex}\ b\ T))\ (\lambda s. \text{eval_fds}\ f\ s * x\ \text{powr}\ s / s)\|$
 $\leq x\ \text{powr}\ b * H * B / T + 3 * (2 + \ln\ (T / b)) * (\sum n \mid x - x / H \leq n \wedge n \leq x + x / H.$

$\|\text{fds_nth}\ f\ n\|)$

$\langle \text{proof} \rangle$

theorem *perron_asymp*:

fixes $b\ x :: \text{real}$

assumes $b: b > 0$ *ereal* $b > \text{abs_conv_abscissa}\ f$

assumes $x: x \geq 2$ $x \notin \mathbb{N}$

defines $L \equiv (\lambda T. \text{linepath}\ (\text{Complex}\ b\ (-T))\ (\text{Complex}\ b\ T))$

shows $((\lambda T. \text{contour_integral}\ (L\ T)\ (\lambda s. \text{eval_fds}\ f\ s * \text{of_real}\ x\ \text{powr}\ s / s))$
 $\longrightarrow 2 * \text{pi} * i * \text{sum_upto}\ (\lambda n. \text{fds_nth}\ f\ n)\ x)$ *at_top*

$\langle \text{proof} \rangle$

unbundle *no_pnt_notation*

end

theory *PNT_with_Remainder*

imports

Relation_of_PNTs

Zeta_Zerofree

Perron_Formula

begin

unbundle *pnt_notation*

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

notation *primes_psi* (ψ)

lemma *zeta_div_bound'*:

assumes $1 + \exp(-4 * \ln(14 + 4 * t)) \leq \sigma$

and $13 / 22 \leq t$

and $z \in \text{cball}(\text{Complex } \sigma t) (1 / 2)$

shows $\|\text{zeta } z / \text{zeta}(\text{Complex } \sigma t)\| \leq \exp(12 * \ln(14 + 4 * t))$

<proof>

lemma *zeta_div_bound*:

assumes $1 + \exp(-4 * \ln(14 + 4 * |t|)) \leq \sigma$

and $13 / 22 \leq |t|$

and $z \in \text{cball}(\text{Complex } \sigma t) (1 / 2)$

shows $\|\text{zeta } z / \text{zeta}(\text{Complex } \sigma t)\| \leq \exp(12 * \ln(14 + 4 * |t|))$

<proof>

definition C_2 **where** $C_2 \equiv 319979520 :: \text{real}$

lemma *C2_gt_zero*: $0 < C_2$ *<proof>*

lemma *logderiv_zeta_order_estimate'*:

$\forall_F t$ *in* (*abs going to at_top*).

$\forall \sigma. 1 - 1 / 7 * C_1 / \ln(|t| + 3) \leq \sigma$

$\longrightarrow \|\logderiv \text{zeta}(\text{Complex } \sigma t)\| \leq C_2 * (\ln(|t| + 3))^2$

<proof>

definition C_3 **where**

$C_3 \equiv \text{SOME } T. 0 < T \wedge$

$(\forall t. T \leq |t| \longrightarrow$

$(\forall \sigma. 1 - 1 / 7 * C_1 / \ln(|t| + 3) \leq \sigma$

$\longrightarrow \|\logderiv \text{zeta}(\text{Complex } \sigma t)\| \leq C_2 * (\ln(|t| + 3))^2)$)

lemma *C3_prop*:

$0 < C_3 \wedge$

$(\forall t. C_3 \leq |t| \longrightarrow$

$(\forall \sigma. 1 - 1 / 7 * C_1 / \ln(|t| + 3) \leq \sigma$

$\longrightarrow \|\logderiv \text{zeta}(\text{Complex } \sigma t)\| \leq C_2 * (\ln(|t| + 3))^2)$)

<proof>

lemma *C3_gt_zero*: $0 < C_3$ *<proof>*

lemma *logderiv_zeta_order_estimate*:

assumes $1 - 1 / 7 * C_1 / \ln(|t| + 3) \leq \sigma$ $C_3 \leq |t|$

shows $\|\logderiv \text{zeta}(\text{Complex } \sigma t)\| \leq C_2 * (\ln(|t| + 3))^2$

