Elementary Facts About the Distribution of Primes

Manuel Eberl

May 26, 2024

Abstract

This entry is a formalisation of Chapter 4 (and parts of Chapter 3) of Apostol's *Introduction to Analytic Number Theory*. The main topics that are addressed are properties of the distribution of prime numbers that can be shown in an elementary way (i. e. without the Prime Number Theorem), the various equivalent forms of the PNT (which imply each other in elementary ways), and consequences that follow from the PNT in elementary ways. The latter include bounds for the number of distinct prime factors of n, the divisor function $d(n)$, Euler's totient function $\varphi(n)$, and $\mathrm{lcm}(1, \ldots, n)$.

Contents

1 Auxiliary material

theory *Prime-Distribution-Elementary-Library*
imports
Zeta-Function.Zeta-Function
Prime-Number-Theorem.Prime-Counting-Functions
Stirling-Formula.Stirling-Formula
begin

lemma *divisor-count-pos* [*intro*]: *n* > *0* ⟹ *divisor-count n* > *0*
⟨*proof*⟩

lemma *divisor-count-eq-0-iff* [*simp*]: *divisor-count n* = *0* ⟷ *n* = *0*
⟨*proof*⟩

lemma *divisor-count-pos-iff* [*simp*]: *divisor-count n* > *0* ⟷ *n* > *0*
⟨*proof*⟩

lemma *smallest-prime-beyond-eval*:
prime n ⟹ *smallest-prime-beyond n* = *n*
¬*prime n* ⟹ *smallest-prime-beyond n* = *smallest-prime-beyond* (*Suc n*)
⟨*proof*⟩

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

lemmas *nth-prime-eval* = *smallest-prime-beyond-eval nth-prime-Suc nth-prime-numeral*

lemma *nth-prime-1* [*simp*]: *nth-prime* (*Suc 0*) = *3*
⟨*proof*⟩

lemma *nth-prime-2* [*simp*]: *nth-prime 2* = *5*
⟨*proof*⟩

lemma *nth-prime-3* [*simp*]: *nth-prime 3* = *7*
⟨*proof*⟩

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 $\exists k.\ x \in \{nth\text{-}prime\ k..{<}nth\text{-}prime\ (Suc\ k)\}$
⟨*proof*⟩

lemma *nth-prime-partition′*:
assumes $x \geq 2$
shows $\exists k.\ x \in \{real\ (nth\text{-}prime\ k)..{<}real\ (nth\text{-}prime\ (Suc\ k))\}$
⟨*proof*⟩

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

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

lemma *asymp-equivD-strong*:
assumes $f \sim[F]\ g\ eventually\ (\lambda x.\ f\ x \neq 0 \vee g\ x \neq 0)\ F$
shows $((\lambda x.\ f\ x\ /\ g\ x) \longrightarrow 1)\ F$
⟨*proof*⟩

lemma *hurwitz-zeta-shift*:
fixes $s :: complex$
assumes $a > 0$ **and** $s \neq 1$
shows $hurwitz\text{-}zeta\ (a + real\ n)\ s = hurwitz\text{-}zeta\ a\ s - (\sum k{<}n.\ (a + real\ k)\ powr\ -s)$
⟨*proof*⟩

lemma *pbernpoly-bigo*: $pbernpoly\ n \in O(\lambda\text{-}.\ 1)$
⟨*proof*⟩

lemma *harm-le*: $n \geq 1 \Longrightarrow harm\ n \leq ln\ n + 1$
⟨*proof*⟩

lemma *sum-upto-1* [*simp*]: $sum\text{-}upto\ f\ 1 = f\ 1$
⟨*proof*⟩

lemma *sum-upto-cong′* [*cong*]:
$(\bigwedge n.\ n > 0 \Longrightarrow real\ n \leq x \Longrightarrow f\ n = f'\ n) \Longrightarrow x = x' \Longrightarrow sum\text{-}upto\ f\ x = sum\text{-}upto\ f'\ x'$
⟨*proof*⟩

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

$\langle proof \rangle$

lemma *frequently-filtermap*: *frequently P* (*filtermap f F*) = *frequently* (λn. *P* (*f n*)) *F*
$\langle proof \rangle$

lemma *frequently-mono-filter*: *frequently P F* $\Longrightarrow$ $F \le F'$ $\Longrightarrow$ *frequently P* F'
$\langle proof \rangle$

lemma π*-at-top*: *filterlim primes-pi at-top at-top*
$\langle proof \rangle$

lemma *sum-upto-ln-stirling-weak-bigo*: (λx. *sum-upto ln x* $-$ $x * ln\ x + x$) $\in O(ln)$
$\langle proof \rangle$

1.1 Various facts about Dirichlet series

lemma *fds-mangoldt'*:
fds mangoldt = *fds-zeta* $*$ *fds-deriv* (*fds moebius-mu*)
$\langle proof \rangle$

lemma *sum-upto-divisor-sum1*:
sum-upto (λn. $\sum d \mid d$ *dvd n. f d* :: *real*) *x* = *sum-upto* (λn. *f n* $*$ *floor* (x / n)) *x*
$\langle proof \rangle$

lemma *sum-upto-divisor-sum2*:
sum-upto (λn. $\sum d \mid d$ *dvd n. f d* :: *real*) *x* = *sum-upto* (λn. *sum-upto f* (x / n)) *x*
$\langle proof \rangle$

lemma *sum-upto-moebius-times-floor-linear*:
sum-upto (λn. *moebius-mu n* $*$ $\lfloor x$ / *real n*$\rfloor$) *x* = (*if* $x \ge 1$ *then 1 else 0*)
$\langle proof \rangle$

lemma *ln-fact-conv-sum-mangoldt*:
sum-upto (λn. *mangoldt n* $*$ $\lfloor x$ / *real n*$\rfloor$) *x* = *ln* (*fact* (*nat* $\lfloor x \rfloor$))
$\langle proof \rangle$

1.2 Facts about prime-counting functions

lemma *abs-*π [*simp*]: |*primes-pi x*| = *primes-pi x*
$\langle proof \rangle$

lemma π*-less-self*:
includes *prime-counting-notation*
assumes $x > 0$
shows $\pi\ x < x$
$\langle proof \rangle$

lemma *π-le-self'*:
  includes *prime-counting-notation*
  assumes $x \geq 1$
  shows $\pi\ x \leq x - 1$
⟨*proof*⟩

lemma *π-le-self*:
  includes *prime-counting-notation*
  assumes $x \geq 0$
  shows $\pi\ x \leq x$
  ⟨*proof*⟩

1.3 Strengthening 'Big-O' bounds

The following two statements are crucial: They allow us to strengthen a 'Big-O' statement for $n \to \infty$ or $x \to \infty$ to a bound for *all* $n \geq n_0$ or all $x \geq x_0$ under some mild conditions.

This allows us to use all the machinery of asymptotics in Isabelle and still get a bound that is applicable over the full domain of the function in the end. This is important because Newman often shows that $f(x) \in O(g(x))$ and then writes

$$\sum_{n \leq x} f(\frac{x}{n}) = \sum_{n \leq x} O(g(\frac{x}{n}))$$

which is not easy to justify otherwise.

lemma *natfun-bigoE*:
  fixes $f :: nat \Rightarrow$ -
  assumes *bigo*: $f \in O(g)$ **and** *nz*: $\bigwedge n.\ n \geq n0 \Longrightarrow g\ n \neq 0$
  obtains c **where** $c > 0\ \bigwedge n.\ n \geq n0 \Longrightarrow norm\ (f\ n) \leq c * norm\ (g\ n)$
⟨*proof*⟩

lemma *bigoE-bounded-real-fun*:
  fixes $f\ g :: real \Rightarrow real$
  assumes $f \in O(g)$
  assumes $\bigwedge x.\ x \geq x0 \Longrightarrow |g\ x| \geq cg\ cg > 0$
  assumes $\bigwedge b.\ b \geq x0 \Longrightarrow bounded\ (f\ `\ \{x0..b\})$
  shows $\exists c{>}0.\ \forall x{\geq}x0.\ |f\ x| \leq c * |g\ x|$
⟨*proof*⟩

lemma *sum-upto-asymptotics-lift-nat-real-aux*:
  fixes $f :: nat \Rightarrow real$ **and** $g :: real \Rightarrow real$
  assumes *bigo*: $(\lambda n.\ (\sum k{=}1..n.\ f\ k) - g\ (real\ n)) \in O(\lambda n.\ h\ (real\ n))$
  assumes *g-bigo-self*: $(\lambda n.\ g\ (real\ n) - g\ (real\ (Suc\ n))) \in O(\lambda n.\ h\ (real\ n))$
  assumes *h-bigo-self*: $(\lambda n.\ h\ (real\ n)) \in O(\lambda n.\ h\ (real\ (Suc\ n)))$
  assumes *h-pos*: $\bigwedge x.\ x \geq 1 \Longrightarrow h\ x > 0$
  assumes *mono-g*: $mono\text{-}on\ \{1..\}\ g \vee mono\text{-}on\ \{1..\}\ (\lambda x.\ - g\ x)$
  assumes *mono-h*: $mono\text{-}on\ \{1..\}\ h \vee mono\text{-}on\ \{1..\}\ (\lambda x.\ - h\ x)$
  shows $\exists c{>}0.\ \forall x{\geq}1.\ sum\text{-}upto\ f\ x - g\ x \leq c * h\ x$

