# Bertrand's postulate 

Julian Biendarra, Manuel Eberl

March 11, 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 $2 n$.

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 ..... 3
0.3 Properties of prime powers ..... 4
0.4 Deriving a recurrence for the psi function ..... 6
0.5 Bounding the psi function ..... 15
0.6 Doubling psi and theta ..... 24
0.7 Proof of the main result ..... 34
0.8 Proof of Mertens' first theorem ..... 35
theory Bertrand
imports
Complex-MainHOL-Number-Theory.Number-Theory
HOL-Library.Discrete
HOL-Decision-Procs.Approximation-Bounds
HOL-Library.Code-Target-Numeral
Pratt-Certificate.Pratt-Certificatebegin

### 0.1 Auxiliary facts

```
lemma ln-2-le:ln 2 \leq 355 / (512 :: real)
proof -
    have ln 2 \leq real-of-float (ub-ln2 12) by (rule ub-ln2)
    also have ub-ln2 12 = Float 5680 (- 13) by code-simp
```

```
    finally show ?thesis by simp
qed
lemma ln-2-ge: ln 2 \geq (5677 / 8192 :: real)
proof -
    have ln 2 \geq real-of-float (lb-ln2 12) by (rule lb-ln2)
    also have lb-ln2 12 = Float 5677 (-13) by code-simp
    finally show ?thesis by simp
qed
lemma ln-2-ge': ln (2 :: real) \geq2/3 and ln-2-le': ln (2 :: real) \leq 16/23
    using ln-2-le ln-2-ge by simp-all
lemma of-nat-ge-1-iff:(of-nat x :: 'a :: linordered-semidom) \geq1 \longleftrightarrowx \geq1
    using of-nat-le-iff[of 1 x] by (subst (asm) of-nat-1)
lemma floor-conv-div-nat:
    of-int (floor (real m / real n)) = real (m div n)
    by (subst floor-divide-of-nat-eq) simp
lemma frac-conv-mod-nat:
    frac (real m / real n) = real (m mod n) / real n
    by (cases n=0)
        (simp-all add: frac-def floor-conv-div-nat field-simps of-nat-mult
                        [symmetric] of-nat-add [symmetric] del: of-nat-mult of-nat-add)
lemma of-nat-prod-mset: prod-mset (image-mset of-nat A) =of-nat (prod-mset A)
    by (induction A) simp-all
lemma prod-mset-pos:(\bigwedgex :: 'a :: linordered-semidom. }x\in#A\Longrightarrowx>0)
prod-mset A>0
    by (induction A) simp-all
lemma ln-msetprod:
    assumes }\x.x\in#I\Longrightarrowx>
    shows (\sump::nat\in#I. ln p)= ln (\prodp\in#I.p)
    using assms by (induction I) (simp-all add: of-nat-prod-mset ln-mult prod-mset-pos)
lemma ln-fact: ln (fact n)=(\sumd=1..n. ln d)
    by (induction n) (simp-all add: ln-mult)
lemma overpower-lemma:
    fixes fg :: real => real
    assumes fa\leqga
    assumes \x.a\leqx\Longrightarrow((\lambdax.g x - f x) has-real-derivative (d x)) (at x)
    assumes \x.a\leqx\Longrightarrowdx\geq0
    assumes a\leqx
    shows fx\leqgx
proof (cases a<x)
```


## case True

with assms have $\exists z . z>a \wedge z<x \wedge g x-f x-(g a-f a)=(x-a) * d z$ by (intro MVT2) auto
then obtain $z$ where $z: z>a z<x g x-f x-(g a-f a)=(x-a) * d z$ by blast
hence $f x=g x+(f a-g a)+(a-x) * d z$ by (simp add: algebra-simps)
also from assms have $f a-g a \leq 0$ by (simp add: algebra-simps)
also from assms $z$ have $(a-x) * d z \leq 0 * d z$
by (intro mult-right-mono) simp-all
finally show ?thesis by simp
qed (insert assms, auto)

### 0.2 Preliminary definitions

definition primepow-even :: nat $\Rightarrow$ bool where

$$
\text { primepow-even } q \longleftrightarrow\left(\exists p k .1 \leq k \wedge \text { prime } p \wedge q=p^{\wedge}(2 * k)\right)
$$

definition primepow-odd :: nat $\Rightarrow$ bool where primepow-odd $q \longleftrightarrow\left(\exists p k .1 \leq k \wedge\right.$ prime $\left.p \wedge q=p^{\wedge}(2 * k+1)\right)$
abbreviation (input) isprimedivisor $::$ nat $\Rightarrow$ nat $\Rightarrow$ bool where
isprimedivisor $q$ p 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 $n=\left(\sum d=1 . . n\right.$. mangoldt $\left.d\right)$
definition psi-even :: nat $\Rightarrow$ real where psi-even $n=\left(\sum d=1 . . n\right.$. mangoldt-even $\left.d\right)$
definition psi-odd :: nat $\Rightarrow$ real where psi-odd $n=\left(\sum d=1 . . n\right.$. mangoldt-odd $\left.d\right)$
abbreviation (input) psi-even-2 :: nat $\Rightarrow$ real where psi-even-2 $n \equiv$ ( $\sum d=$ 2..n. mangoldt-even $\left.d\right)$
abbreviation (input) psi-odd-2 :: nat $\Rightarrow$ real where psi-odd-2 $n \equiv\left(\sum d=2 . . n\right.$. mangoldt-odd d $)$
definition theta $::$ nat $\Rightarrow$ real where
theta $n=\left(\sum p=1 . . n\right.$. 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 -
    from assms obtain pk where 1 \leq k prime p n= p^(2*k)
        unfolding primepow-even-def by blast
    moreover from <1\leqk\rangle have 2 *k>0
        by simp
    ultimately show ?thesis unfolding primepow-def by blast
qed
```

lemma primepow-odd-imp-primepow:
assumes primepow-odd $n$
shows primepow $n$
proof -
from assms obtain $p k$ where $1 \leq k$ prime $p n=p^{\wedge}(2 * k+1)$
unfolding primepow-odd-def by blast
moreover from $\langle 1 \leq k\rangle$ have Suc $(2 * k)>0$
by $\operatorname{simp}$
ultimately show ?thesis unfolding primepow-def
by (auto simp del: power-Suc)
qed
lemma primepow-odd-altdef:
primepow-odd $n \longleftrightarrow$
primepow $n \wedge$ odd (multiplicity (aprimedivisor $n$ ) $n$ ) $\wedge$ multiplicity (aprimedivisor
n) $n>1$
proof (intro iffI conjI; (elim conjE)?)
assume primepow-odd $n$
then obtain $p k$ where $n: k \geq 1$ prime $p n=p^{\wedge}(2 * k+1)$
by (auto simp: primepow-odd-def)
thus odd (multiplicity (aprimedivisor n) n) multiplicity (aprimedivisor n) $n>1$
by (simp-all add: aprimedivisor-primepow prime-elem-multiplicity-mult-distrib)
next
assume A: primepow $n$ and $B$ : odd (multiplicity (aprimedivisor n) n)
and C: multiplicity (aprimedivisor $n$ ) $n>1$
from $A$ obtain $p k$ where $n: k \geq 1$ prime $p n=p^{\wedge} k$
by (auto simp: primepow-def Suc-le-eq)
with $B C$ have odd $k k>1$
by (simp-all add: aprimedivisor-primepow prime-elem-multiplicity-mult-distrib)
then obtain $j$ where $j: k=2 * j+1 j>0$ by (auto elim!: oddE)
with $n$ show primepow-odd $n$ by (auto simp: primepow-odd-def intro!: exI[of -
p, OF exI[of - j]])
qed (auto dest: primepow-odd-imp-primepow)
lemma primepow-even-altdef:
primepow-even $n \longleftrightarrow$ primepow $n \wedge$ even (multiplicity (aprimedivisor $n$ ) $n$ )
proof (intro iffI conjI; (elim conjE)?)
assume primepow-even $n$
then obtain $p k$ where $n: k \geq 1$ prime $p n=p^{\wedge}(2 * k)$
by (auto simp: primepow-even-def)
thus even (multiplicity (aprimedivisor n) n)
by (simp-all add: aprimedivisor-primepow prime-elem-multiplicity-mult-distrib)
next
assume $A$ : primepow $n$ and $B$ : even (multiplicity (aprimedivisor $n$ ) $n$ )
from $A$ obtain $p k$ where $n: k \geq 1$ prime $p n=p^{\wedge} k$
by (auto simp: primepow-def Suc-le-eq)
with $B$ have even $k$
by (simp-all add: aprimedivisor-primepow prime-elem-multiplicity-mult-distrib)
then obtain $j$ where $j: k=2 * j$ by (auto elim!: evenE)
from $j n$ have $j \neq 0$ by (intro notI) simp-all
with $j n$ show primepow-even $n$
by (auto simp: primepow-even-def intro!: exI[of - p, OF exI[of - j]])
qed (auto dest: primepow-even-imp-primepow)
lemma primepow-odd-mult:
assumes $d>$ Suc 0
shows primepow-odd (aprimedivisor $d * d) \longleftrightarrow$ primepow-even $d$ using assms
by (auto simp: primepow-odd-altdef primepow-even-altdef primepow-mult-aprimedivisorI aprimedivisor-primepow prime-aprimedivisor' aprimedivisor-dvd ${ }^{\prime}$ prime-elem-multiplicity-mult-distrib prime-elem-aprimedivisor-nat dest!: primepow-multD)
lemma pre-mangoldt-primepow:
assumes primepow $n$ aprimedivisor $n=p$
shows pre-mangoldt $n=p$
using assms by (simp add: pre-mangoldt-def)
lemma pre-mangoldt-notprimepow:
assumes $\neg$ primepow $n$
shows pre-mangoldt $n=1$
using assms by (simp add: pre-mangoldt-def)
lemma primepow-cases:
primepow $d \longleftrightarrow$
( primepow-even $d \wedge \neg$ primepow-odd $d \wedge \neg$ prime $d) \vee$
$(\neg$ primepow-even $d \wedge$ primepow-odd $d \wedge \neg$ prime $d) \vee$
$(\neg$ primepow-even $d \wedge \neg$ primepow-odd $d \wedge$ prime $d)$
by (auto simp: primepow-even-altdef primepow-odd-altdef multiplicity-aprimedivisor-Suc-0-iff elim!: oddE intro!: Nat.grOI)

### 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) \leq1+ln n
proof -
    have }\foralln\in{0<..}.\existsz>\mathrm{ real n. z<real (n+1)^ real (n+1)*ln (real (n+
1)) -
                real n * ln (real n) =(real (n+1) - real n)*(lnz+1)
    by (intro ballI MVT2) (auto intro!: derivative-eq-intros)
    hence }\foralln\in{0<..}. \existsz>\mathrm{ real n. z<real (n+1)^real (n+1)*ln(real (n+
1)) -
                real n* ln (real n)=(lnz+1) by (simp add:algebra-simps)
    from bchoice[OF this] obtain k:: nat }=>\mathrm{ real
        where lb: real n<kn and ub: kn< real (n+1) and
                mvt: real (n+1)*ln (real (n+1)) - real n*ln (real n) = ln (kn) + 1
                if n>0 for n::nat by blast
    have *: (n+1)*\operatorname{ln}(n+1)=(\sumi=1..n. ln(ki)+1) for n::nat
    proof (induction n)
    case (Suc n)
            have (\sumi=1..n+1. ln (ki) + 1) = (\sumi=1..n. ln (ki) + 1) + ln (k
(n+1))+1
            by simp
            also from Suc.IH have (\sumi=1..n. ln (ki)+1)=real (n+1)*\operatorname{ln}(\mathrm{ real}
(n+1))..
            also from mvt[of n+1] have ... = real (n+2) * ln (real (n+2)) - ln (k
(n+1))-1
            by simp
    finally show ?case
            by simp
    qed simp
    have **: abs((\sumi=1..n+1. ln i) - ((n+1)*\operatorname{ln}(n+1)-(n+1)))\leq1+
ln(n+1) for n::nat
    proof -
        have (\sumi=1..n+1. ln i)\leq(\sumi=1..n.ln i) + ln (n+1)
            by simp
    also have (\sumi=1..n. ln i)\leq(\sumi=1..n. ln (ki))
            by (intro sum-mono, subst ln-le-cancel-iff) (auto simp: Suc-le-eq dest: lb ub)
    also have ... = (\sumi=1..n. ln (ki)+1) - n
            by (simp add: sum.distrib)
    also from * have ... = (n+1)*ln (n+1) - n
            by simp
    finally have a-minus-b: (\sumi=1..n+1. ln i) - ((n+1)* ln (n+1) - (n+1))
< 1 + ln (n+1)
            by simp
    from * have (n+1)*ln (n+1) - n=(\sumi=1..n. ln (ki)+1)-n
                by simp
    also have ... = (\sumi=1..n. ln (ki))
            by (simp add: sum.distrib)
```

```
    also have ... \leq (\sumi=1..n. ln (i+1))
            by (intro sum-mono, subst ln-le-cancel-iff) (auto simp: Suc-le-eq dest: lb ub)
    also from sum.shift-bounds-cl-nat-ivl[of ln 11 n] have ... = (\sumi=1+1..n+1.
ln i) ..
    also have ... =(\sumi=1..n+1. ln i)
        by (rule sum.mono-neutral-left) auto
    finally have b-minus-a: ((n+1)*\operatorname{ln}(n+1)-(n+1))-(\sumi=1..n+1.ln i)
\leq1
    by simp
    have 0\leqln (n+1)
        by simp
    with b-minus-a have }((n+1)*\operatorname{ln}(n+1)-(n+1))-(\sumi=1..n+1.ln i)
1+ln(n+1)
        by linarith
    with a-minus-b show ?thesis
        by linarith
    qed
    from \langlen> 0` have n\geq1 by simp
    thus ?thesis
    proof (induction n rule: dec-induct)
        case base
        then show ?case by simp
    next
        case (step n)
        from ln-fact[of n+1] **[of n] show ?case by simp
    qed
qed
lemma ln-fact-diff-bounds:
    abs(ln}(fact n)-2*\operatorname{ln}(fact (n\operatorname{div}2))-n*\operatorname{ln}2)\leq4*\operatorname{ln}(\mathrm{ if }n=0\mathrm{ then 1
else n) + 3
proof (cases n div 2 = 0)
    case True
    hence }n\leq1\mathrm{ by simp
    with ln-le-minus-one[of 2::real] show ?thesis by (cases n) simp-all
next
    case False
    then have n>1 by simp
    let ?a = real n*ln 2
    let ?b}=4*\operatorname{ln}(\mathrm{ real n) + 3
    let ?l1 = ln (fact (n div 2))
    let ?a1 = real (n div 2)* ln (real (n div 2)) - real ( }n\mathrm{ div 2)
    let ?b1 = 1 + ln (real (n div 2))
    let ?12 = ln (fact n)
    let ?a2 = real n*ln (real n) - real n
    let ?b2 = 1 + ln (real n)
    have abs-a:abs(?a - (?a2 - 2 *?a1)) \leq?b - 2*?b1 - ?b2
    proof (cases even n)
    case True
```

then have real $(2 *(n \operatorname{div} 2))=$ real $n$
by simp
then have $n$-div-2: real $(n$ div 2$)=$ real $n / 2$
by $\operatorname{simp}$
from $\langle n>1\rangle$ have $*: \operatorname{abs}(? a-(? a 2-2 * ? a 1))=0$
by (simp add: n-div-2 ln-div algebra-simps)
from $\langle$ even $n\rangle$ and $\langle n>1\rangle$ have $0 \leq \ln ($ real $n)-\ln ($ real ( $n$ div 2))
by (auto elim: evenE)
also have $2 * \ldots \leq 3 * \ln ($ real $n)-2 * \ln ($ real $(n$ div 2) $)$
using $\langle n>1\rangle$ by (auto intro!: ln-ge-zero)
also have $\ldots=? b-2 * ? b 1-? b 2$ by simp
finally show ?thesis using * by simp

