

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

About the formalization of some results by Chebyshev in number theory via the Matita ITP

Dipartimento di Scienze dell'Informazione
Mura Anteo Zamboni 7, Bologna
`asperti@cs.unibo.it`

January 19, 2009

Outline

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebishev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

1 Introduction

2 The factorization of $n!$

- Upper and lower bounds for B

3 Chebishev's Ψ function

4 Bertrand's postulate

- Erdős approach (1932)
- Automatic check

Matita in a nutshell

Introduction

The
factorization of
 $n!$

Upper and lower
bounds for B

Chebyshev's ψ
function

Bertrand's
postulate

Erdős approach
(1932)

Automatic check

Matita in a nutshell

A light version of Coq.

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Matita in a nutshell

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

A light version of Coq.

Some distinctive features:

- a primitive notion of metavariable
- a sophisticated disambiguation mechanism
- a powerful coercion system
- tynicals
- a mathml compliant goal window
- semantic selection, cut & paste

Style of the talk

Introduction

The
factorization of
 $n!$

Upper and lower
bounds for B

Chebyshev's ψ
function

Bertrand's
postulate

Erdős approach
(1932)

Automatic check

Style of the talk

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

I will describe the subject in a way **suited to formalization** but not the formal details.

Style of the talk

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

I will describe the subject in a way **suited to formalization** but not the formal details.

At a few points I will point out some **tricky aspects** of the formal encoding.

The Prime Number Theorem

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Let $\pi(n)$ denote the number of primes not exceeding n .

Theorem (Hadamard and La Vallée Poussin, 1896)

$$\pi(n) \sim n/\log(n)$$

The Prime Number Theorem

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Let $\pi(n)$ denote the number of primes not exceeding n .

Theorem (Hadamard and La Vallée Poussin, 1896)

$$\pi(n) \sim n/\log(n)$$

Formalized by Avigad et al. in Isabelle (ACM-TOCL 9(1), 2007), following Selberg's “elementary” proof (1949).

Chebyshev's Theorem

Theorem (Chebyshev, 1850)

There are two constants c_1 and c_2 such that, for any n

$$c_1 \frac{n}{\log(n)} \leq \pi(n) \leq c_2 \frac{n}{\log(n)}$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Chebyshev's Theorem

Theorem (Chebyshev, 1850)

There are two constants c_1 and c_2 such that, for any n

$$c_1 \frac{n}{\log(n)} \leq \pi(n) \leq c_2 \frac{n}{\log(n)}$$

Motivations for the formalization:

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Chebyshev's Theorem

Theorem (Chebyshev, 1850)

There are two constants c_1 and c_2 such that, for any n

$$c_1 \frac{n}{\log(n)} \leq \pi(n) \leq c_2 \frac{n}{\log(n)}$$

Motivations for the formalization:

- important machinery for number theory: ψ, θ, \dots

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Chebyshev's Theorem

Theorem (Chebyshev, 1850)

There are two constants c_1 and c_2 such that, for any n

$$c_1 \frac{n}{\log(n)} \leq \pi(n) \leq c_2 \frac{n}{\log(n)}$$

Motivations for the formalization:

- important machinery for number theory: ψ, θ, \dots
- methodology: provide a **purely arithmetical** (and constructive) formalization

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Chebyshev's Theorem

Theorem (Chebyshev, 1850)

There are two constants c_1 and c_2 such that, for any n

$$c_1 \frac{n}{\log(n)} \leq \pi(n) \leq c_2 \frac{n}{\log(n)}$$

Motivations for the formalization:

- important machinery for number theory: ψ, θ, \dots
- methodology: provide a **purely arithmetical** (and constructive) formalization

To spare logs:

$$2^{c_1 n} \leq n^{\pi(n)} \leq 2^{c_2 n}$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Outline

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

1 Introduction

2 The factorization of $n!$

- Upper and lower bounds for B

3 Chebyshev's Ψ function

4 Bertrand's postulate

- Erdős approach (1932)
- Automatic check

The factorization of $n!$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Chebyshev's approach: exploit the decomposition of the number $n!$ as a product of prime numbers.

The factorization of $n!$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Chebyshev's approach: exploit the decomposition of the number $n!$ as a product of prime numbers.

