Bertrand's postulate

Julian Biendarra, Manuel Eberl

January 18, 2017

Abstract

Bertrand's postulate is an early result on the distribution of prime numbers: For every positive integer n, there exists a prime number that lies strictly between n and $2n$.

The proof is ported from John Harrison's formalisation in HOL Light [1]. It proceeds by first showing that the property is true for all n greater than or equal to 600 and then showing that it also holds for all n below 600 by case distinction.

Contents

1 Bertrand's postulate

theory *Bertrand-Discrete-Sqrt*
imports *Main* ~~/*src*/*HOL*/*Library*/*Discrete*
begin

1.1 Facts about the discrete square root

lemma *Suc-sqrt-power2-gt*: $n < (Suc\ (Discrete.sqrt\ n))\ \hat{}\ 2$
⟨*proof*⟩

lemma *le-sqrt-iff*: $x \leq Discrete.sqrt\ y \longleftrightarrow x\ \hat{}\ 2 \leq y$
⟨*proof*⟩

lemma *le-sqrtI*: $x\ \hat{}\ 2 \leq y \Longrightarrow x \leq Discrete.sqrt\ y$
⟨*proof*⟩

lemma *sqrt-le-iff*: *Discrete.sqrt* $y \leq x \longleftrightarrow (\forall z.\ z\hat{}2 \leq y \longrightarrow z \leq x)$
⟨*proof*⟩

lemma *sqrt-leI*:
$(\bigwedge z.\ z\hat{}2 \leq y \Longrightarrow z \leq x) \Longrightarrow$ *Discrete.sqrt* $y \leq x$
⟨*proof*⟩

lemma *sqrt-Suc*:
Discrete.sqrt (*Suc* n) = (*if* $\exists m.$ *Suc* $n = m\hat{}2$ *then Suc* (*Discrete.sqrt* n) *else Discrete.sqrt* n)
⟨*proof*⟩

end

theory *Bertrand*
imports
Complex-Main
~~/*src*/*HOL*/*Number-Theory*/*Number-Theory*
~~/*src*/*HOL*/*Library*/*Discrete*
~~/*src*/*HOL*/*Decision-Procs*/*Approximation*
Bertrand-Discrete-Sqrt
begin

1.2 Preliminary definitions

definition *primepow* :: *nat* ⇒ *bool* **where**
primepow $q \longleftrightarrow (\exists\ p\ k.\ 1 \leq k \wedge$ *prime* $p \wedge q = p\hat{}k)$

definition *primepows* :: *nat* ⇒ *nat set* **where**
primepows $n = \{x{::}nat.$ *primepow* $x \wedge x$ *dvd* $n\}$

definition *primepow-even* :: *nat* ⇒ *bool* **where**
primepow-even $q \longleftrightarrow (\exists\ p\ k.\ 1 \leq k \wedge$ *prime* $p \wedge q = p\hat{}(2{*}k))$

definition *primepow-odd* :: *nat* ⇒ *bool* **where**
primepow-odd $q \longleftrightarrow (\exists\ p\ k.\ 1 \leq k \wedge$ *prime* $p \wedge q = p\hat{}(2{*}k{+}1))$

abbreviation *isprimedivisor* :: *nat* ⇒ *nat* ⇒ *bool* **where**
isprimedivisor $q\ p \equiv$ *prime* $p \wedge p$ *dvd* q

definition *aprimedivisor* :: *nat* ⇒ *nat* **where**
aprimedivisor q = (*LEAST* p. *isprimedivisor* $q\ p$)

definition *pre-mangoldt* :: *nat* ⇒ *nat* **where**
pre-mangoldt d = (*if primepow* d *then aprimedivisor* d *else* 1)

definition *mangoldt* :: *nat* ⇒ *real* **where**
mangoldt d = (*if primepow* d *then ln* (*aprimedivisor* d) *else* 0)

definition *mangoldt-even* :: *nat* ⇒ *real* **where**
mangoldt-even d = (*if primepow-even d then ln* (*aprimedivisor d*) *else 0*)

