The Prime Number Theorem

Manuel Eberl and Larry Paulson

March 17, 2025

Abstract

This article provides a short proof of the Prime Number Theorem in several equivalent forms, most notably $\pi(x) \sim x/\ln x$ where $\pi(x)$ is the number of primes no larger than x. It also defines other basic number-theoretic functions related to primes like Chebyshev's ϑ and ψ and the "n-th prime number" function p_n. We also show various bounds and relationship between these functions are shown. Lastly, we derive Mertens' First and Second Theorem, i. e. $\sum_{p\leq x} \frac{\ln p}{p} = \ln x + O(1)$ and $\sum_{p\leq x} \frac{1}{p} = \ln\ln x + M + O(1/\ln x)$. We also give explicit bounds for the remainder terms.

The proof of the Prime Number Theorem builds on a library of Dirichlet series and analytic combinatorics. We essentially follow the presentation by Newman [6]. The core part of the proof is a Tauberian theorem for Dirichlet series, which is proven using complex analysis and then used to strengthen Mertens' First Theorem to $\sum_{p\leq x} \frac{\ln p}{p} = \ln x + c + o(1)$.

A variant of this proof has been formalised before by Harrison in HOL Light [5], and formalisations of Selberg's elementary proof exist both by Avigad *et al.* [2] in Isabelle and by Carneiro [3] in Metamath. The advantage of the analytic proof is that, while it requires more powerful mathematical tools, it is considerably shorter and clearer. This article attempts to provide a short and clear formalisation of all components of that proof using the full range of mathematical machinery available in Isabelle, staying as close as possible to Newman's simple paper proof.

Contents

1 Auxiliary material

theory *Prime-Number-Theorem-Library*
imports
Zeta-Function.Zeta-Function
HOL−Real-Asymp.Real-Asymp
begin

Conflicting notation from *HOL−Analysis.Infinite-Sum*

no-notation *Infinite-Sum.abs-summable-on* (**infixr** ‹*abs′-summable′-on*› *46*)

lemma *homotopic-loopsI*:
fixes $h :: real \times real \Rightarrow -$
assumes *continuous-on* $(\{0..1\} \times \{0..1\})$ h
h ‘ $(\{0..1\} \times \{0..1\}) \subseteq s$
$\bigwedge x.\ x \in \{0..1\} \Longrightarrow h\ (0,\ x) = p\ x$
$\bigwedge x.\ x \in \{0..1\} \Longrightarrow h\ (1,\ x) = q\ x$
$\bigwedge x.\ x \in \{0..1\} \Longrightarrow$ *pathfinish* $(h \circ Pair\ x) =$ *pathstart* $(h \circ Pair\ x)$
shows *homotopic-loops s p q*
⟨*proof*⟩

lemma *homotopic-pathsI*:
fixes $h :: real \times real \Rightarrow -$
assumes *continuous-on* $(\{0..1\} \times \{0..1\})$ h
assumes h ‘ $(\{0..1\} \times \{0..1\}) \subseteq s$
assumes $\bigwedge x.\ x \in \{0..1\} \Longrightarrow h\ (0,\ x) = p\ x$
assumes $\bigwedge x.\ x \in \{0..1\} \Longrightarrow h\ (1,\ x) = q\ x$
assumes $\bigwedge x.\ x \in \{0..1\} \Longrightarrow$ *pathstart* $(h \circ Pair\ x) =$ *pathstart p*
assumes $\bigwedge x.\ x \in \{0..1\} \Longrightarrow$ *pathfinish* $(h \circ Pair\ x) =$ *pathfinish p*
shows *homotopic-paths s p q*
⟨*proof*⟩

lemma *sum-upto-ln-conv-sum-upto-mangoldt*:
sum-upto $(\lambda n.\ ln\ (real\ n))\ x =$ *sum-upto* $(\lambda n.\ mangoldt\ n * nat\ \lfloor x\ /\ real\ n \rfloor)\ x$
⟨*proof*⟩

lemma *ln-fact-conv-sum-upto-mangoldt*:
$ln\ (fact\ n) =$ *sum-upto* $(\lambda k.\ mangoldt\ k * (n\ div\ k))\ n$
⟨*proof*⟩

lemma *fds-abs-converges-comparison-test*:
fixes $s :: 'a ::$ *dirichlet-series*
assumes *eventually* $(\lambda n.\ norm\ (fds\text{-}nth\ f\ n) \leq fds\text{-}nth\ g\ n)$ *at-top* **and** *fds-converges* $g\ (s \cdot 1)$
shows *fds-abs-converges f s*
⟨*proof*⟩

lemma *fds-converges-scaleR* [*intro*]:
assumes *fds-converges f s*

shows *fds-converges* $(c *_R f)$ s
⟨*proof*⟩

lemma *fds-abs-converges-scaleR* [*intro*]:
assumes *fds-abs-converges* f s
shows *fds-abs-converges* $(c *_R f)$ s
⟨*proof*⟩

lemma *conv-abscissa-scaleR*: *conv-abscissa* (*scaleR* c f) ≤ *conv-abscissa* f
⟨*proof*⟩

lemma *abs-conv-abscissa-scaleR*: *abs-conv-abscissa* (*scaleR* c f) ≤ *abs-conv-abscissa* f
⟨*proof*⟩

lemma *fds-abs-converges-mult-const-left* [*intro*]:
fds-abs-converges f s ⟹ *fds-abs-converges* (*fds-const* c ∗ f) s
⟨*proof*⟩

lemma *conv-abscissa-mult-const-left*:
conv-abscissa (*fds-const* c ∗ f) ≤ *conv-abscissa* f
⟨*proof*⟩

lemma *abs-conv-abscissa-mult-const-left*:
abs-conv-abscissa (*fds-const* c ∗ f) ≤ *abs-conv-abscissa* f
⟨*proof*⟩

lemma *fds-abs-converges-mult-const-right* [*intro*]:
fds-abs-converges f s ⟹ *fds-abs-converges* (f ∗ *fds-const* c) s
⟨*proof*⟩

lemma *conv-abscissa-mult-const-right*:
conv-abscissa (f ∗ *fds-const* c) ≤ *conv-abscissa* f
⟨*proof*⟩

lemma *abs-conv-abscissa-mult-const-right*:
abs-conv-abscissa (f ∗ *fds-const* c) ≤ *abs-conv-abscissa* f
⟨*proof*⟩

lemma *bounded-coeffs-imp-fds-abs-converges*:
fixes s :: $'a$ :: *dirichlet-series* **and** f :: $'a$ *fds*
assumes *Bseq* (*fds-nth* f) s · 1 > 1
shows *fds-abs-converges* f s
⟨*proof*⟩

lemma *bounded-coeffs-imp-fds-abs-converges'*:
fixes s :: $'a$ :: *dirichlet-series* **and** f :: $'a$ *fds*
assumes *Bseq* (λn. *fds-nth* f n ∗ *nat-power* n *s0*) s · 1 > 1 − *s0* · 1

shows *fds-abs-converges f s*
⟨*proof*⟩

lemma *bounded-coeffs-imp-abs-conv-abscissa-le*:
fixes *s* :: *'a* :: *dirichlet-series* **and** *f* :: *'a fds* **and** *c* :: *ereal*
assumes *Bseq* (λ*n*. *fds-nth f n* ∗ *nat-power n s*) *1* − *s* · *1* ≤ *c*
shows *abs-conv-abscissa f* ≤ *c*
⟨*proof*⟩

lemma *bounded-coeffs-imp-abs-conv-abscissa-le-1*:
fixes *s* :: *'a* :: *dirichlet-series* **and** *f* :: *'a fds*
assumes *Bseq* (λ*n*. *fds-nth f n*)
shows *abs-conv-abscissa f* ≤ *1*
⟨*proof*⟩

lemma
fixes *a b c* :: *real*
assumes *ab*: *a* + *b* > *0* **and** *c*: *c* < −*1*
shows *set-integrable-powr-at-top*: (λ*x*. (*b* + *x*) *powr c*) *absolutely-integrable-on* {*a*<..}
and *set-lebesgue-integral-powr-at-top*:
(∫ *x*∈{*a*<..}. ((*b* + *x*) *powr c*) ∂*lborel*) = −((*b* + *a*) *powr* (*c* + *1*) / (*c* + *1*))
and *powr-has-integral-at-top*:
((λ*x*. (*b* + *x*) *powr c*) *has-integral* −((*b* + *a*) *powr* (*c* + *1*) / (*c* + *1*))) {*a*<..}
⟨*proof*⟩

lemma *fds-converges-altdef2*:
fds-converges f s ⟷ *convergent* (λ*N*. *eval-fds* (*fds-truncate N f*) *s*)
⟨*proof*⟩

lemma *tendsto-eval-fds-truncate*:
assumes *fds-converges f s*
shows (λ*N*. *eval-fds* (*fds-truncate N f*) *s*) ⟶ *eval-fds f s*
⟨*proof*⟩

lemma *linepath-translate-left*: *linepath* (*c* + *a*) (*c* + *a*) = (λ*x*. *c* + *a*) ∘ *linepath a b*
⟨*proof*⟩

lemma *linepath-translate-right*: *linepath* (*a* + *c*) (*b* + *c*) = (λ*x*. *x* + *c*) ∘ *linepath a b*
⟨*proof*⟩

lemma *has-contour-integral-linepath-same-Im-iff*:
fixes *a b* :: *complex* **and** *f* :: *complex* ⇒ *complex*
assumes *Im a* = *Im b Re a* < *Re b*

shows (*f has-contour-integral I*) (*linepath a b*) ⟷
((λ*x*. *f* (*of-real x* + *Im a* ∗ i)) *has-integral I*) {*Re a*..*Re b*}
⟨*proof*⟩

lemma *contour-integrable-linepath-same-Im-iff*:
fixes *a b* :: *complex* **and** *f* :: *complex* ⇒ *complex*
assumes *Im a* = *Im b Re a* < *Re b*
shows (*f contour-integrable-on linepath a b*) ⟷
(λ*x*. *f* (*of-real x* + *Im a* ∗ i)) *integrable-on* {*Re a*..*Re b*}
⟨*proof*⟩

lemma *contour-integral-linepath-same-Im*:
fixes *a b* :: *complex* **and** *f* :: *complex* ⇒ *complex*
assumes *Im a* = *Im b Re a* < *Re b*
shows *contour-integral* (*linepath a b*) *f* = *integral* {*Re a*..*Re b*} (λ*x*. *f* (*x* + *Im a* ∗ i))
⟨*proof*⟩

lemmas [*simp del*] = *div-mult-self3 div-mult-self4 div-mult-self2 div-mult-self1*

interpretation *cis*: *periodic-fun-simple cis 2* ∗ *pi*
⟨*proof*⟩

lemma *analytic-onE-box*:
assumes *f analytic-on A s* ∈ *A*
obtains *a b* **where** *Re a* < *Re b Im a* < *Im b s* ∈ *box a b f analytic-on box a b*
⟨*proof*⟩

lemma *Re-image-box*:
assumes *Re a* < *Re b Im a* < *Im b*
shows *Re* ‘ *box a b* = {*Re a*<..<*Re b*}
⟨*proof*⟩

lemma *Im-image-box*:
assumes *Re a* < *Re b Im a* < *Im b*
shows *Im* ‘ *box a b* = {*Im a*<..<*Im b*}
⟨*proof*⟩

lemma *Re-image-cbox*:
assumes *Re a* ≤ *Re b Im a* ≤ *Im b*
shows *Re* ‘ *cbox a b* = {*Re a*..*Re b*}
⟨*proof*⟩

lemma *Im-image-cbox*:
assumes *Re a* ≤ *Re b Im a* ≤ *Im b*
shows *Im* ‘ *cbox a b* = {*Im a*..*Im b*}
⟨*proof*⟩

lemma *analytic-onE-cball*:
assumes *f analytic-on A s* ∈ *A ub* > (*0*::*real*)
obtains *R* **where** *R* > *0 R* < *ub f analytic-on cball s R*
⟨*proof*⟩