For any prime p , the numbers $1, 2, \dots, n$ include just $\frac{n}{p}$ multiples of p , $\frac{n}{p^2}$ multiples of p^2 , and so on. Hence

$$n! = \prod_{p \leq n} \prod_{i < \log_p(n)} p^{n/p^{i+1}} \quad (1)$$

(see e.g. **Hardy & Wright's**, pag. 342).

A formal proof:(1) the factorization of n

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Every integer n may be uniquely decomposed as the product of all its prime factors.

Let us write $ord_p(n)$ for the multiplicity of p in n ; then

$$n = \prod_{p \leq n} p^{ord_p(n)} = \prod_{p \leq n} \prod_{\substack{i < \log_p(n) \\ p^{i+1} | n}} p \quad (2)$$

for p prime.

A formal proof:(2) the factorization of n

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

A **direct proof** by induction on the upper bound of the product.

A formal proof:(2) the factorization of n

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

A **direct proof** by induction on the upper bound of the product. We have to rephrase the statement in the form

$$\forall m > c(n), n = \prod_{p \leq m} p^{\text{ord}_p(n)}$$

A formal proof:(2) the factorization of n

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

A **direct proof** by induction on the upper bound of the product. We have to rephrase the statement in the form

$$\forall m > c(n), n = \prod_{p \leq m} p^{\text{ord}_p(n)}$$

To make induction work $c(n)$ must be **minimal**: in this case, the **largest prime factor** of n ($mpf(n)$)

$$\forall m > mpf(n), n = \prod_{p \leq m} p^{\text{ord}_p(n)}$$

A formal proof:(3) the factorization of n in matita

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

definition $\text{mpf } n := \max n (\lambda i . \text{primeb } i \wedge i \mid n)$.

theorem $\text{lt_max_to_pi_p_primeb}$:

$\forall m, n.$

$0 < n \rightarrow$

$\text{mpf } n < m \rightarrow$

$n = \text{pi_p } m (\lambda i . \text{primeb } i \wedge i \mid n) (\lambda p . p^{\text{ord } n p})$.

A formal proof:(4) the factorization of $n!$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

$$\begin{aligned}n! &= \prod_{1 \leq m \leq n} m \\&= \prod_{1 \leq m \leq n} \prod_{p \leq m} \prod_{\substack{i < \log_p(m) \\ p^{i+1} | m}} p \\&= \prod_{p \leq n} \prod_{p \leq m \leq n} \prod_{\substack{i < \log_p(m) \\ p^{i+1} | m}} p \\&= \prod_{p \leq n} \prod_{i < \log_p(n)} \prod_{\substack{m \leq n \\ p^{i+1} | m}} p \\&= \prod_{p \leq n} \prod_{i < \log_p(n)} p^{n/p^{i+1}}\end{aligned}$$

The binomial coefficient $B(2n) = \binom{2n}{n}$

For $2n$ we have:

$$2n! = \prod_{p \leq 2n} \prod_{i < \log_p(2n)} p^{2n/p^{i+1}} \quad (3)$$

But

$$\frac{2n}{p^{i+1}} = 2 \frac{n}{p^{i+1}} + \left(\frac{2n}{p^{i+1}} \bmod 2 \right)$$

Moreover, if $n \leq p$ or $\log_p(n) \leq i$ we have

$$\frac{n}{p^{i+1}} = O$$

Hence, if we define

$$B(n) = \prod_{p \leq n} \prod_{i < \log_p(n)} p^{(n/p^{i+1} \bmod 2)}$$

equation (3) becomes

$$2n! = n!^2 B(2n) \quad (4)$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Upper and lower bounds for B

By induction on n we easily prove:

$$\frac{2^{2n}}{2n} \leq B(2n) = \frac{2n!}{n!^2} \leq 2^{2n-1}$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Upper and lower bounds for B

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

By induction on n we easily prove:

$$\frac{2^{2n}}{2n} \leq B(2n) = \frac{2n!}{n!^2} \leq 2^{2n-1}$$

For technical reasons, we need a slightly stronger results, namely,

$$B(2n) = \frac{2n!}{n!^2} \leq 2^{2n-2}$$

that holds for any n larger than 4.