definition *mangoldt-odd* :: *nat* ⇒ *real* **where**
mangoldt-odd d = (*if primepow-odd d then ln* (*aprimedivisor d*) *else 0*)

definition *mangoldt-1* :: *nat* ⇒ *real* **where**
mangoldt-1 d = (*if prime d then ln d else 0*)

definition *psi* :: *nat* ⇒ *real* **where**
psi n = (∑ *d*=*1*..*n*. *mangoldt d*)

definition *psi-even* :: *nat* ⇒ *real* **where**
psi-even n = (∑ *d*=*1*..*n*. *mangoldt-even d*)

definition *psi-odd* :: *nat* ⇒ *real* **where**
psi-odd n = (∑ *d*=*1*..*n*. *mangoldt-odd d*)

abbreviation (*input*) *psi-even-2* :: *nat* ⇒ *real* **where**
psi-even-2 n ≡ (∑ *d*=*2*..*n*. *mangoldt-even d*)

abbreviation (*input*) *psi-odd-2* :: *nat* ⇒ *real* **where**
psi-odd-2 n ≡ (∑ *d*=*2*..*n*. *mangoldt-odd d*)

definition *theta* :: *nat* ⇒ *real* **where**
theta n = (∑ *p*=*1*..*n*. *if prime p then ln* (*real p*) *else 0*)

1.3 Properties of prime powers

lemma
assumes *n* ≠ *0 n* ≠ *1*
shows *prime-aprimedivisor*: *prime* (*aprimedivisor n*)
and *aprimedivisor-dvd*: *aprimedivisor n dvd n*
⟨*proof*⟩

lemma *finite-primepows* [*simp*]: *n* ≠ *0* ⟹ *finite* (*primepows n*)
⟨*proof*⟩

lemma *primepow-gt-Suc-0*: *primepow n* ⟹ *n* > *Suc 0*
⟨*proof*⟩

lemma *aprimedivisor-of-prime* [*simp*]: *prime p* ⟹ *aprimedivisor p* = *p*
⟨*proof*⟩

lemma *aprimedivisor-primepow-power*:
assumes *primepow n k* > *0*
shows *aprimedivisor* (*n* ^ *k*) = *aprimedivisor n*
⟨*proof*⟩

lemma *aprimedivisor-prime-power*:
assumes *prime p k* > *0*
shows *aprimedivisor* (*p* ^ *k*) = *p*
⟨*proof*⟩

lemma *prime-factorization-primepow*:
assumes *primepow n*
shows *prime-factorization n* =
replicate-mset (*multiplicity* (*aprimedivisor n*) *n*) (*aprimedivisor n*)
⟨*proof*⟩

lemma *primepow-decompose*:
assumes *primepow n*
shows *aprimedivisor n* ^ *multiplicity* (*aprimedivisor n*) *n* = *n*
⟨*proof*⟩

lemma *aprimedivisor-vimage*:
assumes *prime p*
shows *aprimedivisor* −‘ {*p*} ∩ *primepows n* = {*p* ^ *k* |*k*. *k* > *0* ∧ *p* ^ *k dvd* *n*}
⟨*proof*⟩

lemma *aprimedivisor-primepows-conv-prime-factorization*:
assumes [*simp*]: *n* ≠ *0*
shows *image-mset aprimedivisor* (*mset-set* (*primepows n*)) = *prime-factorization* *n*
(**is** *?lhs* = *?rhs*)
⟨*proof*⟩

lemma *aprimedivisor*:
assumes *n* ≠ *1*
shows *prime* (*aprimedivisor n*) *aprimedivisor n dvd n*
⟨*proof*⟩

lemma *aprimedivisor-gt-1*:
assumes *n* ≠ *1*
shows *aprimedivisor n* > *1*
⟨*proof*⟩

lemma *aprimedivisor-le*:
assumes *n* > *1*
shows *aprimedivisor n* ≤ *n*
⟨*proof*⟩

lemma *primepow-even-imp-primepow*:
assumes *primepow-even n*
shows *primepow n*
⟨*proof*⟩

lemma *primepow-odd-imp-primepow*:
assumes *primepow-odd n*
shows *primepow n*
⟨*proof*⟩