## next

case False
then have $\operatorname{real}(2 *(n \operatorname{div} 2))=\operatorname{real}(n-1)$
by $\operatorname{simp}$
with $\langle n>1\rangle$ have $n$-div-2: real $(n$ div 2$)=($ real $n-1) / 2$
by $\operatorname{simp}$
from 〈odd $n\rangle\langle n$ div $2 \neq 0\rangle$ have $n \geq 3$
by presburger
have $? a-(? a 2-2 * ? a 1)=$ real $n * \ln 2-\operatorname{real} n * \ln ($ real $n)+$ real $n+$ $2 * \operatorname{real}(n \operatorname{div} 2) * \ln (\operatorname{real}(n \operatorname{div} 2))-2 * \operatorname{real}(n \operatorname{div} 2)$
by (simp add: algebra-simps)
also from $n$-div-2 have $2 *$ real $(n \operatorname{div} 2)=$ real $n-1$
by $\operatorname{simp}$
also have real $n * \ln 2-$ real $n * \ln ($ real $n)+$ real $n+$

$$
(\text { real } n-1) * \ln (\text { real }(n \operatorname{div} 2))-(\text { real } n-1)
$$

$$
=\operatorname{real} n *(\ln (\text { real } n-1)-\ln (\text { real } n))-\ln (\text { real }(n \text { div } 2))+1
$$

using $\langle n>1\rangle$ by (simp add: algebra-simps $n$-div-2 ln-div)
finally have $\operatorname{lhs}: a b s(? a-(? a 2-2 * ? a 1))=$ $\operatorname{abs}(\operatorname{real} n *(\ln ($ real $n-1)-\ln ($ real $n))-\ln ($ real $(n \operatorname{div} 2))+1)$
by $\operatorname{simp}$
from $\langle n>1\rangle$ have real $n *(\ln ($ real $n-1)-\ln ($ real $n)) \leq 0$
by (simp add: algebra-simps mult-left-mono)
moreover from $\langle n>1\rangle$ have $\ln ($ real ( $n$ div 2) $) \leq \ln ($ real $n)$ by simp
moreover \{
have exp $1 \leq(3::$ real $)$ by (rule exp-le)
also from $\langle n \geq 3\rangle$ have $\ldots \leq \exp (\ln ($ real $n))$ by $\operatorname{simp}$
finally have $\ln ($ real $n) \geq 1$ by simp
\}
ultimately have $u b$ : real $n *(\ln ($ real $n-1)-\ln ($ real $n))-\ln ($ real $(n$ div 2)) $+1 \leq$

$$
3 * \ln (\text { real } n)-2 * \ln (\text { real }(n \operatorname{div} 2)) \text { by } \operatorname{simp}
$$

have mon: real $n^{\prime} *\left(\ln \left(\right.\right.$ real $\left.n^{\prime}\right)-\ln \left(\right.$ real $\left.\left.n^{\prime}-1\right)\right) \leq$ real $n *(\ln ($ real $n)-\ln ($ real $n-1))$
if $n \geq 3 n^{\prime} \geq n$ for $n n^{\prime}::$ nat
proof (rule DERIV-nonpos-imp-nonincreasing[where $f=\lambda x . x *(\ln x-\ln$ $(x-1))])$
fix $t$ assume $t$ : real $n \leq t t \leq$ real $n^{\prime}$
with that have $1 /(t-1) \geq \ln (1+1 /(t-1))$
by (intro ln-add-one-self-le-self) simp-all
also from $t$ that have $\ln (1+1 /(t-1))=\ln t-\ln (t-1)$
by (simp add: ln-div [symmetric] field-simps)
finally have $\ln t-\ln (t-1) \leq 1 /(t-1)$.
with that $t$
show $\exists y .((\lambda x . x *(\ln x-\ln (x-1)))$ has-field-derivative $y)($ at $t) \wedge y \leq 0$ by $($ intro exI[of - $1 /(1-t)+\ln t-\ln (t-1)])$
(force intro!: derivative-eq-intros simp: field-simps)+
qed (use that in simp-all)
from $\langle n>1\rangle$ have $\ln 2=\ln ($ real $n)-\ln ($ real $n / 2)$
by (simp add: ln-div)
also from $\langle n>1\rangle$ have $\ldots \leq \ln ($ real $n)-\ln ($ real $(n$ div 2) $)$
by $\operatorname{simp}$
finally have $*: 3 * \ln 2+\ln ($ real $(n$ div 2$)) \leq 3 * \ln ($ real $n)-2 * \ln ($ real $(n$ div 2))
by $\operatorname{simp}$
have $-\operatorname{real} n *(\ln ($ real $n-1)-\ln ($ real $n))+\ln (\operatorname{real}(n \operatorname{div} 2))-1=$ real $n *(\ln ($ real $n)-\ln ($ real $n-1))-1+\ln ($ real $(n$ div 2 $))$
by (simp add: algebra-simps)
also have real $n *(\ln ($ real $n)-\ln ($ real $n-1)) \leq 3 *(\ln 3-\ln (3-1))$
using mon $[O F-\langle n \geq 3\rangle]$ by $\operatorname{simp}$
also \{
have Some (Float $3(-1))=u b-\ln 13$ by code-simp
from $u b-\ln (1)[$ OF this $]$ have $\ln 3 \leq(1.6::$ real) by simp
also have $1.6-1 / 3 \leq 2 *(2 / 3::$ real $)$ by simp
also have $2 / 3 \leq \ln$ (2 :: real) by (rule ln-2-ge')
finally have $\ln 3-1 / 3 \leq 2 * \ln (2::$ real $)$ by $\operatorname{simp}$
\}
hence $3 *(\ln 3-\ln (3-1))-1 \leq 3 * \ln (2::$ real $)$ by simp
also note *
finally have $-\operatorname{real} n *(\ln ($ real $n-1)-\ln ($ real $n))+\ln ($ real $(n$ div 2 $))-$ $1 \leq$

$$
3 * \ln (\text { real } n)-2 * \ln (\text { real }(n \text { div 2 })) \text { by } \operatorname{simp}
$$

hence $l h^{\prime}: \operatorname{abs}($ real $n *(\ln ($ real $n-1)-\ln ($ real $n))-\ln ($ real $(n$ div 2) $)+$ 1) $\leq$

$$
3 * \ln (\operatorname{real} n)-2 * \ln (\operatorname{real}(n \operatorname{div} 2))
$$