Outline

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

1 Introduction

2 The factorization of $n!$

- Upper and lower bounds for B

3 Chebyshev's ψ function

4 Bertrand's postulate

- Erdős approach (1932)
- Automatic check

Chebyshev's Ψ function

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

$$\Psi(n) = \prod_{\mathbf{p} \leq n} p^{\log_p(n)}$$

Chebyshev's Ψ function

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

$$\Psi(n) = \prod_{\mathbf{p} \leq n} p^{\log_p(n)}$$

Chebyshev's ψ is the naperian logarithm of Ψ :

$$\psi = \sum_{\mathbf{p} \leq n} \frac{\log n}{\log p} \log p$$

Relation between Ψ and π

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

$$\Psi(n) = \prod_{p \leq n} p^{\log_p(n)} \leq \prod_{p \leq n} n = n^{\pi(n)} \quad (5)$$

$$n^{\pi(n)} \leq \prod_{p \leq n} p^{\log_p(n)+1} \leq \prod_{p \leq n} p^{2\log_p(n)} = \Psi(n)^2 \quad (6)$$

Relation between Ψ and π

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

$$\Psi(n) = \prod_{p \leq n} p^{\log_p(n)} \leq \prod_{p \leq n} n = n^{\pi(n)} \quad (5)$$

$$n^{\pi(n)} \leq \prod_{p \leq n} p^{\log_p(n)+1} \leq \prod_{p \leq n} p^{2 \log_p(n)} = \Psi(n)^2 \quad (6)$$

Next: provide lower and upper bounds for Ψ .

Ψ lower bound

We have:

$$\Psi(n) = \prod_{\mathbf{p} \leq n} p^{\log_p(n)} = \prod_{\mathbf{p} \leq n} \prod_{i < \log_p(n)} p \geq B(n)$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Ψ lower bound

We have:

$$\Psi(n) = \prod_{p \leq n} p^{\log_p(n)} = \prod_{p \leq n} \prod_{i < \log_p(n)} p \geq B(n)$$

Hence, the lower bound for B gives a lower bound for Ψ :

$$2^{2n}/2n \leq B(2n) \leq \Psi(2n) \quad (7)$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Ψ lower bound

We have:

$$\Psi(n) = \prod_{p \leq n} p^{\log_p(n)} = \prod_{p \leq n} \prod_{i < \log_p(n)} p \geq B(n)$$

Hence, the lower bound for B gives a lower bound for Ψ :

$$2^{2n}/2n \leq B(2n) \leq \Psi(2n) \quad (7)$$

In particular, since Ψ is **monotonic**

$$2^{n/2} \leq \Psi(n) \quad (8)$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Ψ upper bound (1)

For the **upper bound**, let us first observe that

$$\Psi(2n) = \left(\prod_{p \leq 2n} \prod_{i < \log_p(2n)} p^{j(n,p,i)} \right) \Psi(n) \quad (9)$$

where $j(n, p, i)$ is 1 if $n < p^{i+1}$ and 0 otherwise.

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Ψ upper bound (1)

For the **upper bound**, let us first observe that

$$\Psi(2n) = \left(\prod_{p \leq 2n} \prod_{i < \log_p(2n)} p^{j(n,p,i)} \right) \Psi(n) \quad (9)$$

where $j(n, p, i)$ is 1 if $n < p^{i+1}$ and 0 otherwise.

Indeed

$$\begin{aligned} \Psi(2n) &= \prod_{p \leq 2n} \prod_{i < \log_p(2n)} p \\ &= \left(\prod_{p \leq 2n} \prod_{i < \log_p(2n)} p^{j(n,p,i)} \right) \left(\prod_{p \leq 2n} \prod_{i < \log_p(2n)} p^{1-j(n,p,i)} \right) \\ &= \left(\prod_{p \leq 2n} \prod_{i < \log_p(2n)} p^{j(n,p,i)} \right) \Psi(n) \end{aligned}$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Ψ upper bound (2)

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Then observe that

$$\prod_{\mathbf{p} \leq 2n} \prod_{i < \log_p(2n)} p^{j(n,p,i)} \leq B(2n) = \prod_{\mathbf{p} \leq 2n} \prod_{i < \log_p(2n)} p^{(2n/p^{i+1} \bmod 2)}$$

since if $n < p^{i+1}$ then $2n/p^{i+1} \bmod 2 = 1$.

