About the Formalization of Some Results by Chebyshev in Number Theory

Andrea Asperti[*] and Wilmer Ricciotti

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

Abstract. We discuss the formalization, in the Matita Interactive Theorem Prover, of a famous result by Chebyshev concerning the distribution of prime numbers, essentially subsuming, as a corollary, Bertrand's postulate. Even if Chebyshev's result has been later superseded by the stronger prime number theorem, his machinery, and in particular the two functions ψ and θ still play a central role in the modern development of number theory. Differently from other recent formalizations of other results in number theory, our proof is entirely arithmetical. It makes use of most part of the machinery of elementary arithmetics, and in particular of properties of prime numbers, factorization, products and summations, providing a natural benchmark for assessing the actual development of the arithmetical knowledge base.

1 Introduction

Let $\pi(n)$ denote the number of primes not exceeding n. The prime number theorem, proved by Hadamard and la Vallé Poussin in 1896 states that $\pi(n)$ is asymptotically equal to $n/\log(n)$, that is the ratio between the two functions tends to 1 when n tends to infinity. In this paper we address a weaker result, due to Chebyshev around 1850, stating that the *order of magnitude* of $\pi(n)$ is $n/\log n$, meaning that we can find two constants c_1 and c_2 such that, for any n

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

Even if Chebyshev's theorem is sensibly simpler than the prime number theorem, already formalized by Avigad et al. in Isabelle [3] and by Harrison in HOL Light [5], it is far form trivial (in Hardy and Wright's famous textbook [7], it takes pages 340-344 of chapter 22). In particular, our point was to give a fully arithmetical (and constructive) proof of this theorem. Even if Selberg's proof of the prime number theorem is "elementary", meaning that it requires no sophisticated tools of analysis except for the properties of logarithms, a fully arithmetical proof of this results looks problematics, considering that the statement involves *in an essential way* the Naperian logarithm. On the other side, the logarithm

[*] On leave at INRIA-Microsoft Research Center, Orsay, France.

S. Berardi, F. Damiani, and U. de'Liguoro (Eds.): TYPES 2008, LNCS 5497, pp. 19–31, 2009.

in Chebyshev's theorem can be in any base, and can be also essentially avoided (at least from the statement), asserting the existence of two constants c_1 and c_2 such that, for any n

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

that is what we actually proved.

As an important byproduct, we also give the first *purely arithmetical* formal proof of Bertrand's postulate, stating that for any n, there exists a prime number between n and $2n$[1].

The paper aims at providing a discussion of the subject in a form suitable to its formalization, without actually entering in implementation details (hence avoiding a direct discussion of the Matita system, but for a few descriptive examples).

2 Primes and the Factorial Function

In the rest of the paper, all functions are defined on natural numbers. In particular, n/m denotes the integer part of the division between n and m, and $\log_a n$ denotes the maximum i such $a^i \leq n$.

Chebyshev's approach to the study of the distribution of prime numbers consists in exploiting the decomposition of the number $n!$ as a product of prime numbers. The idea is that the numbers $1, 2, \ldots, n$ include just $\frac{n}{p}$ multiples of p, $\frac{n}{p^2}$ multiples of p^2, an so on. Hence (the variable bound by the product is written in bold)

$$n! = \prod_{\mathbf{p} \leq n} \prod_{\mathbf{i} < \log_p n} p^{n/p^{i+1}} \tag{1}$$

The previous one is a good example of a typical mathematical argumentation (see e.g. [7], p. 342). Looking more carefully, you see that it provides you (almost) no information, since it is essentially a mere rephrasing of the statement: it is a gentle invitation to work it out by yourself, just a bit less unsympathetic than a brutal "trivial".