using $u b$ by simp
have rhs: ?b-2*?b1-?b2 $=3 * \ln ($ real $n)-2 * \ln ($ real $(n \operatorname{div} 2))$
by $\operatorname{simp}$
from $\langle n>1\rangle$ have $\ln ($ real $(n$ div 2) $) \leq 3 * \ln ($ real $n)-2 * \ln ($ real $(n$ div 2))
by $\operatorname{simp}$
with rhs lhs $l h s^{\prime}$ show ?thesis

```
    by \(\operatorname{simp}\)
    qed
    then have minus- \(a:-? a \leq ? b-2 * ? b 1-? b 2-(? a 2-2 * ? a 1)\)
    by \(\operatorname{simp}\)
    from \(a b s-a\) have \(a: ? a \leq ? b-2 * ? b 1-? b 2+? a 2-2 * ? a 1\)
    by ( \(\operatorname{simp}\) )
from ln-fact-bounds[of \(n\) div 2] False have abs-l1: abs(?l1 - ?a1) \(\leq ? b 1\)
    by (simp add: algebra-simps)
    then have minus-l1: ?a1 - ?l1 \(\leq ? b 1\)
    by linarith
    from abs-l1 have l1: ?l1 - ? \(a 1 \leq\) ?b1
    by linarith
    from \(l n\)-fact-bounds[of \(n\) ] False have abs-l2: abs(?l2 - ?a2) \(\leq ? b 2\)
    by (simp add: algebra-simps)
    then have l2: ?12 - ?a2 \(\leq ? b 2\)
    by \(\operatorname{simp}\)
    from abs-l2 have minus-l2: ?a2 - ?l2 \(\leq\) ?b2
    by \(\operatorname{simp}\)
from minus-a minus-l1 l2 have ?l2 - 2 * ?l1 - ?a \(\leq ? b\)
    by \(\operatorname{simp}\)
    moreover from a l1 minus-l2 have -? \(12+2 * ? l 1+? a \leq ? b\)
    by \(\operatorname{simp}\)
    ultimately have \(a b s((? l 2-2 * ? l 1)-? a) \leq ? b\)
    by \(\operatorname{simp}\)
    then show?thesis
    by \(\operatorname{simp}\)
qed
lemma ln-primefact:
    assumes \(n \neq(0::\) nat \()\)
    shows \(\ln n=\left(\sum d=1 . . n\right.\). if primepow \(d \wedge d\) dvd \(n\) then \(\ln\) (aprimedivisor \(d\) )
else 0)
            (is ?lhs =?rhs)
proof -
    have ? \(r\) hs \(=\left(\sum d \in\{x \in\{1 . . n\}\right.\). primepow \(x \wedge x d v d n\}\). \(\ln\) (real (aprimedivisor
d)))
    unfolding primepow-factors-def by (subst sum.inter-filter [symmetric]) simp-all
    also have \(\{x \in\{1 . . n\}\). primepow \(x \wedge x d v d n\}=\) primepow-factors \(n\)
        using assms by (auto simp: primepow-factors-def dest: dvd-imp-le prime-
pow-gt-Suc-0)
    finally have \(*:\left(\sum d \in\right.\) primepow-factors \(n . \ln (\) real \((\) aprimedivisor \(\left.d))\right)=\) ?rhs ..
    from in-prime-factors-imp-prime prime-gt-0-nat
        have pf-pos: \(\bigwedge p . p \in \#\) prime-factorization \(n \Longrightarrow p>0\)
        by blast
    from ln-msetprod[of prime-factorization \(n\), OF pf-pos] assms
        have \(\ln n=\left(\sum p \in \#\right.\) prime-factorization \(\left.n . \ln p\right)\)
            by (simp add: of-nat-prod-mset)
    also from * sum-prime-factorization-conv-sum-primepow-factors[of \(n \ln , O F\)
\(\operatorname{assms}(1)]\)
```

```
    have ... = ?rhs by simp
    finally show ?thesis.
qed
context
begin
private lemma divisors:
    fixes x d::nat
    assumes }x\in{1..n
    assumes d dvd x
    shows }\existsk\in{1..n div d}.x=d*
proof -
    from assms have }x\leq
        by simp
    then have ub: x div d}\leqn\mathrm{ div d
    by (simp add: div-le-mono <x \leqn>)
    from assms have 1\leqx div d by (auto elim!:dvdE)
    with ub have x div d}\in{1..n div d
    by simp
    with 〈d dvd x\rangle show ?thesis by (auto intro!: bexI[of - x div d])
qed
lemma ln-fact-conv-mangoldt: ln (fact n) = (\sumd=1..n. mangoldt d * floor (n /
d))
proof -
    have *: (\sumda=1..n. if primepow da ^ da dvd d then ln (aprimedivisor da) else
0) =
    (\sum(da::nat)=1..d. if primepow da ^ da dvd d then ln (aprimedivisor
da) else 0)
    if d:d\in{1..n} for }
    by (rule sum.mono-neutral-right, insert d) (auto dest: dvd-imp-le)
    have (\sumd=1..n. \sumda=1..d. if primepow da }
        da dvd d then ln (aprimedivisor da) else 0) =
        ( }\sumd=1..n. \sumda=1..n. if primepow da ^
        da dvd d then ln (aprimedivisor da) else 0)
    by (rule sum.cong) (insert *, simp-all)
    also have ... = (\sumda=1..n. \sumd=1..n. if primepow da ^
                                    da dvd d then ln (aprimedivisor da) else 0)
    by (rule sum.swap)
    also have ... = sum (\lambdad. mangoldt d * floor (n/d)) {1..n}
    proof (rule sum.cong)
    fix d assume d:d \in{1..n}
    have ( }\sumda=1..n. if primepow d \wedged dvd da then ln (real (aprimedivisor d))
else 0) =
            ( }\sumda=1..n. if d dvd da then mangoldt d else 0)
        by (intro sum.cong) (simp-all add: mangoldt-def)
```



```
            by (subst sum.inter-filter [symmetric]) (simp-all add: algebra-simps)
```

```
    also {
            have {x.x\in{1..n}}\wedgeddvdx}={x.\existsk\in{1..n div d}. x=k*d
            proof safe
            fix }x\mathrm{ assume }x\in{1..n} d dvd x
            thus \existsk\in{1..n div d}. x = k*d using divisors[of x n d] by auto
            next
            fix }xk\mathrm{ assume }k:k\in{1..n div d
            from k have k*d\leqn div d*d by (intro mult-right-mono) simp-all
            also have n div d*d\leqn div d*d + n mod d by (rule le-add1)
            also have ... = n by simp
            finally have }k*d\leqn
            thus }k*d\in{1..n}\mathrm{ using d k by auto
            qed auto
            also have ... = (\lambdak.k*d)'{1..n div d}
            by fast
            also have card ... = card {1..n div d}
            by (rule card-image) (simp add: inj-on-def)
            also have ... = n div d
            by simp
            also have ... = \n/d\rfloor
            by (simp add: floor-divide-of-nat-eq)
            finally have real (card {x.x\in{1..n} \wedged dvd x})=real-of-int \lfloorn / d\rfloor
            by force
    }
    finally show ( }\sumda=1..n. if primepow d \wedged dvd da then ln (real (aprimedivisor
d)) else 0)=
            mangoldt d * real-of-int \lfloorreal n / real d\rfloor.
    qed simp-all
    finally have ( }\sumd=1..n. \sumda=1..d. if primepow da ^
            da dvd d then ln (aprimedivisor da) else 0)=
            sum (\lambdad. mangoldt d * floor (n/d)) {1..n} .
    with ln-primefact have (\sumd=1..n. ln d) =
        (\sumd=1..n. mangoldt d * floor ( }n/d)\mathrm{ )
        by simp
    with ln-fact show ?thesis
        by simp
qed
end
context
begin
private lemma div-2-mult-2-bds:
    fixes nd :: nat
    assumes d>0
    shows 0\leq\lfloorn/d\rfloor-2* \(n div 2) / d\rfloor\lfloorn/d\rfloor-2 * \lfloor(n div 2) / d\rfloor\leq1
proof -
    have \lfloor2::real\rfloor*\lfloor(n div 2) / d\rfloor\leq\lfloor2*((n div 2) / d) \rfloor
```

```
    by (rule le-mult-floor) simp-all
    also from assms have ... \leq n / d\rfloor by (intro floor-mono) (simp-all add:
field-simps)
    finally show 0\leq\lfloorn/d\rfloor-2*\lfloor(ndiv 2) / d\rfloor by (simp add: algebra-simps)
next
    have real (n div d) \leq real (2* ((n div 2) div d ) + 1)
    by (subst div-mult2-eq [symmetric], simp only: mult.commute, subst div-mult2-eq)
simp
    thus \lfloorn/d\rfloor-2* \(n div 2) / d\rfloor\leq1
        unfolding of-nat-add of-nat-mult floor-conv-div-nat [symmetric] by simp-all
qed
private lemma n-div-d-eq-1:d \in{n div 2 + 1..n} \Longrightarrow\lfloorreal n / real d d=1
    by (cases }n=d\mathrm{ ) (auto simp: field-simps intro: floor-eq)
lemma psi-bounds-ln-fact:
    shows ln (fact n) - 2* ln (fact (n div 2)) \leq psi n
        psi n-psi(ndiv 2) \leqln (fact n) - 2* ln (fact (n div 2))
proof -
    fix n::nat
    let ? k = n div 2 and ?d = n mod 2
    have *: \lfloor?k / d\rfloor=0 if d> ?k for d
    proof -
            from that div-less have 0=?k div d by simp
            also have ... = \?k / d\rfloor by (rule floor-divide-of-nat-eq [symmetric])
            finally show \lfloor?k / d\rfloor=0 by simp
    qed
    have sum-eq: (\sumd=1..2*?k+?d. mangoldt d * \lfloor?k / d\rfloor) = (\sumd=1..?k. man-
goldt d * \?k / d\rfloor)
            by (intro sum.mono-neutral-right) (auto simp: *)
    from ln-fact-conv-mangoldt have ln (fact n) = (\sumd=1..n. mangoldt d * \n/
d\rfloor).
    also have ... =(\sumd=1..n. mangoldt d * \lfloor(2*(n div 2) + n mod 2) / d\rfloor)
        by simp
    also have \ldots.\leq(\sumd=1..n. mangoldt d *(2*\lfloor?k/d\rfloor+1))
        using div-2-mult-2-bds(2)[of - n]
        by (intro sum-mono mult-left-mono, subst of-int-le-iff)
            (auto simp: algebra-simps mangoldt-nonneg)
    also have ... = 2 * (\sumd=1..n. mangoldt d * \lfloor(n div 2) / d\rfloor) +( \sumd=1..n.
mangoldt d)
    by (simp add: algebra-simps sum.distrib sum-distrib-left)
    also have ... = 2 * (\sumd=1..2*? % +?d. mangoldt d * \lfloor(n div 2) / d\rfloor) +
(\sumd=1..n. mangoldt d)
    by presburger
    also from sum-eq have ... =2 * (\sumd=1..?k. mangoldt d * \(n div 2) / d\rfloor)
+ (\sumd=1..n. mangoldt d)
    by presburger
    also from ln-fact-conv-mangoldt psi-def have ... =2 * ln (fact ?k) + psi n
        by presburger
```

```
    finally show \(\ln (f a c t n)-2 * \ln (f a c t(n \operatorname{div} 2)) \leq p s i n\)
    by \(\operatorname{simp}\)
next
    fix \(n\) ::nat
    let \(? k=n \operatorname{div} 2\) and \(? d=n \bmod 2\)
    from psi-def have psin-psi ?k=( \(\sum d=1 . .2 * ? k+? d\). mangoldt \(\left.d\right)-\left(\sum d=1 . . ? k\right.\).
mangoldt d)
    by presburger
    also have \(\ldots=\operatorname{sum}\) mangoldt \((\{1 . .2 *(n \operatorname{div} 2)+n \bmod 2\}-\{1 . . n \operatorname{div} 2\})\)
    by (subst sum-diff) simp-all
    also have \(\ldots=\left(\sum d \in(\{1 . .2 *(n \operatorname{div} 2)+n \bmod 2\}-\{1 . . n \operatorname{div} 2\})\right.\).
                            (if \(d \leq\) ? \(k\) then 0 else mangoldt \(d\) ))
    by (intro sum.cong) simp-all
    also have \(\ldots=\left(\sum d=1 . .2 * ? k+? d .(\right.\) if \(d \leq ? k\) then 0 else mangoldt \(\left.d)\right)\)
    by (intro sum.mono-neutral-left) auto
    also have \(\ldots=\left(\sum d=1 . . n\right.\). (if \(d \leq ? k\) then 0 else mangoldt \(\left.\left.d\right)\right)\)
    by presburger
    also have \(\ldots=\left(\sum d=1 . . n\right.\). (if \(d \leq\) ?k then mangoldt \(d * 0\) else mangoldt \(\left.d\right)\) )
    by (intro sum.cong) simp-all
    also from div-2-mult-2-bds(1) have \(\ldots \leq\left(\sum d=1\right.\).. \(n\). (if \(d \leq ? k\) then mangoldt
\(d *(\lfloor n / d\rfloor-2 *\lfloor ? k / d\rfloor)\) else mangoldt \(d))\)
    by (intro sum-mono)
        (auto simp: algebra-simps mangoldt-nonneg intro!: mult-left-mono simp del:
of-int-mult)
    also from \(n\)-div- \(d\)-eq- 1 have \(\ldots=\left(\sum d=1 . . n\right.\). (if \(d \leq ? k\) then mangoldt \(d *\)
\((\lfloor n / d\rfloor-2 *\lfloor ? k / d\rfloor)\) else mangoldt \(d *\lfloor n / d\rfloor))\)
    by (intro sum.cong refl) auto
    also have \(\ldots=\left(\sum d=1\right.\)..n. mangoldt \(d *\) real-of-int \((\lfloor\) real \(n /\) real \(d\rfloor)-\)
                            (if \(d \leq ? k\) then \(2 *\) mangoldt \(d *\) real-of-int \(\lfloor\) real ? \(k /\) real \(d\rfloor\) else
0))
    by (intro sum.cong refl) (auto simp: algebra-simps)
    also have \(\ldots=\left(\sum d=1\right.\)..n. mangoldt \(d *\) real-of-int \((\lfloor\) real \(n /\) real \(\left.d\rfloor)\right)-\)
                    ( \(\sum d=1\)..n. (if \(d \leq ? k\) then \(2 *\) mangoldt \(d *\) real-of-int \(\lfloor\) real ? \(k /\)
real d」else 0))
    by (rule sum-subtractf)
    also have \(\left(\sum d=1 \ldots n\right.\). (if \(d \leq ? k\) then \(2 *\) mangoldt \(d *\) real-of-int \(\lfloor\) real ? \(k /\)
real \(d\rfloor\) else 0\()\) ) \(=\)
                    ( \(\sum d=1 . . ? k\). (if \(d \leq ? k\) then \(2 *\) mangoldt \(d *\) real-of-int \(\lfloor\) real \(? k /\)
real d」else 0))
    by (intro sum.mono-neutral-right) auto
    also have \(\ldots=\left(\sum d=1 . . ? k\right.\). \(2 *\) mangoldt \(d *\) real-of-int \(\lfloor\) real \(? k /\) real \(\left.d\rfloor\right)\)
    by (intro sum.cong) simp-all
    also have \(\ldots=2 *\left(\sum d=1 . . ? k\right.\). mangoldt \(d *\) real-of-int \(\lfloor\) real ? \(k /\) real \(\left.d\rfloor\right)\)
        by (simp add: sum-distrib-left mult-ac)
    also have \(\left(\sum d=1\right.\)..n. mangoldt \(d *\) real-of-int \(\lfloor\) real \(n /\) real \(\left.d\rfloor\right)-\ldots=\)
                        \(\ln (f a c t n)-2 * \ln (f a c t(n \operatorname{div} 2))\)
    by (simp add: ln-fact-conv-mangoldt)
    finally show \(p\) si \(n-p s i(n \operatorname{div} 2) \leq \ln (f a c t n)-2 * \ln (f a c t(n \operatorname{div} 2))\).
qed
```


## end

```
lemma psi-bounds-induct:
    real n*ln 2 - (4*ln (real (if n=0 then 1 else n)) + 3)\leqpsi n
    psi n - psi (n div 2) \leq real n*ln 2 + (4* ln (real (if n=0 then 1 else n)) +
3)
proof -
    from le-imp-neg-le[OF ln-fact-diff-bounds]
        have n*ln 2 - (4* ln (if n=0 then 1 else n) + 3)
            \leqn*ln 2 - abs(ln (fact n) - 2* ln (fact (ndiv 2)) - n*ln 2)
    by simp
    also have ... \leqln (fact n) - 2* ln (fact (n div 2))
    by simp
    also from psi-bounds-ln-fact (1) have ... \leq psi n
        by simp
    finally show real n*ln 2 - (4*\operatorname{ln}(\mathrm{ real (if n=0 then 1 else n)) + 3) < psi}
n.
next
    from psi-bounds-ln-fact (2) have psi n - psi(n div 2) \leqln (fact n) - 2*ln
(fact (n div 2)).
    also have \ldots\leq n*ln 2 + abs(ln (fact n) - 2 * ln (fact (ndiv 2)) - n*\operatorname{ln}2)
        by simp
    also from ln-fact-diff-bounds [of n]
        have abs(ln (fact n) - 2 * ln (fact (ndiv 2)) - n*ln 2)
                        \leq(4* ln (real (if n=0 then 1 else n)) + 3) by simp
    finally show psi n-psi (n div 2) \leq real n*ln 2 + (4* ln (real (if n=0 then
1 else n)) + 3)
    by simp
qed
```


### 0.5 Bounding the psi function

In this section, we will first prove the relatively tight estimate psin $n \mathbf{3} / 2$ $+\ln 2 *$ real $n$ for $n \leq\left(128::^{\prime} a\right)$ and then use the recurrence we have just derived to extend it to $p$ si $n \leq 551 / 256$ for $n \leq\left(1024::{ }^{\prime} a\right)$, 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 $n \leq\left(128:::^{\prime} a\right)$ using reflection and approximation.

