

Bertrand's postulate

Julian Biendarra, Manuel Eberl

May 26, 2024

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

0.1	Auxiliary facts	1
0.2	Preliminary definitions	2
0.3	Properties of prime powers	3
0.4	Deriving a recurrence for the psi function	4
0.5	Bounding the psi function	5
0.6	Doubling psi and theta	8
0.7	Proof of the main result	10
0.8	Proof of Mertens' first theorem	10

theory *Bertrand*

imports

Complex-Main

HOL-Number-Theory.Number-Theory

HOL-Library.Discrete

HOL-Decision-Proc.Approximation-Bounds

HOL-Library.Code-Target-Numeral

Pratt-Certificate.Pratt-Certificate

begin

0.1 Auxiliary facts

lemma *ln-2-le*: $\ln 2 \leq 355 / (512 :: \text{real})$

<proof>

lemma *ln-2-ge*: $\ln 2 \geq (5677 / 8192 :: \text{real})$

<proof>

lemma *ln-2-ge'*: $\ln (2 :: \text{real}) \geq 2/3$ **and** *ln-2-le'*: $\ln (2 :: \text{real}) \leq 16/23$
<proof>

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

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

lemma *frac-conv-mod-nat*:
frac $(\text{real } m / \text{real } n) = \text{real } (m \text{ mod } n) / \text{real } n$
<proof>

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

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

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

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

lemma *overpower-lemma*:
fixes $f g :: \text{real} \Rightarrow \text{real}$
assumes $f a \leq g a$
assumes $\bigwedge x. a \leq x \implies ((\lambda x. g x - f x) \text{ has-real-derivative } (d x)) (\text{at } x)$
assumes $\bigwedge x. a \leq x \implies d x \geq 0$
assumes $a \leq x$
shows $f x \leq g x$
<proof>

0.2 Preliminary definitions

definition *primepow-even* :: $\text{nat} \Rightarrow \text{bool}$ **where**
primepow-even $q \iff (\exists p k. 1 \leq k \wedge \text{prime } p \wedge q = p^{2*k})$

definition *primepow-odd* :: $\text{nat} \Rightarrow \text{bool}$ **where**
primepow-odd $q \iff (\exists p k. 1 \leq k \wedge \text{prime } p \wedge q = p^{2*k+1})$

abbreviation *(input) isprimedivisor* :: $\text{nat} \Rightarrow \text{nat} \Rightarrow \text{bool}$ **where**

$isprimedivisor\ q\ p \equiv prime\ p \wedge p\ dvd\ q$

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

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

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

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

definition $psi :: nat \Rightarrow real$ **where**
 $psi\ n = (\sum\ d=1..n.\ mangoldt\ d)$

definition $psi-even :: nat \Rightarrow real$ **where**
 $psi-even\ n = (\sum\ d=1..n.\ mangoldt-even\ d)$

definition $psi-odd :: nat \Rightarrow real$ **where**
 $psi-odd\ n = (\sum\ d=1..n.\ mangoldt-odd\ d)$

abbreviation (*input*) $psi-even-2 :: nat \Rightarrow real$ **where**
 $psi-even-2\ n \equiv (\sum\ d=2..n.\ mangoldt-even\ d)$

abbreviation (*input*) $psi-odd-2 :: nat \Rightarrow real$ **where**
 $psi-odd-2\ n \equiv (\sum\ d=2..n.\ mangoldt-odd\ d)$

definition $theta :: nat \Rightarrow real$ **where**
 $theta\ n = (\sum\ p=1..n.\ if\ prime\ p\ then\ ln\ (real\ p)\ else\ 0)$

0.3 Properties of prime powers

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 $primepow-odd-altdef$:
 $primepow-odd\ n \longleftrightarrow$
 $primepow\ n \wedge odd\ (multiplicity\ (aprimedivisor\ n)\ n) \wedge multiplicity\ (aprimedivisor\ n)\ n > 1$
(*proof*)

lemma *primepow-even-altdef*:
primepow-even $n \longleftrightarrow \text{primepow } n \wedge \text{even } (\text{multiplicity } (\text{aprimedivisor } n) \ n)$
 ⟨*proof*⟩

lemma *primepow-odd-mult*:
assumes $d > \text{Suc } 0$
shows $\text{primepow-odd } (\text{aprimedivisor } d * d) \longleftrightarrow \text{primepow-even } d$
 ⟨*proof*⟩

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

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

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

0.4 Deriving a recurrence for the psi function

lemma *ln-fact-bounds*:
assumes $n > 0$
shows $\text{abs}(\ln (\text{fact } n) - n * \ln n + n) \leq 1 + \ln n$
 ⟨*proof*⟩

lemma *ln-fact-diff-bounds*:
 $\text{abs}(\ln (\text{fact } n) - 2 * \ln (\text{fact } (n \ \text{div } 2)) - n * \ln 2) \leq 4 * \ln (\text{if } n = 0 \text{ then } 1$
 $\text{else } n) + 3$
 ⟨*proof*⟩