lemma *not-primepow-0* [*simp*]: ¬*primepow 0*
⟨*proof*⟩

lemma *not-primepow-Suc-0* [*simp*]: ¬*primepow* (*Suc 0*)
⟨*proof*⟩

lemma *aprimedivisor-primepow*:
assumes *prime p p dvd n primepow n*
shows *aprimedivisor* (*p* ∗ *n*) = *p aprimedivisor n* = *p*
⟨*proof*⟩

lemma *primepow-power-iff*:
primepow (*p* ^ *n*) ⟷ *primepow p* ∧ *n* > *0*
⟨*proof*⟩

lemma *primepow-prime* [*simp*]: *prime n* ⟹ *primepow n*
⟨*proof*⟩

lemma *primepow-prime-power* [*simp*]: *prime p* ⟹ *primepow* (*p* ^ *n*) ⟷ *n* > *0*
⟨*proof*⟩

lemma *primepow-multD*:
assumes *primepow* (*a* ∗ *b*)
shows *a* = *1* ∨ *primepow a b* = *1* ∨ *primepow b*
⟨*proof*⟩

lemma *primepow-mult-aprimedivisorI*:
assumes *primepow n*
shows *primepow* (*aprimedivisor n* ∗ *n*)
⟨*proof*⟩

lemma *primepow-odd-altdef*:
primepow-odd n ⟷
primepow n ∧ *odd* (*multiplicity* (*aprimedivisor n*) *n*) ∧ *multiplicity* (*aprimedivisor n*) *n* > *1*
⟨*proof*⟩

lemma *primepow-even-altdef*:
primepow-even n ⟷ *primepow n* ∧ *even* (*multiplicity* (*aprimedivisor n*) *n*)
⟨*proof*⟩

lemma *prime-elem-aprimedivisor*: *d* > *1* ⟹ *prime-elem* (*aprimedivisor d*)
⟨*proof*⟩

lemma *aprimedivisor-gt-0* [*simp*]: $d > 1 \Longrightarrow$ *aprimedivisor* $d > 0$
⟨*proof*⟩

lemma *aprimedivisor-not-zero* [*simp*]: $d > 1 \Longrightarrow$ *aprimedivisor* $d \neq 0$
⟨*proof*⟩

lemma *aprimedivisor-gt-Suc-0* [*simp*]: $d > 1 \Longrightarrow$ *aprimedivisor* $d >$ *Suc 0*
⟨*proof*⟩

lemma *aprimedivisor-not-Suc-0* [*simp*]: $d > 1 \Longrightarrow$ *aprimedivisor* $d \neq$ *Suc 0*
⟨*proof*⟩

lemma *multiplicity-aprimedivisor-gt-0* [*simp*]:
$d > 1 \Longrightarrow$ *multiplicity* (*aprimedivisor* d) $d > 0$
⟨*proof*⟩

lemma *primepow-odd-mult*:
assumes $d > 1$
shows *primepow-odd* (*aprimedivisor* $d * d$) $\longleftrightarrow$ *primepow-even* d
⟨*proof*⟩

lemma *primepowI*:
prime $p \Longrightarrow k \geq 1 \Longrightarrow p \hat{} k = n \Longrightarrow$ *primepow* $n \wedge$ *aprimedivisor* $n = p$
⟨*proof*⟩

lemma *not-primepowI*:
assumes *prime* p *prime* q $p \neq q$ p *dvd* n q *dvd* n
shows $\neg$*primepow* n
⟨*proof*⟩

lemma *pre-mangoldt-primepow*:
assumes *primepow* n *aprimedivisor* $n = p$
shows *pre-mangoldt* $n = p$
⟨*proof*⟩

lemma *pre-mangoldt-notprimepow*:
assumes $\neg$*primepow* n
shows *pre-mangoldt* $n = 1$
⟨*proof*⟩

lemma *not-primepow-1*: $\neg$*primepow 1* ⟨*proof*⟩

lemma *sum-prime-factorization-conv-sum-primepows*:
assumes $n \neq 0$
shows $(\sum q \in$ *primepows* $n.\ f\ ($*aprimedivisor* $q)) = (\sum p \in \#$ *prime-factorization* $n.\ f\ p)$
⟨*proof*⟩