⟨*proof*⟩

lemma *sum-upto-asymptotics-lift-nat-real*:
fixes f :: *nat* ⇒ *real* **and** g :: *real* ⇒ *real*
assumes *bigo*: $(\lambda n.\ (\sum k{=}1..n.\ f\ k) - g\ (real\ n)) \in O(\lambda n.\ h\ (real\ n))$
assumes *g-bigo-self*: $(\lambda n.\ g\ (real\ n) - g\ (real\ (Suc\ n))) \in O(\lambda n.\ h\ (real\ n))$
assumes *h-bigo-self*: $(\lambda n.\ h\ (real\ n)) \in O(\lambda n.\ h\ (real\ (Suc\ n)))$
assumes *h-pos*: $\bigwedge x.\ x \geq 1 \Longrightarrow h\ x > 0$
assumes *mono-g*: *mono-on* {*1..*} g ∨ *mono-on* {*1..*} $(\lambda x.\ -\ g\ x)$
assumes *mono-h*: *mono-on* {*1..*} h ∨ *mono-on* {*1..*} $(\lambda x.\ -\ h\ x)$
shows $\exists c{>}0.\ \forall x{\geq}1.\ |sum\text{-}upto\ f\ x - g\ x| \leq c * h\ x$
⟨*proof*⟩

lemma (**in** *factorial-semiring*) *primepow-divisors-induct* [*case-names zero unit factor*]:
assumes $P\ 0$ $\bigwedge x.\ is\text{-}unit\ x \Longrightarrow P\ x$
$\bigwedge p\ k\ x.\ prime\ p \Longrightarrow k > 0 \Longrightarrow \neg p\ dvd\ x \Longrightarrow P\ x \Longrightarrow P\ (p\ \hat{}\ k * x)$
shows $P\ x$
⟨*proof*⟩

end

2 Miscellaneous material

theory *More-Dirichlet-Misc*
imports
Prime-Distribution-Elementary-Library
Prime-Number-Theorem.Prime-Counting-Functions
begin

2.1 Generalised Dirichlet products

definition *dirichlet-prod'* :: (*nat* ⇒ *'a* :: *comm-semiring-1*) ⇒ (*real* ⇒ *'a*) ⇒ *real* ⇒ *'a* **where**
dirichlet-prod' $f\ g\ x$ = *sum-upto* $(\lambda m.\ f\ m * g\ (x\ /\ real\ m))\ x$

lemma *dirichlet-prod'-one-left*:
dirichlet-prod' $(\lambda n.\ if\ n = 1\ then\ 1\ else\ 0)\ f\ x = (if\ x \geq 1\ then\ f\ x\ else\ 0)$
⟨*proof*⟩

lemma *dirichlet-prod'-cong*:
assumes $\bigwedge n.\ n > 0 \Longrightarrow real\ n \leq x \Longrightarrow f\ n = f'\ n$
assumes $\bigwedge y.\ y \geq 1 \Longrightarrow y \leq x \Longrightarrow g\ y = g'\ y$
assumes $x = x'$
shows *dirichlet-prod'* $f\ g\ x$ = *dirichlet-prod'* $f'\ g'\ x'$
⟨*proof*⟩

lemma *dirichlet-prod'-assoc*:

dirichlet-prod′ f (*λy. dirichlet-prod′ g h y*) *x* = *dirichlet-prod′* (*dirichlet-prod f g*) *h x*
⟨*proof*⟩

lemma *dirichlet-prod′-inversion1*:
assumes ∀ *x*≥*1*. *g x* = *dirichlet-prod′ a f x x* ≥ *1*
dirichlet-prod a ainv = (*λn. if n* = *1 then 1 else 0*)
shows *f x* = *dirichlet-prod′ ainv g x*
⟨*proof*⟩

lemma *dirichlet-prod′-inversion2*:
assumes ∀ *x*≥*1*. *f x* = *dirichlet-prod′ ainv g x x* ≥ *1*
dirichlet-prod a ainv = (*λn. if n* = *1 then 1 else 0*)
shows *g x* = *dirichlet-prod′ a f x*
⟨*proof*⟩

lemma *dirichlet-prod′-inversion*:
assumes *dirichlet-prod a ainv* = (*λn. if n* = *1 then 1 else 0*)
shows (∀ *x*≥*1*. *g x* = *dirichlet-prod′ a f x*) ⟷ (∀ *x*≥*1*. *f x* = *dirichlet-prod′ ainv g x*)
⟨*proof*⟩

lemma *dirichlet-prod′-inversion′*:
assumes *a 1* ∗ *y* = *1*
defines *ainv* ≡ *dirichlet-inverse a y*
shows (∀ *x*≥*1*. *g x* = *dirichlet-prod′ a f x*) ⟷ (∀ *x*≥*1*. *f x* = *dirichlet-prod′ ainv g x*)
⟨*proof*⟩

lemma *dirichlet-prod′-floor-conv-sum-upto*:
dirichlet-prod′ f (*λx. real-of-int* (*floor x*)) *x* = *sum-upto* (*λn. sum-upto f* (*x* / *n*)) *x*
⟨*proof*⟩

lemma (**in** *completely-multiplicative-function*) *dirichlet-prod-self*:
dirichlet-prod f f n = *f n* ∗ *of-nat* (*divisor-count n*)
⟨*proof*⟩

lemma *completely-multiplicative-imp-moebius-mu-inverse*:
fixes *f* :: *nat* ⇒ *′a* :: {*comm-ring-1*}
assumes *completely-multiplicative-function f*
shows *dirichlet-prod f* (*λn. moebius-mu n* ∗ *f n*) *n* = (*if n* = *1 then 1 else 0*)
⟨*proof*⟩

lemma *dirichlet-prod-inversion-completely-multiplicative*:
fixes *a* :: *nat* ⇒ *′a* :: *comm-ring-1*

assumes *completely-multiplicative-function a*
shows $(\forall x\geq 1.\ g\ x = \textit{dirichlet-prod}'\ a\ f\ x) \longleftrightarrow$
$(\forall x\geq 1.\ f\ x = \textit{dirichlet-prod}'\ (\lambda n.\ \textit{moebius-mu}\ n * a\ n)\ g\ x)$
⟨*proof*⟩

lemma *divisor-sigma-conv-dirichlet-prod*:
divisor-sigma x n = *dirichlet-prod* (λ*n. real n powr x*) (λ-. *1*) *n*
⟨*proof*⟩

2.2 Legendre's identity

definition *legendre-aux* :: *real* ⇒ *nat* ⇒ *nat* **where**
legendre-aux x p = (*if prime p then* ($\sum$ *m* | *m* > *0* ∧ *real* (*p* ^ *m*) ≤ *x*. *nat* ⌊*x* / *p* ^ *m*⌋) *else 0*)

lemma *legendre-aux-not-prime* [*simp*]: ¬*prime p* ⟹ *legendre-aux x p* = *0*
⟨*proof*⟩

lemma *legendre-aux-eq-0*:
assumes *real p* > *x*
shows *legendre-aux x p* = *0*
⟨*proof*⟩

lemma *legendre-aux-posD*:
assumes *legendre-aux x p* > *0*
shows *prime p real p* ≤ *x*
⟨*proof*⟩

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

lemma *finite-sum-legendre-aux*:
assumes *prime p*
shows *finite* {*m. m* > *0* ∧ *real* (*p* ^ *m*) ≤ *x*}
⟨*proof*⟩

lemma *legendre-aux-set-eq*:
assumes *prime p x* ≥ *1*
shows {*m. m* > *0* ∧ *real* (*p* ^ *m*) ≤ *x*} = {*0*<..*nat* ⌊*log* (*real p*) *x*⌋}
⟨*proof*⟩

lemma *legendre-aux-altdef1*:
legendre-aux x p = (*if prime p* ∧ *x* ≥ *1 then*
($\sum$ *m*∈{*0*<..*nat* ⌊*log* (*real p*) *x*⌋}. *nat* ⌊*x* / *p* ^ *m*⌋) *else 0*)
⟨*proof*⟩

lemma *legendre-aux-altdef2*:

assumes $x \geq 1$ *prime p real p* $\widehat{}$ *Suc k* $> x$
shows *legendre-aux x p* $= (\sum m \in \{0 <..k\}.$ *nat* $\lfloor x \ / \ p \ \widehat{} \ m \rfloor)$
⟨*proof*⟩

theorem *legendre-identity*:
sum-upto ln x = *prime-sum-upto* (λp. *legendre-aux x p* $*$ *ln p*) *x*
⟨*proof*⟩

lemma *legendre-identity'*:
fact (*nat* $\lfloor x \rfloor$) = ($\prod p$ | *prime p* $\wedge$ *real p* $\leq x$. *p* $\widehat{}$ *legendre-aux x p*)
⟨*proof*⟩

