Formalization of the prime number theorem and Dirichlet's theorem

Mario Carneiro
Pure and Applied Logic program
Carnegie Mellon University, Pittsburgh PA, USA
di.gama@gmail.com

Abstract

We present the formalization of Dirichlet's theorem on the infinitude of primes in arithmetic progressions, and Selberg's elementary proof of the prime number theorem, which asserts that the number $\pi(x)$ of primes less than x is asymptotic to $x/\log x$, within the proof system Metamath.

1 Introduction

Dirichlet's theorem, or the Dirichlet prime number theorem, states that for any $N \in \mathbb{N}$ and $A \in \mathbb{Z}$ such that $\gcd(A, N) = 1$, there are infinitely many primes in the progression $A + kN$, or equivalently there are infinitely many $p_k \equiv A \pmod{N}$. Euler was the first to make progress on this theorem, proving it in the case $A = 1$, and it was shown in full generality by Dirichlet in 1837 [Dir37].

The prime number theorem gives an overall order of growth of the number of primes less than x. Letting $\pi(x)$ denote the number of primes in the interval $[1, x]$ (where x is not necessarily an integer), the prime number theorem asserts that $\pi(x) \sim \frac{x}{\log x}$. This was first conjectured by Legendre in 1797, and was first proven using complex analysis and the zeta function by Jacques Hadamard and Charles Jean de la Vallée-Poussin in 1896. Two "elementary" proofs were later discovered by Selberg and Erdős in 1949 [Sel49, Erd49].

The first formal proof of the prime number theorem was written by Jeremy Avigad et. al. in 2004 [Avi07], in the Isabelle proof language, following Selberg's proof, a landmark result for mathematics formalization. Hadamard and Vallée-Poussin's proof was formalized in HOL Light by John Harrison in 2009 [Har09]. John Harrison also later formalized Dirichlet's theorem in HOL Light, in 2010 [Har10].

Metamath is a formal proof language and computer verification software developed for the purpose of formalizing mathematics in a minimalistic foundational theory [Meg07]. On May 12, 2016 and June 1, 2016 respectively, the author formally verified the following theorems in the Metamath formal system:

Theorem 1 (dirith, Dirichlet's theorem)**.**

$$N \in \mathbb{N} \wedge A \in \mathbb{Z} \wedge \gcd(A, N) = 1 \;\rightarrow\; \{p \in \mathbb{P} \mid N|(p - A)\} \approx \mathbb{N}$$

Theorem 2 (pnt, The prime number theorem)**.**

$$\left(x \in (1, \infty) \mapsto \frac{\pi(x)}{x/\log x}\right) \rightsquigarrow 1$$

The latter expression is Metamath's notation for $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$, restricted to $x > 1$, which is the domain of definition of the function.

These two theorems are interesting formalization targets as they both have simple statements and "deep" proofs, and they are also both members of the "Formalizing 100 theorems" list maintained by Freek Wiedijk [Wie16], which tracks formalizations of 100 of the most famous theorems in mathematics.

Both proofs were written concurrently, over the course of about seven weeks between April 7 and June 1, 2016. This was done mostly because both theorems are in the same general subject (elementary number theory) and required similar techniques (mostly asymptotic approximation of finite sums of reals). The primary informal text used for the proof was Shapiro [Sha83], which devotes a section to Dirichlet's theorem and the whole final chapter to Selberg and Erdős's proof of the prime number theorem.

2 Background

The present work is only a broad overview of the problem and proof method. Interested readers are invited to consult the main theorems pnt and dirith at [Met16], where the exact proof is discussed in detail.