1.4 Bounding the psi function

context
begin

private lemma *Ball-insertD*:
assumes $\forall x{\in}insert\ y\ A.\ P\ x$
shows $P\ y\ \forall x{\in}A.\ P\ x$
⟨*proof*⟩ **lemma** *meta-eq-TrueE*: $PROP\ A \equiv Trueprop\ True \Longrightarrow PROP\ A$
⟨*proof*⟩ **lemma** *pre-mangoldt-pos*: $pre\text{-}mangoldt\ n > 0$
⟨*proof*⟩ **lemma** *psi-conv-pre-mangoldt*: $psi\ n = ln\ (real\ (prod\ pre\text{-}mangoldt\ \{1..n\}))$
⟨*proof*⟩ **lemma** *eval-psi-aux1*: $psi\ 0 = ln\ (real\ (numeral\ Num.One))$
⟨*proof*⟩ **lemma** *eval-psi-aux2*:
assumes $psi\ m = ln\ (real\ (numeral\ x))\ pre\text{-}mangoldt\ n = y\ m + 1 = n\ numeral\ x * y = z$
shows $psi\ n = ln\ (real\ z)$
⟨*proof*⟩ **lemma** *Ball-atLeast0AtMost-doubleton*:
assumes $psi\ 0 \le 4407\ /\ 2048 * ln\ 2 * real\ 0$
assumes $psi\ 1 \le 4407\ /\ 2048 * ln\ 2 * real\ 1$
shows $(\forall x{\in}\{0..1\}.\ psi\ x \le 4407\ /\ 2048 * ln\ 2 * real\ x)$
⟨*proof*⟩ **lemma** *Ball-atLeast0AtMost-insert*:
assumes $(\forall x{\in}\{0..m\}.\ psi\ x \le 4407\ /\ 2048 * ln\ 2 * real\ x)$
assumes $psi\ (numeral\ n) \le 4407\ /\ 2048 * ln\ 2 * real\ (numeral\ n)\ m = pred\text{-}numeral\ n$
shows $(\forall x{\in}\{0..numeral\ n\}.\ psi\ x \le 4407\ /\ 2048 * ln\ 2 * real\ x)$
⟨*proof*⟩ **lemma** *eval-psi-ineq-aux*:
assumes $psi\ n = x\ x \le 4407\ /\ 2048 * ln\ 2 * n$
shows $psi\ n \le 4407\ /\ 2048 * ln\ 2 * n$
⟨*proof*⟩ **definition** *prime-nat-consts* **where**
$prime\text{-}nat\text{-}consts\ (A :: nat\ set) \equiv Trueprop\ (\forall p{\in}A.\ 1 < p \wedge \{\} \neq \{Suc\ 0\} \wedge (\forall n{\in}\{1<..<p\}.\ \neg\ n\ dvd\ p) \wedge (0 = Suc\ 0 \wedge 1 = (2{::}nat) \wedge (2{::}nat) = 3))$

⟨*ML*⟩

end

lemma *of-nat-prod-mset*: $prod\text{-}mset\ (image\text{-}mset\ of\text{-}nat\ A) = of\text{-}nat\ (prod\text{-}mset\ A)$
⟨*proof*⟩

lemma *prod-mset-pos*: $(\bigwedge x :: 'a :: linordered\text{-}semidom.\ x \in\# A \Longrightarrow x > 0) \Longrightarrow prod\text{-}mset\ A > 0$
⟨*proof*⟩

lemma *ln-msetprod*:
assumes $\bigwedge x.\ x \in\# I \Longrightarrow x > 0$
shows $(\sum p{::}nat{\in}\#I.\ ln\ p) = ln\ (\prod p{\in}\#I.\ p)$
⟨*proof*⟩

lemma *ln-fact*: $ln\ (fact\ n) = (\sum d{=}1..n.\ ln\ d)$

⟨*proof*⟩

lemma *ln-primefact*:
assumes $n \neq 0$
shows $ln\ n = (\sum d{=}1..n.\ if\ primepow\ d \wedge d\ dvd\ n\ then\ ln\ (aprimedivisor\ d)\ else\ 0)$
(**is** *?lhs* = *?rhs*)
⟨*proof*⟩