The formal proof requires a bit more work. The starting point is that every integer n may be uniquely decomposed as the product of all its prime factors. Le us write $ord_p(n)$ for the multiplicity of p in n; then

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

for p prime. At the time we started this work, the mathematical library of Matita already contained the proof of the Fundamental Theorem of Arithmetic, namely the existence and uniqueness of the decomposition in prime factors. This was

[1] Providing a good upper bound to the search for the next prime, in systems based on logics like the Calculus of Inductive Constructions, is essential to define a reasonably efficient enumeration function for all primes.

proved by giving a factorization function returning for each natural number n a list of multiplicities of its prime factors (for a given factorization strategy), a function computing the products of the elements in the list, and proving that they are inverse of each other. However, passing from this result to the formulation of equation 2 is not so evident. Since, on the other hand, all the needed machinery was already in the library, we opted for a direct proof. The idea is to work by induction on the upper bound of the product. However, we cannot directly work on n, since this must be the *constant* argument of $ord_p(n)$. So have to rephrase the statement in the form

$$\forall m > c(n), n = \prod_{\mathbf{p} \leq m} p^{ord_p(n)}$$

Where $c(n)$ is a suitable function of n. The naive idea to take $c(n) = n$ does not work: in fact, in order to ensure that the induction works properly, we must take a *minimum* bound, that in this case is the largest prime factor of n. This is the actual statement we proved:

```
theorem lt_max_to_pi_p_primeb:
\forall q,m.
 O < m \to
  max m (\lambda i.primeb i \land divides_b i m) < q \to
   m = pi_p q (\lambda i.primeb i \land divides_b i m)
        (\lambda p.exp p (ord m p)).
```

From the previous result we obtain equation 2 as a simple corollary. So,

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

In, particular, for $2n$ we have:

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

But

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

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

$$\frac{n}{p^{i+1}} = 0$$

Hence, if we define

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

equation (3) becomes

$$(2n)! = n!^2 B(2n) \tag{4}$$

$B(2n)$ is thus the binomial coefficient $\binom{2n}{n}$.

2.1 Upper and Lower Bounds for B

For all n, $(2n)! \leq 2^{2n-1} n!^2$. For technical reasons, we need however a slightly stronger result, namely,

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

that holds for any n larger than 4. The proof is by induction.

The base case amounts to check that $10! \leq 2^8 5!^2$, which can be proved by a mere computation (after some simplification).

In the inductive case

$$\begin{aligned}(2 \cdot (n+1))! &= (2n+2)(2n+1)(2n)! \\ &\leq (2n+2)(2n+1)2^{2n-2} n!^2 \\ &\leq (2n+2)(2n+2)2^{2n-2} n!^2 \\ &= 2^{2n}(n+1)!^2\end{aligned}$$

So, by equation (4), we conclude that, for any n

$$B(2n) \leq 2^{2n-1} \tag{5}$$

and when n is larger than 4,

$$B(2n) \leq 2^{2n-2} \tag{6}$$

Similarly, we prove that, for any $n > 0$,

$$2^{2n} n!^2 \leq 2n(2n)!$$

The proof is by induction on n. For $n = 1$ both sides reduce to 4. For $n > 1$,

$$\begin{aligned} 2^{2n+2}(n+1)!^2 &= 4(n+1)^2 2^{2n} n! \\ &= 4(n+1)^2 2n(2n)! \\ &= 4(n+1)(n+1)2n(2n)! \\ &\leq 4(n+1)(n+1)(2n+1)(2n)! \\ &= 2(n+1)(2n+2)(2n+1)(2n)! \\ &= 2(n+1)(2n+2)! \end{aligned}$$

By equation (4) we conclude that

$$2^{2n} \leq 2nB(2n) \tag{7}$$

and since for any n, $2n \leq 2^n$,

$$2^n \leq B(2n) \tag{8}$$

3 Chebyshev's Ψ Function

Let us now consider the following function

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

where the product is over all *primes* less or equal to n. Chebyshev ψ function is the naperian logarithm of Ψ, but as we mentioned in the introduction, we try to avoid the use of logarithms as far as possible. The relation between Ψ and π should be clear:

$$\Psi(n) = \prod_{\mathbf{p} \leq n} p^{\log_p n} \leq \prod_{\mathbf{p} \leq n} n = n^{\pi(n)} \tag{9}$$