## context <br> begin

private lemma Ball-insertD:
assumes $\forall x \in$ insert $y A . P x$
shows $\quad P y \forall x \in A . P x$
using assms by auto

```
private lemma meta-eq-TrueE: PROP A \equiv Trueprop True \LongrightarrowPROP A
    by simp
private lemma pre-mangoldt-pos: pre-mangoldt n > 0
    unfolding pre-mangoldt-def by (auto simp: primepow-gt-Suc-0)
private lemma psi-conv-pre-mangoldt: psi }n=\operatorname{ln}(\mathrm{ real (prod pre-mangoldt {1..n}))
    by (auto simp: psi-def mangoldt-def pre-mangoldt-def ln-prod primepow-gt-Suc-0
intro!: sum.cong)
private lemma eval-psi-aux1: psi 0 = ln (real (numeral Num.One))
    by (simp add: psi-def)
private lemma eval-psi-aux2:
    assumes psi m=ln(real (numeral x)) pre-mangoldt n=ym+1=nnumeral
x*y=z
    shows psi n = ln (real z)
proof -
    from assms(2) [symmetric] have [simp]: y>0 by (simp add: pre-mangoldt-pos)
    have psi n = psi (Suc m) by (simp add: assms(3) [symmetric])
    also have ... = ln (real y * (\prodx=Suc 0..m. real (pre-mangoldt x)))
    using assms(2,3) [symmetric] by (simp add: psi-conv-pre-mangoldt prod.nat-ivl-Suc'
mult-ac)
    also have ... = ln (real y) + psi m
    by (subst ln-mult) (simp-all add: pre-mangoldt-pos prod-pos psi-conv-pre-mangoldt)
    also have psi m=ln (real (numeral x)) by fact
    also have ln (real y) + .. = ln (real (numeral x * y)) by (simp add: ln-mult)
    finally show ?thesis by (simp add: assms(4) [symmetric])
qed
private lemma Ball-atLeast0AtMost-doubleton:
    assumes psi 0\leq3/2*\operatorname{ln}2* real 0
    assumes psi 1\leq3/2*ln 2 * real 1
    shows (\forallx\in{0..1}.psix\leq3/2*ln 2* real x)
    using assms unfolding One-nat-def atLeastO-atMost-Suc ball-simps by auto
private lemma Ball-atLeast0AtMost-insert:
    assumes ( }\forallx\in{0..m}.psix\leq3/2*\operatorname{ln}2* real x
    assumes psi(numeral n)\leq3/2*ln 2* real (numeral n) m= pred-numeral
n
    shows }(\forallx\in{0..numeral n}.psi x \leq 3/2*\operatorname{ln 2 * real x)
    using assms
    by (subst numeral-eq-Suc[of n], subst atLeast0-atMost-Suc,
        subst ball-simps, simp only: numeral-eq-Suc [symmetric])
private lemma eval-psi-ineq-aux:
    assumes psi}n=xx\leq3/2*\operatorname{ln}2*
    shows psin\leq3/2*ln 2*n
    using assms by simp-all
```

```
private lemma eval-psi-ineq-aux2:
    assumes numeral m^ 2 \leq (2::nat) ^ (3*n)
    shows ln (real (numeral m))\leq3/2*\operatorname{ln}2* real n
proof -
    have ln (real (numeral m)) \leq 3/2* ln 2* real n \longleftrightarrow
                2 * log 2 (real (numeral m))}\leq3*\mathrm{ real n
    by (simp add: field-simps log-def)
    also have 2 * log 2 (real (numeral m)) = log 2 (real (numeral m^ 2))
    by (subst of-nat-power, subst log-nat-power) simp-all
    also have \ldots\leq _ % real n\longleftrightarrow real ((numeral m)^ 2) \leq2 powr real (3*n)
    by (subst Transcendental.log-le-iff) simp-all
    also have 2 powr (3*n) = real (2 ^ ( 3*n))
    by (simp add: powr-realpow [symmetric])
    also have real ((numeral m)^ 2) \leq .. \longleftrightarrow numeral m^2 \ (2::nat)^ (3*
n)
    by (rule of-nat-le-iff)
    finally show ?thesis using assms by blast
qed
private lemma eval-psi-ineq-aux-mono:
    assumes psi n=x psim=x psin\leq3/2*ln 2*nn\leqm
    shows psim\leq3/2*ln 2*m
proof -
    from assms have psi m=psi n by simp
    also have \ldots\leq3/2*\operatorname{ln}2*n by fact
    also from <n\leqm> have \ldots\leq3/2*ln 2*m by simp
    finally show ?thesis.
qed
lemma not-primepow-1-nat: \negprimepow (1 :: nat) by auto
ML-file〈bertrand.ML〉
local-setup \(\langle f n\) lthy \(=>\)
let
    fun tac ctxt =
        let
            val psi-cache = Bertrand.prove-psi ctxt 129
            fun prove-psi-ineqs ctxt =
                    let
                    fun tac goal-ctxt =
                    HEADGOAL (resolve-tac goal-ctxt @{thms eval-psi-ineq-aux2} THEN'
                            Simplifier.simp-tac goal-ctxt)
                    fun prove-by-approx n thm =
                    let
                        val thm = thm RS @{thm eval-psi-ineq-aux}
                        val [prem] = Thm.prems-of thm
```

```
            val prem = Goal.prove ctxt [] [] prem (tac o #context)
            in
            prem RS thm
        end
    fun prove-by-mono last-thm last-thm' thm =
        let
            val thm =@{thm eval-psi-ineq-aux-mono} OF [last-thm, thm,last-thm']
            val [prem] = Thm.prems-of thm
            val prem =
                Goal.prove ctxt [] [] prem (fn {context = goal-ctxt, ...} =>
                HEADGOAL (Simplifier.simp-tac goal-ctxt))
            in
            prem RS thm
        end
    fun go - acc [] = acc
        | go last acc (( }n,x,\mathrm{ thm) :: xs) =
            let
                val thm'=
                    case last of
                                    NONE => prove-by-approx n thm
                            | SOME (last-x, last-thm, last-thm') =>
                                    if last-x = x then
                                    prove-by-mono last-thm last-thm' thm
                                    else
                                    prove-by-approx n thm
                    in
                        go (SOME (x, thm, thm')) (thm' :: acc) xs
                        end
    in
        rev o go NONE []
    end
val psi-ineqs = prove-psi-ineqs ctxt psi-cache
fun prove-ball ctxt (thm1 :: thm2 :: thms) =
    let
        val thm =@{thm Ball-atLeast0AtMost-doubleton} OF [thm1, thm2]
        fun solve-prem thm =
            let
                val thm' =
                    Goal.prove ctxt [] [] (Thm.cprem-of thm 1 |> Thm.term-of)
                    (fn {context = goal-ctxt, ...} =>
                        HEADGOAL (Simplifier.simp-tac goal-ctxt))
            in
                thm' RS thm
            end
            fun go thm thm'=(@{thm Ball-atLeastOAtMost-insert } OF [thm',
thm]) |> solve-prem
    in
        fold go thms thm
```

```
                end
            | prove-ball - = raise Match
    in
            HEADGOAL (resolve-tac ctxt [prove-ball ctxt psi-ineqs])
        end
    val thm = Goal.prove lthy [] [] @{prop \foralln\in{0..128}.psi n\leq3 / 2*ln 2*n}
(tac o #context)
in
    Local-Theory.note ((@{binding psi-ubound-log-128}, []), [thm]) lthy |> snd
end
>
end
context
begin
private lemma psi-ubound-aux:
    defines }f\equiv\lambdax::real. (4*\operatorname{ln}x+3)/(ln2*x
    assumes }x\geq2x\leq
    shows fx\geqfy
using assms(3)
proof (rule DERIV-nonpos-imp-nonincreasing, goal-cases)
    case (1 t)
    define f}\mp@subsup{f}{}{\prime}\mathrm{ where f}\mp@subsup{f}{}{\prime}=(\lambdax.(1-4*\operatorname{ln}x)/x`2 / ln 2 :: real
    from 1 assms(2) have ( f has-real-derivative f't) (at t) unfolding f-def f'-def
        by (auto intro!: derivative-eq-intros simp: field-simps power2-eq-square)
    moreover {
        from ln-2-ge have 1/4\leqln (2::real) by simp
        also from assms(2) 1 have .. S \leqln t by simp
        finally have ln t\geq1/4.
    }
    with 1 assms(2) have f't\leq0 by (simp add: f'-def field-simps)
    ultimately show ?case by (intro exI[of-\mp@subsup{f}{}{\prime}t]) simp-all
qed
```

These next rules are used in combination with real ? $n * \ln 2-(4 * \ln$ (real $($ if $? n=0$ then 1 else ? $n))+3) \leq p s i ? n$
psi ? $n-p s i(? n$ 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 $p$ si 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 $\bigwedge n . n \leq m \Longrightarrow$ psi $n \leq c * \ln 2 *$ real $n n \leq m^{\prime} m^{\prime}=2 * m$

$$
c \leq c^{\prime} c \geq 0 m \geq 1 c^{\prime} \geq 1+c / 2+(4 * \ln (m+1)+3) /(\ln 2 *(m+1))
$$

shows psin$\leq c^{\prime} * \ln 2 *$ real $n$ proof (cases $n>m$ )
case False
hence psi $n \leq c * \ln 2 *$ real $n$ by (intro assms) simp-all
also have $c \leq c^{\prime}$ by fact
finally show ?thesis by - (simp-all add: mult-right-mono)

## next

case True
hence $n: n \geq m+1$ by simp
from psi-bounds-induct(2)[of n] True
have $p$ si $n \leq$ real $n * \ln 2+4 * \ln ($ real $n)+3+p s i(n$ div 2) by simp
also from assms have psi ( $n$ div 2) $\leq c * \ln 2 *$ real ( $n$ div 2)
by (intro assms) simp-all
also have real (n div 2) $\leq$ real $n / 2$ by $\operatorname{simp}$
also have $c * \ln 2 * \ldots=c / 2 * \ln 2 *$ real $n$ by $\operatorname{simp}$
also have real $n * \ln 2+4 * \ln ($ real $n)+3+\ldots=$

$$
(1+c / 2) * \ln 2 * \text { real } n+(4 * \ln (\text { real } n)+3) \text { by }(\operatorname{simp} \text { add: }
$$

field-simps)
also \{
have $(4 * \ln ($ real $n)+3) /(\ln 2 *($ real $n)) \leq(4 * \ln (m+1)+3) /(\ln 2$

* $(m+1))$
using $n$ assms by (intro psi-ubound-aux) simp-all
also from assms have $(4 * \ln (m+1)+3) /(\ln 2 *(m+1)) \leq c^{\prime}-1-c / 2$
by (simp add: algebra-simps)
finally have $4 * \ln ($ real $n)+3 \leq\left(c^{\prime}-1-c / 2\right) * \ln 2 *$ real $n$
using $n$ by (simp add: field-simps)
\}
also have $(1+c / 2) * \ln 2 *$ real $n+\left(c^{\prime}-1-c / 2\right) * \ln 2 *$ real $n=c^{\prime}$ * $\ln 2$ * real $n$
by (simp add: field-simps)
finally show? ?thesis using $\langle c \geq 0\rangle$ by (simp-all add: mult-left-mono)


## qed

end
lemma psi-ubound-log-double-cases:
assumes $\forall n \leq m$. psi $n \leq c * \ln 2 *$ real $n$

$$
\begin{aligned}
& c^{\prime} \geq 1+c / 2+(4 * \ln (m+1)+3) /(\ln 2 *(m+1)) \\
& m^{\prime}=2 * m c \leq c^{\prime} c \geq 0 m \geq 1
\end{aligned}
$$

shows $\forall n \leq m^{\prime}$. psi $n \leq c^{\prime} * \ln 2 *$ real $n$
using assms(1) by (intro allI impI assms psi-ubound-log-double-cases'[of m c$m^{\prime} c$ ]) auto
lemma psi-ubound-log-1024:
$\forall n \leq 1024$. psi $n \leq 551 / 256 * \ln 2 *$ real $n$
proof -
from psi-ubound-log-128 have $\forall n \leq 128$. psi $n \leq 3 / 2 * \ln 2 *$ real $n$ by simp

```
    hence }\foralln\leq256.psi n\leq1025 / 512 * ln 2 * real n
    proof (rule psi-ubound-log-double-cases, goal-cases)
    case 1
    have Some (Float 624 (-7)) = ub-ln 9 129 by code-simp
    from ub-ln(1)[OF this] and ln-2-ge show ?case by (simp add: field-simps)
    qed simp-all
    hence }\foralln\leq512.psi n\leq549 / 256*ln 2 * real n
    proof (rule psi-ubound-log-double-cases, goal-cases)
    case 1
    have Some (Float 180 (-5)) = ub-ln 7 257 by code-simp
    from ub-ln(1)[OF this] and ln-2-ge show ?case by (simp add: field-simps)
    qed simp-all
    thus \foralln\leq1024. psi }n\leq551/256*\operatorname{ln}2*\mathrm{ real n
    proof (rule psi-ubound-log-double-cases, goal-cases)
    case 1
    have Some (Float 203 (-5)) = ub-ln 7 513 by code-simp
    from ub-ln(1)[OF this] and ln-2-ge show ?case by (simp add: field-simps)
    qed simp-all
qed
lemma psi-bounds-sustained-induct:
    assumes 4 * ln (1+2` j) + 3 \leqd*ln 2 * (1+2`j)
    assumes 4/(1 + 2^j) \leqd*ln 2
    assumes 0 \leqc
    assumes c/2 +d+1\leqc
    assumes j\leqk
    assumes \n.n\leq 2`k\Longrightarrowpsin\leqc*ln 2*n
    assumes n\leq 2`(Suc k)
    shows psi n\leqc*ln2*n
proof (cases n\leq2`k)
    case True
    with assms(6) show ?thesis.
next
    case False
    from psi-bounds-induct(2)
    have psi n - psi (n div 2) \leq real n*ln 2 + (4*ln(real (if n=0 then 1 else
n)) + 3).
    also from False have (if n=0 then 1 else n)=n
    by simp
finally have psi n\leq real n*\operatorname{ln}2+(4*\operatorname{ln}(\mathrm{ real n) + 3) + psi (n div 2)}
    by simp
    also from assms(6,7) have psi( n div 2) \leqc*ln 2 *( }n\mathrm{ div 2)
    by simp
also have real (n div 2) \leq real n / 2
    by simp
    also have real n*\operatorname{ln}2~(4*\operatorname{ln}(\mathrm{ real n) + 3) +c*ln 2 * (n/2) }\leqc*\operatorname{ln}2
* real n
    proof (rule overpower-lemma[of
        \lambdax. x* ln 2 + (4*\operatorname{ln}x+3)+c*\operatorname{ln}2*(x/2) 1+2^j
```