lemma *divisors*:
fixes $x\ d{::}nat$
assumes $x \in \{1..n\}$
assumes $d\ dvd\ x$
shows $\exists k{\in}\{1..n\ div\ d\}.\ x = d * k$
⟨*proof*⟩

lemma *ln-fact-conv-mangoldt*:
shows $ln\ (fact\ n) = (\sum d{=}1..n.\ mangoldt\ d * floor\ (n\ /\ d))$
⟨*proof*⟩

lemma *mangoldt-pos*: $0 \leq mangoldt\ d$
⟨*proof*⟩

lemma *floor-conv-div-nat*:
$of\text{-}int\ (floor\ (real\ m\ /\ real\ n)) = real\ (m\ div\ n)$
⟨*proof*⟩

lemma *frac-conv-mod-nat*:
$frac\ (real\ m\ /\ real\ n) = real\ (m\ mod\ n)\ /\ real\ n$
⟨*proof*⟩

lemma *div-2-mult-2-bds*:
fixes $n\ d :: nat$
assumes $d > 0$
shows $0 \leq \lfloor n\ /\ d \rfloor - 2 * \lfloor (n\ div\ 2)\ /\ d \rfloor\ \lfloor n\ /\ d \rfloor - 2 * \lfloor (n\ div\ 2)\ /\ d \rfloor \leq 1$
⟨*proof*⟩

lemma *n-div-d-eq-1*: $d \in \{n\ div\ 2 + 1..n\} \Longrightarrow \lfloor real\ n\ /\ real\ d \rfloor = 1$
⟨*proof*⟩

lemma *psi-bounds-ln-fact*:
shows $ln\ (fact\ n) - 2 * ln\ (fact\ (n\ div\ 2)) \leq psi\ n$
$psi\ n - psi\ (n\ div\ 2) \leq ln\ (fact\ n) - 2 * ln\ (fact\ (n\ div\ 2))$
⟨*proof*⟩

lemma *ln-fact-bounds*:
assumes $n > 0$
shows $abs(ln\ (fact\ n) - n * ln\ n + n) \leq 1 + ln\ n$

⟨*proof*⟩

lemma *ln-fact-diff-bounds*:
abs(*ln* (*fact n*) − *2* ∗ *ln* (*fact* (*n div 2*)) − *n* ∗ *ln 2*) ≤ *4* ∗ *ln* (*if n* = *0 then 1 else n*) + *3*
⟨*proof*⟩

lemma *psi-bounds-induct*:
real n ∗ *ln 2* − (*4* ∗ *ln* (*real* (*if n* = *0 then 1 else n*)) + *3*) ≤ *psi n*
psi n − *psi* (*n div 2*) ≤ *real n* ∗ *ln 2* + (*4* ∗ *ln* (*real* (*if n* = *0 then 1 else n*)) + *3*)
⟨*proof*⟩

lemma *overpower-lemma*:
fixes *f g* :: *real* ⇒ *real*
assumes *f a* ≤ *g a*
assumes ⋀*x*. *a* ≤ *x* ⟹ ((λ*x*. *g x* − *f x*) *has-real-derivative* (*d x*)) (*at x*)
assumes ⋀*x*. *a* ≤ *x* ⟹ *d x* ≥ *0*
assumes *a* ≤ *x*
shows *f x* ≤ *g x*
⟨*proof*⟩

lemma *psi-bounds-sustained-induct*:
assumes *4* ∗ *ln* (*1* + *2* ^ *j*) + *3* ≤ *d* ∗ *ln 2* ∗ (*1* + *2*^*j*)
assumes *4* / (*1* + *2*^*j*) ≤ *d* ∗ *ln 2*
assumes *0* ≤ *c*
assumes *c* / *2* + *d* + *1* ≤ *c*
assumes *j* ≤ *k*
assumes ⋀*n*. *n* ≤ *2*^*k* ⟹ *psi n* ≤ *c* ∗ *ln 2* ∗ *n*
assumes *n* ≤ *2*^(*Suc k*)
shows *psi n* ≤ *c* ∗ *ln 2* ∗ *n*
⟨*proof*⟩