Since moreover, $n < a^{\log_a n + 1}$ we also have $n < a^{2 \log_a n}$, so that, easily,

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

Let us now rewrite $\Psi(n)$ in the following equivalent form:

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

It is then clear that, for any n,

$$B(n) \leq \Psi'(n) = \Psi(n)$$

Hence, the lower bound for B immediately gives a lower bound for Ψ, namely

$$2^n \leq 2^{2n}/2n \leq \Psi(2n) \tag{11}$$

For the upper bound, let us first observe that

$$\Psi(2n) = \Psi(n) \prod_{\mathbf{p} \leq 2n} \prod_{\mathbf{i} < \log_p 2n} p^{j(n,p,i)} \tag{12}$$

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

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

Then observe that

$$\prod_{\mathbf{p} \leq 2n} \prod_{\mathbf{i} < \log_p 2n} p^{j(n,p,i)} \leq B(2n) = \prod_{\mathbf{p} \leq 2n} \prod_{\mathbf{i} < \log_p 2n} p^{(2n/p^{i+1} \mod 2)} \tag{13}$$

since if $n < p^{i+1}$ then $2n/p^{i+1} \mod 2 = 1$. So we may conclude that

$$\Psi(2n) \leq B(2n)\Psi(n) \tag{14}$$

and in particular, for any n

$$\Psi(2n) \leq 2^{2n-1}\Psi(n) \tag{15}$$

and for $4 < n$

$$\Psi(2n) \leq 2^{2n-2}\Psi(n) \tag{16}$$

We may now use inductively these estimates to prove

$$\Psi(n) \leq 2^{2n-3} \tag{17}$$

For the proof, we need the monotonicity of Ψ, that is easily proved:

$$\Psi(n) = \prod_{\mathbf{p} \leq n} p^{\log_p n} \leq \prod_{\mathbf{p} \leq n} p^{\log_p (n+1)} \leq \prod_{\mathbf{p} \leq n+1} p^{\log_p (n+1)} = \Psi(n+1) \tag{18}$$

Then we check that the property holds for any $n \leq 8$, which can be done by direct computation. If n is larger than 8 we distinguish two cases, according to n is even or odd. We only consider the case $n = 2m+1$ that is the most interesting one. Observe first that $8 < 2m+1$ implies $4 < m$. Then we have:

$$\begin{aligned} \Psi(n) &= \Psi(2m+1) \\ &\leq \Psi(2m+2) \\ &\leq 2^{2m}\Psi(m+1) \\ &\leq 2^{2m}2^{2(m+1)-3} \\ &\leq 2^{2(2m+1)-3} \end{aligned}$$

In conclusion, we have

$$2^{n/2} \leq \Psi(n) \leq n^{\pi(n)} \leq \Psi(n)^2 \leq 2^{4n-6} \leq 2^{4n} \tag{19}$$

4 Bertrand's Postulate

Our approach to Chebyshev's theorem, as most modern presentations of the subject, essentially follows Chebyshev's original idea, but in a rudimentary form which provides a result that is numerically less precise, though of a similar nature. In particular, Chebyshev was able to prove the asymptotic estimates

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

with

$$\begin{aligned} c_1 &= \log(2^{1/2}3^{1/3}5^{1/5}30^{-1/30}) \approx 0.92129 \\ c_2 &= 6/5c_1 \approx 1.10555 \end{aligned}$$

In particular, since $c_2 < 2c_1$, this implies that

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

for all large n. Actually, by direct computation, Chebyshev proved that the inequality remains true for all n, confirming a famous conjecture known as *Bertrand's postulate.*