corollary *analytic-pre-zeta'* [*analytic-intros*]:
assumes *f analytic-on A a* > *0*
shows (λ*x*. *pre-zeta a* (*f x*)) *analytic-on A*
⟨*proof*⟩

corollary *analytic-hurwitz-zeta'* [*analytic-intros*]:
assumes *f analytic-on A* (⋀*x*. *x* ∈ *A* ⟹ *f x* ≠ *1*) *a* > *0*
shows (λ*x*. *hurwitz-zeta a* (*f x*)) *analytic-on A*
⟨*proof*⟩

corollary *analytic-zeta'* [*analytic-intros*]:
assumes *f analytic-on A* (⋀*x*. *x* ∈ *A* ⟹ *f x* ≠ *1*)
shows (λ*x*. *zeta* (*f x*)) *analytic-on A*
⟨*proof*⟩

lemma *logderiv-zeta-analytic*: (λ*s*. *deriv zeta s* / *zeta s*) *analytic-on* {*s*. *Re s* ≥ *1*}
− {*1*}
⟨*proof*⟩

lemma *mult-real-sqrt*: *x* ≥ *0* ⟹ *x* ∗ *sqrt y* = *sqrt* (*x* ^ *2* ∗ *y*)
⟨*proof*⟩

lemma *arcsin-pos*: *x* ∈ {*0*<..*1*} ⟹ *arcsin x* > *0*
⟨*proof*⟩

lemmas *analytic-imp-holomorphic'* = *holomorphic-on-subset*[*OF analytic-imp-holomorphic*]

lemma *residue-simple'*:
assumes *open s 0* ∈ *s f holomorphic-on s*
shows *residue* (λ*w*. *f w* / *w*) *0* = *f 0*
⟨*proof*⟩

lemma *fds-converges-cong*:
assumes *eventually* (λ*n*. *fds-nth f n* = *fds-nth g n*) *at-top s* = *s'*
shows *fds-converges f s* ⟷ *fds-converges g s'*
⟨*proof*⟩

lemma *fds-abs-converges-cong*:
assumes *eventually* (λ*n*. *fds-nth f n* = *fds-nth g n*) *at-top s* = *s'*
shows *fds-abs-converges f s* ⟷ *fds-abs-converges g s'*
⟨*proof*⟩

lemma *conv-abscissa-cong*:
assumes *eventually* (λ*n*. *fds-nth f n* = *fds-nth g n*) *at-top*
shows *conv-abscissa f* = *conv-abscissa g*
⟨*proof*⟩

lemma *abs-conv-abscissa-cong*:
assumes *eventually* (λ*n*. *fds-nth f n* = *fds-nth g n*) *at-top*
shows *abs-conv-abscissa f* = *abs-conv-abscissa g*
⟨*proof*⟩

definition *fds-remainder* **where**
fds-remainder m = *fds-subseries* (λ*n*. *n* > *m*)

lemma *fds-nth-remainder*: *fds-nth* (*fds-remainder m f*) = (λ*n*. *if n* > *m then fds-nth f n else 0*)
⟨*proof*⟩

lemma *fds-converges-remainder-iff* [*simp*]:
fds-converges (*fds-remainder m f*) *s* ⟷ *fds-converges f s*
⟨*proof*⟩

lemma *fds-abs-converges-remainder-iff* [*simp*]:
fds-abs-converges (*fds-remainder m f*) *s* ⟷ *fds-abs-converges f s*
⟨*proof*⟩

lemma *fds-converges-remainder* [*intro*]:
fds-converges f s ⟹ *fds-converges* (*fds-remainder m f*) *s*
and *fds-abs-converges-remainder* [*intro*]:
fds-abs-converges f s ⟹ *fds-abs-converges* (*fds-remainder m f*) *s*
⟨*proof*⟩

lemma *conv-abscissa-remainder* [*simp*]:
conv-abscissa (*fds-remainder m f*) = *conv-abscissa f*
⟨*proof*⟩

lemma *abs-conv-abscissa-remainder* [*simp*]:
abs-conv-abscissa (*fds-remainder m f*) = *abs-conv-abscissa f*
⟨*proof*⟩

lemma *eval-fds-remainder*:
eval-fds (*fds-remainder m f*) *s* = (∑ *n*. *fds-nth f* (*n* + *Suc m*) / *nat-power* (*n* + *Suc m*) *s*)
(**is** - = *suminf* (λ*n*. *?f* (*n* + *Suc m*)))
⟨*proof*⟩

lemma *fds-truncate-plus-remainder*: *fds-truncate m f* + *fds-remainder m f* = *f*
⟨*proof*⟩

lemma *holomorphic-fds-eval'* [*holomorphic-intros*]:
assumes *g holomorphic-on A* $\bigwedge x.\ x \in A \Longrightarrow Re\ (g\ x) > conv\text{-}abscissa\ f$
shows $(\lambda x.\ eval\text{-}fds\ f\ (g\ x))$ *holomorphic-on A*
⟨*proof*⟩

lemma *analytic-fds-eval'* [*analytic-intros*]:
assumes *g analytic-on A* $\bigwedge x.\ x \in A \Longrightarrow Re\ (g\ x) > conv\text{-}abscissa\ f$
shows $(\lambda x.\ eval\text{-}fds\ f\ (g\ x))$ *analytic-on A*
⟨*proof*⟩

lemma *continuous-on-linepath* [*continuous-intros*]:
assumes *continuous-on A a continuous-on A b continuous-on A f*
shows *continuous-on A* $(\lambda x.\ linepath\ (a\ x)\ (b\ x)\ (f\ x))$
⟨*proof*⟩

lemma *continuous-on-part-circlepath* [*continuous-intros*]:
assumes *continuous-on A c continuous-on A r continuous-on A a continuous-on A b*
continuous-on A f
shows *continuous-on A* $(\lambda x.\ part\text{-}circlepath\ (c\ x)\ (r\ x)\ (a\ x)\ (b\ x)\ (f\ x))$
⟨*proof*⟩

lemma *homotopic-loops-part-circlepath*:
assumes *sphere c r* $\subseteq A$ **and** $r \geq 0$ **and**
$b1 = a1 + 2 * of\text{-}int\ k * pi$ **and** $b2 = a2 + 2 * of\text{-}int\ k * pi$
shows *homotopic-loops A* (*part-circlepath c r a1 b1*) (*part-circlepath c r a2 b2*)
⟨*proof*⟩

lemma *part-circlepath-conv-subpath*:
part-circlepath c r a b = *subpath* (*a* / (2∗*pi*)) (*b* / (2∗*pi*)) (*circlepath c r*)
⟨*proof*⟩

lemma *homotopic-paths-part-circlepath*:
assumes $a \leq b\ b \leq c$
assumes *path-image* (*part-circlepath C r a c*) $\subseteq A\ r \geq 0$
shows *homotopic-paths A* (*part-circlepath C r a c*)
(*part-circlepath C r a b* +++ *part-circlepath C r b c*)
(**is** *homotopic-paths - ?g* (*?h1* +++ *?h2*))
⟨*proof*⟩

lemma *path-image-part-circlepath-subset*:
assumes $a \leq a'\ a' \leq b'\ b' \leq b$
shows *path-image* (*part-circlepath c r a' b'*) $\subseteq$ *path-image* (*part-circlepath c r a b*)
⟨*proof*⟩

lemma *part-circlepath-mirror*:

assumes $a' = a + pi + 2 * pi * of\text{-}int\ k\ b' = b + pi + 2 * pi * of\text{-}int\ k\ c' = -c$
shows $-part\text{-}circlepath\ c\ r\ a\ b = part\text{-}circlepath\ c'\ r\ a'\ b'$
⟨*proof*⟩

lemma *path-mirror* [*intro*]: $path\ (g :: - \Rightarrow 'b{::}topological\text{-}group\text{-}add) \Longrightarrow path\ (-g)$
⟨*proof*⟩

lemma *path-mirror-iff* [*simp*]: $path\ (-g :: - \Rightarrow 'b{::}topological\text{-}group\text{-}add) \longleftrightarrow path\ g$
⟨*proof*⟩

lemma *valid-path-mirror* [*intro*]: $valid\text{-}path\ g \Longrightarrow valid\text{-}path\ (-g)$
⟨*proof*⟩

lemma *valid-path-mirror-iff* [*simp*]: $valid\text{-}path\ (-g) \longleftrightarrow valid\text{-}path\ g$
⟨*proof*⟩

lemma *pathstart-mirror* [*simp*]: $pathstart\ (-g) = -pathstart\ g$
and *pathfinish-mirror* [*simp*]: $pathfinish\ (-g) = -pathfinish\ g$
⟨*proof*⟩

lemma *path-image-mirror*: $path\text{-}image\ (-g) = uminus\ `\ path\text{-}image\ g$
⟨*proof*⟩

lemma *cos-le-zero*:
assumes $x \in \{pi/2..3*pi/2\}$
shows $cos\ x \leq 0$
⟨*proof*⟩

lemma *cos-le-zero'*: $x \in \{-3*pi/2..-pi/2\} \Longrightarrow cos\ x \leq 0$
⟨*proof*⟩

lemma *winding-number-join-pos-combined'*:
$[\![valid\text{-}path\ \gamma1 \wedge z \notin path\text{-}image\ \gamma1 \wedge 0 < Re\ (winding\text{-}number\ \gamma1\ z);$
$valid\text{-}path\ \gamma2 \wedge z \notin path\text{-}image\ \gamma2 \wedge 0 < Re\ (winding\text{-}number\ \gamma2\ z);$
$pathfinish\ \gamma1 = pathstart\ \gamma2]\!]$
$\Longrightarrow valid\text{-}path(\gamma1\ +\!+\!+\ \gamma2) \wedge z \notin path\text{-}image(\gamma1\ +\!+\!+\ \gamma2) \wedge 0 < Re(winding\text{-}number(\gamma1\ +\!+\!+\ \gamma2)\ z)$
⟨*proof*⟩

lemma *Union-atLeastAtMost-real-of-nat*:
assumes $a < b$
shows $(\bigcup n{\in}\{a..{<}b\}.\ \{real\ n..real\ (n + 1)\}) = \{real\ a..real\ b\}$
⟨*proof*⟩

lemma *nat-sum-has-integral-floor*:
fixes $f :: nat \Rightarrow 'a :: banach$
assumes *mn*: $m < n$

shows $((\lambda x.\ f\ (nat\ \lfloor x \rfloor))\ has\text{-}integral\ sum\ f\ \{m..<n\})\ \{real\ m..real\ n\}$
⟨*proof*⟩

lemma *nat-sum-has-integral-ceiling*:
fixes $f :: nat \Rightarrow 'a :: banach$
assumes *mn*: $m < n$
shows $((\lambda x.\ f\ (nat\ \lceil x \rceil))\ has\text{-}integral\ sum\ f\ \{m<..n\})\ \{real\ m..real\ n\}$
⟨*proof*⟩

lemma *zeta-partial-sum-le*:
fixes $x :: real$ **and** $m :: nat$
assumes *x*: $x \in \{0<..1\}$
shows $(\sum k{=}1..m.\ real\ k\ powr\ (x - 1)) \leq real\ m\ powr\ x\ /\ x$
⟨*proof*⟩

lemma *zeta-partial-sum-le'*:
fixes $x :: real$ **and** $m :: nat$
assumes *x*: $x > 0$ **and** *m*: $m > 0$
shows $(\sum n{=}1..m.\ real\ n\ powr\ (x - 1)) \leq m\ powr\ x * (1\ /\ x + 1\ /\ m)$
⟨*proof*⟩

lemma *natfun-bigo-1E*:
assumes $(f :: nat \Rightarrow -) \in O(\lambda\text{-}.\ 1)$
obtains *C* **where** $C \geq lb \bigwedge n.\ norm\ (f\ n) \leq C$
⟨*proof*⟩

lemma *natfun-bigo-iff-Bseq*: $f \in O(\lambda\text{-}.\ 1) \longleftrightarrow Bseq\ f$
⟨*proof*⟩

lemma *enn-decreasing-sum-le-set-nn-integral*:
fixes $f :: real \Rightarrow ennreal$
assumes *decreasing*: $\bigwedge x\ y.\ 0 \leq x \Longrightarrow x \leq y \Longrightarrow f\ y \leq f\ x$
shows $(\sum n.\ f\ (real\ (Suc\ n))) \leq set\text{-}nn\text{-}integral\ lborel\ \{0..\}\ f$
⟨*proof*⟩

lemma *abs-summable-on-uminus-iff*:
$(\lambda x.\ -f\ x)\ abs\text{-}summable\text{-}on\ A \longleftrightarrow f\ abs\text{-}summable\text{-}on\ A$
⟨*proof*⟩

lemma *abs-summable-on-cmult-right-iff*:
fixes $f :: 'a \Rightarrow 'b :: \{banach, real\text{-}normed\text{-}field, second\text{-}countable\text{-}topology\}$
assumes $c \neq 0$
shows $(\lambda x.\ c * f\ x)\ abs\text{-}summable\text{-}on\ A \longleftrightarrow f\ abs\text{-}summable\text{-}on\ A$
⟨*proof*⟩

lemma *abs-summable-on-cmult-left-iff*:
fixes $f :: 'a \Rightarrow 'b :: \{banach, real\text{-}normed\text{-}field, second\text{-}countable\text{-}topology\}$
assumes $c \neq 0$
shows $(\lambda x.\ f\ x * c)\ abs\text{-}summable\text{-}on\ A \longleftrightarrow f\ abs\text{-}summable\text{-}on\ A$