2.3 A weighted sum of the Möbius μ function

context
fixes *M* :: *real* $\Rightarrow$ *real*
defines *M* $\equiv$ (λx. *sum-upto* (λn. *moebius-mu n* / *n*) *x*)
begin

lemma *abs-sum-upto-moebius-mu-over-n-less*:
assumes *x*: $x \geq 2$
shows $|M\ x| < 1$
⟨*proof*⟩

lemma *sum-upto-moebius-mu-over-n-eq*:
assumes $x < 2$
shows *M x* = (*if* $x \geq 1$ *then 1 else 0*)
⟨*proof*⟩

lemma *abs-sum-upto-moebius-mu-over-n-le*: $|M\ x| \leq 1$
⟨*proof*⟩

end

end

3 The Prime ω function

theory *Primes-Omega*
imports *Dirichlet-Series.Dirichlet-Series Dirichlet-Series.Divisor-Count*
begin

The prime ω function $\omega(n)$ counts the number of distinct prime factors of n.

definition *primes-omega* :: *nat* $\Rightarrow$ *nat* **where**
primes-omega n = *card* (*prime-factors n*)

lemma *primes-omega-prime* [*simp*]: *prime p* $\Longrightarrow$ *primes-omega p* = *1*

⟨*proof*⟩

lemma *primes-omega-0* [*simp*]: *primes-omega 0* = *0*
⟨*proof*⟩

lemma *primes-omega-1* [*simp*]: *primes-omega 1* = *0*
⟨*proof*⟩

lemma *primes-omega-Suc-0* [*simp*]: *primes-omega* (*Suc 0*) = *0*
⟨*proof*⟩

lemma *primes-omega-power* [*simp*]: *n* > *0* ⟹ *primes-omega* (*x* ^ *n*) = *primes-omega x*
⟨*proof*⟩

lemma *primes-omega-primepow* [*simp*]: *primepow n* ⟹ *primes-omega n* = *1*
⟨*proof*⟩

lemma *primes-omega-eq-0-iff*: *primes-omega n* = *0* ⟷ *n* = *0* ∨ *n* = *1*
⟨*proof*⟩

lemma *primes-omega-pos* [*simp*, *intro*]: *n* > *1* ⟹ *primes-omega n* > *0*
⟨*proof*⟩

lemma *primes-omega-mult-coprime*:
assumes *coprime x y x* > *0* ∨ *y* > *0*
shows *primes-omega* (*x* ∗ *y*) = *primes-omega x* + *primes-omega y*
⟨*proof*⟩

lemma *divisor-count-squarefree*:
assumes *squarefree n n* > *0*
shows *divisor-count n* = *2* ^ *primes-omega n*
⟨*proof*⟩

end

4 The Primorial function

theory *Primorial*
imports *Prime-Distribution-Elementary-Library Primes-Omega*
begin

4.1 Definition and basic properties

definition *primorial* :: *real* ⇒ *nat* **where**
primorial x = ∏{*p*. *prime p* ∧ *real p* ≤ *x*}

lemma *primorial-mono*: *x* ≤ *y* ⟹ *primorial x* ≤ *primorial y*
⟨*proof*⟩

lemma *prime-factorization-primorial*:
prime-factorization (*primorial* x) = *mset-set* {*p*. *prime p* ∧ *real p* ≤ x}
⟨*proof*⟩

lemma *prime-factors-primorial* [*simp*]:
prime-factors (*primorial* x) = {*p*. *prime p* ∧ *real p* ≤ x}
⟨*proof*⟩

lemma *primorial-pos* [*simp*, *intro*]: *primorial* $x > 0$
⟨*proof*⟩

lemma *primorial-neq-zero* [*simp*]: *primorial* $x \neq 0$
⟨*proof*⟩

lemma *of-nat-primes-omega-primorial* [*simp*]: *real* (*primes-omega* (*primorial* x)) = *primes-pi* x
⟨*proof*⟩

lemma *primes-omega-primorial*: *primes-omega* (*primorial* x) = *nat* ⌊*primes-pi* x⌋
⟨*proof*⟩

lemma *prime-dvd-primorial-iff*: *prime p* ⟹ *p dvd primorial* x ⟷ $p \leq x$
⟨*proof*⟩

lemma *squarefree-primorial* [*intro*]: *squarefree* (*primorial* x)
⟨*proof*⟩

lemma *primorial-ge*: *primorial* $x \geq 2$ *powr primes-pi* x
⟨*proof*⟩

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

lemma *totient-primorial*:
real (*totient* (*primorial* x)) =
real (*primorial* x) ∗ (∏*p* | *prime p* ∧ *real p* ≤ x. *1* − *1* / *real p*) **for** x
⟨*proof*⟩

lemma *ln-primorial*: *ln* (*primorial* x) = *primes-theta* x
⟨*proof*⟩

lemma *divisor-count-primorial*: *divisor-count* (*primorial* x) = *2 powr primes-pi* x
⟨*proof*⟩

4.2 An alternative view on primorials

The following function is an alternative representation of primorials; instead of taking the product of all primes up to a given real bound x, it takes the product of the first k primes. This is sometimes more convenient.

definition *primorial′* :: *nat* ⇒ *nat* **where**
primorial′ n = (∏ *k*<*n*. *nth-prime k*)

lemma *primorial′-0* [*simp*]: *primorial′ 0* = *1*
and *primorial′-1* [*simp*]: *primorial′ 1* = *2*
and *primorial′-2* [*simp*]: *primorial′ 2* = *6*
and *primorial′-3* [*simp*]: *primorial′ 3* = *30*
⟨*proof*⟩

lemma *primorial′-Suc*: *primorial′* (*Suc n*) = *nth-prime n* ∗ *primorial′ n*
⟨*proof*⟩

lemma *primorial′-pos* [*intro*]: *primorial′ n* > *0*
⟨*proof*⟩

lemma *primorial′-neq-0* [*simp*]: *primorial′ n* ≠ *0*
⟨*proof*⟩

lemma *strict-mono-primorial′*: *strict-mono primorial′*
⟨*proof*⟩

lemma *prime-factorization-primorial′*:
prime-factorization (*primorial′ k*) = *mset-set* (*nth-prime* ‘ {..<*k*})
⟨*proof*⟩

lemma *prime-factors-primorial′*: *prime-factors* (*primorial′ k*) = *nth-prime* ‘ {..<*k*}
⟨*proof*⟩

lemma *primes-omega-primorial′* [*simp*]: *primes-omega* (*primorial′ k*) = *k*
⟨*proof*⟩

lemma *squarefree-primorial′* [*intro*]: *squarefree* (*primorial′ x*)
⟨*proof*⟩

lemma *divisor-count-primorial′* [*simp*]: *divisor-count* (*primorial′ k*) = *2* ^ *k*
⟨*proof*⟩

lemma *totient-primorial′*:
totient (*primorial′ k*) = *primorial′ k* ∗ (∏ *i*<*k*. *1* − *1* / *nth-prime i*)
⟨*proof*⟩

lemma *primorial-conv-primorial′*: *primorial x* = *primorial′* (*nat* ⌊*primes-pi x*⌋)
⟨*proof*⟩

lemma *primorial′-conv-primorial*:
assumes *n* > *0*
shows *primorial′ n* = *primorial* (*nth-prime* (*n* − *1*))
⟨*proof*⟩

4.3 Maximal compositeness of primorials

Primorials are maximally composite, i. e. any number with k distinct prime factors is as least as big as the primorial with k distinct prime factors, and and number less than a primorial has strictly less prime factors.

lemma *nth-prime-le-prime-sequence*:
  fixes p :: *nat* ⇒ *nat*
  assumes *strict-mono-on* {..<n} p **and** ⋀k. $k < n \Longrightarrow$ *prime* (p k) **and** $k < n$
  shows *nth-prime* $k \le p$ k
  ⟨*proof*⟩

theorem *primorial′-primes-omega-le*:
  fixes n :: *nat*
  assumes n: $n > 0$
  shows *primorial′* (*primes-omega* n) $\le n$
⟨*proof*⟩

lemma *primes-omega-less-primes-omega-primorial*:
  fixes n :: *nat*
  assumes n: $n > 0$ **and** $n <$ *primorial* x
  shows *primes-omega* $n <$ *primes-omega* (*primorial* x)
⟨*proof*⟩

lemma *primes-omega-le-primes-omega-primorial*:
  fixes n :: *nat*
  assumes $n \le$ *primorial* x
  shows *primes-omega* $n \le$ *primes-omega* (*primorial* x)
⟨*proof*⟩

end

5 The LCM of the first n natural numbers

theory *Lcm-Nat-Upto*
  imports *Prime-Number-Theorem.Prime-Counting-Functions*
begin

In this section, we examine *Lcm* {*1*..n}. In particular, we will show that it is equal to $e^{\psi(n)}$ and thus (by the PNT) $e^{n+o(n)}$.

lemma *multiplicity-Lcm*:
  fixes A :: *′a* :: {*semiring-Gcd*, *factorial-semiring-gcd*} *set*
  assumes *finite* A $A \neq$ {} *prime* p *0* $\notin A$
  shows *multiplicity* p (*Lcm* A) = *Max* (*multiplicity* p ‘ A)
  ⟨*proof*⟩

The multiplicity of any prime p in *Lcm* {*1*..n} differs from that in *Lcm* {*1*..n − *1*} iff n is a power of p, in which case it is greater by 1.