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

context
begin

private lemma *divisors*:

fixes $x d :: nat$

assumes $x \in \{1..n\}$

assumes $d \text{ dvd } x$

shows $\exists k \in \{1..n \text{ div } d\}. x = d * k$

<proof>

lemma *ln-fact-conv-mangoldt*: $\ln (\text{fact } n) = (\sum_{d=1..n}. \text{mangoldt } d * \text{floor } (n / d))$

<proof>

end

context

begin

private lemma *div-2-mult-2-bds*:

fixes $n d :: nat$

assumes $d > 0$

shows $0 \leq \lfloor n / d \rfloor - 2 * \lfloor (n \text{ div } 2) / d \rfloor \leq \lfloor n / d \rfloor - 2 * \lfloor (n \text{ div } 2) / d \rfloor \leq 1$

<proof> **lemma** *n-div-d-eq-1*: $d \in \{n \text{ div } 2 + 1..n\} \implies \lfloor \text{real } n / \text{real } d \rfloor = 1$

<proof>

lemma *psi-bounds-ln-fact*:

shows $\ln (\text{fact } n) - 2 * \ln (\text{fact } (n \text{ div } 2)) \leq \text{psi } n$

$\text{psi } n - \text{psi } (n \text{ div } 2) \leq \ln (\text{fact } n) - 2 * \ln (\text{fact } (n \text{ div } 2))$

<proof>

end

lemma *psi-bounds-induct*:

$\text{real } n * \ln 2 - (4 * \ln (\text{real } (\text{if } n = 0 \text{ then } 1 \text{ else } n)) + 3) \leq \text{psi } n$

$\text{psi } n - \text{psi } (n \text{ div } 2) \leq \text{real } n * \ln 2 + (4 * \ln (\text{real } (\text{if } n = 0 \text{ then } 1 \text{ else } n)) + 3)$

<proof>

0.5 Bounding the psi function

In this section, we will first prove the relatively tight estimate $\text{psi } n \leq 3 / 2 + \ln 2 * \text{real } n$ for $n \leq (128::'a)$ and then use the recurrence we have just derived to extend it to $\text{psi } n \leq 551 / 256$ for $n \leq (1024::'a)$, at which point applying the recurrence can be used to prove the same bound for arbitrarily big numbers.

First of all, we will prove the bound for $n \leq (128::'a)$ using reflection and approximation.

context

begin

private lemma *Ball-insertD*:
assumes $\forall x \in \text{insert } y \ A. \ P \ x$
shows $P \ y \ \forall x \in A. \ P \ x$
 $\langle \text{proof} \rangle$ **lemma** *meta-eq-TrueE*: $PROP \ A \equiv \text{Trueprop } \text{True} \implies PROP \ A$
 $\langle \text{proof} \rangle$ **lemma** *pre-mangoldt-pos*: $\text{pre-mangoldt } n > 0$
 $\langle \text{proof} \rangle$ **lemma** *psi-conv-pre-mangoldt*: $\text{psi } n = \ln (\text{real } (\text{prod } \text{pre-mangoldt } \{1..n\}))$
 $\langle \text{proof} \rangle$ **lemma** *eval-psi-aux1*: $\text{psi } 0 = \ln (\text{real } (\text{numeral } \text{Num.One}))$
 $\langle \text{proof} \rangle$ **lemma** *eval-psi-aux2*:
assumes $\text{psi } m = \ln (\text{real } (\text{numeral } x)) \ \text{pre-mangoldt } n = y \ m + 1 = n \ \text{numeral}$
 $x * y = z$
shows $\text{psi } n = \ln (\text{real } z)$
 $\langle \text{proof} \rangle$ **lemma** *Ball-atLeast0AtMost-doubleton*:
assumes $\text{psi } 0 \leq 3 / 2 * \ln 2 * \text{real } 0$
assumes $\text{psi } 1 \leq 3 / 2 * \ln 2 * \text{real } 1$
shows $(\forall x \in \{0..1\}. \ \text{psi } x \leq 3 / 2 * \ln 2 * \text{real } x)$
 $\langle \text{proof} \rangle$ **lemma** *Ball-atLeast0AtMost-insert*:
assumes $(\forall x \in \{0..m\}. \ \text{psi } x \leq 3 / 2 * \ln 2 * \text{real } x)$
assumes $\text{psi } (\text{numeral } n) \leq 3 / 2 * \ln 2 * \text{real } (\text{numeral } n) \ m = \text{pred-numeral}$
 n
shows $(\forall x \in \{0..\text{numeral } n\}. \ \text{psi } x \leq 3 / 2 * \ln 2 * \text{real } x)$
 $\langle \text{proof} \rangle$ **lemma** *eval-psi-ineq-aux*:
assumes $\text{psi } n = x \ x \leq 3 / 2 * \ln 2 * n$
shows $\text{psi } n \leq 3 / 2 * \ln 2 * n$
 $\langle \text{proof} \rangle$ **lemma** *eval-psi-ineq-aux2*:
assumes $\text{numeral } m \wedge 2 \leq (2::\text{nat}) \wedge (3 * n)$
shows $\ln (\text{real } (\text{numeral } m)) \leq 3 / 2 * \ln 2 * \text{real } n$
 $\langle \text{proof} \rangle$ **lemma** *eval-psi-ineq-aux-mono*:
assumes $\text{psi } n = x \ \text{psi } m = x \ \text{psi } n \leq 3 / 2 * \ln 2 * n \ n \leq m$
shows $\text{psi } m \leq 3 / 2 * \ln 2 * m$
 $\langle \text{proof} \rangle$