With our rough estimates, we could only prove the existence of a prime number between n and $5n$, for n sufficiently large. There exists however an alternative approach to the proof of Bertrand's postulate due to Erdös [4] (see also [7], p. 344) that is well suited to a formal encoding in arithmetics[2].
Let

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

Then, B can also be written as

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

We now split this product in two parts B_1 and B_2, according to $k(n,p) = 1$ or $k(n,p) > 1$. Suppose that Bertrand postulate is $false$, hence there is no prime between n and $2n$. Moreover, if $\frac{2n}{3} < p \leq n$, then $2n/p = 2$ and for $i > 1$ and $n \geq 6$ $2n/p^i = 0$ since

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

[2] Erdös' argument was already exploited by Théry in his proof of Bertrand postulate [11]; however he failed to provide a fully arithmetical proof, being forced to make use of the (classical, axiomatic) library of Coq reals to solve the remaining inequalities. Similarly, Riccardi's formalization of Bertrand's postulate in Mizar [8] makes an essential use of real numbers.

so $k(2n,p)=0$. Summing up, under the assumption that Bertrand postulate is *false*,

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

On the other side, note that $k(n,p) \leq \log_p n$, so if $k(2n,p) \geq 2$ we also have $\log_p 2n \geq 2$ that implies $p \leq \sqrt{2n}$. So

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

For $n \geq 15$, $\pi(n) \leq n/2-1$. Hence, for any $n \geq 2^7 > 15^2$, we have

$$B_2(2n) \leq (2n)^{\sqrt{2n}/2-1}$$

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

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

Observe that

$$2^{2n} = 2^{2(2n/3)}2^{2n/3}$$

so, by cancellation,

$$2^{2n/3} \leq (2n)^{\sqrt{2n}/2}$$

and taking logarithms

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

We want to find, *by arithmetical means*, an integer m such that for all values larger than m the previous equation is false; moreover, the integer m must be sufficiently small to allow to check the remaining cases automatically in a feasible time.

We must prove

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

The strict inequality is the first source of trouble, so we prove instead

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

using the fact that

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

for any $n \geq m^2$ (in our case, $n \geq 8$). By means of simple manipulations, it is easy to transform the last equation in the following simpler form

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

or equivalently

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

We now use the fact that for any $a > 0$ and any $n \geq 4a$

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

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

$$2(\log n + 2)^2 \leq 4(\log n)^2 = 2^2(\log n)^2 \leq 2^{\log n} \leq n$$

4.1 Automatic Check

To complete the proof, we have still to check that Bertrand's postulate remains true for all integers less then 2^8. This is very simple in principle: it is sufficient to

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 can be performed automatically. All we have to do is to 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.

Since before this formalization, Matita has contained in its library the machinery necessary to perform this check – particularly a function `primeb` capable of deciding whether its argument is a prime number or not. `primeb` is implemented in the trivial way: it computes the smallest factor of its argument n by repeatedly dividing it by any $m \leq n$, and finally checks whether it equals n or not. The proof of correctness is, of course, straightforward; however, this comes at the cost of an inefficient algorithm, whose use is practical only for small values of n.

As it is often the case, to get better performance we must resort to a different algorithm, whose proof of correctness is less trivial. The sieve of Eratosthenes came as a good candidate, since it directly computes the list of the first primes up to a given number, which is precisely what we need. Furthermore, it has a simple implementation and an elementary, though a bit involved, proof of correctness, which is also interesting in itself as a small case of software verification. This is the actual code of the sieve, written in the Matita language:

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

definition sieve : nat \to list nat \def
  \lambda m.sieve_aux [] (list_n m) m.
```

The function sieve_aux takes in input a list of primes (initially empty), a list of integers yet to sieve (initially comprising all natural numbers between 2 and a given number m), and an integer that is supposed to be larger than the length of the second list (initially m). This last parameter is used as recursive parameter to ensure termination. The algorithm simply takes the first element of the second list, adds it to the first list, and removes from the second list all its multiples.

Here is the function checking that each element of the list is less than twice its successor (we also check that the last element is 2):