⟨*proof*⟩

lemma *decreasing-sum-le-integral*:
fixes $f :: real \Rightarrow real$
assumes *nonneg*: $\bigwedge x.\ x \geq 0 \Longrightarrow f\ x \geq 0$
assumes *decreasing*: $\bigwedge x\ y.\ 0 \leq x \Longrightarrow x \leq y \Longrightarrow f\ y \leq f\ x$
assumes *integral*: $(f\ has\text{-}integral\ I)\ \{0..\}$
shows *summable* $(\lambda i.\ f\ (real\ (Suc\ i)))$ **and** $suminf\ (\lambda i.\ f\ (real\ (Suc\ i))) \leq I$
⟨*proof*⟩

lemma *decreasing-sum-le-integral'*:
fixes $f :: real \Rightarrow real$
assumes $\bigwedge x.\ x \geq 0 \Longrightarrow f\ x \geq 0$
assumes $\bigwedge x\ y.\ 0 \leq x \Longrightarrow x \leq y \Longrightarrow f\ y \leq f\ x$
assumes $(f\ has\text{-}integral\ I)\ \{0..\}$
shows *summable* $(\lambda i.\ f\ (real\ i))$ **and** $suminf\ (\lambda i.\ f\ (real\ i)) \leq f\ 0 + I$
⟨*proof*⟩

lemma *of-nat-powr-neq-1-complex* [*simp*]:
assumes $n > 1$ $Re\ s \neq 0$
shows $of\text{-}nat\ n\ powr\ s \neq (1::complex)$
⟨*proof*⟩

lemma *fds-logderiv-completely-multiplicative*:
fixes $f :: 'a :: \{real\text{-}normed\text{-}field\}\ fds$
assumes $completely\text{-}multiplicative\text{-}function\ (fds\text{-}nth\ f)$ $fds\text{-}nth\ f\ 1 \neq 0$
shows $fds\text{-}deriv\ f\ /\ f = -\ fds\ (\lambda n.\ fds\text{-}nth\ f\ n * mangoldt\ n)$
⟨*proof*⟩

lemma *fds-nth-logderiv-completely-multiplicative*:
fixes $f :: 'a :: \{real\text{-}normed\text{-}field\}\ fds$
assumes $completely\text{-}multiplicative\text{-}function\ (fds\text{-}nth\ f)$ $fds\text{-}nth\ f\ 1 \neq 0$
shows $fds\text{-}nth\ (fds\text{-}deriv\ f\ /\ f)\ n = -fds\text{-}nth\ f\ n * mangoldt\ n$
⟨*proof*⟩

lemma *eval-fds-logderiv-completely-multiplicative*:
fixes $s :: 'a :: dirichlet\text{-}series$ **and** $l :: 'a$ **and** $f :: 'a\ fds$
defines $h \equiv fds\text{-}deriv\ f\ /\ f$
assumes $completely\text{-}multiplicative\text{-}function\ (fds\text{-}nth\ f)$ **and** [*simp*]: $fds\text{-}nth\ f\ 1 \neq 0$
assumes $s \cdot 1 > abs\text{-}conv\text{-}abscissa\ f$
shows $(\lambda p.\ of\text{-}real\ (ln\ (real\ p)) * (1\ /\ (1 - fds\text{-}nth\ f\ p\ /\ nat\text{-}power\ p\ s) - 1))$
$abs\text{-}summable\text{-}on\ \{p.\ prime\ p\}$ (**is** *?th1*)
and $eval\text{-}fds\ h\ s = -(\sum_a p \mid prime\ p.\ of\text{-}real\ (ln\ (real\ p)) *$
$(1\ /\ (1 - fds\text{-}nth\ f\ p\ /\ nat\text{-}power\ p\ s) - 1))$ (**is** *?th2*)
⟨*proof*⟩

lemma *eval-fds-logderiv-zeta*:
assumes $Re\ s > 1$

shows $(\lambda p.\ of\text{-}real\ (ln\ (real\ p))\ /\ (p\ powr\ s - 1))$
$abs\text{-}summable\text{-}on\ \{p.\ prime\ p\}$ (**is** *?th1*)
and $deriv\ zeta\ s\ /\ zeta\ s =$
$-(\sum_a p \mid prime\ p.\ of\text{-}real\ (ln\ (real\ p))\ /\ (p\ powr\ s - 1))$ (**is** *?th2*)
⟨*proof*⟩

lemma *sums-logderiv-zeta*:
assumes $Re\ s > 1$
shows $(\lambda p.\ if\ prime\ p\ then\ of\text{-}real\ (ln\ (real\ p))\ /\ (of\text{-}nat\ p\ powr\ s - 1)\ else\ 0)$
sums
$-(deriv\ zeta\ s\ /\ zeta\ s)$ (**is** *?f sums* -)
⟨*proof*⟩

lemma *range-add-nat*: $range\ (\lambda n.\ n + c) = \{(c::nat)..\}$
⟨*proof*⟩

lemma *abs-summable-hurwitz-zeta*:
assumes $Re\ s > 1\ a + real\ b > 0$
shows $(\lambda n.\ 1\ /\ (of\text{-}nat\ n + a)\ powr\ s)\ abs\text{-}summable\text{-}on\ \{b..\}$
⟨*proof*⟩

lemma *hurwitz-zeta-nat-conv-infsetsum*:
assumes $a > 0$ **and** $Re\ s > 1$
shows $hurwitz\text{-}zeta\ (real\ a)\ s = (\sum_a n.\ of\text{-}nat\ (n + a)\ powr\ -s)$
$hurwitz\text{-}zeta\ (real\ a)\ s = (\sum_a n{\in}\{a..\}.\ of\text{-}nat\ n\ powr\ -s)$
⟨*proof*⟩

lemma *pre-zeta-bound*:
assumes $0 < Re\ s$ **and** a: $a > 0$
shows $norm\ (pre\text{-}zeta\ a\ s) \leq (1 + norm\ s\ /\ Re\ s)\ /\ 2 * a\ powr\ -Re\ s$
⟨*proof*⟩

lemma *pre-zeta-bound′*:
assumes $0 < Re\ s$ **and** a: $a > 0$
shows $norm\ (pre\text{-}zeta\ a\ s) \leq norm\ s\ /\ (Re\ s * a\ powr\ Re\ s)$
⟨*proof*⟩

lemma *deriv-zeta-eq*:
assumes s: $s \neq 1$
shows $deriv\ zeta\ s = deriv\ (pre\text{-}zeta\ 1)\ s - 1\ /\ (s - 1)^2$
⟨*proof*⟩

lemma *zeta-remove-zero*:
assumes $Re\ s \geq 1$
shows $(s - 1) * pre\text{-}zeta\ 1\ s + 1 \neq 0$
⟨*proof*⟩

lemma *eval-fds-deriv-zeta*:
assumes $Re\ s > 1$

shows *eval-fds* (*fds-deriv fds-zeta*) *s* = *deriv zeta s*
⟨*proof*⟩

lemma *le-nat-iff'*: $x \leq nat\ y \longleftrightarrow x = 0 \wedge y \leq 0 \vee int\ x \leq y$
⟨*proof*⟩

lemma *sum-upto-plus1*:
assumes $x \geq 0$
shows *sum-upto f* (*x* + *1*) = *sum-upto f x* + *f* (*Suc* (*nat* ⌊*x*⌋))
⟨*proof*⟩

lemma *sum-upto-minus1*:
assumes $x \geq 1$
shows *sum-upto f* (*x* − *1*) = (*sum-upto f x* − *f* (*nat* ⌊*x*⌋) :: *'a* :: *ab-group-add*)
⟨*proof*⟩

lemma *integral-smallo*:
fixes *f g g'* :: *real* ⇒ *real*
assumes *f* ∈ *o*(*g'*) **and** *filterlim g at-top at-top*
assumes ⋀*a' x*. *a* ≤ *a'* ⟹ *a'* ≤ *x* ⟹ *f integrable-on* {*a'*..*x*}
assumes *deriv*: ⋀*x*. *x* ≥ *a* ⟹ (*g has-field-derivative g' x*) (*at x*)
assumes *cont*: *continuous-on* {*a*..} *g'*
assumes *nonneg*: ⋀*x*. *x* ≥ *a* ⟹ *g' x* ≥ *0*
shows (λ*x*. *integral* {*a*..*x*} *f*) ∈ *o*(*g*)
⟨*proof*⟩

lemma *integral-bigo*:
fixes *f g g'* :: *real* ⇒ *real*
assumes *f* ∈ *O*(*g'*) **and** *filterlim g at-top at-top*
assumes ⋀*a' x*. *a* ≤ *a'* ⟹ *a'* ≤ *x* ⟹ *f integrable-on* {*a'*..*x*}
assumes *deriv*: ⋀*x*. *x* ≥ *a* ⟹ (*g has-field-derivative g' x*) (*at x within* {*a*..})
assumes *cont*: *continuous-on* {*a*..} *g'*
assumes *nonneg*: ⋀*x*. *x* ≥ *a* ⟹ *g' x* ≥ *0*
shows (λ*x*. *integral* {*a*..*x*} *f*) ∈ *O*(*g*)
⟨*proof*⟩

lemma *primepows-le-subset*:
assumes *x*: *x* > *0* **and** *l*: *l* > *0*
shows {(*p*, *i*). *prime p* ∧ *l* ≤ *i* ∧ *real* (*p* ^ *i*) ≤ *x*} ⊆ {..*nat* ⌊*root l x*⌋} × {..*nat* ⌊*log 2 x*⌋}
⟨*proof*⟩

lemma *mangoldt-non-primepow*: ¬*primepow n* ⟹ *mangoldt n* = *0*
⟨*proof*⟩

lemma *ln-minus-ln-floor-bigo*: (λ*x*. *ln x* − *ln* (*real* (*nat* ⌊*x*⌋))) ∈ *O*(λ-. *1*)
⟨*proof*⟩

lemma *cos-geD*:
assumes $cos\ x \geq cos\ a\ 0 \leq a\ a \leq pi\ -pi \leq x\ x \leq pi$
shows $x \in \{-a..a\}$
⟨*proof*⟩

lemma *path-image-part-circlepath-same-Re*:
assumes $0 \leq b\ b \leq pi\ a = -b\ r \geq 0$
shows *path-image* (*part-circlepath c r a b*) = *sphere c r* ∩ {*s*. *Re s* ≥ *Re c* + *r* ∗ *cos a*}
⟨*proof*⟩