lemma *not-primepow-1-nat*: $\neg \text{primepow } (1 :: \text{nat})$ $\langle \text{proof} \rangle$

$\langle ML \rangle$

end

context
begin

private lemma *psi-ubound-aux*:
defines $f \equiv \lambda x::\text{real}. (4 * \ln x + 3) / (\ln 2 * x)$
assumes $x \geq 2 \ x \leq y$
shows $f \ x \geq f \ y$
 $\langle \text{proof} \rangle$

These next rules are used in combination with $\text{real } ?n * \ln 2 - (4 * \ln (\text{real } (if ?n = 0 \text{ then } 1 \text{ else } ?n)) + 3) \leq \text{psi } ?n$

$psi\ ?n - psi\ (?n\ div\ 2) \leq real\ ?n * ln\ 2 + (4 * ln\ (real\ (if\ ?n = 0\ then\ 1\ else\ ?n)) + 3)$ and $\forall n \in \{0..128\}. psi\ n \leq 3 / 2 * ln\ 2 * real\ n$ to extend the upper bound for psi from values no greater than 128 to values no greater than 1024. The constant factor of the upper bound changes every time, but once we have reached 1024, the recurrence is self-sustaining in the sense that we do not have to adjust the constant factor anymore in order to double the range.

lemma *psi-ubound-log-double-cases'*:

assumes $\bigwedge n. n \leq m \implies psi\ n \leq c * ln\ 2 * real\ n$
 $n \leq m' \ m' = 2 * m$
 $c \leq c' \ c \geq 0 \ m \geq 1 \ c' \geq 1 + c/2 + (4 * ln\ (m+1) + 3) / (ln\ 2 * (m+1))$

shows $psi\ n \leq c' * ln\ 2 * real\ n$

<proof>

end

lemma *psi-ubound-log-double-cases*:

assumes $\forall n \leq m. psi\ n \leq c * ln\ 2 * real\ n$
 $c' \geq 1 + c/2 + (4 * ln\ (m+1) + 3) / (ln\ 2 * (m+1))$
 $m' = 2 * m \ c \leq c' \ c \geq 0 \ m \geq 1$

shows $\forall n \leq m'. psi\ n \leq c' * ln\ 2 * real\ n$

<proof>

lemma *psi-ubound-log-1024*:

$\forall n \leq 1024. psi\ n \leq 551 / 256 * ln\ 2 * real\ n$
<proof>

lemma *psi-bounds-sustained-induct*:

assumes $4 * ln\ (1 + 2^{\wedge}j) + 3 \leq d * ln\ 2 * (1 + 2^{\wedge}j)$

assumes $4 / (1 + 2^{\wedge}j) \leq d * ln\ 2$

assumes $0 \leq c$

assumes $c / 2 + d + 1 \leq c$

assumes $j \leq k$

assumes $\bigwedge n. n \leq 2^{\wedge}k \implies psi\ n \leq c * ln\ 2 * n$

assumes $n \leq 2^{\wedge}(Suc\ k)$

shows $psi\ n \leq c * ln\ 2 * n$

<proof>

lemma *psi-bounds-sustained*:

assumes $\bigwedge n. n \leq 2^{\wedge}k \implies psi\ n \leq c * ln\ 2 * n$

assumes $4 * ln\ (1 + 2^{\wedge}k) + 3 \leq (c/2 - 1) * ln\ 2 * (1 + 2^{\wedge}k)$

assumes $4 / (1 + 2^{\wedge}k) \leq (c/2 - 1) * ln\ 2$

assumes $c \geq 0$

shows $psi\ n \leq c * ln\ 2 * n$

<proof>

lemma *psi-ubound-log*: $psi\ n \leq 551 / 256 * ln\ 2 * n$

<proof>

lemma *psi-ubound-3-2*: $\psi n \leq 3/2 * n$
{proof}

0.6 Doubling psi and theta

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

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

lemma *primepow-iff-even-sqr*:
 $\text{primepow } n \iff \text{primepow-even } (n^2)$
{proof}