lemma *multiplicity-Lcm-atLeast1AtMost-Suc*:

fixes *p n* :: *nat*
assumes *p*: *prime p* **and** *n*: *n* > *0*
shows *multiplicity p* (*Lcm* {*1..Suc n*}) =
(*if* ∃*k*. *Suc n* = *p* ^ *k then 1 else 0*) + *multiplicity p* (*Lcm* {*1..n*})
⟨*proof*⟩

Consequently, *Lcm* {*1..n*} differs from *Lcm* {*1..n* − *1*} iff n is of the form p^k for some prime p, in which case it is greater by a factor of p.

lemma *Lcm-atLeast1AtMost-Suc*:
Lcm {*1..Suc n*} = *Lcm* {*1..n*} ∗ (*if primepow* (*Suc n*) *then aprimedivisor* (*Suc n*) *else 1*)
⟨*proof*⟩

It follows by induction that Lcm $\{1..n\} = e^{\psi(n)}$.

lemma *Lcm-atLeast1AtMost-conv-ψ*:
includes *prime-counting-notation*
shows *real* (*Lcm* {*1..n*}) = *exp* (*ψ* (*real n*))
⟨*proof*⟩

lemma *Lcm-upto-real-conv-ψ*:
includes *prime-counting-notation*
shows *real* (*Lcm* {*1..nat* ⌊*x*⌋}) = *exp* (*ψ x*)
⟨*proof*⟩

end

6 Shapiro's Tauberian Theorem

theory *Shapiro-Tauberian*
imports
More-Dirichlet-Misc
Prime-Number-Theorem.Prime-Counting-Functions
Prime-Distribution-Elementary-Library
begin

6.1 Proof

Given an arithmeticla function $a(n)$, Shapiro's Tauberian theorem relates the sum $\sum_{n\leq x} a(n)$ to the weighted sums $\sum_{n\leq x} a(n)\lfloor\frac{x}{n}\rfloor$ and $\sum_{n\leq x} a(n)/n$. More precisely, it shows that if $\sum_{n\leq x} a(n)\lfloor\frac{x}{n}\rfloor = x\ln x + O(x)$, then:

- $\sum_{n\leq x} \frac{a(n)}{n} = \ln x + O(1)$
- $\sum_{n\leq x} a(n) \leq Bx$ for some constant $B \geq 0$ and all $x \geq 0$
- $\sum_{n\leq x} a(n) \geq Cx$ for some constant $C > 0$ and all $x \geq 1/C$

locale *shapiro-tauberian* =
fixes $a :: nat \Rightarrow real$ **and** $A\ S\ T :: real \Rightarrow real$
defines $A \equiv sum\text{-}upto\ (\lambda n.\ a\ n\ /\ n)$
defines $S \equiv sum\text{-}upto\ a$
defines $T \equiv (\lambda x.\ dirichlet\text{-}prod'\ a\ floor\ x)$
assumes *a-nonneg*: $\bigwedge n.\ n > 0 \Longrightarrow a\ n \geq 0$
assumes *a-asymptotics*: $(\lambda x.\ T\ x - x * ln\ x) \in O(\lambda x.\ x)$
begin

lemma *fin*: *finite X* **if** $X \subseteq \{n.\ real\ n \leq x\}$ **for** *X x*
⟨*proof*⟩

lemma *S-mono*: $S\ x \leq S\ y$ **if** $x \leq y$ **for** *x y*
⟨*proof*⟩

lemma *split*:
fixes $f :: nat \Rightarrow real$
assumes $\alpha \in \{0..1\}$
shows $sum\text{-}upto\ f\ x = sum\text{-}upto\ f\ (\alpha * x) + (\sum n \mid n > 0 \land real\ n \in \{\alpha * x <..x\}.\ f\ n)$
⟨*proof*⟩

lemma *S-diff-T-diff*: $S\ x - S\ (x\ /\ 2) \leq T\ x - 2 * T\ (x\ /\ 2)$
⟨*proof*⟩

lemma
shows *diff-bound-strong*: $\exists c \geq 0.\ \forall x \geq 0.\ x * A\ x - T\ x \in \{0..c * x\}$
and *asymptotics*: $(\lambda x.\ A\ x - ln\ x) \in O(\lambda\text{-}.\ 1)$
and *upper*: $\exists c \geq 0.\ \forall x \geq 0.\ S\ x \leq c * x$
and *lower*: $\exists c > 0.\ \forall x \geq 1/c.\ S\ x \geq c * x$
and *bigtheta*: $S \in \Theta(\lambda x.\ x)$
⟨*proof*⟩

end

6.2 Applications to the Chebyshev functions

We can now apply Shapiro's Tauberian theorem to ψ and ϑ.

lemma *dirichlet-prod-mangoldt1-floor-bigo*:
includes *prime-counting-notation*
shows $(\lambda x.\ dirichlet\text{-}prod'\ (\lambda n.\ ind\ prime\ n * ln\ n)\ floor\ x - x * ln\ x) \in O(\lambda x.\ x)$
⟨*proof*⟩

lemma *dirichlet-prod′-mangoldt-floor-asymptotics*:
$(\lambda x.\ dirichlet\text{-}prod'\ mangoldt\ floor\ x - x * ln\ x + x) \in O(ln)$
⟨*proof*⟩

interpretation *ψ*: *shapiro-tauberian mangoldt sum-upto* (*λn. mangoldt n / n*) *primes-psi*
dirichlet-prod′ mangoldt floor
⟨*proof*⟩

thm *ψ.asymptotics ψ.upper ψ.lower*

interpretation *ϑ*: *shapiro-tauberian λn. ind prime n ∗ ln n*
sum-upto (*λn. ind prime n ∗ ln n / n*) *primes-theta dirichlet-prod′* (*λn. ind prime n ∗ ln n*) *floor*
⟨*proof*⟩

thm *ϑ.asymptotics ϑ.upper ϑ.lower*

lemma *sum-upto-ψ-x-over-n-asymptotics*:
(*λx. sum-upto* (*λn. primes-psi* (*x / n*)) *x − x ∗ ln x + x*) ∈ *O*(*ln*)
and *sum-upto-ϑ-x-over-n-asymptotics*:
(*λx. sum-upto* (*λn. primes-theta* (*x / n*)) *x − x ∗ ln x*) ∈ *O*(*λx. x*)
⟨*proof*⟩

end

7 Bounds on partial sums of the ζ function

theory *Partial-Zeta-Bounds*
imports
Euler-MacLaurin.Euler-MacLaurin-Landau
Zeta-Function.Zeta-Function
Prime-Number-Theorem.Prime-Number-Theorem-Library
Prime-Distribution-Elementary-Library
begin

We employ Euler–MacLaurin's summation formula to obtain asymptotic estimates for the partial sums of the Riemann $\zeta(s)$ function for fixed real a, i. e. the function

$$f(n) = \sum_{k=1}^{n} k^{-s}\ .$$

We distinguish various cases. The case $s = 1$ is simply the Harmonic numbers and is treated apart from the others.

lemma *harm-asymp-equiv*: *sum-upto* (*λn. 1 / n*) ∼[*at-top*] *ln*
⟨*proof*⟩

lemma
fixes *s* :: *real*

assumes *s*: $s > 0$ $s \neq 1$
shows *zeta-partial-sum-bigo-pos*:
$(\lambda n.\ (\sum k{=}1..n.\ real\ k\ powr\ -s) - real\ n\ powr\ (1 - s)\ /\ (1 - s) - Re\ (zeta\ s))$
$\in O(\lambda x.\ real\ x\ powr\ -s)$
and *zeta-partial-sum-bigo-pos'*:
$(\lambda n.\ \sum k{=}1..n.\ real\ k\ powr\ -s) =o$
$(\lambda n.\ real\ n\ powr\ (1 - s)\ /\ (1 - s) + Re\ (zeta\ s)) +o\ O(\lambda x.\ real\ x\ powr\ -s)$
⟨*proof*⟩

lemma *zeta-tail-bigo*:
fixes *s* :: *real*
assumes *s*: $s > 1$
shows $(\lambda n.\ Re\ (hurwitz\text{-}zeta\ (real\ n + 1)\ s)) \in O(\lambda x.\ real\ x\ powr\ (1 - s))$
⟨*proof*⟩

lemma *zeta-tail-bigo'*:
fixes *s* :: *real*
assumes *s*: $s > 1$
shows $(\lambda n.\ Re\ (hurwitz\text{-}zeta\ (real\ n)\ s)) \in O(\lambda x.\ real\ x\ powr\ (1 - s))$
⟨*proof*⟩

lemma
fixes *s* :: *real*
assumes *s*: $s > 0$
shows *zeta-partial-sum-bigo-neg*:
$(\lambda n.\ (\sum i{=}1..n.\ real\ i\ powr\ s) - n\ powr\ (1 + s)\ /\ (1 + s)) \in O(\lambda n.\ n\ powr\ s)$
and *zeta-partial-sum-bigo-neg'*:
$(\lambda n.\ (\sum i{=}1..n.\ real\ i\ powr\ s)) =o\ (\lambda n.\ n\ powr\ (1 + s)\ /\ (1 + s)) +o\ O(\lambda n.\ n\ powr\ s)$
⟨*proof*⟩

