Bertrand's postulate

Julian Biendarra, Manuel Eberl

February 23, 2021

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

theory *Bertrand*
imports
Complex-Main
HOL−Number-Theory.Number-Theory
HOL−Library.Discrete
HOL−Decision-Procs.Approximation-Bounds
HOL−Library.Code-Target-Numeral
Pratt-Certificate.Pratt-Certificate
begin

0.1 Auxiliary facts

lemma *ln-2-le*: $ln\ 2 \leq 355\ /\ (512 :: real)$
⟨*proof*⟩

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

⟨*proof*⟩

lemma *ln-2-ge'*: *ln* (*2* :: *real*) ≥ *2/3* **and** *ln-2-le'*: *ln* (*2* :: *real*) ≤ *16/23*
⟨*proof*⟩

lemma *of-nat-ge-1-iff*: (*of-nat x* :: *'a* :: *linordered-semidom*) ≥ *1* ⟷ *x* ≥ *1*
⟨*proof*⟩

lemma *floor-conv-div-nat*:
of-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 *of-nat-prod-mset*: *prod-mset* (*image-mset of-nat A*) = *of-nat* (*prod-mset A*)
⟨*proof*⟩

lemma *prod-mset-pos*: (⋀*x* :: *'a* :: *linordered-semidom*. *x* ∈# *A* ⟹ *x* > *0*) ⟹ *prod-mset A* > *0*
⟨*proof*⟩

lemma *ln-msetprod*:
assumes ⋀*x*. *x* ∈#*I* ⟹ *x* > *0*
shows (∑ *p*::*nat*∈#*I*. *ln p*) = *ln* (∏ *p*∈#*I*. *p*)
⟨*proof*⟩

lemma *ln-fact*: *ln* (*fact n*) = (∑ *d*=*1*..*n*. *ln d*)
⟨*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*⟩

0.2 Preliminary definitions

definition *primepow-even* :: *nat* ⇒ *bool* **where**
primepow-even q ⟷ (∃ *p k*. *1* ≤ *k* ∧ *prime p* ∧ *q* = *p*^(*2*∗*k*))

definition *primepow-odd* :: *nat* ⇒ *bool* **where**
primepow-odd q ⟷ (∃ *p k*. *1* ≤ *k* ∧ *prime p* ∧ *q* = *p*^(*2*∗*k*+*1*))

abbreviation (*input*) *isprimedivisor* :: *nat* ⇒ *nat* ⇒ *bool* **where**

isprimedivisor q p ≡ prime p ∧ p dvd q

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

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

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

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 ⟷
primepow n ∧ odd (multiplicity (aprimedivisor n) n) ∧ multiplicity (aprimedivisor n) n > 1
⟨*proof*⟩

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

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

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

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

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

0.4 Deriving a recurrence for the psi function

lemma *ln-fact-bounds*:
assumes *n* > *0*
shows *abs*(*ln* (*fact n*) − *n* ∗ *ln n* + *n*) ≤ *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 *ln-primefact*:
assumes *n* ≠ (*0*::*nat*)
shows *ln n* = (∑ *d*=*1*..*n*. *if primepow d* $\wedge$ *d dvd n then ln* (*aprimedivisor d*) *else 0*)
(**is** *?lhs* = *?rhs*)
⟨*proof*⟩

context
begin

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

end

context
begin

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

end

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

0.5 Bounding the psi function

In this section, we will first prove the relatively tight estimate $psi\ n \leq 3\ /\ 2 + ln\ 2 * real\ n$ for $n \leq (128::'a)$ and then use the recurrence we have just derived to extend it to $psi\ n \leq 551\ /\ 256$ 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 $\forall x{\in}insert\ y\ A.\ P\ x$
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 $psi\ 0 \leq 3\ /\ 2 * ln\ 2 * real\ 0$
assumes $psi\ 1 \leq 3\ /\ 2 * ln\ 2 * real\ 1$
shows $(\forall x{\in}\{0..1\}.\ psi\ x \leq 3\ /\ 2 * ln\ 2 * real\ x)$
⟨*proof*⟩ **lemma** *Ball-atLeast0AtMost-insert*:
assumes $(\forall x{\in}\{0..m\}.\ psi\ x \leq 3\ /\ 2 * ln\ 2 * real\ x)$
assumes $psi\ (numeral\ n) \leq 3\ /\ 2 * ln\ 2 * real\ (numeral\ n)\ m = pred\text{-}numeral\ n$
shows $(\forall x{\in}\{0..numeral\ n\}.\ psi\ x \leq 3\ /\ 2 * ln\ 2 * real\ x)$
⟨*proof*⟩ **lemma** *eval-psi-ineq-aux*:
assumes $psi\ n = x\ x \leq 3\ /\ 2 * ln\ 2 * n$
shows $psi\ n \leq 3\ /\ 2 * ln\ 2 * n$
⟨*proof*⟩ **lemma** *eval-psi-ineq-aux2*:
assumes $numeral\ m\ \hat{}\ 2 \leq (2{::}nat)\ \hat{}\ (3 * n)$
shows $ln\ (real\ (numeral\ m)) \leq 3\ /\ 2 * ln\ 2 * real\ n$
⟨*proof*⟩ **lemma** *eval-psi-ineq-aux-mono*:
assumes $psi\ n = x\ psi\ m = x\ psi\ n \leq 3\ /\ 2 * ln\ 2 * n\ n \leq m$
shows $psi\ m \leq 3\ /\ 2 * ln\ 2 * m$
⟨*proof*⟩