lemma *part-circlepath-rotate-left*:
part-circlepath c r (*x* + *a*) (*x* + *b*) = (λ*z*. *c* + *cis x* ∗ (*z* − *c*)) ∘ *part-circlepath c r a b*
⟨*proof*⟩

lemma *part-circlepath-rotate-right*:
part-circlepath c r (*a* + *x*) (*b* + *x*) = (λ*z*. *c* + *cis x* ∗ (*z* − *c*)) ∘ *part-circlepath c r a b*
⟨*proof*⟩

lemma *path-image-semicircle-Re-ge*:
assumes $r \geq 0$
shows *path-image* (*part-circlepath c r* (−*pi*/2) (*pi*/2)) =
sphere c r ∩ {*s*. *Re s* ≥ *Re c*}
⟨*proof*⟩

lemma *sphere-rotate*: (λ*z*. *c* + *cis x* ∗ (*z* − *c*)) ‘ *sphere c r* = *sphere c r*
⟨*proof*⟩

lemma *path-image-semicircle-Re-le*:
assumes $r \geq 0$
shows *path-image* (*part-circlepath c r* (*pi*/2) (3/2∗*pi*)) =
sphere c r ∩ {*s*. *Re s* ≤ *Re c*}
⟨*proof*⟩

lemma *path-image-semicircle-Im-ge*:
assumes $r \geq 0$
shows *path-image* (*part-circlepath c r 0 pi*) =
sphere c r ∩ {*s*. *Im s* ≥ *Im c*}
⟨*proof*⟩

lemma *path-image-semicircle-Im-le*:
assumes $r \geq 0$
shows *path-image* (*part-circlepath c r pi* (2 ∗ *pi*)) =
sphere c r ∩ {*s*. *Im s* ≤ *Im c*}
⟨*proof*⟩

lemma *eval-fds-logderiv-zeta-real*:
assumes $x > (1 :: real)$
shows $(\lambda p.\ ln\ (real\ p)\ /\ (p\ powr\ x - 1))$ *abs-summable-on* $\{p.\ prime\ p\}$ (**is** *?th1*)
and *deriv zeta* (*of-real x*) / *zeta* (*of-real x*) =
$-of\text{-}real\ (\sum_a p \mid prime\ p.\ ln\ (real\ p)\ /\ (p\ powr\ x - 1))$ (**is** *?th2*)
⟨*proof*⟩

lemma
fixes *a b c d* :: *real*
assumes *ab*: $d * a + b \geq 1$ **and** *c*: $c < -1$ **and** *d*: $d > 0$
defines $C \equiv -((ln\ (d * a + b) - 1\ /\ (c + 1)) * (d * a + b)\ powr\ (c + 1)\ /\ (d * (c + 1)))$
shows *set-integrable-ln-powr-at-top*:
$(\lambda x.\ (ln\ (d * x + b) * ((d * x + b)\ powr\ c)))$ *absolutely-integrable-on* $\{a<..\}$ (**is** *?th1*)
and *set-lebesgue-integral-ln-powr-at-top*:
$(\int x{\in}\{a<..\}.\ (ln\ (d * x + b) * ((d * x + b)\ powr\ c))\ \partial lborel) = C$ (**is** *?th2*)
and *ln-powr-has-integral-at-top*:
$((\lambda x.\ ln\ (d * x + b) * (d * x + b)\ powr\ c)\ has\text{-}integral\ C)\ \{a<..\}$ (**is** *?th3*)
⟨*proof*⟩

lemma *ln-fact-conv-sum-upto*: $ln\ (fact\ n) = sum\text{-}upto\ ln\ n$
⟨*proof*⟩

lemma *sum-upto-ln-conv-ln-fact*: $sum\text{-}upto\ ln\ x = ln\ (fact\ (nat\ \lfloor x \rfloor))$
⟨*proof*⟩

lemma *real-of-nat-div*: $real\ (a\ div\ b) = real\text{-}of\text{-}int\ \lfloor real\ a\ /\ real\ b \rfloor$
⟨*proof*⟩

lemma *measurable-sum-upto* [*measurable*]:
fixes $f :: 'a \Rightarrow nat \Rightarrow real$
assumes [*measurable*]: $\bigwedge y.\ (\lambda t.\ f\ t\ y) \in M \to_M borel$
assumes [*measurable*]: $x \in M \to_M borel$
shows $(\lambda t.\ sum\text{-}upto\ (f\ t)\ (x\ t)) \in M \to_M borel$
⟨*proof*⟩

end

2 Ingham's Tauberian Theorem

theory *Newman-Ingham-Tauberian*
imports
HOL−Real-Asymp.Real-Asymp
Prime-Number-Theorem-Library
begin

In his proof of the Prime Number Theorem, Newman [6] uses a Tauberian theorem that was first proven by Ingham. Newman gives a nice and straightforward proof of this theorem based on contour integration. This section will be concerned with proving this theorem.

This Tauberian theorem is probably the part of the Newman's proof of the Prime Number Theorem where most of the "heavy lifting" is done. Its purpose is to extend the summability of a Dirichlet series with bounded coefficients from the region $\Re(s) > 1$ to $\Re(s) \geq 1$.

In order to show it, we first require a number of auxiliary bounding lemmas.

lemma *newman-ingham-aux1*:
fixes R :: *real* **and** z :: *complex*
assumes R: $R > 0$ **and** z : *norm* $z = R$
shows *norm* $(1 \,/\, z + z \,/\, R^2) = 2 * |Re\ z| \,/\, R^2$
⟨*proof*⟩

lemma *newman-ingham-aux2*:
fixes m :: *nat* **and** $w\ z$ :: *complex*
assumes $1 \leq m\ 1 \leq Re\ w\ 0 < Re\ z$ **and** f: $\bigwedge n.\ 1 \leq n \Longrightarrow norm\ (f\ n) \leq C$
shows *norm* $(\sum n{=}1..m.\ f\ n \,/\, n\ powr\ (w - z)) \leq C * (m\ powr\ Re\ z) * (1 \,/\, m + 1 \,/\, Re\ z)$
⟨*proof*⟩

lemma *hurwitz-zeta-real-bound-aux*:
fixes $a\ x$ :: *real*
assumes *ax*: $a > 0\ x > 1$
shows $(\sum i.\ (a + real\ (Suc\ i))\ powr\ (-x)) \leq a\ powr\ (1 - x) \,/\, (x - 1)$
⟨*proof*⟩

Given a function that is analytic on some vertical line segment, we can find a rectangle around that line segment on which the function is also analytic.

lemma *analytic-on-axis-extend*:
fixes *y1 y2 x* :: *real*
defines $S \equiv \{z.\ Re\ z = x \wedge Im\ z \in \{y1..y2\}\}$
assumes $y1 \leq y2$
assumes f *analytic-on* S
obtains *x1 x2* :: *real* **where** $x1 < x\ x2 > x$ f *analytic-on cbox* (*Complex x1 y1*) (*Complex x2 y2*)
⟨*proof*⟩

We will now prove the theorem. The precise setting is this: Consider a Dirichlet series $F(s) = \sum a_n n^{-s}$ with bounded coefficients. Clearly, this converges to an analytic function $f(s)$ on $\{s \mid \Re(s) > 1\}$.

If $f(s)$ is analytic on the larger set $\{s \mid \Re(s) \geq 1\}$, F converges to $f(s)$ for all $\Re(s) \geq 1$.

The proof follows Newman's argument very closely, but some of the precise bounds we use are a bit different from his. Also, like Harrison, we choose a

combination of a semicircle and a rectangle as our contour, whereas Newman uses a circle with a vertical cut-off. The result of the Residue theorem is the same in both cases, but the bounding of the contributions of the different parts is somewhat different.

The reason why we picked Harrison's contour over Newman's is because we could not understand how his bounding of the different contributions fits to his contour, and it seems likely that this is also the reason why Harrison altered the contour in the first place.

lemma *Newman-Ingham-1*:
  fixes F :: *complex fds* **and** f :: *complex* ⇒ *complex*
  assumes *coeff-bound*: *fds-nth* $F \in O(\lambda\text{-}.\ 1)$
  assumes *f-analytic*: f *analytic-on* $\{s.\ Re\ s \geq 1\}$
  assumes *F-conv-f*: $\bigwedge s.\ Re\ s > 1 \Longrightarrow$ *eval-fds* $F\ s = f\ s$
  assumes w: $Re\ w \geq 1$
  shows *fds-converges* $F\ w$ **and** *eval-fds* $F\ w = f\ w$
⟨*proof*⟩

The theorem generalises in a trivial way; we can replace the requirement that the coefficients of $f(s)$ be $O(1)$ by $O(n^{\sigma-1})$ for some $\sigma \in \mathbb{R}$, then $f(s)$ converges for $\mathfrak{R}(s) > \sigma$. If it can be analytically continued to $\mathfrak{R}(s) \geq \sigma$, it is also convergent there.

theorem *Newman-Ingham*:
  fixes F :: *complex fds* **and** f :: *complex* ⇒ *complex*
  assumes *coeff-bound*: *fds-nth* $F \in O(\lambda n.\ n\ powr\ of\text{-}real\ (\sigma - 1))$
  assumes *f-analytic*: f *analytic-on* $\{s.\ Re\ s \geq \sigma\}$
  assumes *F-conv-f*: $\bigwedge s.\ Re\ s > \sigma \Longrightarrow$ *eval-fds* $F\ s = f\ s$
  assumes w: $Re\ w \geq \sigma$
  shows *fds-converges* $F\ w$ **and** *eval-fds* $F\ w = f\ w$
⟨*proof*⟩

end

3 Prime-Counting Functions

theory *Prime-Counting-Functions*
  imports *Prime-Number-Theorem-Library*
begin

We will now define the basic prime-counting functions π, ϑ, and ψ. Additionally, we shall define a function M that is related to Mertens' theorems and Newman's proof of the Prime Number Theorem. Most of the results in this file are not actually required to prove the Prime Number Theorem, but are still nice to have.

3.1 Definitions

definition *prime-sum-upto* :: (*nat* ⇒ *'a*) ⇒ *real* ⇒ *'a* :: *semiring-1* **where**

prime-sum-upto f x = $(\sum p \mid \textit{prime } p \wedge \textit{real } p \leq x.\ f\ p)$

lemma *prime-sum-upto-altdef1*:
prime-sum-upto f x = *sum-upto* $(\lambda p.\ \textit{ind prime } p * f\ p)$ *x*
⟨*proof*⟩

lemma *prime-sum-upto-altdef2*:
prime-sum-upto f x = $(\sum p \mid \textit{prime } p \wedge p \leq \textit{nat } \lfloor x \rfloor.\ f\ p)$
⟨*proof*⟩

lemma *prime-sum-upto-altdef3*:
prime-sum-upto f x = $(\sum p \leftarrow \textit{primes-upto } (\textit{nat } \lfloor x \rfloor).\ f\ p)$
⟨*proof*⟩

lemma *prime-sum-upto-eqI*:
assumes $a \leq b$ $\bigwedge k.\ k \in \{\textit{nat } \lfloor a \rfloor <..\textit{nat} \lfloor b \rfloor\} \Longrightarrow \neg \textit{prime } k$
shows *prime-sum-upto f a* = *prime-sum-upto f b*
⟨*proof*⟩

lemma *prime-sum-upto-eqI'*:
assumes $a' \leq \textit{nat } \lfloor a \rfloor$ $a \leq b$ $\textit{nat } \lfloor b \rfloor \leq b'$ $\bigwedge k.\ k \in \{a' <..b'\} \Longrightarrow \neg \textit{prime } k$
shows *prime-sum-upto f a* = *prime-sum-upto f b*
⟨*proof*⟩

lemmas *eval-prime-sum-upto* = *prime-sum-upto-altdef3*[*unfolded primes-upto-sieve*]

lemma *of-nat-prime-sum-upto*: *of-nat* (*prime-sum-upto f x*) = *prime-sum-upto* $(\lambda p.\ \textit{of-nat } (f\ p))$ *x*
⟨*proof*⟩

lemma *prime-sum-upto-mono*:
assumes $\bigwedge n.\ n > 0 \Longrightarrow f\ n \geq (0 :: \textit{real})$ $x \leq y$
shows *prime-sum-upto f x* ≤ *prime-sum-upto f y*
⟨*proof*⟩

lemma *prime-sum-upto-nonneg*:
assumes $\bigwedge n.\ n > 0 \Longrightarrow f\ n \geq (0 :: \textit{real})$
shows *prime-sum-upto f x* ≥ 0
⟨*proof*⟩

lemma *prime-sum-upto-eq-0*:
assumes $x < 2$
shows *prime-sum-upto f x* = 0
⟨*proof*⟩

lemma *measurable-prime-sum-upto* [*measurable*]:
fixes $f :: 'a \Rightarrow \textit{nat} \Rightarrow \textit{real}$
assumes [*measurable*]: $\bigwedge y.\ (\lambda t.\ f\ t\ y) \in M \to_M \textit{borel}$
assumes [*measurable*]: $x \in M \to_M \textit{borel}$

shows $(\lambda t.\ \textit{prime-sum-upto}\ (f\ t)\ (x\ t)) \in M \to_M \textit{borel}$
⟨*proof*⟩