<proof>

definition *zeta_zerofree_region*

where $\text{zeta_zerofree_region} \equiv \{s. s \neq 1 \wedge 1 - C_1 / \ln(|\text{Im } s| + 2) < \text{Re } s\}$

definition *logderiv_zeta_region*

where $\text{logderiv_zeta_region} \equiv \{s. C_3 \leq |\text{Im } s| \wedge 1 - 1 / 7 * C_1 / \ln(|\text{Im } s| + 3) \leq \text{Re } s\}$

definition *zeta_strip_region*

where $\text{zeta_strip_region } \sigma T \equiv \{s. s \neq 1 \wedge \sigma \leq \text{Re } s \wedge |\text{Im } s| \leq T\}$

definition *zeta_strip_region'*

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

lemma *strip_in_zerofree_region*:

assumes $1 - C_1 / \ln (T + 2) < \sigma$

shows $\text{zeta_strip_region}' \sigma T \subseteq \text{zeta_zerofree_region}$

<proof>

lemma *strip_in_logderiv_zeta_region*:

assumes $1 - 1 / 7 * C_1 / \ln (T + 3) \leq \sigma$

shows $\text{zeta_strip_region}' \sigma T \subseteq \text{logderiv_zeta_region}$

<proof>

lemma *strip_condition_imp*:

assumes $0 \leq T \wedge 1 - 1 / 7 * C_1 / \ln (T + 3) \leq \sigma$

shows $1 - C_1 / \ln (T + 2) < \sigma$

<proof>

lemma *zeta_zerofree_region*:

assumes $s \in \text{zeta_zerofree_region}$

shows $\text{zeta } s \neq 0$

<proof>

lemma *logderiv_zeta_region_estimate*:

assumes $s \in \text{logderiv_zeta_region}$

shows $\|\text{logderiv } \text{zeta } s\| \leq C_2 * (\ln (|\text{Im } s| + 3))^2$

<proof>

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

lemma *C4_prop*:

$\forall_F x \text{ in } \text{at_top}. C_4 / \ln x \leq C_1 / (7 * \ln (x + 3))$

<proof>

lemma *C4_gt_zero*: $0 < C_4$ *<proof>*

definition *C5_prop* **where**

$C_{5_prop} C_5 \equiv$

$0 < C_5 \wedge (\forall_F x \text{ in } \text{at_top}. (\forall t. |t| \leq x$

$\longrightarrow \|\text{logderiv } \text{zeta } (\text{Complex } (1 - C_4 / \ln x) t)\| \leq C_5 * (\ln x)^2)$)

lemma *logderiv_zeta_bound_vertical'*:

$\exists C_5. C_{5_prop} C_5$

<proof>

definition C_5 **where** $C_5 \equiv \text{SOME } C_5. C_{5_prop} C_5$

lemma

C5_gt_zero: $0 < C_5$ (**is** *?prop_1*) **and**

logderiv_zeta_bound_vertical:

$\forall_F x \text{ in } \text{at_top}. \forall t. |t| \leq x$

$\longrightarrow \|\text{logderiv } \text{zeta } (\text{Complex } (1 - C_4 / \ln x) t)\| \leq C_5 * (\ln x)^2$ (**is** *?prop_2*)