lemma *zeta-partial-sum-le-pos*:
assumes $s > 0$ $s \neq 1$
defines $z \equiv Re\ (zeta\ (complex\text{-}of\text{-}real\ s))$
shows $\exists c{>}0.\ \forall x{\geq}1.\ |sum\text{-}upto\ (\lambda n.\ n\ powr\ -s)\ x - (x\ powr\ (1{-}s)\ /\ (1{-}s) + z)| \leq c * x\ powr\ -s$
⟨*proof*⟩

lemma *zeta-partial-sum-le-pos'*:
assumes $s > 0$ $s \neq 1$
defines $z \equiv Re\ (zeta\ (complex\text{-}of\text{-}real\ s))$
shows $\exists c{>}0.\ \forall x{\geq}1.\ |sum\text{-}upto\ (\lambda n.\ n\ powr\ -s)\ x - x\ powr\ (1{-}s)\ /\ (1{-}s)| \leq c$
⟨*proof*⟩

lemma *zeta-partial-sum-le-pos''*:

assumes $s > 0$ $s \neq 1$
shows $\exists c{>}0.\ \forall x{\geq}1.\ |\mathit{sum\text{-}upto}\ (\lambda n.\ n\ \mathit{powr}\ -s)\ x| \leq c * x\ \mathit{powr}\ \mathit{max}\ 0\ (1 - s)$
⟨*proof*⟩

lemma *zeta-partial-sum-le-pos-bigo*:
assumes $s > 0$ $s \neq 1$
shows $(\lambda x.\ \mathit{sum\text{-}upto}\ (\lambda n.\ n\ \mathit{powr}\ -s)\ x) \in O(\lambda x.\ x\ \mathit{powr}\ \mathit{max}\ 0\ (1 - s))$
⟨*proof*⟩

lemma *zeta-partial-sum-01-asymp-equiv*:
assumes $s \in \{0{<}..{<}1\}$
shows $\mathit{sum\text{-}upto}\ (\lambda n.\ n\ \mathit{powr}\ -s) \sim[\mathit{at\text{-}top}]\ (\lambda x.\ x\ \mathit{powr}\ (1 - s)\ /\ (1 - s))$
⟨*proof*⟩

lemma *zeta-partial-sum-gt-1-asymp-equiv*:
fixes $s :: \mathit{real}$
assumes $s > 1$
defines $\zeta \equiv \mathit{Re}\ (\mathit{zeta}\ s)$
shows $\mathit{sum\text{-}upto}\ (\lambda n.\ n\ \mathit{powr}\ -s) \sim[\mathit{at\text{-}top}]\ (\lambda x.\ \zeta)$
⟨*proof*⟩

lemma *zeta-partial-sum-pos-bigtheta*:
assumes $s > 0$ $s \neq 1$
shows $\mathit{sum\text{-}upto}\ (\lambda n.\ n\ \mathit{powr}\ -s) \in \Theta(\lambda x.\ x\ \mathit{powr}\ \mathit{max}\ 0\ (1 - s))$
⟨*proof*⟩

lemma *zeta-partial-sum-le-neg*:
assumes $s > 0$
shows $\exists c{>}0.\ \forall x{\geq}1.\ |\mathit{sum\text{-}upto}\ (\lambda n.\ n\ \mathit{powr}\ s)\ x - x\ \mathit{powr}\ (1 + s)\ /\ (1 + s)| \leq c * x\ \mathit{powr}\ s$
⟨*proof*⟩

lemma *zeta-partial-sum-neg-asymp-equiv*:
assumes $s > 0$
shows $\mathit{sum\text{-}upto}\ (\lambda n.\ n\ \mathit{powr}\ s) \sim[\mathit{at\text{-}top}]\ (\lambda x.\ x\ \mathit{powr}\ (1 + s)\ /\ (1 + s))$
⟨*proof*⟩

end

8 The summatory Möbius μ function

theory *Moebius-Mu-Sum*
imports
More-Dirichlet-Misc
Dirichlet-Series.Partial-Summation
Prime-Number-Theorem.Prime-Counting-Functions
Dirichlet-Series.Arithmetic-Summatory-Asymptotics
Shapiro-Tauberian

Partial-Zeta-Bounds
Prime-Number-Theorem.Prime-Number-Theorem-Library
Prime-Distribution-Elementary-Library
begin

In this section, we shall examine the summatory Möbius μ function $M(x) := \sum_{n \leq x} \mu(n)$. The main result is that $M(x) \in o(x)$ is equivalent to the Prime Number Theorem.

context
includes *prime-counting-notation*
fixes M H :: *real* ⇒ *real*
defines $M \equiv$ *sum-upto moebius-mu*
defines $H \equiv$ *sum-upto* (λn. *moebius-mu* $n * ln\ n$)
begin

lemma *sum-upto-moebius-mu-integral*: $x > 1 \Longrightarrow ((\lambda t.\ M\ t\ /\ t)$ *has-integral* $M\ x * ln\ x - H\ x)\ \{1..x\}$
and *sum-upto-moebius-mu-integrable*: $a \geq 1 \Longrightarrow (\lambda t.\ M\ t\ /\ t)$ *integrable-on* $\{a..b\}$
⟨*proof*⟩

lemma *sum-moebius-mu-bound*:
assumes $x \geq 0$
shows $|M\ x| \leq x$
⟨*proof*⟩

lemma *sum-moebius-mu-aux1*: $(\lambda x.\ M\ x\ /\ x - H\ x\ /\ (x * ln\ x)) \in O(\lambda x.\ 1\ /\ ln\ x)$
⟨*proof*⟩

lemma *sum-moebius-mu-aux2*: $((\lambda x.\ M\ x\ /\ x - H\ x\ /\ (x * ln\ x)) \longrightarrow 0)$ *at-top*
⟨*proof*⟩

lemma *sum-moebius-mu-ln-eq*: $H = (\lambda x.\ -$ *dirichlet-prod'* *moebius-mu* $\psi\ x)$
⟨*proof*⟩

theorem *PNT-implies-sum-moebius-mu-sublinear*:
assumes ψ ∼[*at-top*] $(\lambda x.\ x)$
shows $M \in o(\lambda x.\ x)$
⟨*proof*⟩

theorem *sum-moebius-mu-sublinear-imp-PNT*:
assumes $M \in o(\lambda x.\ x)$
shows ψ ∼[*at-top*] $(\lambda x.\ x)$
⟨*proof*⟩

We now turn to a related fact: For the weighted sum $A(x) := \sum_{n \leq x} \mu(n)/n$, the asymptotic relation $A(x) \in o(1)$ is also equivalent to the Prime Number Theorem. Like Apostol, we only show one direction, namely that $A(x) \in o(1)$ implies the PNT.

context
fixes *A* **defines** $A \equiv$ *sum-upto* ($\lambda n.$ *moebius-mu n / n*)
begin

lemma *sum-upto-moebius-mu-integral'*: $x > 1 \Longrightarrow$ (*A has-integral x ∗ A x − M x*) {*1..x*}
and *sum-upto-moebius-mu-integrable'*: $a \geq 1 \Longrightarrow$ *A integrable-on* {*a..b*}
⟨*proof*⟩

theorem *sum-moebius-mu-div-n-smallo-imp-PNT*:
assumes *smallo*: $A \in o(\lambda\text{-}.\ 1)$
shows $M \in o(\lambda x.\ x)$ **and** $\psi \sim$[*at-top*] $(\lambda x.\ x)$
⟨*proof*⟩

end

end

end

9 Elementary bounds on $\pi(x)$ and p_n

theory *Elementary-Prime-Bounds*
imports
Prime-Number-Theorem.Prime-Counting-Functions
Prime-Distribution-Elementary-Library
More-Dirichlet-Misc
begin

In this section, we will follow Apostol and give elementary proofs of Chebyshev-type lower and upper bounds for $\pi(x)$, i. e. $c_1 x/\ln x < \pi(x) < c_2 x/\ln x$. From this, similar bounds for p_n follow as easy corollaries.

9.1 Preliminary lemmas

The following two estimates relating the central Binomial coefficient to powers of 2 and 4 form the starting point for Apostol's elementary bounds for $\pi(x)$:

lemma *twopow-le-central-binomial*: *2* ^ $n \leq$ ((*2* ∗ *n*) *choose n*)
⟨*proof*⟩

lemma *fourpow-gt-central-binomial*:
assumes $n > 0$

shows $4 \mathbin{\hat{}} n > ((2 * n) \ choose \ n)$
⟨*proof*⟩

9.2 Lower bound for $\pi(x)$

context
includes *prime-counting-notation*
fixes $S :: nat \Rightarrow nat \Rightarrow int$
defines $S \equiv (\lambda n\ p.\ (\sum m{\in}\{0{<}..nat\ \lfloor log\ p\ (2{*}n)\rfloor\}.\ \lfloor 2{*}n/p\hat{}m\rfloor - 2 * \lfloor n/p\hat{}m\rfloor))$
begin

We now first prove the bound $\pi(x) \geq \frac{1}{6}x/\ln x$ for $x \geq 2$. The constant could probably be improved for starting points greater than 2; this is true for most of the constants in this section.