The following theorem breaks down a sum over all prime powers no greater than fixed bound into a nicer form.

lemma *sum-upto-primepows*:
fixes $f :: \textit{nat} \Rightarrow {'a} :: \textit{comm-monoid-add}$
assumes $\bigwedge n.\ \neg \textit{primepow}\ n \Longrightarrow f\ n = 0\ \bigwedge p\ i.\ \textit{prime}\ p \Longrightarrow i > 0 \Longrightarrow f\ (p\ \hat{}\ i) = g\ p\ i$
shows $\textit{sum-upto}\ f\ x = (\sum (p,\ i) \mid \textit{prime}\ p \wedge i > 0 \wedge \textit{real}\ (p\ \hat{}\ i) \leq x.\ g\ p\ i)$
⟨*proof*⟩

definition *primes-pi* **where** $\textit{primes-pi} = \textit{prime-sum-upto}\ (\lambda p.\ 1 :: \textit{real})$
definition *primes-theta* **where** $\textit{primes-theta} = \textit{prime-sum-upto}\ (\lambda p.\ \textit{ln}\ (\textit{real}\ p))$
definition *primes-psi* **where** $\textit{primes-psi} = \textit{sum-upto}\ (\textit{mangoldt} :: \textit{nat} \Rightarrow \textit{real})$
definition *primes-M* **where** $\textit{primes-M} = \textit{prime-sum-upto}\ (\lambda p.\ \textit{ln}\ (\textit{real}\ p)\ /\ \textit{real}\ p)$

Next, we define some nice optional notation for these functions.

open-bundle *prime-counting-syntax*
begin
notation *primes-pi* ($\langle\pi\rangle$)
notation *primes-theta* ($\langle\vartheta\rangle$)
notation *primes-psi* ($\langle\psi\rangle$)
notation *primes-M* ($\langle\mathfrak{M}\rangle$)
end

lemmas $\pi\text{-}def = \textit{primes-pi-def}$
lemmas $\vartheta\text{-}def = \textit{primes-theta-def}$
lemmas $\psi\text{-}def = \textit{primes-psi-def}$

lemmas $\textit{eval-}\pi = \textit{primes-pi-def}[\textit{unfolded eval-prime-sum-upto}]$
lemmas $\textit{eval-}\vartheta = \textit{primes-theta-def}[\textit{unfolded eval-prime-sum-upto}]$
lemmas $\textit{eval-}\mathfrak{M} = \textit{primes-M-def}[\textit{unfolded eval-prime-sum-upto}]$

3.2 Basic properties

The proofs in this section are mostly taken from Apostol [1].

lemma $\pi\text{-}\textit{measurable}\ [\textit{measurable}]: \pi \in \textit{borel} \to_M \textit{borel}$
and $\vartheta\text{-}\textit{measurable}\ [\textit{measurable}]: \vartheta \in \textit{borel} \to_M \textit{borel}$
and $\psi\text{-}\textit{measurable}\ [\textit{measurable}]: \psi \in \textit{borel} \to_M \textit{borel}$
and $\textit{primes-M-measurable}\ [\textit{measurable}]: \mathfrak{M} \in \textit{borel} \to_M \textit{borel}$
⟨*proof*⟩

lemma $\pi\text{-}\textit{eq-0}\ [\textit{simp}]: x < 2 \Longrightarrow \pi\ x = 0$
and $\vartheta\text{-}\textit{eq-0}\ [\textit{simp}]: x < 2 \Longrightarrow \vartheta\ x = 0$
and $\textit{primes-M-eq-0}\ [\textit{simp}]: x < 2 \Longrightarrow \mathfrak{M}\ x = 0$

⟨*proof*⟩

lemma π-*nat-cancel* [*simp*]: $\pi\ (nat\ x) = \pi\ x$
and ϑ-*nat-cancel* [*simp*]: $\vartheta\ (nat\ x) = \vartheta\ x$
and *primes-M-nat-cancel* [*simp*]: $\mathfrak{M}\ (nat\ x) = \mathfrak{M}\ x$
and ψ-*nat-cancel* [*simp*]: $\psi\ (nat\ x) = \psi\ x$
and π-*floor-cancel* [*simp*]: $\pi\ (of\text{-}int\ \lfloor y \rfloor) = \pi\ y$
and ϑ-*floor-cancel* [*simp*]: $\vartheta\ (of\text{-}int\ \lfloor y \rfloor) = \vartheta\ y$
and *primes-M-floor-cancel* [*simp*]: $\mathfrak{M}\ (of\text{-}int\ \lfloor y \rfloor) = \mathfrak{M}\ y$
and ψ-*floor-cancel* [*simp*]: $\psi\ (of\text{-}int\ \lfloor y \rfloor) = \psi\ y$
⟨*proof*⟩

lemma π-*nonneg* [*intro*]: $\pi\ x \geq 0$
and ϑ-*nonneg* [*intro*]: $\vartheta\ x \geq 0$
and *primes-M-nonneg* [*intro*]: $\mathfrak{M}\ x \geq 0$
⟨*proof*⟩

lemma π-*mono* [*intro*]: $x \leq y \Longrightarrow \pi\ x \leq \pi\ y$
and ϑ-*mono* [*intro*]: $x \leq y \Longrightarrow \vartheta\ x \leq \vartheta\ y$
and *primes-M-mono* [*intro*]: $x \leq y \Longrightarrow \mathfrak{M}\ x \leq \mathfrak{M}\ y$
⟨*proof*⟩

lemma π-*pos-iff*: $\pi\ x > 0 \longleftrightarrow x \geq 2$
⟨*proof*⟩

lemma π-*pos*: $x \geq 2 \Longrightarrow \pi\ x > 0$
⟨*proof*⟩

lemma ψ-*eq-0* [*simp*]:
assumes $x < 2$
shows $\psi\ x = 0$
⟨*proof*⟩

lemma ψ-*nonneg* [*intro*]: $\psi\ x \geq 0$
⟨*proof*⟩

lemma ψ-*mono*: $x \leq y \Longrightarrow \psi\ x \leq \psi\ y$
⟨*proof*⟩

3.3 The n-th prime number

Next we define the n-th prime number, where counting starts from 0. In traditional mathematics, it seems that counting usually starts from 1, but it is more natural to start from 0 in HOL and the asymptotics of the function are the same.

definition *nth-prime* :: *nat* ⇒ *nat* **where**
nth-prime n = (*THE p*. *prime p* ∧ *card* {*q*. *prime q* ∧ *q* < *p*} = *n*)

lemma *finite-primes-less* [*intro*]: *finite* {*q*::*nat*. *prime q* ∧ *q* < *p*}
⟨*proof*⟩

lemma *nth-prime-unique-aux*:
fixes *p p'* :: *nat*
assumes *prime p card* {*q*. *prime q* ∧ *q* < *p*} = *n*
assumes *prime p' card* {*q*. *prime q* ∧ *q* < *p'*} = *n*
shows *p* = *p'*
⟨*proof*⟩

lemma *π-smallest-prime-beyond*:
π (*real* (*smallest-prime-beyond m*)) = *π* (*real* (*m* − *1*)) + *1*
⟨*proof*⟩

lemma *π-inverse-exists*: ∃ *n*. *π* (*real n*) = *real m*
⟨*proof*⟩

lemma *nth-prime-exists*: ∃ *p*::*nat*. *prime p* ∧ *card* {*q*. *prime q* ∧ *q* < *p*} = *n*
⟨*proof*⟩

lemma *nth-prime-exists1*: ∃!*p*::*nat*. *prime p* ∧ *card* {*q*. *prime q* ∧ *q* < *p*} = *n*
⟨*proof*⟩

lemma *prime-nth-prime* [*intro*]: *prime* (*nth-prime n*)
and *card-less-nth-prime* [*simp*]: *card* {*q*. *prime q* ∧ *q* < *nth-prime n*} = *n*
⟨*proof*⟩

lemma *card-le-nth-prime* [*simp*]: *card* {*q*. *prime q* ∧ *q* ≤ *nth-prime n*} = *Suc n*
⟨*proof*⟩

lemma *π-nth-prime* [*simp*]: *π* (*real* (*nth-prime n*)) = *real n* + *1*
⟨*proof*⟩

lemma *nth-prime-eqI*:
assumes *prime p card* {*q*. *prime q* ∧ *q* < *p*} = *n*
shows *nth-prime n* = *p*
⟨*proof*⟩

lemma *nth-prime-eqI'*:
assumes *prime p card* {*q*. *prime q* ∧ *q* ≤ *p*} = *Suc n*
shows *nth-prime n* = *p*
⟨*proof*⟩

lemma *nth-prime-eqI''*:
assumes *prime p π* (*real p*) = *real n* + *1*
shows *nth-prime n* = *p*
⟨*proof*⟩

lemma *nth-prime-0* [*simp*]: *nth-prime 0* = *2*

⟨*proof*⟩

lemma *nth-prime-Suc*: *nth-prime* (*Suc n*) = *smallest-prime-beyond* (*Suc* (*nth-prime n*))
⟨*proof*⟩

lemmas *nth-prime-code* [*code*] = *nth-prime-0 nth-prime-Suc*

lemma *strict-mono-nth-prime*: *strict-mono nth-prime*
⟨*proof*⟩

lemma *nth-prime-le-iff* [*simp*]: *nth-prime m* ≤ *nth-prime n* ⟷ *m* ≤ *n*
⟨*proof*⟩

lemma *nth-prime-less-iff* [*simp*]: *nth-prime m* < *nth-prime n* ⟷ *m* < *n*
⟨*proof*⟩

lemma *nth-prime-eq-iff* [*simp*]: *nth-prime m* = *nth-prime n* ⟷ *m* = *n*
⟨*proof*⟩

lemma *nth-prime-ge-2*: *nth-prime n* ≥ *2*
⟨*proof*⟩

lemma *nth-prime-lower-bound*: *nth-prime n* ≥ *Suc* (*Suc n*)
⟨*proof*⟩

lemma *nth-prime-at-top*: *filterlim nth-prime at-top at-top*
⟨*proof*⟩

lemma *π-at-top*: *filterlim π at-top at-top*
⟨*proof*⟩

An unbounded, strictly increasing sequence a_n partitions $[a_0; \infty)$ into segments of the form $[a_n; a_{n+1})$.