Ψ upper bound (2)

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Then observe that

$$\prod_{\mathbf{p} \leq 2n} \prod_{i < \log_p(2n)} p^{j(n,p,i)} \leq B(2n) = \prod_{\mathbf{p} \leq 2n} \prod_{i < \log_p(2n)} p^{(2n/p^{i+1} \bmod 2)}$$

since if $n < p^{i+1}$ then $2n/p^{i+1} \bmod 2 = 1$.

Hence:

$$\Psi(2n) \leq B(2n)\Psi(n) \tag{10}$$

Ψ upper bound (2)

Using B upper estimates, we have, for any n

$$\Psi(2n) \leq 2^{2n-1} \Psi(n) \quad (11)$$

and for $4 < n$

$$\Psi(2n) \leq 2^{2n-2} \Psi(n) \quad (12)$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Ψ upper bound (2)

Using B upper estimates, we have, for any n

$$\Psi(2n) \leq 2^{2n-1} \Psi(n) \quad (11)$$

and for $4 < n$

$$\Psi(2n) \leq 2^{2n-2} \Psi(n) \quad (12)$$

We may now use **inductively** these estimates to prove

$$\Psi(n) \leq 2^{2n-3} \quad (13)$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Summary

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

In conclusion,

$$\frac{2^{2n}}{2n} \leq B(2n) \leq 2^{2n-1}$$

$$\frac{2^n}{n} \leq \psi(n) \leq 2^{2n-3}$$

$$2^{n/2} \leq \frac{2^n}{n} \leq \psi(n) \leq n^{\pi(n)} \leq \psi(n)^2 \leq 2^{4n-6} \leq 2^{4n} \quad (14)$$

Outline

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebishev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

1 Introduction

2 The factorization of $n!$

- Upper and lower bounds for B

3 Chebishev's Ψ function

4 Bertrand's postulate

- Erdős approach (1932)
- Automatic check

Bertrand's postulate

Chebyshev's approach was similar but more precise:

$$(c_1 + o(1)) \frac{n}{\log n} \leq \pi(n) \leq (c_2 + o(1)) \frac{n}{\log n} \quad (n \rightarrow \infty)$$

with

$$c_1 = \log(2^{1/2} 3^{1/3} 5^{1/5} 30^{-1/30}) \approx 0.92129$$

$$c_2 = 6/5 c_1 \approx 1.10555$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Bertrand's postulate

Chebyshev's approach was similar but more precise:

$$(c_1 + o(1)) \frac{n}{\log n} \leq \pi(n) \leq (c_2 + o(1)) \frac{n}{\log n} \quad (n \rightarrow \infty)$$

with

$$c_1 = \log(2^{1/2} 3^{1/3} 5^{1/5} 30^{-1/30}) \approx 0.92129$$

$$c_2 = 6/5 c_1 \approx 1.10555$$

In particular, since $c_2 < 2c_1$

$$\pi(2n) > \pi(n)$$

for all large n (**Bertrand's postulate**).

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Erdős approach (1932)

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Let

$$k(n, p) = \sum_{i < \log_p n} (n/p^{i+1} \bmod 2)$$

Then,

$$B(n) = \prod_{p \leq n} p^{k(n, p)}$$

We now split this product in two parts B_1 and B_2 , according to $k(n, p) = 1$ or $k(n, p) > 1$.

case $k(n, p) = 1$

Suppose that Bertrand postulate is **false**: there is no prime between n and $2n$.

Moreover, if $\frac{2n}{3} < p \leq n$, then

$$k(2n, p) = \sum_{i < \log_p n} (n/p^{i+1} \bmod 2) = 0$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

case $k(n, p) = 1$

Suppose that Bertrand postulate is **false**: there is no prime between n and $2n$.