The first step is to show a slightly stronger bound for even numbers, where the constant is $\frac{1}{2}\ln 2 \approx 0.347$:

lemma
fixes $n :: nat$
assumes n: $n \geq 1$
shows π*-bounds-aux*: $ln\ (fact\ (2 * n)) - 2 * ln\ (fact\ n) =$ $prime\text{-}sum\text{-}upto\ (\lambda p.\ S\ n\ p * ln\ p)\ (2 * n)$
and π*-lower-bound-ge-strong*: $\pi\ (2 * n) \geq ln\ 2\ /\ 2 * (2 * n)\ /\ ln\ (2 * n)$
⟨*proof*⟩

lemma *ln-2-ge-56-81*: $ln\ 2 \geq (56\ /\ 81 :: real)$
⟨*proof*⟩

The bound for any real number $x \geq 2$ follows fairly easily, although some ugly accounting for error terms has to be done.

theorem π*-lower-bound*:
fixes $x :: real$
assumes x: $x \geq 2$
shows $\pi\ x > (1\ /\ 6) * (x\ /\ ln\ x)$
⟨*proof*⟩

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

9.3 Upper bound for $\vartheta(x)$

In this section, we prove a linear upper bound for ϑ. This is somewhat unnecessary because we already have a considerably better bound on $\vartheta(x)$ using a proof that has roughly the same complexity as this one and also only uses elementary means. Nevertheless, here is the proof from Apostol's book; it is quite nice and it would be a shame not to formalise it.

The idea is to first show a bound for $\vartheta(2n) - \vartheta(n)$ and then deduce one for $\vartheta(2^n)$ from this by telescoping, which then yields one for general x by monotonicity.

lemma *ϑ-double-less*:
  fixes n :: *nat*
  assumes n: $n > 0$
  shows $\vartheta\ (2 * real\ n) - \vartheta\ (real\ n) < real\ n * ln\ 4$
⟨*proof*⟩

lemma *ϑ-twopow-less*: $\vartheta\ (2\ \hat{}\ r) < 2\ \hat{}\ (r + 1) * ln\ 2$
⟨*proof*⟩

theorem *ϑ-upper-bound-weak*:
  fixes n :: *nat*
  assumes n: $n > 0$
  shows $\vartheta\ n < 4 * ln\ 2 * n$
⟨*proof*⟩

9.4 Upper bound for $\pi(x)$

We use our upper bound for $\vartheta(x)$ (the strong one, not the one from the previous section) to derive an upper bound for $\pi(x)$.

As a first step, we show the following lemma about the global maximum of the function $\ln x/x^c$ for $c > 0$:

lemma *π-upper-bound-aux*:
  fixes c :: *real*
  assumes $c > 0$
  defines $f \equiv (\lambda x.\ x\ powr\ (-c) * ln\ x)$
  assumes x: $x > 0$
  shows $f\ x \leq 1\ /\ (c * exp\ 1)$
⟨*proof*⟩

Following Apostol, we first show a generic bound depending on some real-valued parameter α:

lemma *π-upper-bound-strong*:
  fixes α :: *real* **and** n :: *nat*
  assumes n: $n \geq 2$ **and** α: $\alpha \in \{0<..<1\}$
  shows $\pi\ n < (1\ /\ ((1 - \alpha) * exp\ 1) + ln\ 4\ /\ \alpha) * n\ /\ ln\ n$
⟨*proof*⟩

The choice $\alpha := \frac{2}{3}$ then leads to the upper bound $\pi(x) < cx/\ln x$ with $c = 3(e^{-1} + \ln 2) \approx 3.183$. This is considerably stronger than Apostol's bound.

theorem *π-upper-bound*:
  fixes x :: *real*
  assumes $x \geq 2$
  shows $\pi\ x < 3 * (exp\ (-1) + ln\ 2) * x\ /\ ln\ x$
⟨*proof*⟩

corollary *π-upper-bound′*:
fixes *x* :: *real*
assumes *x* ≥ *2*
shows π *x* < *443* / *139* ∗ (*x* / *ln x*)
⟨*proof*⟩

corollary *π-upper-bound″*:
fixes *x* :: *real*
assumes *x* ≥ *2*
shows π *x* < *4* ∗ (*x* / *ln x*)
⟨*proof*⟩

In particular, we have now shown a weak version of the Prime Number Theorem, namely that $\pi(x) \in \Theta(x/\ln x)$:

lemma *π-bigtheta*: π ∈ Θ(λ*x*. *x* / *ln x*)
⟨*proof*⟩

9.5 Bounds for p_n

By some rearrangements, the lower and upper bounds for $\pi(x)$ give rise to analogous bounds for p_n:

lemma *nth-prime-lower-bound-gen*:
assumes *c*: *c* > *0* **and** *n*: *n* > *0*
assumes ⋀*n*. *n* ≥ *2* ⟹ π (*real n*) < (*1* / *c*) ∗ (*real n* / *ln* (*real n*))
shows *nth-prime* (*n* − *1*) ≥ *c* ∗ (*real n* ∗ *ln* (*real n*))
⟨*proof*⟩

corollary *nth-prime-lower-bound*:
n > *0* ⟹ *nth-prime* (*n* − *1*) ≥ (*139* / *443*) ∗ (*n* ∗ *ln n*)
⟨*proof*⟩

corollary *nth-prime-upper-bound*:
assumes *n*: *n* > *0*
shows *nth-prime* (*n* − *1*) < *12* ∗ (*n* ∗ *ln n* + *n* ∗ *ln* (*12* / *exp 1*))
⟨*proof*⟩

We can thus also conclude that $p_n \sim n \ln n$:

corollary *nth-prime-bigtheta*: *nth-prime* ∈ Θ(λ*n*. *n* ∗ *ln n*)
⟨*proof*⟩

end

end

10 The asymptotics of the summatory divisor σ function

theory *Summatory-Divisor-Sigma-Bounds*

imports *Partial-Zeta-Bounds More-Dirichlet-Misc*
begin

In this section, we analyse the asymptotic behaviour of the summatory divisor functions $\sum_{n \leq x} \sigma_\alpha(n)$ for real α. This essentially tells us what the average value of these functions is for large x.

The case $\alpha = 0$ is not treated here since σ_0 is simply the divisor function, for which precise asymptotics are already available in the AFP.

10.1 Case 1: $\alpha = 1$

If $\alpha = 1$, $\sigma_\alpha(n)$ is simply the sum of all divisors of n. Here, the asymptotics is

$$\sum_{n \leq x} \sigma_1(n) = \frac{\pi^2}{12} x^2 + O(x \ln x) \ .$$

theorem *summatory-divisor-sum-asymptotics*:
sum-upto divisor-sum =o (λx. pi^2 */ 12 ∗ x ^ 2) +o O(λx. x ∗ ln x)*
⟨*proof*⟩

10.2 Case 2: $\alpha > 0$, $\alpha \neq 1$

Next, we consider the case $\alpha > 0$ and $\alpha \neq 1$. We then have:

$$\sum_{n \leq x} \sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1} x^{\alpha+1} + O\left(x^{\max(1,\alpha)}\right)$$

theorem *summatory-divisor-sigma-asymptotics-pos*:
fixes *α :: real*
assumes *α: α > 0 α ≠ 1*
defines *ζ ≡ Re (zeta (α + 1))*
shows *sum-upto (divisor-sigma α) =o*
(λx. ζ / (α + 1) ∗ x powr (α + 1)) +o O(λx. x powr max 1 α)
⟨*proof*⟩

10.3 Case 3: $\alpha < 0$

Last, we consider the case of a negative exponent. We have for $\alpha > 0$:

$$\sum_{n \leq x} \sigma_{-\alpha}(n) = \zeta(\alpha+1) x + O(R(x))$$

where $R(x) = \ln x$ if $\alpha = 1$ and $R(x) = x^{\max(0,1-\alpha)}$ otherwise.

theorem *summatory-divisor-sigma-asymptotics-neg*:
fixes *α :: real*
assumes *α: α > 0*

defines $\delta \equiv$ *max 0* $(1 - \alpha)$
defines $\zeta \equiv$ *Re* (*zeta* $(\alpha + 1)$)
shows *sum-upto* (*divisor-sigma* $(-\alpha)$) =*o* (*if* $\alpha = 1$ *then* ($\lambda x.$ *pi*^{2}/*6* $*$ *x*) +*o* *O*(*ln*)
else ($\lambda x.$ ζ $*$ *x*) +*o* *O*($\lambda x.$ *x powr* δ))
⟨*proof*⟩

end

11 Selberg's asymptotic formula

theory *Selberg-Asymptotic-Formula*
imports
More-Dirichlet-Misc
Prime-Number-Theorem.Prime-Counting-Functions
Shapiro-Tauberian
Euler-MacLaurin.Euler-MacLaurin-Landau
Partial-Zeta-Bounds
begin