The main arithmetic functions used in the formalization are:

$$\pi(x) = |\{p \in \mathbb{P} \mid p \le x\}| = \sum_{p \le x} 1 \qquad \theta(x) = \sum_{p \le x} \log p$$

$$\Lambda(n) = \begin{cases} \log p & \exists p \in \mathbb{P}, k > 0 : n = p^k \\ 0 & o.w. \end{cases} \qquad \psi(x) = \sum_{n \le x} \Lambda(n)$$

Additionally, the Möbius function $\mu(n)$ is a very useful tool in sum manipulations. It is the unique multiplicative function such that $\mu(1) = 1$ and $\sum_{d|n} \mu(d) = 0$ for $n > 1$. This yields the Möbius inversion formula: if $f(n) = \sum_{d|n} g(d)$, then $g(n) = \sum_{d|n} \mu(d) f(d)$. Since $|\mu(n)| \le 1$, this is a very powerful technique for estimating sums "by inversion".

The proof of Hadamard and Vallée-Poussin relies on some deep theorems in complex analysis, such as Cauchy's theorem, which were not available at the time of this formalization, so instead we targeted the "elementary" proof discovered half a century later semi-independently by Erdős and Selberg. The key step in both proofs is the Selberg symmetry formula:

Theorem 3 (selberg, Selberg symmetry formula)**.**

$$\sum_{n \le x} \Lambda(n) \log n + \sum_{uv \le x} \Lambda(u)\Lambda(v) = 2x \log x + O(x).$$

In Selberg's proof, we leverage this theorem to produce a bound on the residual $R(x) = \psi(x) - x$:

Theorem 4 (pntrlog2bnd)**.**

$$|R(x)| \log^2 x \le 2 \sum_{n \le x} |R(x/n)| \log n + O(x \log x).$$

The goal is to show $\pi(x) \sim \frac{x}{\log x}$, but it is easily shown that $\psi(x) \sim \theta(x) \sim \pi(x) \log x$, so it is equivalent to show that $\psi(x) \sim x$, or $R(x)/x \to 0$, to establish the PNT. Given an eventual bound $|R(x)| \le ax$ and the estimation $\sum_{n \le x} \frac{\log n}{n} = \frac{1}{2} \log^2 x + O(\frac{\log x}{x})$, an application of Theorem 4 reproduces the original estimate $|R(x)| \le ax + o(x)$, but using improved bounds on $R(x)$ on small intervals we can improve the estimate to $|R(x)| \le (a - ca^3)x + o(x)$ for a fixed constant c, which produces a sequence of eventual bounds approaching zero, which proves $R(x)/x \to 0$ as desired.

In Dirichlet's theorem, the focal point is instead the Dirichlet characters $\bmod N$, which are group homomorphisms from $(\mathbb{Z}/N\mathbb{Z})^*$ to $\mathbb{C}^*$, extended to $\mathbb{Z}/N\mathbb{Z}$ with value 0 at non-units, but the general theme of estimation of sums involving $\mu, \Lambda, \log$ and the characters $\chi(n)$ is the same.

3 Formalization

In keeping with Metamath's tradition of minimal complexity, we used a minimum of definition. Asymptotic estimations are reduced to the class $O(1)$ of eventually bounded functions, partial functions $\mathbb{R} \to \mathbb{C}$ such that for some c, A, $x \ge c$ implies $|f(x)| \le A$. An equation such as $f \in O(g)$ is rewritten as $f/g \in O(1)$ (which is correct as long as g is eventually nonzero, which is always true in cases of interest), and similarly $f \in o(g)$ is rewritten as $f/g \rightsquigarrow 0$.

A few finite summation theorems take us a long way; two number-theory specific summation theorems are the following divisor sum commutations:

$$\sum_{k|n}\sum_{d|k} A(k,d) = \sum_{d|n}\sum_{m|n/d} A(dm,d)$$

$$\sum_{n\le x}\sum_{d|n} A(n,d) = \sum_{d\le x}\sum_{m\le n/d} A(dm,d)$$

A small amount of calculus was used in the proof, mostly through the following sum estimation theorem, which for example evaluates $\sum_{n\le x}\frac{\log n}{n} = \frac{1}{2}\log^2 x + O(\frac{\log x}{x})$:

Theorem 5 (dvfsumrlim)**.** *If F is a differentiable function with $F' = f$, and f is a positive decreasing function that converges to zero, then $g(x) = \sum_{n\le x} f(n) - F(x)$ converges to some L and $|g(x) - L| \le f(x)$.*

4 Comparison and Conclusion

Table 1: Comparison of the present proof with [Har10, Avi07]. "?" marks an estimated or unknown value.