## $\lambda x . c * \ln 2 * x \lambda x . c * \ln 2-\ln 2-4 / x-c / 2 * \ln 2$

 real $n]$ ）from $\operatorname{assms}(1)$ have $4 * \ln (1+2 \uparrow j)+3 \leq d * \ln 2 *(1+2 \uparrow j)$ ．
also from $\operatorname{assms}(4)$ have $d \leq c-c / 2-1$
by $\operatorname{simp}$
also have $(\ldots) * \ln 2 *\left(1+2^{\wedge} j\right)=c * \ln 2 *\left(1+2^{\wedge} j\right)-c / 2 * \ln 2$ ＊$\left(1+2^{\wedge} j\right)$
$-\left(1+2^{\wedge} j\right) * \ln 2$
by（simp add：left－diff－distrib）
finally have $4 * \ln (1+2 \widehat{j})+3 \leq c * \ln 2 *\left(1+\boldsymbol{2}^{\wedge} j\right)-c / 2 * \ln 2$ ＊$\left(1+2^{へ} j\right)$

$$
-\left(1+2{ }^{-} j\right) * \ln 2
$$

by（simp add：add－pos－pos）
then show $\left(1+2^{\wedge} j\right) * \ln 2+\left(4 * \ln \left(1+2^{\wedge} j\right)+3\right)$

$$
+c * \ln \mathscr{2} *\left(\left(1+\mathfrak{2}^{\wedge} j\right) / \mathfrak{2}\right) \leq c * \ln \mathfrak{2} *\left(1+\mathfrak{2}^{へ} j\right)
$$

by $\operatorname{simp}$
next
fix $x$ ：：real
assume $x: 1+2 \widehat{j} \leq x$
moreover have $1+2^{\wedge} j>(0::$ real $)$ by（simp add：add－pos－pos）
ultimately have $x$－pos：$x>0$ by linarith
show $((\lambda x . c * \ln 2 * x-(x * \ln 2+(4 * \ln x+3)+c * \ln 2 *(x / 2)))$ has－real－derivative $c * \ln 2-\ln 2-4 / x-c / 2 * \ln 2)($ at $x)$
by（rule derivative－eq－intros refl $\mid$ simp add：$\langle 0<x\rangle)+$
from $\langle 0<x\rangle\langle 0<1+2 ` j\rangle$ have $0<x *(1+2 \widehat{ }$ ）
by（rule mult－pos－pos）
have $4 / x \leq 4 /(1+2 へ j)$
by（intro divide－left－mono mult－pos－pos add－pos－pos $x$ x－pos）simp－all
also from $\operatorname{assms}(2)$ have $4 /(1+2 \widehat{j}) \leq d * \ln 2$ ．
also from $\operatorname{assms}(4)$ have $d \leq c-c / 2-1$ by $\operatorname{simp}$
also have $\ldots * \ln 2=c * \ln 2-c / 2 * \ln 2-\ln 2$ by $(s i m p a d d$ ： algebra－simps）
finally show $0 \leq c * \ln 2-\ln 2-4 / x-c / 2 * \ln 2$ by $\operatorname{simp}$ next
have $1+2^{\wedge} j=$ real $(1+2 \uparrow j)$ by simp
also from $\operatorname{assms}(5)$ have $\ldots \leq$ real $(1+2 \wedge k)$ by $\operatorname{simp}$
also from False have $2^{\wedge} k \leq n-1$ by simp
finally show $1+2 \widehat{2} \leq$ real $n$ using False by simp
qed
finally show ？thesis using assms by－（simp－all add：mult－left－mono） qed
lemma psi－bounds－sustained：
assumes $\bigwedge n . n \leq \mathscr{2}^{\wedge} k \Longrightarrow$ 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－

```
    have psi n\leqc*ln 2 * n if n\leq2` }j\mathrm{ for }j
    using that
    proof (induction j arbitrary: n)
    case 0
    with assms(4) 0 show ?case unfolding psi-def mangoldt-def by (cases n)
auto
    next
        case (Suc j)
        show ?case
            proof (cases k}\leqj
                case True
                from assms(4) have c-div-2: c/2 + (c/2 - 1) + 1\leqc
                    by simp
                from psi-bounds-sustained-induct[of k c/2 - 1 c j,
                    OF assms(2) assms(3) assms(4) c-div-2 True Suc.IH Suc.prems]
                    show ?thesis by simp
        next
                case False
                then have j-lt-k: Suc j\leqk by simp
                from Suc.prems have n\leq2 ^ Suc j .
                also have (2::nat) ^ Suc j \leq 2 ^ k
                    using power-increasing[of Suc j k 2::nat, OF j-lt-k]
                    by simp
                finally show ?thesis using assms(1) by simp
            qed
    qed
    from less-exp this [of n n] show ?thesis by simp
qed
lemma psi-ubound-log: psi n\leq551 / 256 * ln 2 * n
proof (rule psi-bounds-sustained)
    show 0\leq551 / (256 :: real) by simp
next
    fix n :: nat assume n\leq2^ 10
    with psi-ubound-log-1024 show psi n\leq551/256*ln 2 * real n by auto
next
    have 4 / (1 + 2^ 10) \leq(551 / 256 / 2 - 1) * (2/3 :: real)
        by simp
    also have \ldots}\leq(551/256/2 - 1)*\operatorname{ln}
        by (intro mult-left-mono ln-2-ge') simp-all
    finally show 4/(1+2^10)\leq(551/256 / 2 - 1)* ln (2 :: real).
next
    have Some (Float 16 (-1)) = ub-ln 3 1025 by code-simp
    from ub-ln(1)[OF this] and ln-2-ge
        have 2048*\operatorname{ln 1025 + 1536\leq39975 * (ln 2::real) by simp}
    thus 4*ln (1+2^10)+3\leq(551/256 / 2 - 1)* ln 2 * (1 + 2^ 10 ::
real)
        by simp
qed
```

```
lemma psi-ubound-3-2: psi }n\leq3/2*
proof -
    have (551 / 256)*\operatorname{ln 2 \leq (551 / 256)* (16/23 :: real)}
        by (intro mult-left-mono ln-2-le)}\mathrm{ ) auto
    also have ... \leq 3 / 2 by simp
    finally have 551 / 256*\operatorname{ln}2\leq3/(2::real).
    with of-nat-0-le-iff mult-right-mono have 551 / 256*ln 2*n\leq3/2*n
        by blast
    with psi-ubound-log[of n] show ?thesis
        by linarith
qed
```


### 0.6 Doubling psi and theta

```
lemma psi-residues-compare-2:
    psi-odd-2 n \leq psi-even-2 n
proof -
    have psi-odd-2 n = (\sumd\in{d.d { {2..n} ^ primepow-odd d}. mangoldt-odd d)
        unfolding mangoldt-odd-def by (rule sum.mono-neutral-right) auto
    also have ... = (\sumd\in{d.d \in{2..n}^ primepow-odd d}.ln (real (aprimedivisor
d)))
    by (intro sum.cong refl) (simp add: mangoldt-odd-def)
also have ... \leq (\sumd\in{d.d \in{2..n} ^ primepow-even d}.ln (real (aprimedivisor
d)))
    proof (rule sum-le-included [where i=\lambday.y* aprimedivisor y]; clarify?)
    fix d:: nat assume d}\in{2..n} primepow-odd d
    note d= this
    then obtain pk where d}\mp@subsup{d}{}{\prime}:k\geq1\mathrm{ prime p d= p^ (2*k+1)
        by (auto simp: primepow-odd-def)
    from d' have p^ (2*k)\leq p^ (2*k+1)
        by (subst power-increasing-iff) (auto simp: prime-gt-Suc-0-nat)
    also from d d' have ... \leqn by simp
    finally have p ^}(2*k)\leqn
    moreover from d' have p ^}(2*k)>
        by (intro one-less-power) (simp-all add: prime-gt-Suc-0-nat)
    ultimately have p^ (2*k) \in{2..n} by simp
    moreover from d' have primepow-even ( p^ (2*k))
        by (auto simp: primepow-even-def)
    ultimately show \existsy\in{d\in{2..n}. primepow-even d}.y* aprimedivisor }y
d^
                        ln}(\mathrm{ real (aprimedivisor d))}\leq\operatorname{ln}(\mathrm{ real (aprimedivisor y)) using d'
        by (intro bexI[of- p``(2*k)])
        (auto simp: aprimedivisor-prime-power aprimedivisor-primepow)
qed (simp-all add: of-nat-ge-1-iff Suc-le-eq)
also have ... = (\sumd\in{d.d\in{2..n} ^ primepow-even d}. mangoldt-even d)
    by (intro sum.cong refl) (simp add: mangoldt-even-def)
also have ... = psi-even-2 n
    unfolding mangoldt-even-def by (rule sum.mono-neutral-left) auto
```

```
    finally show ?thesis.
qed
lemma psi-residues-compare:
    psi-odd n \leq psi-even n
proof -
    have }\neg\mathrm{ primepow-odd 1 by (simp add: primepow-odd-def)
    hence *: mangoldt-odd 1 = 0 by (simp add: mangoldt-odd-def)
    have }\neg\mathrm{ primepow-even 1
        using primepow-gt-Suc-0[OF primepow-even-imp-primepow, of 1] by auto
    with mangoldt-even-def have **: mangoldt-even 1 = 0
        by simp
    from psi-odd-def have psi-odd n = (\sumd=1..n. mangoldt-odd d)
        by simp
    also from * have ... = psi-odd-2 n
        by (cases n \geq 1) (simp-all add: eval-nat-numeral sum.atLeast-Suc-atMost)
    also from psi-residues-compare-2 have ... \leqpsi-even-2 n .
    also from ** have ... = psi-even n
            by (cases n \geq 1) (simp-all add: eval-nat-numeral sum.atLeast-Suc-atMost
psi-even-def)
    finally show ?thesis.
qed
lemma primepow-iff-even-sqr:
    primepow }n\longleftrightarrow\mathrm{ primepow-even ( }n\wedge~2
    by (cases n=0)
        (auto simp: primepow-even-altdef aprimedivisor-primepow-power primepow-power-iff-nat
                prime-elem-multiplicity-power-distrib prime-aprimedivisor' prime-imp-prime-elem
                    unit-factor-nat-def primepow-gt-0-nat dest: primepow-gt-Suc-0)
lemma psi-sqrt: psi (Discrete.sqrt n) = psi-even n
proof (induction n)
    case 0
    with psi-def psi-even-def show ?case by simp
next
    case (Suc n)
    then show ?case
        proof cases
            assume asm: \exists m. Suc n=m^2
            with sqrt-Suc have sqrt-seq: Discrete.sqrt(Suc n) = Suc(Discrete.sqrt n)
                by simp
            from asm obtain m}\mathrm{ where Suc n=m^2
                by blast
            with sqrt-seq have Suc(Discrete.sqrt n)=m
                by simp
            with 〈Suc n=m^2` have suc-sqrt-n-sqrt: (Suc(Discrete.sqrt n) ^^2 = Suc n
                by simp
            from sqrt-seq have psi(Discrete.sqrt (Suc n)) = psi (Suc (Discrete.sqrt n))
            by simp
```

also from $p s i$-def have $\ldots=p s i($ Discrete.sqrt $n)+$ mangoldt (Suc (Discrete.sqrt n))
by $\operatorname{simp}$
also from Suc.IH have psi (Discrete.sqrt $n)=$ psi-even $n$.
also have mangoldt (Suc (Discrete.sqrt $n)$ ) $=$ mangoldt-even (Suc $n$ )
proof (cases primepow (Suc(Discrete.sqrt $n)$ ))
case True
with primepow-iff-even-sqr have True2: primepow-even ((Suc(Discrete.sqrt
n) へ~2)
by $\operatorname{simp}$
from suc-sqrt- $n$-sqrt have mangoldt-even $($ Suc $n)=$ mangoldt-even $((S u c($ Discrete.sqrt n) へ~2)
by $\operatorname{simp}$
also from mangoldt-even-def True2
have $\ldots=\ln$ (aprimedivisor $(($ Suc (Discrete.sqrt n))^2))
by $\operatorname{simp}$
also from True have aprimedivisor $\left((\text { Suc }(\text { Discrete.sqrt } n))^{\wedge} 2\right)=$ aprime-
divisor (Suc (Discrete.sqrt n))
by (simp add: aprimedivisor-primepow-power)
also from True have $\ln (\ldots)=$ mangoldt (Suc (Discrete.sqrt $n)$ )
by (simp add: mangoldt-def)
finally show ?thesis ..
next
case False
with primepow-iff-even-sqr
have False2: ᄀ primepow-even $\left((\operatorname{Suc}(\text { Discrete.sqrt } n))^{\text {^2 }}\right)$
by $\operatorname{simp}$
from suc-sqrt-n-sqrt have mangoldt-even $($ Suc $n)=$ mangoldt-even $(($ Suc $($ Discrete.sqrt n) (~2)
by $\operatorname{simp}$
also from mangoldt-even-def False2
have ... = 0
by $\operatorname{simp}$
also from False have $\ldots=$ mangoldt (Suc (Discrete.sqrt $n$ ) $)$
by (simp add: mangoldt-def)
finally show ?thesis ..
qed
also from psi-even-def have psi-even $n+$ mangoldt-even $($ Suc $n)=p s i$-even
(Suc n)
by simp
finally show ?case .
next
assume asm: $\neg(\exists m$. Suc $n=m ` 2)$
with sqrt-Suc have sqrt-eq: Discrete.sqrt (Suc n) $=$ Discrete.sqrt $n$ by $\operatorname{simp}$
then have lhs: psi (Discrete.sqrt (Suc n)) $=$ psi $($ Discrete.sqrt $n)$
by $\operatorname{simp}$
have $\neg$ primepow-even (Suc n)
proof

```
                assume primepow-even (Suc n)
                with primepow-even-def obtain pk
                    where 1\leqk^ prime p}\wedge\mathrm{ Suc n= p^(2*k)
                    by blast
            with power-even-eq have Suc n=( ( ^ k)^2
                by simp
                with asm show False by blast
        qed
    with psi-even-def mangoldt-even-def
        have rhs: psi-even (Suc n) = psi-even n
        by simp
    from Suc.IH lhs rhs show ?case
        by simp
    qed
qed
lemma mangoldt-split:
    mangoldt d = mangoldt-1 d + mangoldt-even d + mangoldt-odd d
proof (cases primepow d)
    case False
    thus ?thesis
    by (auto simp: mangoldt-def mangoldt-1-def mangoldt-even-def mangoldt-odd-def
                dest: primepow-even-imp-primepow primepow-odd-imp-primepow)
next
    case True
    thus ?thesis
    by (auto simp: mangoldt-def mangoldt-1-def mangoldt-even-def mangoldt-odd-def
primepow-cases)
qed
lemma psi-split: psi }n=\mathrm{ theta }n+\mathrm{ psi-even }n+psi-odd 
    by (induction n)
            (simp-all add: psi-def theta-def psi-even-def psi-odd-def mangoldt-1-def man-
goldt-split)
lemma psi-mono: m\leqn\Longrightarrow psi m}\leq\mathrm{ psi n unfolding psi-def
    by (intro sum-mono2 mangoldt-nonneg) auto
lemma psi-pos: 0 \leqpsin
    by (auto simp: psi-def intro!: sum-nonneg mangoldt-nonneg)
lemma mangoldt-odd-pos: 0 \leq mangoldt-odd d
    using aprimedivisor-gt-Suc-O[of d]
    by (auto simp: mangoldt-odd-def of-nat-le-iff[of 1, unfolded of-nat-1] Suc-le-eq
        intro!: ln-ge-zero dest!: primepow-odd-imp-primepow primepow-gt-Suc-0)
lemma psi-odd-mono: m\leqn\Longrightarrow psi-odd m}\leq\mathrm{ psi-odd n
    using mangoldt-odd-pos sum-mono2[of {1..n} {1..m} mangoldt-odd]
    by (simp add: psi-odd-def)
```