Following Apostol, we first show an inversion formula: Consider a function $f(x)$ for $x \in \mathbb{R}_{>0}$. Define $g(x) := \ln x \cdot \sum_{n\leq x} f(x/n)$. Then:

$$f(x)\ln x + \sum_{n\leq x} \Lambda(n) f(x/n) = \sum_{n\leq x} \mu(n) g(x/n)$$

locale *selberg-inversion* =
fixes *F G* :: *real* $\Rightarrow$ *'a* :: {*real-algebra-1*, *comm-ring-1*}
defines $G \equiv$ ($\lambda x.$ *of-real* (*ln x*) $*$ *sum-upto* ($\lambda n.$ *F* (*x* / *n*)) *x*)
begin

lemma *eq*:
assumes $x \geq 1$
shows *F x* $*$ *of-real* (*ln x*) + *dirichlet-prod'* *mangoldt F x* = *dirichlet-prod'* *moebius-mu G x*
⟨*proof*⟩

end

We can now show Selberg's formula

$$\psi(x)\ln x + \sum_{n\leq x} \Lambda(n)\psi(x/n) = 2x\ln x + O(x)\ .$$

theorem *selberg-asymptotic-formula*:
includes *prime-counting-notation*
shows ($\lambda x.$ ψ *x* $*$ *ln x* + *dirichlet-prod'* *mangoldt* ψ *x*) =*o*
($\lambda x.$ *2* $*$ *x* $*$ *ln x*) +*o* *O*($\lambda x.$ *x*)

⟨*proof*⟩

end

12 Consequences of the Prime Number Theorem

theory *PNT-Consequences*
imports
Elementary-Prime-Bounds
Prime-Number-Theorem.Mertens-Theorems
Prime-Number-Theorem.Prime-Counting-Functions
Moebius-Mu-Sum
Lcm-Nat-Upto
Primorial
Primes-Omega
begin

In this section, we will define a locale that assumes the Prime Number Theorem in order to explore some of its elementary consequences.

12.1 Statement and alternative forms of the PNT

⟨*proof*⟩⟨*proof*⟩⟨*proof*⟩⟨*proof*⟩⟨*proof*⟩⟨*proof*⟩⟨*proof*⟩⟨*proof*⟩⟨*proof*⟩
locale *prime-number-theorem* =
assumes *prime-number-theorem* [*asymp-equiv-intros*]: $\pi \sim[\mathit{at\text{-}top}]\ (\lambda x.\ x\ /\ \mathit{ln}\ x)$
begin

corollary *ϑ-asymptotics* [*asymp-equiv-intros*]: $\vartheta \sim[\mathit{at\text{-}top}]\ (\lambda x.\ x)$
⟨*proof*⟩

corollary *ψ-asymptotics* [*asymp-equiv-intros*]: $\psi \sim[\mathit{at\text{-}top}]\ (\lambda x.\ x)$
⟨*proof*⟩

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

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

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

corollary *moebius-mu-smallo*: $\mathit{sum\text{-}upto}\ \mathit{moebius\text{-}mu} \in o(\lambda x.\ x)$
⟨*proof*⟩

lemma *ln-ϑ-asymptotics*:
includes *prime-counting-notation*
shows $(\lambda x.\ \mathit{ln}\ (\vartheta\ x) - \mathit{ln}\ x) \in o(\lambda\text{-}.\ 1)$

⟨*proof*⟩

lemma *ln-ϑ-asymp-equiv* [*asymp-equiv-intros*]:
includes *prime-counting-notation*
shows (λ*x*. *ln* (ϑ *x*)) ∼[*at-top*] *ln*
⟨*proof*⟩

lemma *ln-nth-prime-asymptotics*:
(λ*n*. *ln* (*nth-prime n*) − (*ln n* + *ln* (*ln n*))) ∈ *o*(λ-. *1*)
⟨*proof*⟩

lemma *ln-nth-prime-asymp-equiv* [*asymp-equiv-intros*]:
(λ*n*. *ln* (*nth-prime n*)) ∼[*at-top*] *ln*
⟨*proof*⟩

The following versions use a little less notation.

corollary *prime-number-theorem′*: ((λ*x*. π *x* / (*x* / *ln x*)) ⟶ *1*) *at-top*
⟨*proof*⟩

corollary *prime-number-theorem″*:
(λ*x*. *card* {*p*. *prime p* ∧ *real p* ≤ *x*}) ∼[*at-top*] (λ*x*. *x* / *ln x*)
⟨*proof*⟩

corollary *prime-number-theorem‴*:
(λ*n*. *card* {*p*. *prime p* ∧ *p* ≤ *n*}) ∼[*at-top*] (λ*n*. *real n* / *ln* (*real n*))
⟨*proof*⟩

end

12.2 Existence of primes in intervals

For fixed ε, The interval $(x;\varepsilon x]$ contains a prime number for any sufficiently large x. This proof was taken from A. J. Hildebrand's lecture notes [2].

lemma (**in** *prime-number-theorem*) *prime-in-interval-exists*:
fixes *c* :: *real*
assumes *c* > *1*
shows *eventually* (λ*x*. ∃ *p*. *prime p* ∧ *real p* ∈ {*x*<..*c*∗*x*}) *at-top*
⟨*proof*⟩

The set of rationals whose numerator and denominator are primes is dense in $\mathbb{R}_{>0}$.

lemma (**in** *prime-number-theorem*) *prime-fractions-dense*:
fixes α ε :: *real*
assumes α > *0* **and** ε > *0*
obtains *p q* :: *nat* **where** *prime p* **and** *prime q* **and** *dist* (*real p* / *real q*) α < ε
⟨*proof*⟩

12.3 The logarithm of the primorial

The PNT directly implies the asymptotics of the logarithm of the primorial function:

context *prime-number-theorem*
begin

lemma *ln-primorial-asymp-equiv* [*asymp-equiv-intros*]:
  (λx. *ln* (*primorial* x)) $\sim$[*at-top*] (λx. x)
  ⟨*proof*⟩

lemma *ln-ln-primorial-asymp-equiv* [*asymp-equiv-intros*]:
  (λx. *ln* (*ln* (*primorial* x))) $\sim$[*at-top*] (λx. *ln* x)
  ⟨*proof*⟩

lemma *ln-primorial′-asymp-equiv* [*asymp-equiv-intros*]:
    (λk. *ln* (*primorial′* k)) $\sim$[*at-top*] (λk. k $*$ *ln* k)
  and *ln-ln-primorial′-asymp-equiv* [*asymp-equiv-intros*]:
    (λk. *ln* (*ln* (*primorial′* k))) $\sim$[*at-top*] (λk. *ln* k)
  and *ln-over-ln-ln-primorial′-asymp-equiv*:
    (λk. *ln* (*primorial′* k) / *ln* (*ln* (*primorial′* k))) $\sim$[*at-top*] (λk. k)
⟨*proof*⟩

end

12.4 Consequences of the asymptotics of ψ and ϑ

Next, we will show some consequences of $\psi(x) \sim x$ and $\vartheta(x) \sim x$. To this end, we first show generically that any function $g = e^{x+o(x)}$ is $o(c^n)$ if $c > e$ and $\omega(c^n)$ if $c < e$.

locale *exp-asymp-equiv-linear* =
  fixes f g :: *real* ⇒ *real*
  assumes *f-asymp-equiv*: f $\sim$[*at-top*] (λx. x)
  assumes g: *eventually* (λx. g x = *exp* (f x)) F
begin

lemma
  fixes ε :: *real* **assumes** $\varepsilon > 0$
  shows *smallo*: $g \in o(\lambda x.\ exp\ ((1 + \varepsilon) * x))$
    and *smallomega*: $g \in \omega(\lambda x.\ exp\ ((1 - \varepsilon) * x))$
⟨*proof*⟩

lemma *smallo′*:
  fixes c :: *real* **assumes** $c >$ *exp 1*
  shows $g \in o(\lambda x.\ c\ powr\ x)$
⟨*proof*⟩

lemma *smallomega′*:

fixes *c* :: *real* **assumes** $c \in \{0<..<exp\ 1\}$
shows $g \in \omega(\lambda x.\ c\ powr\ x)$
⟨*proof*⟩

end

The primorial fulfils $x\# = e^{\vartheta(x)}$ and is therefore one example of this.

context *prime-number-theorem*
begin

sublocale *primorial*: *exp-asymp-equiv-linear* ϑ $\lambda x.$ *real* (*primorial x*)
⟨*proof*⟩

end

The LCM of the first n natural numbers is equal to $e^{\psi(n)}$ and is therefore another example.

context *prime-number-theorem*
begin

sublocale *Lcm-upto*: *exp-asymp-equiv-linear* ψ $\lambda x.$ *real* (*Lcm* $\{1..nat\ \lfloor x \rfloor\}$)
⟨*proof*⟩

end

12.5 Bounds on the prime ω function

Next, we will examine the asymptotic behaviour of the prime ω function $\omega(n)$, i.e. the number of distinct prime factors of n. These proofs are again taken from A. J. Hildebrand's lecture notes [2].

lemma *ln-gt-1*:
assumes $x > (3 :: real)$
shows $ln\ x > 1$
⟨*proof*⟩

lemma (**in** *prime-number-theorem*) *primes-omega-primorial′-asymp-equiv*:
($\lambda k.$ *primes-omega* (*primorial′ k*)) $\sim$[*at-top*]
($\lambda k.$ *ln* (*primorial′ k*) / *ln* (*ln* (*primorial′ k*)))
⟨*proof*⟩

The number of distinct prime factors of n has maximal order $\ln n / \ln \ln n$:

theorem (**in** *prime-number-theorem*)
limsup-primes-omega: *limsup* ($\lambda n.$ *primes-omega n* / (*ln n* / *ln* (*ln n*))) = *1*
⟨*proof*⟩

12.6 Bounds on the divisor function

In this section, we shall examine the growth of the divisor function $\sigma_0(n)$. In particular, we will show that $\sigma_0(n) < 2^{c \ln n / \ln \ln n}$ for all sufficiently large n if $c > 1$ and $\sigma_0(n) > 2^{c \ln n / \ln \ln n}$ for infinitely many n if $c < 1$.