lemma *psi-bounds-sustained*:
assumes ⋀*n*. *n* ≤ *2*^*k* ⟹ *psi n* ≤ *c* ∗ *ln 2* ∗ *n*
assumes *4* ∗ *ln* (*1* + *2*^*k*) + *3* ≤ (*c*/*2* − *1*) ∗ *ln 2* ∗ (*1* + *2*^*k*)
assumes *4* / (*1* + *2*^*k*) ≤ (*c*/*2* − *1*) ∗ *ln 2*
assumes *c* ≥ *0*
shows *psi n* ≤ *c* ∗ *ln 2* ∗ *n*
⟨*proof*⟩

lemma *psi-ubound-log*: *psi n* ≤ *4407* / *2048* ∗ *ln 2* ∗ *n*
⟨*proof*⟩

lemma *psi-ubound-3-2*: *psi n* ≤ *3*/*2* ∗ *n*
⟨*proof*⟩

1.5 Doubling psi and theta

lemma *of-nat-ge-1-iff*: $(of\text{-}nat\ x :: 'a :: linordered\text{-}semidom) \geq 1 \longleftrightarrow x \geq 1$
⟨*proof*⟩

lemma *psi-residues-compare-2*:
$psi\text{-}odd\text{-}2\ n \leq psi\text{-}even\text{-}2\ n$
⟨*proof*⟩

lemma *psi-residues-compare*:
$psi\text{-}odd\ n \leq psi\text{-}even\ n$
⟨*proof*⟩

lemma *primepow-iff-even-sqr*:
$primepow\ n \longleftrightarrow primepow\text{-}even\ (n\hat{}2)$
⟨*proof*⟩

lemma *psi-sqrt*: $psi\ (Discrete.sqrt\ n) = psi\text{-}even\ n$
⟨*proof*⟩

lemma *primepow-gt-0*: $primepow\ n \Longrightarrow n > 0$
⟨*proof*⟩

lemma *multiplicity-aprimedivisor-Suc-0-iff*:
assumes $primepow\ n$
shows $multiplicity\ (aprimedivisor\ n)\ n = Suc\ 0 \longleftrightarrow prime\ n$
⟨*proof*⟩

lemma *primepow-cases*:
$primepow\ d \longleftrightarrow$
$(\ \ primepow\text{-}even\ d \wedge \neg\ primepow\text{-}odd\ d \wedge \neg\ prime\ d) \vee$
$(\neg\ primepow\text{-}even\ d \wedge\ \ primepow\text{-}odd\ d \wedge \neg\ prime\ d) \vee$
$(\neg\ primepow\text{-}even\ d \wedge \neg\ primepow\text{-}odd\ d \wedge\ \ prime\ d)$
⟨*proof*⟩

lemma *mangoldt-split*:
$mangoldt\ d = mangoldt\text{-}1\ d + mangoldt\text{-}even\ d + mangoldt\text{-}odd\ d$
⟨*proof*⟩

lemma *psi-split*: $psi\ n = theta\ n + psi\text{-}even\ n + psi\text{-}odd\ n$
⟨*proof*⟩

lemma *psi-mono*: $m \leq n \Longrightarrow psi\ m \leq psi\ n$
⟨*proof*⟩

lemma *psi-pos*: $0 \leq psi\ n$
⟨*proof*⟩

lemma *mangoldt-odd-pos*: $0 \leq mangoldt\text{-}odd\ d$
⟨*proof*⟩

lemma *psi-odd-mono*: $m \leq n \Longrightarrow$ *psi-odd* $m \leq$ *psi-odd* n
⟨*proof*⟩

lemma *psi-odd-pos*: $0 \leq$ *psi-odd* n
⟨*proof*⟩

lemma *psi-theta*:
theta n + *psi* (*Discrete.sqrt* n) ≤ *psi* n *psi* $n \leq$ *theta* $n + 2 *$ *psi* (*Discrete.sqrt* n)
⟨*proof*⟩