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

⟨*ML*⟩

end

context
begin

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

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

*psi ?n − psi (?n div 2) ≤ real ?n * ln 2 + (4 * ln (real (if ?n = 0 then 1 else ?n)) + 3)* and *∀ n∈{0..128}. psi n ≤ 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 *⋀n. n ≤ m ⟹ psi n ≤ c * ln 2 * real n n ≤ m' m' = 2*m*
    *c ≤ c' c ≥ 0 m ≥ 1 c' ≥ 1 + c/2 + (4 * ln (m+1) + 3) / (ln 2 * (m+1))*
  shows *psi n ≤ c' * ln 2 * real n*
⟨*proof*⟩

end

lemma *psi-ubound-log-double-cases*:
  assumes *∀ n≤m. psi n ≤ c * ln 2 * real n*
    *c' ≥ 1 + c/2 + (4 * ln (m+1) + 3) / (ln 2 * (m+1))*
    *m' = 2*m c ≤ c' c ≥ 0 m ≥ 1*
  shows *∀ n≤m'. psi n ≤ c' * ln 2 * real n*
  ⟨*proof*⟩

lemma *psi-ubound-log-1024*:
  *∀ n≤1024. psi n ≤ 551 / 256 * ln 2 * real n*
⟨*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 ≤ 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-odd-2 n $\leq$ *psi-even-2 n*
⟨*proof*⟩

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

lemma *primepow-iff-even-sqr*:
primepow n $\longleftrightarrow$ *primepow-even* (*n*^*2*)
⟨*proof*⟩

lemma *psi-sqrt*: *psi* (*Discrete.sqrt n*) = *psi-even n*
⟨*proof*⟩

lemma *mangoldt-split*:
mangoldt d = *mangoldt-1 d* + *mangoldt-even d* + *mangoldt-odd d*
⟨*proof*⟩

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

context
begin

private lemma *sum-minus-one*:
(∑ x ∈ {1..y}. (− 1 :: real) ^ (x + 1)) = (*if odd y then 1 else 0*)
⟨*proof*⟩ **lemma** *div-invert*:
fixes *x y n* :: *nat*
assumes *x* > *0 y* > *0 y* ≤ *n div x*
shows *x* ≤ *n div y*
⟨*proof*⟩

lemma *sum-expand-lemma*:
(∑ d=1..n. (−1) ^ (d + 1) ∗ *psi* (*n div d*)) =
(∑ 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* ≠ *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*)) = (∑ d=1..n. (−1)^(d+1) ∗ *psi* (*n div d*))
⟨*proof*⟩

end

lemma *psi-expansion-cutoff*:
assumes *m* ≤ *p*
shows (∑ d=1..2∗m. (−1)^(d+1) ∗ *psi* (*n div d*)) ≤ (∑ d=1..2∗p. (−1)^(d+1) ∗ *psi* (*n div d*))
(∑ d=1..2∗p+1. (−1)^(d+1) ∗ *psi* (*n div d*)) ≤ (∑ d=1..2∗m+1. (−1)^(d+1) ∗ *psi* (*n div d*))
⟨*proof*⟩

lemma *fact-psi-bound-even*:
assumes *even k*
shows (∑ d=1..k. (−1)^(d+1) ∗ *psi* (*n div d*)) ≤ *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*)) ≤ (∑ d=1..k. (−1)^(d+1) ∗ *psi* (*n div d*))
⟨*proof*⟩

lemma *fact-psi-bound-2-3*:
psi n − *psi* (*n div 2*) ≤ *ln* (*fact n*) − *2* ∗ *ln* (*fact* (*n div 2*))
ln (*fact n*) − *2* ∗ *ln* (*fact* (*n div 2*)) ≤ *psi n* − *psi* (*n div 2*) + *psi* (*n div 3*)
⟨*proof*⟩

lemma *ub-ln-1200*: $ln\ 1200 \leq 57\ /\ (8 :: real)$
⟨*proof*⟩

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

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

0.7 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*⟩

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

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

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

shows $|(\sum i{\in}I.\ mangoldt\ i\ /\ i) - (\sum p \mid prime\ p \wedge p \in I.\ ln\ p\ /\ p)| \leq 3$
(**is** $|?lhs| \leq 3$)
⟨*proof*⟩

proposition *Mertens*:
assumes $n \neq 0$
shows $|(\sum p \mid prime\ p \wedge p \leq n.\ ln\ p\ /\ of\text{-}nat\ p) - ln\ n| \leq 7$
⟨*proof*⟩

end

References

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