An equivalent statement is that $\ln(\sigma_0(n))$ has maximal order $\ln 2 \cdot \ln n / \ln \ln n$.

Following Apostol's somewhat didactic approach, we first show a generic bounding lemma for σ_0 that depends on some function f that we will specify later.

lemma *divisor-count-bound-gen*:
  fixes *f* :: *nat* ⇒ *real*
  assumes *eventually* (*λn. f n* ≥ *2*) *at-top*
  defines *c* ≡ (*8* / *ln 2* :: *real*)
  defines *g* ≡ (*λn.* (*ln n* + *c* ∗ *f n* ∗ *ln* (*ln n*)) / (*ln* (*f n*)))
  shows *eventually* (*λn. divisor-count n* < *2 powr g n*) *at-top*
⟨*proof*⟩
  include *prime-counting-notation*
  ⟨*proof*⟩

Now, Apostol explains that one can choose $f(n) := \ln n/(\ln \ln n)^2$ to obtain the desired bound.

proposition *divisor-count-upper-bound*:
  fixes *ε* :: *real*
  assumes *ε* > *0*
  shows *eventually* (*λn. divisor-count n* < *2 powr* ((*1* + *ε*) ∗ *ln n* / *ln* (*ln n*))) *at-top*
⟨*proof*⟩

Next, we will examine the 'worst case'. Since any prime factor of n with multiplicity k contributes a factor of $k+1$, it is intuitively clear that $\sigma_0(n)$ is largest w.r.t. n if it is a product of small distinct primes.

We show that indeed, if $n := x\#$ (where $x\#$ denotes the primorial), we have $\sigma_0(n) = 2^{\pi(x)}$, which, by the Prime Number Theorem, indeed exceeds $c \ln n / \ln \ln n$.

theorem (**in** *prime-number-theorem*) *divisor-count-primorial-gt*:
  assumes *ε* > *0*
  defines *h* ≡ *primorial*
  shows *eventually* (*λx. divisor-count* (*h x*) > *2 powr* ((*1* − *ε*) ∗ *ln* (*h x*) / *ln* (*ln* (*h x*)))) *at-top*
⟨*proof*⟩

Since $h(x) \longrightarrow \infty$, this gives us our infinitely many values of n that exceed the bound.

corollary (**in** *prime-number-theorem*) *divisor-count-lower-bound*:
  assumes *ε* > *0*
  shows *frequently* (*λn. divisor-count n* > *2 powr* ((*1* − *ε*) ∗ *ln n* / *ln* (*ln n*))) *at-top*

⟨*proof*⟩

A different formulation that is not quite as tedious to prove is this one:

lemma (**in** *prime-number-theorem*) *ln-divisor-count-primorial′-asymp-equiv*:
 (λk. *ln* (*divisor-count* (*primorial′ k*))) ∼[*at-top*]
  (λk. *ln 2* ∗ *ln* (*primorial′ k*) / *ln* (*ln* (*primorial′ k*)))
⟨*proof*⟩

It follows that the maximal order of the divisor function is $\ln 2 \cdot \ln n / \ln \ln n$.

theorem (**in** *prime-number-theorem*) *limsup-divisor-count*:
 limsup (λn. *ln* (*divisor-count n*) ∗ *ln* (*ln n*) / *ln n*) = *ln 2*
⟨*proof*⟩

12.7 Mertens' Third Theorem

In this section, we will show that

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{C}{\ln x} + O\left(\frac{1}{\ln^2 x}\right)$$

with explicit bounds for the factor in the 'Big-O'. Here, C is the following constant:

definition *third-mertens-const* :: *real* **where**
 third-mertens-const =
  exp (−($\sum$ *p*::*nat*. *if prime p then* −*ln* (*1* − *1* / *real p*) − *1* / *real p else 0*) − *meissel-mertens*)

This constant is actually equal to $e^{-\gamma}$ where γ is the Euler–Mascheroni constant, but showing this is quite a bit of work, which we shall not do here.

lemma *third-mertens-const-pos*: *third-mertens-const* > *0*
 ⟨*proof*⟩

theorem
 defines *C* ≡ *third-mertens-const*
 shows *mertens-third-theorem-strong*:
  eventually (λx. |($\prod$ *p* | *prime p* ∧ *real p* ≤ *x*. *1* − *1* / *p*) − *C* / *ln x*| ≤
   10 ∗ *C* / *ln x* ^ *2*) *at-top*
 and *mertens-third-theorem*:
  (λx. ($\prod$ *p* | *prime p* ∧ *real p* ≤ *x*. *1* − *1* / *p*) − *C* / *ln x*) ∈ *O*(λx. *1* / *ln x* ^ *2*)
⟨*proof*⟩

lemma *mertens-third-theorem-asymp-equiv*:
 (λx. ($\prod$ *p* | *prime p* ∧ *real p* ≤ *x*. *1* − *1* / *real p*)) ∼[*at-top*]
  (λx. *third-mertens-const* / *ln x*)
 ⟨*proof*⟩

We now show an equivalent version where $\prod_{p \leq x}(1 - 1/p)$ is replaced by $\prod_{i=1}^{k}(1 - 1/p_i)$:

lemma *mertens-third-convert*:
assumes $n > 0$
shows $(\prod k{<}n.\ 1 - 1\ /\ real\ (nth\text{-}prime\ k)) =$
$(\prod p \mid prime\ p \wedge p \leq nth\text{-}prime\ (n - 1).\ 1 - 1\ /\ p)$
⟨*proof*⟩

lemma (**in** *prime-number-theorem*) *mertens-third-theorem-asymp-equiv′*:
$(\lambda n.\ (\prod k{<}n.\ 1 - 1\ /\ nth\text{-}prime\ k)) \sim[at\text{-}top]\ (\lambda x.\ third\text{-}mertens\text{-}const\ /\ ln\ x)$
⟨*proof*⟩

12.8 Bounds on Euler's totient function

Similarly to the divisor function, we will show that $\varphi(n)$ has minimal order $Cn/\ln\ln n$.

The first part is to show the lower bound:

theorem *totient-lower-bound*:
fixes ε :: *real*
assumes $\varepsilon > 0$
defines $C \equiv third\text{-}mertens\text{-}const$
shows *eventually* $(\lambda n.\ totient\ n > (1 - \varepsilon) * C * n\ /\ ln\ (ln\ n))$ *at-top*
⟨*proof*⟩
include *prime-counting-notation*
⟨*proof*⟩

Next, we examine the 'worst case' of $\varphi(n)$ where n is the primorial of x. In this case, we have $\varphi(n) < cn/\ln\ln n$ for any $c > C$ for all sufficiently large n.

theorem (**in** *prime-number-theorem*) *totient-primorial-less*:
fixes ε :: *real*
defines $C \equiv third\text{-}mertens\text{-}const$ **and** $h \equiv primorial$
assumes $\varepsilon > 0$
shows *eventually* $(\lambda x.\ totient\ (h\ x) < (1 + \varepsilon) * C * h\ x\ /\ ln\ (ln\ (h\ x)))$ *at-top*
⟨*proof*⟩

It follows that infinitely many values of n exceed $cn/\ln(\ln n)$ when c is chosen larger than C.

corollary (**in** *prime-number-theorem*) *totient-upper-bound*:
assumes $\varepsilon > 0$
defines $C \equiv third\text{-}mertens\text{-}const$
shows *frequently* $(\lambda n.\ totient\ n < (1 + \varepsilon) * C * n\ /\ ln\ (ln\ n))$ *at-top*
⟨*proof*⟩

Again, the following alternative formulation is somewhat nicer to prove:

lemma (**in** *prime-number-theorem*) *totient-primorial′-asymp-equiv*:

(λk. *totient* (*primorial′ k*)) ∼[*at-top*] (λk. *third-mertens-const* ∗ *primorial′ k* / *ln* *k*)
⟨*proof*⟩

lemma (**in** *prime-number-theorem*) *totient-primorial′-asymp-equiv′*:
(λk. *totient* (*primorial′ k*)) ∼[*at-top*]
(λk. *third-mertens-const* ∗ *primorial′ k* / *ln* (*ln* (*primorial′ k*)))
⟨*proof*⟩

All in all, $\varphi(n)$ has minimal order $cn/\ln\ln n$:

theorem (**in** *prime-number-theorem*)
liminf-totient: *liminf* (λn. *totient n* ∗ *ln* (*ln n*) / *n*) = *third-mertens-const*
(**is** - = *ereal ?c*)
⟨*proof*⟩
end

References

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

[2] A. Hildebrand. Introduction to Analytic Number Theory (lecture notes). hhttps://faculty.math.illinois.edu/~hildebr/ant/.