	Dirichlet (author)	PNT (author)	Dirichlet [Har10]	PNT [Avi07]
Total time spent	2 weeks	5 weeks	5 days	12 weeks?
Lines of code	3595	5100	1183	19713
Compressed bytes (gzip)	109683	156226	11762	97470
Informal text	10 pp.	37 pp.	192 lines	37 pp.
Informal text (gzip)	5500?	20350?	2524	20350?
de Bruijn factor	19.9?	7.67?	4.66	4.78?
Verification time	0.18 s	0.23 s	450 s	1800 s?

The comparison of parallel proof attempts in different systems is usually confounded by the many other factors, so these statistics should not be given undue credence. According to [Avi07], Avigad's PNT project was a year-long project by four people, with the majority of the work happening during one summer, while this was a solo project over about seven work weeks. Dirichlet's theorem is 10 pages of informal text of [Sha83], and the PNT is 37 pages. Although the number of lines in the current proofs seem competitive, this is lost in the gzipped version, because the stored Metamath proof is already largely compressed, while the Isabelle and HOL scripts are plain text.

The de Bruijn factors for this work had to be estimated because the TeX source for the informal text was not available, but indications suggest that it fares poorly with comparatively large factors 19.9 and 7.67, respectively. However, when reading these statistics it is important to realize that Metamath stores *proofs*, not *proof scripts* like Isabelle and HOL. Every inference in the proof is an axiom or theorem of the system, and no proof searches are conducted by the verifier. This is reflected in the incredibly small verification time, which is normal for Metamath proofs. We do not have exact data on verification time for HOL Light, but it is believed to be on the order of minutes to hours.

These proofs are important milestones for the Metamath project. They demonstrate that even the largest of formalization projects in high level languages can also be conducted in a "full transparency"-style system like Metamath, with entirely worked-out proofs and with all automation offloaded from the verifier to the proof generation.

References

[Dir37] Dirichlet, P. G. L.: Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. Abhand. Ak. Wiss. Berlin **48**, 313–342 (1837)

[Sel49] Selberg, A.: An elementary proof of the prime-number theorem. Ann. of Math. (2), Vol. 50, pp. 305–313; reprinted in Atle Selberg Collected Papers, Springer–Verlag, Berlin Heidelberg New York, 1989 **1**, 379–387 (1949)

[Erd49] Erdős, P.: On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. Proc. Nat. Acad. Scis. U.S.A. **35**, 374–384 (1949)

[Avi07] Avigad, J., Donnelly, K., Gray, D., Raff, P.: A formally verified proof of the prime number theorem. ACM Trans. Comput. Logic **9** (1:2), 1–23 (2007)

[Har09] Harrison, J.: Formalizing an analytic proof of the Prime Number Theorem (dedicated to Mike Gordon on the occasion of his 60th birthday). Journal of Automated Reasoning, 43:243–261 (2009)

[Har10] Harrison, J.: A formalized proof of Dirichlet's theorem on primes in arithmetic progression. Journal of Formalized Reasoning, [S.l.], **2** (1), 63–83 (2010)

[Wie16] Wiedijk, F.: Formalizing 100 Theorems, `http://www.cs.ru.nl/~freek/100/` (accessed 20 May 2016)

[Meg07] Megill, N.: Metamath: *A Computer Language for Pure Mathematics.* Lulu Publishing, Morrisville, North Carolina (2007)

[Sha83] Shapiro, H.: *Introduction to the theory of numbers.* John Wiley & Sons Inc., New York (1983)

[Met16] Metamath Proof Explorer, `http://us.metamath.org/mpegif/mmset.html` (accessed 20 May 2016)