<proof>

7 Deducing prime number theorem using Perron's formula

locale *prime_number_theorem* =

fixes $c \ \varepsilon :: \text{real}$

assumes $Hc: 0 < c$ and $Hc': c * c < 2 * C_4$ and $H\varepsilon: 0 < \varepsilon < 2 * \varepsilon < c$

begin

notation *primes_psi* (ψ)

definition *H* where $H \ x \equiv \exp (c / 2 * (\ln x) \text{ powr } (1 / 2))$ for $x :: \text{real}$

definition *T* where $T \ x \equiv \exp (c * (\ln x) \text{ powr } (1 / 2))$ for $x :: \text{real}$

definition *a* where $a \ x \equiv 1 - C_4 / (c * (\ln x) \text{ powr } (1 / 2))$ for $x :: \text{real}$

definition *b* where $b \ x \equiv 1 + 1 / (\ln x)$ for $x :: \text{real}$

definition *B* where $B \ x \equiv 5 / 4 * \ln x$ for $x :: \text{real}$

definition *f* where $f \ x \ s \equiv x \text{ powr } s / s * \text{logderiv zeta } s$ for $x :: \text{real}$ and $s :: \text{complex}$

definition *R* where $R \ x \equiv$

$x \text{ powr } (b \ x) * H \ x * B \ x / T \ x + 3 * (2 + \ln (T \ x / b \ x))$

$* (\sum n \mid x - x / H \ x \leq n \wedge n \leq x + x / H \ x. \|\text{fds_nth } (\text{fds mangoldt_complex}) \ n\|)$ for $x :: \text{real}$

definition *Rc'* where $Rc' \equiv O(\lambda x. x * \exp (- (c / 2 - \varepsilon) * \ln x \text{ powr } (1 / 2)))$

definition *Rc* where $Rc \equiv O(\lambda x. x * \exp (- (c / 2 - 2 * \varepsilon) * \ln x \text{ powr } (1 / 2)))$

definition *z₁* where $z_1 \ x \equiv \text{Complex } (a \ x) (- T \ x)$ for x

definition *z₂* where $z_2 \ x \equiv \text{Complex } (b \ x) (- T \ x)$ for x

definition *z₃* where $z_3 \ x \equiv \text{Complex } (b \ x) (T \ x)$ for x

definition *z₄* where $z_4 \ x \equiv \text{Complex } (a \ x) (T \ x)$ for x

definition *rect* where $\text{rect } x \equiv \text{cbox } (z_1 \ x) (z_3 \ x)$ for x

definition *rect'* where $\text{rect}' \ x \equiv \text{rect } x - \{1\}$ for x

definition *P_t* where $P_t \ x \ t \equiv \text{linepath } (\text{Complex } (a \ x) \ t) (\text{Complex } (b \ x) \ t)$ for $x \ t$

definition *P₁* where $P_1 \ x \equiv \text{linepath } (z_1 \ x) (z_4 \ x)$ for x

definition *P₂* where $P_2 \ x \equiv \text{linepath } (z_2 \ x) (z_3 \ x)$ for x

definition *P₃* where $P_3 \ x \equiv P_t \ x (- T \ x)$ for x

definition *P₄* where $P_4 \ x \equiv P_t \ x (T \ x)$ for x

definition *P_r* where $P_r \ x \equiv \text{rectpath } (z_1 \ x) (z_3 \ x)$ for x

lemma *Rc_eq_rem_est*:

$Rc = \text{rem_est } (c / 2 - 2 * \varepsilon) (1 / 2) 0$

$\langle \text{proof} \rangle$

lemma *residue_f*:

$\text{residue } (f \ x) \ 1 = - \ x$

$\langle \text{proof} \rangle$

lemma *rect_in_strip*:

$\text{rect } x - \{1\} \subseteq \text{zeta_strip_region } (a \ x) (T \ x)$

$\langle \text{proof} \rangle$

lemma *rect_in_strip'*:

$\{s \in \text{rect } x. C_3 \leq |\text{Im } s|\} \subseteq \text{zeta_strip_region}' (a \ x) (T \ x)$

$\langle \text{proof} \rangle$

lemma

$\text{rect}'_in_zerofree: \forall_F \ x \ \text{in } \text{at_top}. \text{rect}' \ x \subseteq \text{zeta_zerofree_region}$ and

$\text{rect_in_logderiv_zeta: } \forall_F \ x \ \text{in } \text{at_top}. \{s \in \text{rect } x. C_3 \leq |\text{Im } s|\} \subseteq \text{logderiv_zeta_region}$