```
let rec check_list l \def
  match l with
  [ nil \Rightarrow true
  | cons (hd:nat) tl \Rightarrow
    match tl with
     [ nil \Rightarrow eqb hd 2
     | cons hd1 tl1 \Rightarrow
      (leb (S hd1) hd \land leb hd (2*hd1) \land check_list tl)
    ]
  ].
```

In order for these procedures to be useful, some properties must hold. First we need to prove correctness and completeness of sieve, which in turn requires us to understand and prove the recursion invariant of sieve_aux. Informally:

> Given a natural number m and two lists $l1$ and $l2$, such that
> - for any natural number p, p is contained in $l1$ if and only if it is prime and less than any number contained in $l2$
> - for any natural number x, x is contained in $l2$ if and only if $2 \leq x \leq m$ and x isn't multiple of any number contained in $l1$

then, assuming $l1$ and $l2$ are respectively sorted decreasingly and increasingly, and t is less than the length of $l2$, `sieve_aux l1 l2 t` is a sorted list of decreasing numbers and p is contained in `sieve_aux l1 l2 t` if and only if p is prime and less than m.

The invariant is relatively complex, due to the mutual dependency of the properties of the two lists $l1$ and $l2$. A proof may be obtained by induction on t and then by cases on $l2$. In the interesting part, for $t = t' + 1$ and $l2 = h :: l$, the statement is obtained by means of the induction hypothesis. The following lemmata are also needed:

1. p is contained in $h :: l1$ if and only if it is prime, less or equal than m, and less than any number contained in l'
2. x is in l' if and only if it is greater or equal than 2, less or equal than m, and it is not divisible by any number contained in $h :: l1$
3. $\mathit{length}\, l' \leq t'$
4. $h :: l1$ is sorted decreasingly
5. l' is sorted increasingly

where l' is l from which any number divisible by h has been removed, preserving the order, that is `filter nat l (\lambda x.notb (divides_b h x))`.

The tricky lemmata are 1 and 2. For the first one, we proceed by cases:

- if $p = h$, p is contained in $h :: l$ (that is $l2$), therefore it is less than m and it isn't divisible by any number in $l1$; since $h :: l$ is sorted, h is also less than any number contained in l (and, in particular, less than any number in l'); this implies p is also a prime number. The opposite direction of the logical equivalence is trivial.
- if $p \neq h$, the implication from left to right is trivial since, under this hypothesis, if p is contained in $h :: l1$, it must be contained in $l1$: by the hypothesis on $l1$, this implies the thesis. In the opposite direction, we must prove that if p is prime, less than m and less than any number contained in l', then p is contained in $l1$. First, $p < h$, otherwise by the hypothesis on l and the definition of l' we could prove p is contained in l', thus obtaining $p < p$, which is absurd. Furthermore, for any x contained in $h :: l$, $h \leq x$, because $h :: l$ is sorted increasingly by hypothesis. Thus we get, for all x in $h :: l$, $p < x$, which implies by the hypothesis on $l1$ that p is contained in $l1$.

The second lemma is less complicated. In the left-to-right implication, the nontrivial part is to see that, if x is contained in l', then it isn't a multiple of any p contained in $h :: l1$. By cases, if $p = h$, the thesis follows by definition of l'; if p is contained in $l1$, it is sufficient to apply the hypothesis on $l1$. The opposite direction of the implication is obtained combining the hypotheses to show that x must be in $h :: l$. Then, x must be different from h (otherwise, we could prove that x doesn't divide itself). Since x must be in l and h doesn't divide x, x must also be in l'.

Last, we prove that if `checklist l = true`, then for any number p contained in l and greater than 2, there exists some number q contained in l, such that $q < p \leq 2q$. The proof is easy by induction.

Combining the correctness and completeness of the sieve and this last property, we finally get that Bertrand's postulate holds for all integers less than 2^8, just by checking that `check_list (sieve (S (exp 2 8))) = true`, a test which only takes some seconds.