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

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

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

lemma *psi-mono*: $m \leq n \implies \psi m \leq \psi n$ {proof}

lemma *psi-pos*: $0 \leq \psi n$
{proof}

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

lemma *psi-odd-mono*: $m \leq n \implies \psi\text{-odd } m \leq \psi\text{-odd } n$
{proof}

lemma *psi-odd-pos*: $0 \leq \psi\text{-odd } n$
{proof}

lemma *psi-theta*:
 $\theta n + \psi (\text{Discrete.sqrt } n) \leq \psi n \leq \theta n + 2 * \psi (\text{Discrete.sqrt } n)$
{proof}

context
begin

private lemma *sum-minus-one*:

$(\sum x \in \{1..y\}. (-1 :: real) \wedge (x + 1)) = (if\ odd\ y\ then\ 1\ else\ 0)$

<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*:

$(\sum d=1..n. (-1) \wedge (d + 1) * psi\ (n\ div\ d)) =$

$(\sum d = 1..n. (if\ odd\ (n\ div\ d)\ then\ 1\ else\ 0) * mangoldt\ d)$

<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*:

$ln\ (fact\ n) - 2 * ln\ (fact\ (n\ div\ 2)) = (\sum d=1..n. (-1) \wedge (d+1) * psi\ (n\ div\ d))$

<proof>

end

lemma *psi-expansion-cutoff*:

assumes $m \leq p$

shows $(\sum d=1..2*m. (-1) \wedge (d+1) * psi\ (n\ div\ d)) \leq (\sum d=1..2*p. (-1) \wedge (d+1) * psi\ (n\ div\ d))$

$(\sum d=1..2*p+1. (-1) \wedge (d+1) * psi\ (n\ div\ d)) \leq (\sum d=1..2*m+1. (-1) \wedge (d+1) * psi\ (n\ div\ d))$

<proof>

lemma *fact-psi-bound-even*:

assumes *even* k

shows $(\sum d=1..k. (-1) \wedge (d+1) * psi\ (n\ div\ d)) \leq ln\ (fact\ n) - 2 * ln\ (fact\ (n\ div\ 2))$

<proof>

lemma *fact-psi-bound-odd*:

assumes *odd* k

shows $ln\ (fact\ n) - 2 * ln\ (fact\ (n\ div\ 2)) \leq (\sum d=1..k. (-1) \wedge (d+1) * psi\ (n\ div\ d))$

<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 *ub-ln-1200*: $\ln 1200 \leq 57 / (8 :: \text{real})$
 ⟨*proof*⟩

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

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

0.7 Proof of the main result

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

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

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

0.8 Proof of Mertens' first theorem

The following proof of Mertens' first theorem was ported from John Harrison's HOL Light proof by Larry Paulson:

lemma *sum-integral-ubound-decreasing'*:
fixes $f :: \text{real} \Rightarrow \text{real}$
assumes $m \leq n$
and *der*: $\bigwedge x. x \in \{\text{of-nat } m - 1 .. \text{of-nat } n\} \implies (g \text{ has-field-derivative } f \ x)$
 (at x)
and *le*: $\bigwedge x \ y. [\text{real } m - 1 \leq x; x \leq y; y \leq \text{real } n] \implies f \ y \leq f \ x$
shows $(\sum k = m .. n. f \ (\text{of-nat } k)) \leq g \ (\text{of-nat } n) - g \ (\text{of-nat } m - 1)$
 ⟨*proof*⟩

lemma *Mertens-lemma*:
assumes $n \neq 0$
shows $|\sum d = 1 .. n. \text{mangoldt } d / \text{real } d - \ln n| \leq 4$
 ⟨*proof*⟩

lemma *Mertens-mangoldt-versus-ln*:
assumes $I \subseteq \{1 .. n\}$

shows $|(\sum_{i \in I} \text{mangoldt } i / i) - (\sum p \mid \text{prime } p \wedge p \in I. \ln p / p)| \leq 3$
(**is** $|\text{lhs}| \leq 3$)
<proof>

proposition *Mertens:*

assumes $n \neq 0$

shows $|(\sum p \mid \text{prime } p \wedge p \leq n. \ln p / \text{of-nat } p) - \ln n| \leq \gamma$
<proof>

end

References

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