## lemma psi-odd-pos: $0 \leq$ psi-odd $n$

by (auto simp: psi-odd-def intro!: sum-nonneg mangoldt-odd-pos)
lemma psi-theta:
theta $n+$ psi $($ Discrete.sqrt $n) \leq$ psi $n$ psi $n \leq$ theta $n+2 * p s i($ Discrete.sqrt n)
using psi-odd-pos[of n] psi-residues-compare[of n] psi-sqrt[of n] psi-split[of n] by simp-all

## context

begin
private lemma sum-minus-one:
$\left(\sum x \in\{1 . . y\} .(-1:: \text { real })^{\wedge}(x+1)\right)=($ if odd $y$ then 1 else 0$)$
by (induction y) simp-all
private 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 -
from $\operatorname{assms}(1,3)$ have $y * x \leq(n \operatorname{div} x) * x$
by $\operatorname{simp}$
also have $\ldots \leq n$
by (simp add: minus-mod-eq-div-mult[symmetric])
finally have $y * x \leq n$.
with $\operatorname{assms}(2)$ show ?thesis using div-le-mono[of $y * x n y$ ] by simp
qed
lemma sum-expand-lemma:

$$
\left(\sum d=1 . . n .(-1) \sim(d+1) * p s i(n \operatorname{div} d)\right)=
$$

( $\sum d=1 . . n$. (if odd $(n$ div d) then 1 else 0$) *$ mangoldt $\left.d\right)$
proof -
have $* *: x \leq n$ if $x \leq n$ div $y$ for $x y$
using div-le-dividend order-trans that by blast
have $\left(\sum d=1 . . n .(-1) \uparrow(d+1) * p s i(n\right.$ div $\left.d)\right)=$
$\left(\sum d=1 . . n .(-1) \wedge(d+1) *\left(\sum e=1 . . n\right.\right.$ div d. mangoldt $\left.\left.e\right)\right)$
by ( simp add: psi-def)
also have $\ldots=\left(\sum d=1 . . n . \sum e=1 . . n\right.$ div $d .(-1) \wedge(d+1) *$ mangoldt $\left.e\right)$ by (simp add: sum-distrib-left)
also from $* *$ have $\ldots=\left(\sum d=1 . . n . \sum e \in\{y \in\{1 . . n\} . y \leq n\right.$ div $d\} .(-1) \mathcal{~}(d+1)$

* mangoldt e)
by (intro sum.cong) auto
also have $\ldots=\left(\sum y=1 . . n . \sum x \mid x \in\{1 . . n\} \wedge y \leq n \operatorname{div} x .(-1) \wedge(x+1)\right.$
* mangoldt y)
by (rule sum.swap-restrict) simp-all
also have $\ldots=\left(\sum y=1 . . n . \sum x \mid x \in\{1 . . n\} \wedge x \leq n\right.$ div $y .(-1)^{\wedge}(x+1)$

```
* mangoldt y)
    by (intro sum.cong) (auto intro: div-invert)
    also from ** have ... = (\sumy=1..n. \sumx\in{1..n div y}. (-1)^^(x+1)*
mangoldt y)
    by (intro sum.cong) auto
    also have ... = (\sumy=1..n. (\sumx\in{1..n div y}. (-1)^ (x+1))* mangoldt
y)
    by (intro sum.cong) (simp-all add: sum-distrib-right)
    also have ... = (\sumy=1..n. (if odd ( }n\mathrm{ div y) then 1 else 0) * mangoldt y)
    by (intro sum.cong refl) (simp-all only: sum-minus-one)
    finally show ?thesis.
qed
private lemma floor-half-interval:
    fixes nd :: nat
    assumes d\not=0
    shows real (n div d) - real (2 * ((n div 2) div d)) = (if odd ( }n\mathrm{ div d) then 1
else 0)
proof -
    have ((n div 2) div d) =( n div (2*d))
        by (rule div-mult2-eq[symmetric])
    also have ... = ((n div d) div 2)
        by (simp add: mult-ac div-mult2-eq)
    also have real (n div d) - real (2*...) = (if odd ( n div d) then 1 else 0)
        by (cases odd ( }n\mathrm{ div d), cases n div d = 0, simp-all)
    finally show ?thesis by simp
qed
lemma fact-expand-psi:
    ln}(fact n) - 2* ln (fact (ndiv 2)) = (\sumd=1..n. (-1)^(d+1)*psi (n div d))
proof -
    have ln (fact n) - 2* ln (fact (n div 2)) =
        (\sumd=1..n. mangoldt d*\lfloorn/d\rfloor) - 2* (\sumd=1..n div 2. mangoldt d * \lfloor(n
div 2) / dj)
    by (simp add: ln-fact-conv-mangoldt)
    also have (\sumd=1..n div 2. mangoldt d*\lfloorreal (n div 2) / d\rfloor)=
                        (\sumd=1..n. mangoldt d * \lfloorreal (n div 2) / d\rfloor)
    by (rule sum.mono-neutral-left) (auto simp: floor-unique[of 0])
    also have 2 * .. = (\sumd=1..n. mangoldt d *2*\lfloorreal (n div 2) / d\rfloor)
    by (simp add: sum-distrib-left mult-ac)
    also have (\sumd=1..n. mangoldt d*\lfloorn/d\rfloor) - ... =
        (\sumd=1..n. (mangoldt d *\lfloorn/d\rfloor- mangoldt d * 2* \real (n div 2)
/ d\rfloor))
        by (simp add: sum-subtractf)
    also have ... =( \sumd=1..n. mangoldt d*(\lfloorn/d\rfloor-2*\lfloorreal (n div 2) / d\rfloor))
    by (simp add: algebra-simps)
    also have ... = (\sumd=1..n. mangoldt d * (if odd(n div d) then 1 else 0))
        by (intro sum.cong refl)
            (simp-all add: floor-conv-div-nat [symmetric] floor-half-interval [symmetric])
```

also have $\ldots=\left(\sum d=1 . . n .(\right.$ if odd $(n$ div $d)$ then 1 else 0$) *$ mangoldt $\left.d\right)$
by (simp add: mult-ac)
also from sum-expand-lemma[symmetric] have $\ldots=\left(\sum d=1 . . n .(-1) \uparrow(d+1)\right.$

* psi ( $n$ div d)) .
finally show ?thesis.
qed
end
lemma psi-expansion-cutoff:
assumes $m \leq p$
shows $\left(\sum d=1 . .2 * m .(-1) \uparrow(d+1) * p s i(n \operatorname{div} d)\right) \leq\left(\sum d=1 . .2 * p .(-1)^{\wedge}(d+1)\right.$
* psi ( $n \operatorname{div} d)$ )
$\left(\sum_{(-1)} d^{\prime}(d+1) * \operatorname{psi}(n \operatorname{div} d)\right)$
using assms
proof (induction $m$ rule: inc-induct)
case (step $k$ )
have $\left(\sum d=1 . .2 * k .(-1) \uparrow(d+1) * p s i(n \operatorname{div} d)\right) \leq$ $\left(\sum d=1 . .2 * \operatorname{Suc} k .(-1) \uparrow(d+1) * p s i(n \operatorname{div} d)\right)$
by (simp add: psi-mono div-le-mono2)
with step. $I H(1)$
show $\left(\sum d=1 . .2 * k .(-1) \uparrow(d+1) * \operatorname{psi}(n \operatorname{div} d)\right)$

$$
\leq\left(\sum d=1 . .2 * p \cdot(-1) \uparrow(d+1) * p s i(n \operatorname{div} d)\right)
$$

by simp
from step.IH(2)
have $\left(\sum d=1 . .2 * p+1 .(-1) \uparrow(d+1) * \operatorname{psi}(n \operatorname{div} d)\right)$ $\leq\left(\sum d=1 . .2 * \operatorname{Suc} k+1 .(-1) \uparrow(d+1) * \sin (n \operatorname{div} d)\right)$.
also have $\ldots \leq\left(\sum d=1 . .2 * k+1 .(-1) \uparrow(d+1) * \operatorname{psi}(n \operatorname{div} d)\right)$
by (simp add: psi-mono div-le-mono2)
finally show $\left(\sum d=1 . .2 * p+1 .(-1) \uparrow(d+1) * p s i(n\right.$ div d $\left.)\right)$ $\leq\left(\sum d=1 . .2 * k+1 .(-1)^{\wedge}(d+1) * p s i(n \operatorname{div} d)\right)$.
qed simp-all
lemma fact-psi-bound-even:
assumes even $k$
shows $\left(\sum d=1 . . k .(-1) \uparrow(d+1) * p s i(n\right.$ div $\left.d)\right) \leq \ln ($ fact $n)-2 * \ln (f a c t$ (n div 2))
proof -
have $\left(\sum d=1 . . k .(-1)^{\wedge}(d+1) * p s i(n\right.$ div $\left.d)\right) \leq\left(\sum d=1 . . n .(-1)^{\wedge}(d+1)\right.$

* psi ( $n \operatorname{div} d)$ )
proof (cases $k \leq n$ )
case True
with psi-expansion-cutoff(1)[of $k$ div $2 n$ div $2 n]$ have $\left(\sum d=1 . .2 *(k \operatorname{div} 2) .(-1) \uparrow(d+1) * \operatorname{psi}(n \operatorname{div} d)\right)$
$\leq\left(\sum d=1 . .2 *(n \operatorname{div} 2) .(-1)^{\wedge}(d+1) * p s i(n \operatorname{div} d)\right)$
by simp
also from assms have $2 *(k$ div 2) $=k$
by $\operatorname{simp}$

```
    also have (\sumd=1..2*(n div 2). (- 1)^ (d+1)* psi (n div d))
        \leq (\sumd=1..n. (-1)^(d+1)*psi (n div d))
    proof (cases even n)
    case True
    then show ?thesis
                by simp
    next
        case False
        from psi-pos have (\sumd=1..2*(n div 2). (- 1)^ (d + 1)* psi (n div d))
                \leq (\sumd=1..2*(n div 2) + 1. (-1)^ (d+1)* psi (n div d )}
                by simp
            with False show ?thesis
            by simp
    qed
    finally show ?thesis .
next
    case False
    hence *: n div 2 \leq (k-1) div 2
    by simp
    have (\sumd=1..k. (-1)^(d+1)*psi(n div d))\leq
            (\sumd=1..2*((k-1) div 2) + 1. (-1)^(d+1)* psi (n div d))
    proof (cases k=0)
            case True
            with psi-pos show ?thesis by simp
    next
        case False
        with sum.cl-ivl-Suc[of \lambdad. (-1)^(d+1) * psi (n div d) 1 k-1]
    have (\sumd=1..k. (-1)^(d+1)*psi (n div d))=(\sumd=1..k-1. (-1)^(d+1)
* psi (n div d))
        +(-1)^(k+1)*psi (n div k)
        by simp
    also from assms psi-pos have (-1)^(k+1)* psi (n div k)\leq0
        by simp
    also from assms False have k-1 = 2*((k-1) div 2) + 1
        by presburger
    finally show ?thesis by simp
    qed
    also from * psi-expansion-cutoff(2)[of n div 2 (k-1) div 2 n]
    have ... \leq (\sumd=1..2*(n div 2) + 1. (-1)^(d+1)* psi (n div d)) by blast
    also have ... \leq (\sumd=1..n. (-1)^ (d+1)*psi (n div d))
    by (cases even n) (simp-all add: psi-def)
    finally show ?thesis .
qed
also from fact-expand-psi have ... = ln (fact n) - 2 * ln (fact (n div 2)) ..
finally show ?thesis.
qed
lemma fact-psi-bound-odd:
    assumes odd k
```

```
    shows ln (fact n) - 2 * ln (fact (n div 2 ) ) \leq (\sumd=1..k. (-1)^(d+1)*psi (n
div d))
proof -
    from fact-expand-psi
    have ln (fact n) - 2 * ln (fact (n div 2)) = (\sumd=1..n. (- 1)^ (d+1)*
psi (n div d)).
    also have ...\leq(\sumd=1..k. (-1)^(d+1)*psi (n div d))
    proof (cases k\leqn)
    case True
    have (\sumd=1..n. (-1)^(d+1)* psi (n div d)) \leq(
                        \sumd=1..2*(n div 2)+1.(-1)^(d+1)* psi (n div d))
            by (cases even n) (simp-all add: psi-pos)
    also from True assms psi-expansion-cutoff(2)[of k div 2 n div 2 n]
        have ... \leq (\sumd=1..k. (-1)`(d+1)*psi (n div d))
                by simp
    finally show ?thesis .
    next
    case False
    have }(\sumd=1..n.(-1)^(d+1)*psi (n div d)) \leq (\sumd=1..2*((n+1) div 2).
(-1)`(d+1) * psi (n div d))
        by (cases even n) (simp-all add: psi-def)
    also from False assms psi-expansion-cutoff(1)[of (n+1) div 2 k div 2 n]
    have (\sumd=1..2*((n+1) div 2). (-1)`(d+1)* psi (n div d ))\leq(\sumd=1..2*(k
div 2). (-1)^(d+1)*psi (n div d))
            by simp
    also from assms have ...\leq(\sumd=1..k. (-1)^(d+1)*psi (n div d))
        by (auto elim: oddE simp: psi-pos)
    finally show ?thesis.
    qed
    finally show ?thesis.
qed
lemma fact-psi-bound-2-3:
    psi n - psi(ndiv 2) \leq ln (fact n) - 2* ln (fact (n div 2))
    ln}(fact n) - 2 * ln (fact (ndiv 2)) \leqpsi n - psi (ndiv 2) + psi (n div 3)
proof -
    show psi n - psi (n div 2) \leq ln (fact n) - 2* ln (fact (n div 2))
    by (rule psi-bounds-ln-fact (2))
next
    from fact-psi-bound-odd[of 3 n] have ln (fact n) - 2* ln (fact (n div 2))
    \leq (\sumd=1..3. (-1)^ (d+1)*psi (n div d))
    by simp
    also have ... = psi n - psi (n div 2) + psi (n div 3)
    by (simp add: sum.atLeast-Suc-atMost numeral-2-eq-2)
    finally show ln (fact n) - 2 * ln (fact (n div 2)) \leqpsi n - psi (n div 2) + psi
(n div 3).
qed
lemma ub-ln-1200:ln 1200\leq57 / (8 :: real)
```

```
proof -
    have Some (Float 57 (-3)) = ub-ln 8 1200 by code-simp
    from ub-ln(1)[OF this] show ?thesis by simp
qed
lemma psi-double-lemma:
    assumes n\geq1200
    shows real n/ 6\leqpsi n - psi(n div 2)
proof -
    from ln-fact-diff-bounds
        have |ln(fact n) - 2 * ln (fact (n div 2)) - real n*ln 2 |
            \leq4* ln (real (if n=0 then 1 else n)) + 3.
    with assms have ln (fact n)-2* ln (fact (n div 2))
         real n* ln 2-4*\operatorname{ln}(\mathrm{ real n) - 3}
    by simp
    moreover have real n*\operatorname{ln}2-4*\operatorname{ln}(\mathrm{ real n) - 3 2 2 / 3*n}
    proof (rule overpower-lemma[of \lambdan. 2/3*n 1200])
        show 2 / 3*1200\leq1200* ln 2 - 4* ln 1200- (3::real)
            using ub-ln-1200 ln-2-ge by linarith
    next
        fix x::real
        assume 1200 \leqx
        then have 0<x
            by simp
    show}((\lambdax.x*\operatorname{ln}2-4*\operatorname{ln}x-3-2/3*x
                has-real-derivative ln 2-4/x-2 / 3) (at x)
            by (rule derivative-eq-intros refl | simp add: <0<x〉)+
    next
        fix x::real
        assume 1200 \leqx
        then have 12 / x\leq12 / 1200 by simp
        then have 0\leq0.67-4/x-2 / 3 by simp
        also have 0.67\leqln (2::real) using ln-2-ge by simp
        finally show 0}\leq\operatorname{ln}2-4/x-2/3 by sim
    next
        from assms show 1200 \leq real n
            by simp
    qed
    ultimately have 2 / 3* real n \leq ln (fact n) - 2 * ln (fact (n div 2))
    by simp
    with psi-ubound-3-2[of n div 3]
        have n/6 + psi(n div 3) \leqln (fact n) - 2* ln (fact (n div 2))
        by simp
    with fact-psi-bound-2-3[of n] show ?thesis
        by simp
qed
lemma theta-double-lemma:
    assumes n\geq1200
```

```
    shows theta (n div 2) < theta n
proof -
    from psi-theta[of n div 2] psi-pos[of Discrete.sqrt (n div 2)]
        have theta-le-psi-n-2: theta ( }n\mathrm{ div 2) }\leq\mathrm{ psi (n div 2)
        by simp
    have (Discrete.sqrt n* 18)^2 \leq 324*n
    by simp
    from mult-less-cancel2[of 324 n n] assms have 324*n< n^2
    by (simp add: power2-eq-square)
    with <(Discrete.sqrt n*18)^2 \leq 324*n> have (Discrete.sqrt n*18)^2<n^2
        by presburger
    with power2-less-imp-less assms have Discrete.sqrt n * 18<n
        by blast
    with psi-ubound-3-2[of Discrete.sqrt n] have 2 * psi(Discrete.sqrt n)<n/6
        by simp
    with psi-theta[of n] have psi-lt-theta-n: psi n - n/ 6< theta n
        by simp
    from psi-double-lemma[OF assms(1)] have psi(n div 2) \leq psin - n/6
        by simp
    with theta-le-psi-n-2 psi-lt-theta-n show ?thesis
        by simp
qed
```