lemma *sum-minus-one*:
$(\sum x \in \{1..y\}.\ (-\ 1 :: real)\ \hat{}\ (x + 1)) = (if\ odd\ y\ then\ 1\ else\ 0)$
⟨*proof*⟩

lemma *div-invert*:
fixes $x\ y\ n :: nat$
assumes $x > 0\ y > 0\ y \leq n\ div\ x$
shows $x \leq n\ div\ y$
⟨*proof*⟩

lemma *sum-expand-lemma*:
$(\sum d{=}1..n.\ (-1)\ \hat{}\ (d + 1) * psi\ (n\ div\ d)) =$
$(\sum d = 1..n.\ (if\ odd\ (n\ div\ d)\ then\ 1\ else\ 0) * mangoldt\ d)$
⟨*proof*⟩

lemma *floor-half-interval*:
fixes $n\ d :: nat$
assumes $d \neq 0$
shows *real* $(n\ div\ d)$ − *real* $(2 * ((n\ div\ 2)\ div\ d)) = (if\ odd\ (n\ div\ d)\ then\ 1\ else\ 0)$
⟨*proof*⟩

lemma *fact-expand-psi*:
ln (*fact* n) − $2 *$ *ln* (*fact* $(n\ div\ 2)$) = $(\sum d{=}1..n.\ (-1)\ \hat{}(d+1) * psi\ (n\ div\ d))$
⟨*proof*⟩

lemma *psi-expansion-cutoff*:
assumes $m \leq p$
shows $(\sum d{=}1..2{*}m.\ (-1)\ \hat{}(d+1) * psi\ (n\ div\ d)) \leq (\sum d{=}1..2{*}p.\ (-1)\ \hat{}(d+1) * psi\ (n\ div\ d))$
$(\sum d{=}1..2{*}p{+}1.\ (-1)\ \hat{}(d+1) * psi\ (n\ div\ d)) \leq (\sum d{=}1..2{*}m{+}1.\ (-1)\ \hat{}(d+1) * psi\ (n\ div\ d))$
⟨*proof*⟩

lemma *fact-psi-bound-even*:
assumes *even* k
shows $(\sum d{=}1..k.\ (-1)\ \hat{}(d+1) * psi\ (n\ div\ d)) \leq ln\ (fact\ n) - 2 * ln\ (fact$

$(n\ div\ 2))$
⟨*proof*⟩

lemma *fact-psi-bound-odd*:
assumes *odd k*
shows $ln\ (fact\ n) - 2 * ln\ (fact\ (n\ div\ 2)) \leq (\sum d{=}1..k.\ (-1)\hat{}(d+1) * psi\ (n\ div\ d))$
⟨*proof*⟩

lemma *fact-psi-bound-2-3*:
$psi\ n - psi\ (n\ div\ 2) \leq ln\ (fact\ n) - 2 * ln\ (fact\ (n\ div\ 2))$
$ln\ (fact\ n) - 2 * ln\ (fact\ (n\ div\ 2)) \leq psi\ n - psi\ (n\ div\ 2) + psi\ (n\ div\ 3)$
⟨*proof*⟩

lemma *psi-double-lemma*:
assumes $n \geq 1200$
shows $n/6 \leq psi\ n - psi\ (n\ div\ 2)$
⟨*proof*⟩

lemma *theta-double-lemma*:
assumes $n \geq 1200$
shows $theta\ (n\ div\ 2) < theta\ n$
⟨*proof*⟩

1.6 Proof of the main result

lemma *theta-mono*: *mono theta*
⟨*proof*⟩

lemma *theta-lessE*:
assumes $theta\ m < theta\ n\ m \geq 1$
obtains p **where** $p \in \{m<..n\}\ prime\ p$
⟨*proof*⟩

theorem *bertrand*:
fixes $n :: nat$
assumes $n > 1$
shows $\exists p{\in}\{n<..<2*n\}.\ prime\ p$
⟨*proof*⟩

end

References

[1] J. Harrison. HOL Light, Bertrand's postulate. https://github.com/jrh13/hol-light/blob/master/100/bertrand.ml.