5 Conclusions

In this paper we presented the formalization, in the Matita interactive theorem prover, of some results by Chebyshev about the distribution of prime numbers. Even if Chebyshev's main result has been later superseded by the stronger prime number theorem, his machinery, and in particular the two functions ψ and θ still play a central role in the modern development of number theory.

As also testified by our own development, Matita is a mature system that already permits the formalization of proofs of not trivial complexity (see . for another recent formalization effort). Although the Matita arithmetical library was already well developed at the time we started the work (see [2]), several integrations were required, concerning the following subjects:

- 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 (303 lines)
- integrations to the library for $\sum$ and $\prod$ (148 lines)
- operations over lists (224 lines)

Apart from these prerequisites, the proofs of Chebyshev's theorem and Bertrand's conjecture take respectively 2073 and 2389 lines (of which 1863 just devoted to the validity check of the conjecture for integers less then 2^8). A good amount of work was also spent in the investigation of related fields (Abel summations, properties of the Θ function, upper and lower bounds for Euler's e constant) that at the end have not been used in the main proof, but still have an interest in themselves. The following table summarizes the dimension of the development, and the total effort in time:

	prereq.	**chebys.**	**Bertrand**	**check**	**other**	**total**
lines	2411	2073	743	526	1863	7616
hours	54	51	21	16	48	190

In Hardy's book [7], the proof of Bertrand's postulate takes 42 lines, while Chebyshev's theorem takes precisely three pages (90 lines): this gives a de Bruijn factor of 20-25, that is in line with other developments in related subjects (see [3,2]). The most interesting datum is however the average time required to formalize a line of mathematical text, that in our case is about 1.5 hours (in [2], on a different arithmetical subject, we gave an estimation of 2 hours per line). The impressive cost of the formalization is the main obstacle towards a larger diffusion of automatic provers in the mathematical community, and all the research effort in the area of formalized reasoning is finally aimed to reduce this cost. Computing this value on large formalizations is an important an effective way to measure the state of the art and to testify its advancement.

References

1. Apostol, T.M.: Introduction to Analytic Number Theory. Springer, Heidelberg (1976)
2. Asperti, A., Armentano, C.: A Page In Number Theory. Journal of Formalized Reasoning 1 (2008) (to appear)
3. Avigad, J., Donnelly, K., Gray, D., Raff, P.: 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)
4. Erdös, P.: Beweis eines Satzes von Tschebyschef. Acta Scientifica Mathematica 5, 194–198 (1932)
5. Harrison, J.: Formalizing an analytic proof of the Prime Number Theorem (extended abstract). In: Participant's proceedings of TTVSI Festschrift in honour of Mike Gordon's 60th birthday (2008)
6. Jameson, G.J.O.: The Prime Number Theorem. London Mathematical Society Student Texts, vol. 53. Cambridge University Press, Cambridge (2003)
7. Hardy, G.H., Wright, E.M.: An introduction to the theory of numbers. Oxford University Press, Oxford (1938) (Fourth edition 1975)
8. Riccardi, M.: Pocklington's Theorem and Bertrand's Postulate. Formalized Mathematics 14(2), 47–52 (2006)
9. Sacerdoti Coen, C., Tassi, E.: A constructive and formal proof of Lebesgues Dominated Convergence Theorem in the interactive theorem prover Matita. Journal of Formalized Reasoning 1(1), 51–89 (2008)
10. Tenenbaum, G., Mendès France, M.: The Prime Numbers and Their Distribution. Student Mathematical Library. American Mathematical Society (2000)
11. Théry, L.: Proving Pearl: Knuth's Algorithm for Prime Numbers. In: Basin, D., Wolff, B. (eds.) TPHOLs 2003. LNCS, vol. 2758, pp. 304–318. Springer, Heidelberg (2003)