### 0.7 Proof of the main result

```
lemma theta-mono: mono theta
by (auto simp: theta-def [abs-def] intro!: monoI sum-mono2)
lemma theta-lessE:
assumes theta \(m<\) theta \(n m \geq 1\)
obtains \(p\) where \(p \in\{m<. . n\}\) prime \(p\)
proof -
from mono-invE[OF theta-mono assms(1)] have \(m \leq n\) by blast
hence theta \(n=\) theta \(m+\left(\sum p \in\{m<. . n\}\right.\). if prime \(p\) then \(\ln (\) real \(p)\) else 0\()\) unfolding theta-def using assms(2)
by (subst sum.union-disjoint [symmetric]) (auto simp: ivl-disj-un)
also note assms(1)
finally have \(\left(\sum p \in\{m<. . n\}\right.\). if prime \(p\) then \(\ln (\) real \(p)\) else 0\() \neq 0\) by simp
then obtain \(p\) where \(p \in\{m<. . n\}\) (if prime \(p\) then \(\ln (\) real \(p)\) else 0\() \neq 0\)
by (rule sum.not-neutral-contains-not-neutral)
thus ?thesis using that \([o f p]\) by (auto intro!: exI \([o f-p]\) split: if-splits)
qed
theorem bertrand:
fixes \(n\) :: nat
assumes \(n>1\)
shows \(\exists p \in\{n<. .<2 * n\}\). prime \(p\)
proof cases
assume \(n\)-less: \(n<600\)
```

define prime-constants
where prime-constants $=\{2,3,5,7,13,23,43,83,163,317,631::$ nat $\}$
from $\langle n>1\rangle n$-less have $\exists p \in$ prime-constants. $n<p \wedge p<2 * n$
unfolding bex-simps greaterThanLessThan-iff prime-constants-def by presburger
moreover have $\forall p \in$ prime-constants. prime $p$
unfolding prime-constants-def ball-simps HOL.simp-thms
by (intro conjI; pratt (silent))
ultimately show ?thesis
unfolding greaterThanLessThan-def greaterThan-def lessThan-def by blast
next
assume $n: \neg(n<600)$
from $n$ have theta $n<$ theta $(2 * n)$ using theta-double-lemma[of $2 * n]$ by simp
with assms obtain $p$ where $p \in\{n<. .2 * n\}$ prime $p$ by (auto elim!: theta-lessE)
moreover from assms have $\neg$ prime $(2 * n)$ by (auto dest!: prime-product)
with $\langle$ prime $p\rangle$ have $p \neq 2 * n$ by auto
ultimately show?thesis
by auto
qed

### 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-nat \(m-1\)..of-nat \(n\} \Longrightarrow(g\) has-field-derivative \(f x)\)
(at \(x\) )
            and le: \(\bigwedge x y . \llbracket\) real \(m-1 \leq x ; x \leq y ; y \leq\) real \(n \rrbracket \Longrightarrow f y \leq f x\)
    shows \(\left(\sum k=m . . n . f(\right.\) of-nat \(\left.k)\right) \leq g(\) of-nat \(n)-g(\) of-nat \(m-1)\)
proof -
    have \(\left(\sum k=\right.\) m..n. \(f(\) of-nat \(\left.k)\right) \leq\left(\sum k=\right.\) m..n. \(g(o f-n a t(\) Suc \(k)-1)-g\)
(of-nat \(k-1\) ))
    proof (rule sum-mono, clarsimp)
        fix \(r\)
    assume \(r\) : \(m \leq r r \leq n\)
    hence \(\exists z>\) real \(r-1 . z<\) real \(r \wedge g(\) real \(r)-g(\) real \(r-1)=(\) real \(r-\)
\((\) real \(r-1)) * f z\)
            using assms by (intro MVT2) auto
    hence \(\exists z \in\{\) of-nat \(r-1\)..of-nat \(r\}\). \(g(\) real \(r)-g(\) real \(r-1)=f z\) by auto
    then obtain \(u\) ::real where \(u: u \in\{o f\)-nat \(r-1\)..of-nat \(r\}\)
                and eq: \(g r-g(o f-n a t r-1)=f u\) by blast
    have real \(m \leq u+1\)
            using \(r u\) by auto
    then have \(f(\) of-nat \(r) \leq f u\)
            using \(r\) (2) and \(u\) by (intro le) auto
    then show \(f(\) of-nat \(r) \leq g r-g(o f\)-nat \(r-1)\)
```