lemma *strict-mono-sequence-partition*:
assumes *strict-mono* (*f* :: *nat* ⇒ *'a* :: {*linorder*, *no-top*})
assumes *x* ≥ *f 0*
assumes *filterlim f at-top at-top*
shows ∃ *k*. *x* ∈ {*f k*..<*f* (*Suc k*)}
⟨*proof*⟩

lemma *nth-prime-partition*:
assumes *x* ≥ *2*
shows ∃ *k*. *x* ∈ {*nth-prime k*..<*nth-prime* (*Suc k*)}
⟨*proof*⟩

lemma *nth-prime-partition'*:
assumes *x* ≥ *2*
shows ∃ *k*. *x* ∈ {*real* (*nth-prime k*)..<*real* (*nth-prime* (*Suc k*))}

⟨*proof*⟩

lemma *between-nth-primes-imp-nonprime*:
assumes $n > \textit{nth-prime}\ k\ n < \textit{nth-prime}\ (\textit{Suc}\ k)$
shows $\neg \textit{prime}\ n$
⟨*proof*⟩

lemma *nth-prime-partition''*:
assumes $x \geq (2 :: \textit{real})$
shows $x \in \{\textit{real}\ (\textit{nth-prime}\ (\textit{nat}\ \lfloor \pi\ x \rfloor - 1))..<\textit{real}\ (\textit{nth-prime}\ (\textit{nat}\ \lfloor \pi\ x \rfloor))\}$
⟨*proof*⟩

3.4 Relations between different prime-counting functions

The ψ function can be expressed as a sum of ϑ.

lemma *ψ-altdef*:
assumes $x > 0$
shows $\psi\ x = \textit{sum-upto}\ (\lambda m.\ \textit{prime-sum-upto}\ \textit{ln}\ (\textit{root}\ m\ x))\ (\textit{log}\ 2\ x)$ (**is** - = *?rhs*)
⟨*proof*⟩

lemma *ψ-conv-ϑ-sum*: $x > 0 \Longrightarrow \psi\ x = \textit{sum-upto}\ (\lambda m.\ \vartheta\ (\textit{root}\ m\ x))\ (\textit{log}\ 2\ x)$
⟨*proof*⟩

lemma *ψ-minus-ϑ*:
assumes *x*: $x \geq 2$
shows $\psi\ x - \vartheta\ x = (\sum i \mid 2 \leq i \wedge \textit{real}\ i \leq \textit{log}\ 2\ x.\ \vartheta\ (\textit{root}\ i\ x))$
⟨*proof*⟩

The following theorems use summation by parts to relate different prime-counting functions to one another with an integral as a remainder term.

lemma *ϑ-conv-π-integral*:
assumes $x \geq 2$
shows $((\lambda t.\ \pi\ t\ /\ t)\ \textit{has-integral}\ (\pi\ x * \textit{ln}\ x - \vartheta\ x))\ \{2..x\}$
⟨*proof*⟩

lemma *π-conv-ϑ-integral*:
assumes $x \geq 2$
shows $((\lambda t.\ \vartheta\ t\ /\ (t * \textit{ln}\ t\ \hat{}\ 2))\ \textit{has-integral}\ (\pi\ x - \vartheta\ x\ /\ \textit{ln}\ x))\ \{2..x\}$
⟨*proof*⟩

lemma *integrable-weighted-ϑ*:
assumes $2 \leq a\ a \leq x$
shows $((\lambda t.\ \vartheta\ t\ /\ (t * \textit{ln}\ t\ \hat{}\ 2))\ \textit{integrable-on}\ \{a..x\})$
⟨*proof*⟩

lemma *ϑ-conv-𝔐-integral*:
assumes $x \geq 2$

shows $(\mathfrak{M}\ \textit{has-integral}\ (\mathfrak{M}\ x * x - \vartheta\ x))\ \{2..x\}$
⟨*proof*⟩

lemma $\mathfrak{M}$*-conv-*ϑ*-integral*:
assumes $x \geq 2$
shows $((\lambda t.\ \vartheta\ t\ /\ t^2)\ \textit{has-integral}\ (\mathfrak{M}\ x - \vartheta\ x\ /\ x))\ \{2..x\}$
⟨*proof*⟩

lemma *integrable-primes-M*: $\mathfrak{M}$ *integrable-on* $\{x..y\}$ **if** $2 \leq x$ **for** $x\ y :: \textit{real}$
⟨*proof*⟩

3.5 Bounds

lemma ϑ*-upper-bound-coarse*:
assumes $x \geq 1$
shows $\vartheta\ x \leq x * \ln x$
⟨*proof*⟩

lemma ϑ*-le-*ψ: $\vartheta\ x \leq \psi\ x$
⟨*proof*⟩

lemma π*-upper-bound-coarse*:
assumes $x \geq 0$
shows $\pi\ x \leq x\ /\ 3 + 2$
⟨*proof*⟩

lemma *le-numeral-iff*: $m \leq \textit{numeral}\ n \longleftrightarrow m = \textit{numeral}\ n \vee m \leq \textit{pred-numeral}\ n$
⟨*proof*⟩

The following nice proof for the upper bound $\theta(x) \leq \ln 4 \cdot x$ is taken from Otto Forster's lecture notes on Analytic Number Theory [4].

lemma *prod-primes-upto-less*:
defines $F \equiv (\lambda n.\ (\prod \{p{::}\textit{nat}.\ \textit{prime}\ p \wedge p \leq n\}))$
shows $n > 0 \Longrightarrow F\ n < 4\ \widehat{}\ n$
⟨*proof*⟩

lemma ϑ*-upper-bound*:
assumes x: $x \geq 1$
shows $\vartheta\ x < \ln 4 * x$
⟨*proof*⟩

lemma ϑ*-bigo*: $\vartheta \in O(\lambda x.\ x)$
⟨*proof*⟩

lemma ψ*-minus-*ϑ*-bound*:
assumes x: $x \geq 2$
shows $\psi\ x - \vartheta\ x \leq 2 * \ln x * \textit{sqrt}\ x$
⟨*proof*⟩

lemma *ψ-minus-ϑ-bigo*: $(\lambda x.\ \psi\ x - \vartheta\ x) \in O(\lambda x.\ ln\ x * sqrt\ x)$
⟨*proof*⟩

lemma *ψ-bigo*: $\psi \in O(\lambda x.\ x)$
⟨*proof*⟩

We shall now attempt to get some more concrete bounds on the difference between $\pi(x)$ and $\theta(x)/\ln x$ These will be essential in showing the Prime Number Theorem later.

We first need some bounds on the integral

$$\int_2^x \frac{1}{\ln^2 t}\,\mathrm{d}t$$

in order to bound the contribution of the remainder term. This integral actually has an antiderivative in terms of the logarithmic integral $\mathrm{li}(x)$, but since we do not have a formalisation of it in Isabelle, we will instead use the following ad-hoc bound given by Apostol:

lemma *integral-one-over-log-squared-bound*:
assumes *x*: $x \geq 4$
shows $integral\ \{2..x\}\ (\lambda t.\ 1\ /\ ln\ t\ \hat{}\ 2) \leq sqrt\ x\ /\ ln\ 2\ \hat{}\ 2 + 4 * x\ /\ ln\ x\ \hat{}\ 2$
⟨*proof*⟩

lemma *integral-one-over-log-squared-bigo*:
$(\lambda x{::}real.\ integral\ \{2..x\}\ (\lambda t.\ 1\ /\ ln\ t\ \hat{}\ 2)) \in O(\lambda x.\ x\ /\ ln\ x\ \hat{}\ 2)$
⟨*proof*⟩

lemma *π-ϑ-bound*:
assumes $x \geq (4 :: real)$
defines $ub \equiv 2\ /\ ln\ 2 * sqrt\ x + 8 * ln\ 2 * x\ /\ ln\ x\ \hat{}\ 2$
shows $\pi\ x - \vartheta\ x\ /\ ln\ x \in \{0..ub\}$
⟨*proof*⟩

The following statement already indicates that the asymptotics of π and ϑ are very closely related, since through it, $\pi(x) \sim x/\ln x$ and $\theta(x) \sim x$ imply each other.

lemma *π-ϑ-bigo*: $(\lambda x.\ \pi\ x - \vartheta\ x\ /\ ln\ x) \in O(\lambda x.\ x\ /\ ln\ x\ \hat{}\ 2)$
⟨*proof*⟩

As a foreshadowing of the Prime Number Theorem, we can already show the following upper bound on $\pi(x)$:

lemma *π-upper-bound*:
assumes $x \geq (4 :: real)$
shows $\pi\ x < ln\ 4 * x\ /\ ln\ x\ +\ 8 * ln\ 2 * x\ /\ ln\ x\ \hat{}\ 2\ +\ 2\ /\ ln\ 2 * sqrt\ x$
⟨*proof*⟩

lemma *π-bigo*: $\pi \in O(\lambda x.\ x\ /\ ln\ x)$
⟨*proof*⟩

3.6 Equivalence of various forms of the Prime Number Theorem

In this section, we show that the following forms of the Prime Number Theorem are all equivalent:

1. $\pi(x) \sim x/\ln x$
2. $\pi(x)\ln\pi(x) \sim x$
3. $p_n \sim n\ln n$
4. $\vartheta(x) \sim x$
5. $\psi(x) \sim x$

We show the following implication chains:

- $(1) \to (2) \to (3) \to (2) \to (1)$
- $(1) \to (4) \to (1)$
- $(4) \to (5) \to (4)$

All of these proofs are taken from Apostol's book.

lemma *PNT1-imp-PNT1'*:
assumes $\pi \sim[at\text{-}top]\ (\lambda x.\ x\ /\ ln\ x)$
shows $(\lambda x.\ ln\ (\pi\ x)) \sim[at\text{-}top]\ ln$
⟨*proof*⟩

lemma *PNT1-imp-PNT2*:
assumes $\pi \sim[at\text{-}top]\ (\lambda x.\ x\ /\ ln\ x)$
shows $(\lambda x.\ \pi\ x * ln\ (\pi\ x)) \sim[at\text{-}top]\ (\lambda x.\ x)$
⟨*proof*⟩

lemma *PNT2-imp-PNT3*:
assumes $(\lambda x.\ \pi\ x * ln\ (\pi\ x)) \sim[at\text{-}top]\ (\lambda x.\ x)$
shows $nth\text{-}prime \sim[at\text{-}top]\ (\lambda n.\ n * ln\ n)$
⟨*proof*⟩

lemma *PNT3-imp-PNT2*:
assumes $nth\text{-}prime \sim[at\text{-}top]\ (\lambda n.\ n * ln\ n)$
shows $(\lambda x.\ \pi\ x * ln\ (\pi\ x)) \sim[at\text{-}top]\ (\lambda x.\ x)$
⟨*proof*⟩

lemma *PNT2-imp-PNT1*:
assumes $(\lambda x.\ \pi\ x * ln\ (\pi\ x)) \sim[at\text{-}top]\ (\lambda x.\ x)$
shows $(\lambda x.\ ln\ (\pi\ x)) \sim[at\text{-}top]\ (\lambda x.\ ln\ x)$

and $\pi \sim[at\text{-}top]\ (\lambda x.\ x\ /\ ln\ x)$
⟨*proof*⟩

lemma *PNT4-imp-PNT5*:
assumes $\vartheta \sim[at\text{-}top]\ (\lambda x.\ x)$
shows $\psi \sim[at\text{-}top]\ (\lambda x.\ x)$
⟨*proof*⟩

lemma *PNT4-imp-PNT1*:
assumes $\vartheta \sim[at\text{-}top]\ (\lambda x.\ x)$
shows $\pi \sim[at\text{-}top]\ (\lambda x.\ x\ /\ ln\ x)$
⟨*proof*⟩

lemma *PNT1-imp-PNT4*:
assumes $\pi \sim[at\text{-}top]\ (\lambda x.\ x\ /\ ln\ x)$
shows $\vartheta \sim[at\text{-}top]\ (\lambda x.\ x)$
⟨*proof*⟩

lemma *PNT5-imp-PNT4*:
assumes $\psi \sim[at\text{-}top]\ (\lambda x.\ x)$
shows $\vartheta \sim[at\text{-}top]\ (\lambda x.\ x)$
⟨*proof*⟩

3.7 The asymptotic form of Mertens' First Theorem

Mertens' first theorem states that $\mathfrak{M}(x) - \ln x$ is bounded, i. e. $\mathfrak{M}(x) = \ln x + O(1)$.