$\langle \text{proof} \rangle$

lemma *zeta_nonzero_in_rect*:

$\forall_F \ x \ \text{in } \text{at_top}. \forall s. s \in \text{rect}' \ x \longrightarrow \text{zeta } s \neq 0$

$\langle \text{proof} \rangle$

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

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

lemma path_image_in_rect_1:
assumes $0 \leq T x \wedge a x \leq b x$
shows $\text{path_image } (P_1 x) \subseteq \text{rect } x \wedge \text{path_image } (P_2 x) \subseteq \text{rect } x$
 ⟨proof⟩

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

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

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

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

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

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

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

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

lemma valid_paths:
 $\text{valid_path } (P_1 x) \text{ valid_path } (P_2 x) \text{ valid_path } (P_3 x) \text{ valid_path } (P_4 x)$
 ⟨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 $\text{contour_integral } (P_3 x) (f x) + \text{contour_integral } (P_2 x) (f x)$
 $- \text{contour_integral } (P_4 x) (f x) - \text{contour_integral } (P_1 x) (f x) = \text{contour_integral } (P_r x) (f x)$
<proof>

lemma P_2_eq :

$\forall_F x$ *in at_top*. $\text{contour_integral } (P_2 x) (f x) + 2 * \pi * i * x$
 $= \text{contour_integral } (P_1 x) (f x) - \text{contour_integral } (P_3 x) (f x) + \text{contour_integral } (P_4 x) (f x)$
<proof>

lemma *estimation_P1*:

$(\lambda x. \|\text{contour_integral } (P_1 x) (f x)\|) \in Rc$
<proof>

lemma *estimation_Pt'*:

assumes h :
 $1 < x \wedge \max 1 C_3 \leq T x a x < 1 \wedge 1 < b x$
 $\{s \in \text{rect } x. C_3 \leq |\text{Im } s|\} \subseteq \text{logderiv_zeta_region}$
 $f x$ *contour_integrable_on* $P_3 x \wedge f x$ *contour_integrable_on* $P_4 x$
and Ht : $|t| = T x$
shows $\|\text{contour_integral } (P_t x t) (f x)\| \leq C_2 * \exp 1 * x / T x * (\ln (T x + 3))^2 * (b x - a x)$
<proof>

lemma *estimation_Pt*:

$(\lambda x. \|\text{contour_integral } (P_3 x) (f x)\|) \in Rc \wedge$
 $(\lambda x. \|\text{contour_integral } (P_4 x) (f x)\|) \in Rc$
<proof>

lemma *Re_path_P2*:

$\bigwedge z. z \in \text{path_image } (P_2 x) \implies \text{Re } z = b x$
<proof>

lemma *estimation_P2*:

$(\lambda x. \|1 / (2 * \pi * i) * \text{contour_integral } (P_2 x) (f x) + x\|) \in Rc$
<proof>

lemma *estimation_R*:

$R \in Rc$
<proof>

lemma *perron_psi*:

$\forall_F x$ *in at_top*. $\|\psi x + 1 / (2 * \pi * i) * \text{contour_integral } (P_2 x) (f x)\| \leq R x$
<proof>

lemma *estimation_perron_psi*:

$(\lambda x. \|\psi x + 1 / (2 * \pi * i) * \text{contour_integral } (P_2 x) (f x)\|) \in Rc$
<proof>

theorem *prime_number_theorem*:

$PNT_3 (c / 2 - 2 * \varepsilon) (1 / 2) 0$
<proof>

no_notation *primes_psi* (ψ)

end

unbundle *prime_counting_notation*

theorem *prime_number_theorem*:

shows $(\lambda x. \pi x - Li x) \in O(\lambda x. x * \exp(-1 / 3653 * (\ln x) \text{ powr } (1 / 2)))$
<proof>

hide_const (**open**) $C_3 C_4 C_5$

unbundle *no_prime_counting_notation*

unbundle *no_pnt_notation*

end