```
    by (simp add: eq)
    qed
    also have ... \leqg(of-nat n) -g(of-nat m - 1)
    using <m \leq n` by (subst sum-Suc-diff) auto
    finally show ?thesis.
qed
lemma Mertens-lemma:
    assumes n\not=0
        shows |(\sumd=1..n. mangoldt d / real d) - ln n| \leq4
proof -
    have *: \llbracketabs(s' - nl + n) \leqa; abs(s' - s)\leq (k-1)*n-a\rrbracket
        \Longrightarrowabs(s-nl)\leqn*k for s'sk nl a::real
    by (auto simp: algebra-simps abs-if split: if-split-asm)
    have le: |(\sumd=1..n. mangoldt d* floor (n/d)) - n* ln n + n| \leq 1 + ln n
    using ln-fact-bounds ln-fact-conv-mangoldt assms by simp
    have |real n* ((\sumd=1..n. mangoldt d / real d) - ln n)|=
        |((\sumd=1..n. real n * mangoldt d / real d) - n*\operatorname{ln}n)|
    by (simp add: algebra-simps sum-distrib-left)
    also have ... \leqreal n*4
    proof (rule * [OF le])
    have |(\sumd=1..n. mangoldt d*\lfloorn/d\rfloor) - (\sumd=1..n.n* mangoldt d /
d)|
        = |\sumd=1..n. mangoldt d * (\lfloorn/d\rfloor-n/d)|
        by (simp add: sum-subtractf algebra-simps)
    also have ... \leqpsin (is |?sm| \leq?rhs)
    proof -
        have -?sm=(\sumd=1..n. mangoldt d * (n/d - \lfloorn/d\rfloor))
        by (simp add: sum-subtractf algebra-simps)
            also have ... \leq (\sumd=1..n. mangoldt d*1)
                by (intro sum-mono mult-left-mono mangoldt-nonneg) linarith+
    finally have -?sm \leq?rhs by (simp add: psi-def)
    moreover
    have ?sm\leq0
            using mangoldt-nonneg by (simp add: mult-le-0-iff sum-nonpos)
            ultimately show ?thesis by (simp add: abs-if)
    qed
    also have ... \leq3/2* real n
        by (rule psi-ubound-3-2)
    also have .. \leq (4-1)* real n - (1 + ln n)
        using ln-le-minus-one [of n] assms by (simp add: divide-simps)
    finally
    show |(\sumd=1 ..n. mangoldt d * real-of-int \real n / real d\rfloor) -
                (\sumd=1..n. real n * mangoldt d / real d)
            \leq(4-1)* real n-(1+ln n).
qed
finally have |real n*((\sumd=1..n. mangoldt d / real d) - ln n)|\leqreal n*&.
then show ?thesis
    using assms mult-le-cancel-left-pos by (simp add:abs-mult)
```


## qed

## lemma Mertens-mangoldt-versus-ln:

$$
\text { assumes } I \subseteq\{1 . . n\}
$$

shows $\mid\left(\sum i \in I\right.$. mangoldt $\left.i / i\right)-\left(\sum p \mid\right.$ prime $\left.p \wedge p \in I . \ln p / p\right) \mid \leq 3$
(is $|? l h s| \leq 3$ )
proof (cases $n=0$ )
case True
with assms show ?thesis by simp
next
case False
have finite I
using assms finite-subset by blast
have $0 \leq\left(\sum i \in I\right.$. mangoldt $i / i-($ if prime $i$ then $\ln i / i$ else 0$\left.)\right)$
using mangoldt-nonneg by (intro sum-nonneg) simp-all
moreover have $\ldots \leq\left(\sum i=1\right.$..n. mangoldt $i / i-$ (if prime $i$ then $\ln i / i$ else 0))
using assms by (intro sum-mono2) (auto simp: mangoldt-nonneg)
ultimately have $*: \mid \sum i \in I$. mangoldt $i / i-$ (if prime $i$ then $\ln i / i$ else 0$) \mid$ $\leq \mid \sum i=1$..n. mangoldt $i / i-($ if prime $i$ then $\ln i / i$ else 0$) \mid$
by linarith
moreover have ?lhs $=\left(\sum i \in I\right.$. mangoldt $i / i-$ (if prime $i$ then $\ln i / i$ else 0))

$$
\begin{aligned}
& \left(\sum i=1 . . n . \text { mangoldt } i / i-(\text { if prime } i \text { then } \ln i / i \text { else } 0)\right) \\
& \quad=\left(\sum d=1 . . n . \text { mangoldt } d / d\right)-\left(\sum p \mid \text { prime } p \wedge p \in\{1 . . n\} .\right.
\end{aligned}
$$

$\ln p / p)$
using sum.inter-restrict $[$ of $-\lambda i . \ln ($ real $i) / i$ Collect prime, symmetric] by (force simp: sum-subtractf〈finite $I\rangle$ intro: sum.cong) +
ultimately have $|? l h s| \leq \mid\left(\sum d=1\right.$..n. mangoldt $\left.d / d\right)-$
$\left(\sum p \mid\right.$ prime $\left.p \wedge p \in\{1 . . n\} . \ln p / p\right) \mid$ by linarith
also have $\ldots \leq 3$
proof -
have eq-sm: $\left(\sum i=1\right.$..n. mangoldt $\left.i / i\right)=$
( $\sum i \in\left\{p^{\wedge} k \mid p k\right.$. prime $\left.p \wedge p^{\wedge} k \leq n \wedge k \geq 1\right\}$. mangoldt $\left.i / i\right)$
proof (intro sum.mono-neutral-right ballI, goal-cases)
case (3i)
hence $\neg$ primepow $i$ by (auto simp: primepow-def Suc-le-eq)
thus ?case by (simp add: mangoldt-def)
qed (auto simp: Suc-le-eq prime-gt-0-nat)
have $\left(\sum i=1\right.$..n. mangoldt $\left.i / i\right)-\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 . . n\}$. $\left.\ln p / p\right)$
( $\sum i \in\left\{p^{\wedge} k \mid p k\right.$. prime $p \wedge p^{\wedge} k \leq n \wedge k \geq$ 2 $\}$. mangoldt $\left.i / i\right)$
proof -
have eq: $\left\{p^{\wedge} k \mid p k\right.$. prime $\left.p \wedge p^{\wedge} k \leq n \wedge 1 \leq k\right\}=$
$\left\{p^{\wedge} k \mid p k\right.$. prime $\left.p \wedge p^{\wedge} k \leq n \wedge 2 \leq k\right\} \cup\{p$. prime $p \wedge p \in$
$\{1 . . n\}\}$
(is $? A=? B \cup ? C$ )
proof (intro equalityI subsetI; (elim UnE)?)
fix $x$ assume $x \in$ ? $A$
then obtain $p k$ where $x=p^{\wedge} k$ prime $p{ }^{\wedge} k \leq n k \geq 1$ by auto thus $x \in ? B \cup$ ? $C$
by (cases $k \geq 2$ ) (auto simp: prime-power-iff Suc-le-eq)
next
fix $x$ assume $x \in ? B$
then obtain $p k$ where $x=p^{\wedge} k$ prime $p p^{\wedge} k \leq n k \geq 1$ by auto
thus $x \in ?$ ? by (auto simp: prime-power-iff Suc-le-eq)
next
fix $x$ assume $x \in$ ? $C$
then obtain $p$ where $x=p^{\wedge} 11 \geq\left(1::\right.$ nat) prime p $p^{\wedge} 1 \leq n$ by auto
thus $x \in$ ?A by blast
qed
have eqln: $\left(\sum p \mid\right.$ prime $\left.p \wedge p \in\{1 . . n\} . \ln p / p\right)=$

$$
\left(\sum p \mid \text { prime } p \wedge p \in\{1 \ldots n\} \text {. mangoldt } p / p\right)
$$

by (rule sum.cong) auto
have $\left(\sum i \in\left\{p^{\wedge} k \mid p k\right.\right.$. prime $\left.p \wedge p^{\wedge} k \leq n \wedge k \geq 1\right\}$. mangoldt $\left.i / i\right)=$ $\left(\sum i \in\left\{p^{\wedge} k \mid p k\right.\right.$. prime $\left.p \wedge p^{\wedge} k \leq n \wedge 2 \leq k\right\} \cup$ \{p. prime $p \wedge p \in\{1 . . n\}\}$. mangoldt $i / i$ ) by (subst eq) simp-all
also have $\ldots=\left(\sum i \in\left\{p^{\wedge} k \mid p k\right.\right.$. prime $p \wedge p^{\wedge} k \leq n \wedge k \geq$ 2 $\}$. mangoldt $i / i)$

$$
+\left(\sum p \mid \text { prime } p \wedge p \in\{1 . . n\} . \text { mangoldt } p / p\right)
$$

by (intro sum.union-disjoint) (auto simp: prime-power-iff finite-nat-set-iff-bounded-le)
also have $\ldots=\left(\sum i \in\left\{p^{\wedge} k \mid p k\right.\right.$. prime $\left.p \wedge p^{\wedge} k \leq n \wedge k \geq 2\right\}$. mangoldt $i / i)$

$$
+\left(\sum p \mid \text { prime } p \wedge p \in\{1 . . n\} . \ln p / p\right) \text { by (simp only: eqln) }
$$

finally show ?thesis using eq-sm by auto
qed
have $\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 . . n\}$. $\left.\ln p / p\right) \leq\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 . . n\}$. mangoldt $p / p$ )
using mangoldt-nonneg by (auto intro: sum-mono)
also have $\ldots \leq\left(\sum i=\right.$ Suc 0..n. mangoldt $\left.i / i\right)$
by (intro sum-mono2) (auto simp: mangoldt-nonneg)
finally have $0 \leq\left(\sum i=1\right.$..n. mangoldt $\left.i / i\right)-\left(\sum p \mid\right.$ prime $p \wedge p \in$ $\{1 . . n\} . \ln p / p$ )
by $\operatorname{simp}$
moreover have $\left(\sum i=1\right.$..n. mangoldt $\left.i / i\right)-\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 . . n\}$.
$\ln p / p) \leq 3$

$$
(\text { is } ? M-? L \leq 3)
$$

proof -
have $*: \exists q . \exists j \in\{1 . . n\}$. prime $q \wedge 1 \leq q \wedge q \leq n \wedge$

$$
(q \wedge j=p \wedge k \wedge \text { mangoldt }(p \wedge k) / \text { real } p \wedge k \leq \ln (\text { real } q) / \text { real } q
$$

${ }^{\wedge}$ j)
if prime $p p^{\wedge} k \leq n 1 \leq k$ for $p k$
proof -
have mangoldt $\left(p^{\wedge} k\right) / \operatorname{real} p^{\wedge} k \leq \ln p / p^{\wedge} k$
using that by (simp add: divide-simps)
moreover have $p \leq n$
using that self-le-power[of plibl by (simp add: prime-ge-Suc-0-nat)
moreover have $k \leq n$
proof -
have $k<2^{\wedge} k$
using of-nat-less-two-power of-nat-less-numeral-power-cancel-iff by
blast
also have $\ldots \leq p^{\wedge} k$
by (simp add: power-mono prime-ge-2-nat that)
also have $\ldots \leq n$
by (simp add: that)
finally show ?thesis by (simp add: that)
qed
ultimately show ?thesis
using prime-ge-1-nat that by auto (use atLeastAtMost-iff in blast)
qed
have finite: finite $\left\{p^{\wedge} k \mid p k\right.$. prime $\left.p \wedge p^{\wedge} k \leq n \wedge 1 \leq k\right\}$
by (rule finite-subset $[o f-\{. . n\}]$ ) auto
have $? M \leq\left(\sum(x, k) \in\{p\right.$. prime $p \wedge p \in\{1 . . n\}\} \times\{1 . . n\} . \ln ($ real $x) /$ real $x^{\wedge} k$ )
by (subst eq-sm, intro sum-le-included $\left[\right.$ where $\left.\left.i=\lambda(p, k), p^{\wedge} k\right]\right)$
(insert $*$ finite, auto)
also have $\ldots=\left(\sum p \mid\right.$ prime $\left.p \wedge p \in\{1 . . n\} .\left(\sum k=1 . . n . \ln p / p^{\wedge} k\right)\right)$
by (subst sum.Sigma) auto
also have $\ldots=? L+\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 . . n\} .\left(\sum k=2 . . n . \ln p /\right.$ $\left.p^{\wedge} k\right)$ )
by (simp add: comm-monoid-add-class.sum.distrib sum.atLeast-Suc-atMost numeral-2-eq-2)
finally have $? M-? L \leq\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 . . n\} .\left(\sum k=2 . . n . \ln p\right.$ ( $\left.p^{\wedge} k\right)$ )
by (simp add: algebra-simps)
also have $\ldots=\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 . . n\} . \ln p *\left(\sum k=2 . . n\right.$. inverse $\left.p^{\wedge} k\right)$ )
by (simp add: field-simps sum-distrib-left)
also have $\ldots=\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 \ldots n\}$.

$$
\left.\ln p *\left(\left((\text { inverse } p)^{2}-\text { inverse } p \wedge \text { Suc } n\right) /(1-\text { inverse } p)\right)\right)
$$

by (intro sum.cong refl) (simp add: sum-gp)
also have $\ldots \leq\left(\sum p \mid\right.$ prime $p \wedge p \in\{1 . . n\}$. In $p *$ inverse (real $(p *(p$ $-1))$ )
by (intro sum-mono mult-left-mono)
(auto simp: divide-simps power2-eq-square of-nat-diff mult-less-0-iff)
also have $\ldots \leq\left(\sum p=2 . . n . \ln p *\right.$ inverse $\left.(\operatorname{real}(p *(p-1)))\right)$
by (rule sum-mono2) (use prime-ge-2-nat in auto)
also have $\ldots \leq\left(\sum i=2 . . n . \ln i /(i-1)^{2}\right)$
unfolding divide-inverse power2-eq-square mult.assoc
by (auto intro: sum-mono mult-left-mono mult-right-mono)
also have $\ldots \leq 3$
proof (cases $n \geq 3$ )
case False then show ?thesis
proof (cases $n \geq$ 2)
case False then show ?thesis by simp

```
    next
            case True
            then have n=2 using False by linarith
            with ln-le-minus-one [of 2] show ?thesis by simp
        qed
    next
            case True
    have (\sumi= 3..n.ln (real i) / (real (i-Suc 0))}\mp@subsup{)}{}{2}
        \leq (ln (of-nat n - 1)) - (ln (of-nat n)) - (ln (of-nat n) / (of-nat n
- 1))+2* ln 2
    proof -
        have 1:((\lambdaz. ln (z-1) - ln z-\operatorname{ln}z/(z-1)) has-field-derivative ln
x/(x-1)}\mp@subsup{)}{}{2}(\mathrm{ at }x
            if x: x { {2..real n} for }
            by (rule derivative-eq-intros | rule refl |
                (use x in 〈force simp: power2-eq-square divide-simps〉))+
            have 2: ln y/(y-1) 2}\leq\operatorname{ln}x/(x-1\mp@subsup{)}{}{2}\mathrm{ if xy:2 }\leqxx\leqyy\leqrea
nfor x y
            proof (cases x=y)
            case False
            define f' :: real m real
                    where f'= (\lambdau. ((u-1)2 /u-lnu*(2*u-2)) / (u-1)^4)
                            have f'-altdef: f'u= inverse }u*\mathrm{ inverse ((u-1)2)-2* ln u/ (u
- 1)^ 3
            if u:u\in{x..y} for u::real unfolding f'-def using u
    by (simp add: eval-nat-numeral divide-simps) (simp add: algebra-simps)?
            have deriv: ((\lambdaz. ln z/(z-1)}\mp@subsup{)}{}{2})\mathrm{ has-field-derivative f'u) (at u)
                    if u:u\in{x..y} for u::real unfolding f'-def
                    by (rule derivative-eq-intros refl | (use u xy in <force simp:di-
vide-simps>))+
            hence }\existsz>x.z<y\wedgelny/(y-1\mp@subsup{)}{}{2}-\operatorname{ln}x/(x-1\mp@subsup{)}{}{2}=(y-x)
f'z
            using xy and }\langlex\not=y\rangle\mathrm{ by (intro MVT2) auto
            then obtain }\xi::\mathrm{ real where }x<\xi\xi<
            and }\xi:\operatorname{ln}y/(y-1\mp@subsup{)}{}{2}-\operatorname{ln}x/(x-1\mp@subsup{)}{}{2}=(y-x)*\mp@subsup{f}{}{\prime}\xi\mathrm{ by blast
            have f}\mp@subsup{f}{}{\prime}\xi\leq
            proof -
            have 2/3\leqln (2::real) by (fact ln-2-ge')
            also have ... \leqln}
                using <x<<\xi` xy by auto
            finally have 1\leq2* ln \xi by simp
            then have *: \xi\leq\xi*(2*ln}\xi
                using <x< < > xy by auto
            hence }\xi-1\leq\operatorname{ln}\xi*2*\xi\mathrm{ by (simp add: algebra-simps)
            hence 1/(\xi*(\xi-1\mp@subsup{)}{}{2})\leq\operatorname{ln}\xi*2/(\xi-1)^3
                using xy <x< < by (simp add: divide-simps power-eq-if)
            thus ?thesis using xy <x<\xi\rangle\langle\xi< y> by (subst f'-altdef) (auto simp:
divide-simps)
    qed
```

```
            then have }(\operatorname{ln}y/(y-1\mp@subsup{)}{}{2}-\operatorname{ln}x/(x-1\mp@subsup{)}{}{2})\leq
                    using <x \leq y by (simp add:mult-le-0-iff \xi)
            then show?thesis by simp
            qed simp-all
            show ?thesis
                    using sum-integral-ubound-decreasing'
                    [OF<3\leqn\rangle, of \lambdaz. ln(z-1)-\operatorname{ln}z-\operatorname{ln}z/(z-1)\lambdaz.lnz/
(z-1)2]
                    12〈3\leqn`
                    by (auto simp: in-Reals-norm of-nat-diff)
            qed
            also have ... \leq2
            proof -
                have ln (real n-1) - ln n\leq0 0 \leq ln n/(real n-1)
                    using < 3 \leq n` by auto
                    then have ln (real n-1) - ln n-lnn/(real n-1)\leq0
                            by linarith
                    with ln-2-less-1 show ?thesis by linarith
            qed
            also have ... \leq 3- ln 2
                using ln-2-less-1 by (simp add: algebra-simps)
            finally show ?thesis
            using True by (simp add: algebra-simps sum.atLeast-Suc-atMost [of 2 n])
        qed
            finally show ?thesis .
            qed
            ultimately show ?thesis
                by linarith
    qed
    finally show ?thesis .
qed
proposition Mertens:
    assumes n}=
    shows |(\sump| prime p}\wedge p\leqn. ln p / of-nat p) - ln n| \leq
proof -
    have |(\sumd=1..n. mangoldt d / real d) - (\sump| prime p}\wedge p\in{1..n}.ln (rea
p) / real p)|
            \leq7-4 using Mertens-mangoldt-versus-ln [of {1..n} n] by simp-all
    also have {p.prime p}\wedgep\in{1..n}}={p.prime p\wedgep\leqn
            using atLeastAtMost-iff prime-ge-1-nat by blast
    finally have |(\sumd=1..n. mangoldt d / real d) - (\sump\in\ldots..ln (real p)/ real
p)| < 7-4.
```



```
    by (rule Mertens-lemma)
    ultimately show ?thesis by linarith
qed
end
```


## References

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