Moreover, if $\frac{2n}{3} < p \leq n$, then

$$k(2n, p) = \sum_{i < \log_p n} (n/p^{i+1} \bmod 2) = 0$$

Indeed

- $2n/p = 2$
- for $i > 1$, and $n \geq 6$, $2n/p^i = 0$, since

$$2n \leq \left(\frac{2n}{3}\right)^2 \leq p^i$$

case $k(n, p) = 1$

Summing up, assuming Bertrand's postulate is **false**,

$$\begin{aligned} B_1(2n) &= \prod_{\substack{p \leq 2n \\ k(2n, p) = 1}} p \\ &= \prod_{p \leq 2n/3} p \\ &\leq \Psi(2n/3) \\ &\leq 2^{2 \cdot (2n/3)} \end{aligned}$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's Ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

case $k(n, p) > 1$

$$k(n, p) = \sum_{i < \log_p n} (n/p^{i+1} \bmod 2) \leq \log_p n$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

case $k(n, p) > 1$

$$k(n, p) = \sum_{i < \log_p n} (n/p^{i+1} \bmod 2) \leq \log_p n$$

$$k(2n, p) \geq 2 \Rightarrow \log_p 2n \geq 2 \Rightarrow p \leq \sqrt{2n}$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

case $k(n, p) > 1$

$$k(n, p) = \sum_{i < \log_p n} (n/p^{i+1} \bmod 2) \leq \log_p n$$

$$k(2n, p) \geq 2 \Rightarrow \log_p 2n \geq 2 \Rightarrow p \leq \sqrt{2n}$$

$$\begin{aligned} B_2(2n) &= \prod_{\substack{\mathbf{p} \leq 2n \\ 2 \leq k(2n, p)}} p^{k(2n, p)} \\ &\leq \prod_{\mathbf{p} \leq \sqrt{2n}} 2n \\ &= (2n)^{\pi(\sqrt{2n})} \\ &\leq (2n)^{\sqrt{2n}/2-1} \end{aligned}$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

A contradictory upper bound

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Putting everything together, assuming Bertrand's postulate is **false**, we would have, for any $n \geq 2^7$

$$2^{2n} \leq 2nB(2n) = 2nB_1(2n)B_2(2n) \leq 2^{2(2n/3)}(2n)^{\sqrt{2n}/2}$$

that, by algebraic manipulations and taking logarithms, gives

$$\frac{2n}{3} \leq \frac{\sqrt{2n}}{2}(\log 2n + 1)$$

Make the contradiction explicit

Introduction

The
factorization of
 $n!$

Upper and lower
bounds for B

Chebyshev's ψ
function

Bertrand's
postulate

**Erdős approach
(1932)**

Automatic check

Make the contradiction explicit

- **find** an integer m such that for all values larger than m the equation

$$\frac{2n}{3} \leq \frac{\sqrt{2n}}{2} (\log 2n + 1)$$

is false

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Make the contradiction explicit

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

- **find** an integer m such that for all values larger than m the equation

$$\frac{2n}{3} \leq \frac{\sqrt{2n}}{2} (\log 2n + 1)$$

is false

- only use arithmetical means

Make the contradiction explicit

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

- **find** an integer m such that for all values larger than m the equation

$$\frac{2n}{3} \leq \frac{\sqrt{2n}}{2} (\log 2n + 1)$$

is false

- only use arithmetical means
- m must be **sufficiently small** to allow to check the remaining cases automatically in a feasible time.

Reduce

$$\frac{\sqrt{2n}}{2}(\log 2n + 1) < \frac{2n}{3}$$

to

$$(*) \quad \frac{\sqrt{2n}}{2}(\log 2n + 1) \leq \frac{2n}{4}$$

using the fact that

$$\frac{n}{m+1} < \frac{n}{m}$$

for any $n \geq m^2$ (in our case, $n \geq 8$).

Then transform (*) to

$$2(\log n + 2)^2 \leq n$$

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Use the fact that for any $a > 0$ and any $n \geq 4a$

$$2^a n^2 \leq 2^n$$

to get, for any $n \geq 2^8$

$$\begin{aligned} 2(\log n + 2)^2 &\leq 4(\log n)^2 \\ &= 2^2(\log n)^2 \\ &\leq 2^{\log n} \\ &= n \end{aligned}$$

Automatic check

To complete the proof, we have to check that Bertrand's postulate is true for all integers less than 2^8 . To this aim, we

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Automatic check

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

To complete the proof, we have to check that Bertrand's postulate is true for all integers less than 2^8 . To this aim, we

- 1 generate the list of all primes up to the first prime larger than 2^8 (in reverse order)

Automatic check

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

To complete the proof, we have to check that Bertrand's postulate is true for all integers less than 2^8 . To this aim, we

- 1 generate the list of all primes up to the first prime larger than 2^8 (in reverse order)
- 2 check that for any pair p_i, p_{i+1} of consecutive primes in such list, $p_i < 2p_{i+1}$

Automatic check

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

To complete the proof, we have to check that Bertrand's postulate is true for all integers less than 2^8 . To this aim, we

- 1 generate the list of all primes up to the first prime larger than 2^8 (in reverse order)
- 2 check that for any pair p_i, p_{i+1} of consecutive primes in such list, $p_i < 2p_{i+1}$

Both the generation of the list and its check are performed **automatically** (takes few seconds).