With some work, one can also show some absolute bounds for $|\mathfrak{M}(x) - \ln x|$, and we will, in fact, do this later. However, this asymptotic form is somewhat easier to obtain and it is (as we shall see) enough to prove the Prime Number Theorem, so we prove the weak form here first for the sake of a smoother presentation.

First of all, we need a very weak version of Stirling's formula for the logarithm of the factorial, namely:

$$\ln(\lfloor x \rfloor !) = \sum_{n \le x} \ln x = x \ln x + O(x)$$

We show this using summation by parts.

lemma *stirling-weak*:
assumes *x*: $x \geq 1$
shows *sum-upto ln x* $\in \{x * ln\ x - x - ln\ x + 1\ ..\ x * ln\ x\}$
⟨*proof*⟩

lemma *stirling-weak-bigo*: $(\lambda x{::}real.\ sum\text{-}upto\ ln\ x - x * ln\ x) \in O(\lambda x.\ x)$
⟨*proof*⟩

lemma *floor-floor-div-eq*:

fixes x :: *real* **and** d :: *nat*
assumes $x \geq 0$
shows $\lfloor nat\ \lfloor x \rfloor\ /\ real\ d \rfloor = \lfloor x\ /\ real\ d \rfloor$
⟨*proof*⟩

The key to showing Mertens' first theorem is the function

$$h(x) := \sum_{n \leq x} \frac{\Lambda(d)}{d}$$

where Λ is the Mangoldt function, which is equal to $\ln p$ for any prime power p^k and 0 otherwise. As we shall see, $h(x)$ is a good approximation for $\mathfrak{M}(x)$, as the difference between them is bounded by a constant.

lemma *sum-upto-mangoldt-over-id-minus-phi-bounded*:
$(\lambda x.\ sum\text{-}upto\ (\lambda d.\ mangoldt\ d\ /\ real\ d)\ x - \mathfrak{M}\ x) \in O(\lambda\text{-}.\ 1)$
⟨*proof*⟩

Next, we show that our $h(x)$ itself is close to $\ln x$, i. e.:

$$\sum_{n \leq x} \frac{\Lambda(d)}{d} = \ln x + O(1)$$

lemma *sum-upto-mangoldt-over-id-asymptotics*:
$(\lambda x.\ sum\text{-}upto\ (\lambda d.\ mangoldt\ d\ /\ real\ d)\ x - ln\ x) \in O(\lambda\text{-}.\ 1)$
⟨*proof*⟩

Combining these two gives us Mertens' first theorem.

theorem *mertens-bounded*: $(\lambda x.\ \mathfrak{M}\ x - ln\ x) \in O(\lambda\text{-}.\ 1)$
⟨*proof*⟩

lemma *primes-M-bigo*: $\mathfrak{M} \in O(\lambda x.\ ln\ x)$
⟨*proof*⟩
end

4 The Prime Number Theorem

theory *Prime-Number-Theorem*
imports
Newman-Ingham-Tauberian
Prime-Counting-Functions
begin

4.1 Constructing Newman's function

Starting from Mertens' first theorem, i. e. $\mathfrak{M}(x) = \ln x + O(1)$, we now want to derive that $\mathfrak{M}(x) = \ln x + c + o(1)$. This result is considerably stronger and it implies the Prime Number Theorem quite directly.

In order to do this, we define the Dirichlet series

$$f(s) = \sum_{n=1}^{\infty} \frac{\mathfrak{M}(n)}{n^s} \ .$$

We will prove that this series extends meromorphically to $\Re(s) \geq 1$ and apply Ingham's theorem to it (after we subtracted its pole at $s = 1$).

definition *fds-newman* **where**
fds-newman = *fds* (λ*n*. *complex-of-real* (𝔐 *n*))

lemma *fds-nth-newman*:
fds-nth fds-newman n = *of-real* (𝔐 *n*)
⟨*proof*⟩

lemma *norm-fds-nth-newman*:
norm (*fds-nth fds-newman n*) = 𝔐 *n*
⟨*proof*⟩

The Dirichlet series $f(s) + \zeta'(s)$ has the coefficients $\mathfrak{M}(n) - \ln n$, so by Mertens' first theorem, $f(s) + \zeta'(s)$ has bounded coefficients.

lemma *bounded-coeffs-newman-minus-deriv-zeta*:
defines *f* ≡ *fds-newman* + *fds-deriv fds-zeta*
shows *Bseq* (λ*n*. *fds-nth f n*)
⟨*proof*⟩

A Dirichlet series with bounded coefficients converges for all s with $\Re(s) > 1$ and so does $\zeta'(s)$, so we can conclude that $f(s)$ does as well.

lemma *abs-conv-abscissa-newman*: *abs-conv-abscissa fds-newman* ≤ *1*
and *conv-abscissa-newman*: *conv-abscissa fds-newman* ≤ *1*
⟨*proof*⟩

We now change the order of summation to obtain an alternative form of $f(s)$ in terms of a sum of Hurwitz ζ functions.

lemma *eval-fds-newman-conv-infsetsum*:
assumes *s*: *Re s* > *1*
shows *eval-fds fds-newman s* = (∑ *a p* | *prime p*. (*ln* (*real p*) / *real p*) ∗ *hurwitz-zeta p s*)
(λ*p*. *ln* (*real p*) / *real p* ∗ *hurwitz-zeta p s*) *abs-summable-on* {*p*. *prime p*}
⟨*proof*⟩

We now define a meromorphic continuation of $f(s)$ on $\Re(s) > \frac{1}{2}$.
To construct $f(s)$, we express it as

$$f(s) = \frac{1}{z-1}\left(\bar{f}(s) - \frac{\zeta'(s)}{\zeta(s)}\right) \ ,$$

where $\bar{f}(s)$ (which we shall call *pre-newman*) is a function that is analytic on $\Re(s) > \frac{1}{2}$, which can be shown fairly easily using the Weierstraß M test.

$\zeta'(s)/\zeta(s)$ is meromorphic except for a single pole at $s = 1$ and one k-th order pole for any k-th order zero of ζ, but for the Prime Number Theorem, we are only concerned with the area $\Re(s) \geq 1$, where ζ does not have any zeros.

Taken together, this means that $f(s)$ is analytic for $\Re(s) \geq 1$ except for a double pole at $s = 1$, which we will take care of later.

context
  fixes *A* :: *nat* ⇒ *complex* ⇒ *complex* **and** *B* :: *nat* ⇒ *complex* ⇒ *complex*
  defines *A* ≡ (λ*p s*. (*s* − *1*) ∗ *pre-zeta* (*real p*) *s* −
                    of-nat p / (*of-nat p powr s* ∗ (*of-nat p powr s* − *1*)))
  defines *B* ≡ (λ*p s*. *of-real* (*ln* (*real p*)) / *of-nat p* ∗ *A p s*)
begin

definition *pre-newman* :: *complex* ⇒ *complex* **where**
  pre-newman s = (∑ *p*. *if prime p then B p s else 0*)

definition *newman* **where** *newman s* = *1* / (*s* − *1*) ∗ (*pre-newman s* − *deriv zeta s* / *zeta s*)

The sum used in the definition of *pre-newman* converges uniformly on any disc within the half-space with $\Re(s) > \frac{1}{2}$ by the Weierstraß M test.

lemma *uniform-limit-pre-newman*:
  assumes *r*: *r* ≥ *0 Re s* − *r* > *1* / *2*
  shows *uniform-limit* (*cball s r*)
        (λ*n s*. ∑ *p*<*n*. *if prime p then B p s else 0*) *pre-newman at-top*
⟨*proof*⟩

lemma *sums-pre-newman*: *Re s* > *1* / *2* ⟹ (λ*p*. *if prime p then B p s else 0*) *sums pre-newman s*
  ⟨*proof*⟩

lemma *analytic-pre-newman* [*THEN analytic-on-subset*, *analytic-intros*]:
  pre-newman analytic-on {*s*. *Re s* > *1* / *2*}
⟨*proof*⟩

lemma *holomorphic-pre-newman* [*holomorphic-intros*]:
  X ⊆ {*s*. *Re s* > *1* / *2*} ⟹ *pre-newman holomorphic-on X*
  ⟨*proof*⟩

lemma *eval-fds-newman*:
  assumes *s*: *Re s* > *1*
  shows *eval-fds fds-newman s* = *newman s*
⟨*proof*⟩

end

Next, we shall attempt to get rid of the pole by subtracting suitable multiples of $\zeta(s)$ and $\zeta'(s)$. To this end, we shall first prove the following alternative

definition of $\zeta'(s)$:

lemma *deriv-zeta-eq'*:
assumes *0 < Re s s ≠ 1*
shows *deriv zeta s = deriv (λz. pre-zeta 1 z * (z − 1)) s / (s − 1) −*
*(pre-zeta 1 s * (s − 1) + 1) / (s − 1)²*
(**is** - = *?rhs*)
⟨*proof*⟩

From this, it follows that $(s-1)\zeta'(s) - \zeta'(s)/\zeta(s)$ is analytic for $\Re(s) \geq 1$:

lemma *analytic-zeta-derivdiff*:
obtains *a* **where**
*(λz. if z = 1 then a else (z − 1) * deriv zeta z − deriv zeta z / zeta z)*
analytic-on {s. Re s ≥ 1}
⟨*proof*⟩

Finally, $f(s) + \zeta'(s) + c\zeta(s)$ is analytic.

lemma *analytic-newman-variant*:
obtains *c a* **where**
*(λz. if z = 1 then a else newman z + deriv zeta z + c * zeta z) analytic-on {s. Re s ≥ 1}*
⟨*proof*⟩

4.2 The asymptotic expansion of $\mathfrak{M}$

Our next goal is to show the key result that $\mathfrak{M}(x) = \ln n + c + o(1)$.

As a first step, we invoke Ingham's Tauberian theorem on the function we have just defined and obtain that the sum

$$\sum_{n=1}^{\infty} \frac{\mathfrak{M}(n) - \ln n + c}{n}$$

exists.

lemma *mertens-summable*:
obtains *c :: real* **where** *summable (λn. (𝔐 n − ln n + c) / n)*
⟨*proof*⟩

Next, we prove a lemma given by Newman stating that if the sum $\sum a_n/n$ exists and $a_n + \ln n$ is nondecreasing, then a_n must tend to 0. Unfortunately, the proof is rather tedious, but so is the paper version by Newman.

lemma *sum-goestozero-lemma*:
fixes *d::real*
assumes *d*: *|∑ i = M..N. a i / i| < d* **and** *le*: *⋀n. a n + ln n ≤ a (Suc n) + ln (Suc n)*
and *0 < M M < N*
shows *a M ≤ d * N / (real N − real M) + (real N − real M) / M ∧*
*−a N ≤ d * N / (real N − real M) + (real N − real M) / M*

⟨*proof*⟩

proposition *sum-goestozero-theorem*:
assumes *summ*: *summable* (λ*i*. *a i* / *i*)
and *le*: ⋀*n*. *a n* + *ln n* ≤ *a* (*Suc n*) + *ln* (*Suc n*)
shows *a* ⟶ *0*
⟨*proof*⟩

This leads us to the main intermediate result:

lemma *Mertens-convergent*: *convergent* (λ*n*::*nat*. 𝔐 *n* − *ln n*)
⟨*proof*⟩

corollary 𝔐-*minus-ln-limit*:
obtains *c* **where** ((λ*x*::*real*. 𝔐 *x* − *ln x*) ⟶ *c*) *at-top*
⟨*proof*⟩

4.3 The asymptotics of the prime-counting functions

We will now use the above result to prove the asymptotics of the prime-counting functions $\vartheta(x) \sim x$, $\psi(x) \sim x$, and $\pi(x) \sim x/\ln x$. The last of these is typically called the Prime Number Theorem, but since these functions can be expressed in terms of one another quite easily, knowing the asymptotics of any of them immediately gives the asymptotics of the other ones.