Using **reflection**, prove that our algorithm for generating primes is correct and complete, and that the previous check is equivalent to Bertrand's postulate, on the given interval.

Eratosthene's sieve

To generate primes we use the following sieve of Eratosthene

```
let rec sieve_aux l1 l2 t on t :=  
  match t with  
  [ O  $\Rightarrow$  l1 (* this case is vacuous *)  
  | S t1  $\Rightarrow$  match l2 with  
    [ nil  $\Rightarrow$  l1  
    | cons n tl  $\Rightarrow$   
      sieve_aux (n::l1)  
        ( filter nat tl  
          ( $\lambda$  x.notb (x | n))) t1 ]].
```

definition sieve m := sieve_aux [] (list_n m) m.

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebichev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Checking Bertrand's condition

To check that each element of the list is less than twice its successor:

```
let rec check_list l \def
  match l with
  [ nil => true
  | cons hd tl =>
    match tl with
    [ nil => hd = 2
    | cons hd1 tl1 => hd1 < hd ^ hd ≤ 2*hd1 ^ check_list tl
    ]
  ]
.
```

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Resources - library integrations

Prerequisites and integrations to the library

- logarithms, square root (632 lines)
- inequalities involving integer division (339 lines)
- magnitude of functions (255 lines)
- decomposition of a number n as a product of its primes (250 lines)
- binomial coefficients (260 lines)
- properties of the factorial function, lower and upper bounds of the binomial coefficient $\binom{2n}{n}$ (303 lines)
- integrations to the library for \sum and \prod (148 lines)
- operations over lists (224 lines)

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Resources - other

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Selection from the garbage collector

- Chebyshev's Θ function (500 lines)
- Abel summation (209 lines)
- Upper and lower bounds for Euler's e constant (1154 lines)

Resources - other

	prereq.	chebys.	bertrand	check	other	total
ln.	2411	2073	743	526	1863	7616
h.	54	51	21	16	48	190

- 1.5 min per script line
- in Hardy's book [6], the proof of Bertrand's postulate takes 42 lines, while Chebyshev's theorem takes precisely three pages (90 lines):
De Bruijn factor ≈ 20 -25
1.5 hours/source mathematical line.

Introduction

The factorization of $n!$

Upper and lower bounds for B









Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check

Bibliography

-  T.M.Apostol. Introduction to Analytic Number Theory. Springer Verlag, 1976.
-  A.Asperti, C.Armentano. A Page In Number Theory. Journal of Formalized Reasoning. Vol.1, 2008.
-  J.Avigad, K.Donnely, D.Gray, P.Raff. A formally verified proof of the prime number theorem. ACM Transactions on Computational Logic, 9(1), 2007. To appear in the ACM Transactions on Computational Logic.
-  P.Erdős. Beweis eines Satzes von Tschebyschef. In Acta Scientifica Mathematica, volume 5, pages 194-198, 1932.
-  G.J.O.Jameson. The Prime Number Theorem. London Mathematical Society Student Texts 53, Cambridge University Press, 2003.
-  G.H.Hardy, E.M.Wright. An introduction to the theory of numbers, Oxford University Press, 1938. Fourth edition 1975.
-  G.Tenenbaum, M.Mendes France. The Prime Numbers and Their Distribution. Student Mathematical Library, American Mathematical Society,2000.
-  L.Théry. Proving Pearl: Knuth's Algorithm for Prime Numbers. Proceedings of TPHOLs'03, LNCS 2758, pp.304-318, 2003.

Introduction

The factorization of $n!$

Upper and lower bounds for B

Chebyshev's ψ function

Bertrand's postulate

Erdős approach (1932)

Automatic check