In this sense, all of the above are equivalent formulations of the Prime Number Theorem. The one we shall tackle first, due to its strong connection to the $\mathfrak{M}$ function, is $\vartheta(x) \sim x$.

We know that $\mathfrak{M}(x)$ has the asymptotic expansion $\mathfrak{M}(x) = \ln x + c + o(1)$. We also know that

$$\vartheta(x) = x\mathfrak{M}(x) - \int_2^x \mathfrak{M}(t)\,\mathrm{d}t\ .$$

Substituting in the above asymptotic equation, we obtain:

$$\begin{aligned}\vartheta(x) &= x\ln x + cx + o(x) - \int_2^x \ln t + c + o(1)\,\mathrm{d}t\\ &= x\ln x + cx + o(x) - (x\ln x - x + cx + o(x))\\ &= x + o(x)\end{aligned}$$

In conclusion, $\vartheta(x) \sim x$.

theorem ϑ-*asymptotics*: ϑ ∼[*at-top*] (λ*x*. *x*)
⟨*proof*⟩

The various other forms of the Prime Number Theorem follow as simple corollaries.

corollary ψ-*asymptotics*: ψ ∼[*at-top*] (λ*x*. *x*)

⟨*proof*⟩

corollary *prime-number-theorem*: $\pi \sim[at\text{-}top]\ (\lambda x.\ x\ /\ ln\ x)$
⟨*proof*⟩

corollary *ln-π-asymptotics*: $(\lambda x.\ ln\ (\pi\ x)) \sim[at\text{-}top]\ ln$
⟨*proof*⟩

corollary *π-ln-π-asymptotics*: $(\lambda x.\ \pi\ x * ln\ (\pi\ x)) \sim[at\text{-}top]\ (\lambda x.\ x)$
⟨*proof*⟩

corollary *nth-prime-asymptotics*: $(\lambda n.\ real\ (nth\text{-}prime\ n)) \sim[at\text{-}top]\ (\lambda n.\ real\ n * ln\ (real\ n))$
⟨*proof*⟩

The following versions use a little less notation.

corollary *prime-number-theorem′*: $((\lambda x.\ \pi\ x\ /\ (x\ /\ ln\ x)) \longrightarrow 1)\ at\text{-}top$
⟨*proof*⟩

corollary *prime-number-theorem″*:
$(\lambda x.\ card\ \{p.\ prime\ p \wedge real\ p \leq x\}) \sim[at\text{-}top]\ (\lambda x.\ x\ /\ ln\ x)$
⟨*proof*⟩

corollary *prime-number-theorem‴*:
$(\lambda n.\ card\ \{p.\ prime\ p \wedge p \leq n\}) \sim[at\text{-}top]\ (\lambda n.\ real\ n\ /\ ln\ (real\ n))$
⟨*proof*⟩
end

5 Mertens' Theorems

theory *Mertens-Theorems*
imports
Prime-Counting-Functions
Stirling-Formula.Stirling-Formula
begin

In this section, we will prove Mertens' First and Second Theorem. These are weaker results than the Prime Number Theorem, and we will derive them without using it.

However, like Mertens himself, we will not only prove them *asymptotically*, but *absolutely*. This means that we will show that the remainder terms are not only "Big-O" of some bound, but we will give concrete (and reasonably tight) upper and lower bounds for them that hold on the entire domain. This makes the proofs a bit more tedious.

5.1 Absolute Bounds for Mertens' First Theorem

We have already shown the asymptotic form of Mertens' first theorem, i. e. $\mathfrak{M}(n) = \ln n + O(1)$. We now want to obtain some absolute bounds on the $O(1)$ remainder term using a more careful derivation than before.

The precise bounds we will show are $\mathfrak{M}(n) - \ln n \in (-1 - \frac{9}{\pi^2}; \ln 4] \approx (-1.9119; 1.3863]$ for $n \in \mathbb{N}$.

First, we need a simple lemma on the finiteness of exponents to consider in a sum of all prime powers up to a certain point:

lemma *exponents-le-finite*:
  assumes $p > (1 :: nat)$ $k > 0$
  shows *finite* $\{i.\ real\ (p\ \hat{}\ (k * i + l)) \leq x\}$
⟨*proof*⟩

Next, we need the following bound on $\zeta'(2)$:

lemma *deriv-zeta-2-bound*: *Re* (*deriv zeta 2*) > −*1*
⟨*proof*⟩

Using the logarithmic derivative of Euler's product formula for $\zeta(s)$ at $s = 2$ and the bound on $\zeta'(2)$ we have just derived, we can obtain the bound

$$\sum_{p^i \leq x, i \geq 2} \frac{\ln p}{p^i} < \frac{9}{\pi^2}\ .$$

lemma *mertens-remainder-aux-bound*:
  fixes $x :: real$
  defines $R \equiv (\sum (p,i) \mid prime\ p \wedge i > 1 \wedge real\ (p\ \hat{}\ i) \leq x.\ ln\ (real\ p)\ /\ p\ \hat{}\ i)$
  shows $R < 9\ /\ pi^2$
⟨*proof*⟩

We now consider the equation

$$\ln(n!) = \sum_{k \leq n} \Lambda(k) \left\lfloor \frac{n}{k} \right\rfloor$$

and estimate both sides in different ways. The left-hand-side can be estimated using Stirling's formula, and we can simplify the right-hand side to

$$\sum_{k \leq n} \Lambda(k) \left\lfloor \frac{n}{k} \right\rfloor = \sum_{p^i \leq x, i \geq 1} \ln p \left\lfloor \frac{n}{p^i} \right\rfloor$$

and then split the sum into those p^i with $i = 1$ and those with $i \geq 2$. Applying the bound we have just shown and some more routine estimates, we obtain the following reasonably strong version of Mertens' First Theorem on the naturals: $\mathfrak{M}(n) - \ln(n) \in (-1 - \frac{9}{\pi^2}; \ln 4]$

theorem *mertens-bound-strong*:

fixes n :: *nat* **assumes** n: $n > 0$
shows $\mathfrak{M}\ n - ln\ n \in \{-1 - 9 / pi^2 <..< ln\ 4\}$
⟨*proof*⟩

As a simple corollary, we obtain a similar bound on the reals.

lemma *mertens-bound-real-strong*:
fixes x :: *real* **assumes** x: $x \geq 1$
shows $\mathfrak{M}\ x - ln\ x \in \{-1 - 9 / pi\ \hat{}\ 2 - ln\ (1 + frac\ x / real\ (nat\ \lfloor x \rfloor)) <.. ln\ 4\}$
⟨*proof*⟩

We weaken this estimate a bit to obtain nicer bounds:

lemma *mertens-bound-real'*:
fixes x :: *real* **assumes** x: $x \geq 1$
shows $\mathfrak{M}\ x - ln\ x \in \{-2 <..< 25/18\}$
⟨*proof*⟩

corollary *mertens-first-theorem*:
fixes x :: *real* **assumes** x: $x \geq 1$
shows $|\mathfrak{M}\ x - ln\ x| < 2$
⟨*proof*⟩

5.2 Mertens' Second Theorem

Mertens' Second Theorem concerns the asymptotics of the Prime Harmonic Series, namely

$$\sum_{p \leq x} \frac{1}{p} = \ln \ln x + M + O\left(\frac{1}{\ln x}\right)$$

where $M \approx 0.261497$ is the Meissel–Mertens constant.

We define the constant in the following way:

definition *meissel-mertens* **where**
meissel-mertens = $1 - ln\ (ln\ 2) + integral\ \{2..\}\ (\lambda t.\ (\mathfrak{M}\ t - ln\ t) / (t * ln\ t\ \hat{}\ 2))$

We will require the value of the integral $\int_a^\infty \frac{t}{\ln^2 t} \mathrm{d}t = \frac{1}{\ln a}$ as an upper bound on the remainder term:

lemma *integral-one-over-x-ln-x-squared*:
assumes a: $(a::real) > 1$
shows *set-integrable lborel* $\{a<..\}$ $(\lambda t.\ 1 / (t * ln\ t\ \hat{}\ 2))$ (**is** *?th1*)
and *set-lebesgue-integral lborel* $\{a<..\}$ $(\lambda t.\ 1 / (t * ln\ t\ \hat{}\ 2)) = 1 / ln\ a$ (**is** *?th2*)
and $((\lambda t.\ 1 / (t * (ln\ t)^2))$ *has-integral* $1 / ln\ a)$ $\{a<..\}$ (**is** *?th3*)
⟨*proof*⟩

We show that the integral in our definition of the Meissel–Mertens constant is well-defined and give an upper bound for its tails:

lemma
  assumes $a > (1 :: real)$
  defines $r \equiv (\lambda t.\ (\mathfrak{M}\ t - ln\ t)\ /\ (t * ln\ t\ \widehat{}\ 2))$
  shows *integrable-meissel-mertens*: *set-integrable lborel* $\{a<..\}$ r
    and *meissel-mertens-integral-le*: *norm* (*integral* $\{a<..\}$ r) $\leq$ $2\ /\ ln\ a$
⟨*proof*⟩

lemma *integrable-on-meissel-mertens*:
  assumes $A \subseteq \{1..\}$ *Inf* $A > 1$ $A \in$ *sets borel*
  shows $(\lambda t.\ (\mathfrak{M}\ t - ln\ t)\ /\ (t * ln\ t\ \widehat{}\ 2))$ *integrable-on* A
⟨*proof*⟩

lemma *meissel-mertens-bounds*: $|meissel\text{-}mertens - 1 + ln\ (ln\ 2)| \leq 2\ /\ ln\ 2$
⟨*proof*⟩

Finally, obtaining Mertens' second theorem from the first one is nothing but a routine summation by parts, followed by a use of the above bound:

theorem *mertens-second-theorem*:
  defines $f \equiv$ *prime-sum-upto* $(\lambda p.\ 1\ /\ p)$
  shows $\bigwedge x.\ x \geq 2 \Longrightarrow |f\ x - ln\ (ln\ x) - meissel\text{-}mertens| \leq 4\ /\ ln\ x$
    and $(\lambda x.\ f\ x - ln\ (ln\ x) - meissel\text{-}mertens) \in O(\lambda x.\ 1\ /\ ln\ x)$
⟨*proof*⟩

corollary *prime-harmonic-asymp-equiv*: *prime-sum-upto* $(\lambda p.\ 1\ /\ p) \sim[at\text{-}top]\ (\lambda x.\ ln\ (ln\ x))$
⟨*proof*⟩

As a corollary, we get the divergence of the prime harmonic series.

corollary *prime-harmonic-diverges*: *filterlim* (*prime-sum-upto* $(\lambda p.\ 1\ /\ p)$) *at-top at-top*
  ⟨*proof*⟩
end

6 Acknowledgements

Paulson was supported by the ERC Advanced Grant ALEXANDRIA (Project 742178) funded by the European Research Council at the University of Cambridge, UK.

References

[1] T. M. Apostol. *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics. Springer-Verlag, 1976.

[2] J. Avigad, K. Donnelly, D. Gray, and P. Raff. A formally verified proof of the prime number theorem. *ACM Trans. Comput. Logic*, 9(1), Dec. 2007.

[3] M. Carneiro. Formalization of the prime number theorem and dirichlet's theorem. In *Proceedings of the 9th Conference on Intelligent Computer Mathematics (CICM 2016)*, pages 10–13, 2016.

[4] O. Forster. Analytic Number Theory (lecture notes). http://www.mathematik.uni-muenchen.de/~forster/v/ann/annth_all.pdf.

[5] J. Harrison. Formalizing an analytic proof of the Prime Number Theorem (dedicated to Mike Gordon on the occasion of his 60th birthday). *Journal of Automated Reasoning*, 43:243–261, 2009.

[6] D. Newman. *Analytic Number Theory*. Number 177 in Graduate Texts in Mathematics. Springer, 1998.