Formalization of the prime number theorem and Dirichlet's theorem

MARIO CARNEIRO

25 JULY 2016

Metamath

- A computer language for representing mathematical proofs
  - The Metamath spec is two pages, one verifier exists in 75 lines of Mathematica
  - Eight independent verifiers exist in eight different languages
  - Two proof assistants (MM-PA and mmj2) with another (smm3) in development
  - (Tomorrow I will talk about the theoretical underpinnings of Metamath)
- A project to formalize modern mathematics from a simple foundation
- Main database is set.mm (ZFC set theory)
  - Over 28000 proofs, 500K lines, 29M file

The prime number theorem

Theorem pnt 19329

Description: The Prime Number Theorem: the number of prime numbers less than x tends asymptotically to x / log(x) as x goes to infinity. (Contributed by Mario Carneiro, 1-Jun-2016.)

Assertion

Ref	Expression
pnt	$\vdash (x \in (1(,)+\infty) \mapsto ((\underline{\pi}\ `x) / (x / (\log\ `x)))) \rightsquigarrow_r 1$

- $\underline{\pi}(x)$ is the Gauss prime π function, the number of primes $\leq x$ (where $x \in \mathbb{R}$)
- $(1(,) + \infty) = (1, \infty)$ is the open interval from 1 to ∞
- $(x \in A \mapsto B(x))$ is the mapping/lambda operation (produces a function on the given domain)
- $F \rightsquigarrow_r a$ means that $\lim_{x \to \infty} F(x) = a$

http://us.metamath.org/mpeuni/pnt.html

The prime number theorem

- First conjectured by Legendre in 1797
- First proof in 1896 by Jacques Hadamard and Charles Jean de la Vallée-Poussin (independently)
  - Uses complex analysis and properties of the Riemann ζ function
- Two “elementary” proofs discovered by Erdős and Selberg (sort of independently) in 1949
- First formal proof by Jeremy Avigad et. al. in 2004 in Isabelle
  - Targets Selberg’s proof
- Later formal proof by John Harrison in 2009 in HOL Light
  - Targets Hadamard / Vallée-Poussin proof
- This proof uses Selberg’s method

Dirichlet's theorem

Theorem dirith 19249

Description: Dirichlet's theorem: there are infinitely many primes in any arithmetic progression coprime to N. Theorem 9.4.1 of [Shapiro], p. 375. See http://metamath-blog.blogspot.com/2016/05/dirichlets-theorem.html for an informal exposition. (Contributed by Mario Carneiro, 12-May-2016.)

Assertion

Ref	Expression
dirith	$\vdash ((N \in \mathbb{N} \wedge A \in \mathbb{Z} \wedge (A \operatorname{gcd} N) = 1) \rightarrow \{p \in \mathbb{P} \mid N \parallel (p - A)\} \approx \mathbb{N})$

Distinct variable groups: A,p N,p

- $(A \operatorname{gcd} B) = \operatorname{gcd}(A, B)$ is the greatest common divisor
- $m \parallel n$ is the divides relation on integers, so $N \parallel (p - A)$ means $p \equiv A \pmod N$
- $S \approx \mathbb{N}$ means S is equinumerous to $\mathbb{N}$, i.e. S is infinite
- $\mathbb{P}$ is the set of prime numbers, $\mathbb{N}$ is the positive integers, $\mathbb{Z}$ is the integers

Dirichlet's theorem

- Partial proof (case $A = 1$) by Euler
- First complete proof by Dirichlet in 1837
- First formal proof by John Harrison in 2010 in HOL Light

Why these two?

- Similar subject, some common theorems
- Same proof style (asymptotic approximation of finite sums)
- Both are Metamath 100 formalization targets (Freek Wiedijk)
  - Currently 58 out of 100 proven

Definitions used

- In keeping with Metamath conventions, very few new definitions were used for these theorems
  - Definitions are only made when they “pay for themselves” in shortening theorem proofs and/or expression sizes
- df-sum: finite sums of complex numbers $\sum_{k \in A} B(k)$
- df-ppi: prime π function, $\underline{\pi}(x) = \#(\mathbb{P} \cap [0, x])$
- df-cht: Chebyshev function $\theta(x) = \sum_{p \leq x} \log p$
- df-vma: von Mangoldt function $\Lambda(p^\alpha) = \log p$
- df-chp: Chebyshev function $\psi(x) = \sum_{n \leq x} \Lambda(n)$
- df-mu: Möbius function $\mu(n) = (-1)^{\#\{p \in \mathbb{P} \mid p \| n\}}$

Definitions used

- In keeping with Metamath conventions, very few new definitions were used for these theorems
  - Definitions are only made when they “pay for themselves” in shortening theorem proofs and/or expression sizes
- df-dchr: Group of Dirichlet characters
- df-o1: Set of eventually bounded functions $f(x) = O(1)$
- df-lo1: Set of eventually upper bounded functions $f(x) \leq O(1)$

Theorem dchrval 19039

Description: Value of the group of Dirichlet characters. (Contributed by Mario Carneiro, 18-Apr-2016.)

Hypotheses

Ref	Expression
dchrval.g	⊢ G = (DChr ‘N)
dchrval.z	⊢ Z = (ℤ/nℤ ‘N)
dchrval.b	⊢ B = (Base ‘Z)
dchrval.u	⊢ U = (Unit ‘Z)
dchrval.n	⊢ (φ → N ∈ ℕ)
dchrval.d	⊢ (φ → D = {x ∈ ((mulGrp ‘Z) MndHom (mulGrp ‘$\mathbb{C}_{\text{fld}}$)) ∣ ((B ∖ U) × {0}) ⊆ x})

Assertion

Ref	Expression
dchrval	⊢ (φ → G = {⟨(Base ‘ndx), D⟩, ⟨($+_g$ ‘ndx), ($\circ_f$ · ↾ (D × D))⟩})

Definitions used

- A trick: Temporary definitions

Theorem selbergr 19283

Description: Selberg's symmetry formula, using the residual of the second Chebyshev function. Equation 10.6.2 of [Shapiro], p. 428. (Contributed by Mario Carneiro, 16-Apr-2016.)

Hypothesis

Ref	Expression
pntrval.r	$\vdash R = (a \in \mathbb{R}^+ \mapsto ((\psi ` a) - a))$

Assertion

Ref	Expression
selbergr	$\vdash (x \in \mathbb{R}^+ \mapsto ((((R ` x) \cdot (\log ` x)) + \Sigma d \in (1...(\llcorner ` x))((\Lambda ` d) \cdot (R ` (x / d)))) / x)) \in O(1)$

Statistics & Comparison

- Dirichlet: 55 theorems, PNT: 83 theorems
- Dirichlet: 8992 proof steps, PNT: 35549 proof steps
- Both proofs were done over a seven week period
- de Bruijn factors 19.9, 7.67 are higher than usual
  - *proofs* not *proof scripts*
- Verification is thousands of times faster
  - New verifier smm3 can verify set.mm in 0.54 s

	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?

Highlights

Theorem pnt 19329

Description: The Prime Number Theorem: the number of prime numbers less than x tends asymptotically to x / log(x) as x goes to infinity. (Contributed by Mario Carneiro, 1-Jun-2016.)

Assertion

Ref	Expression
pnt	$\vdash (x \in (1(,)+\infty) \mapsto ((\underline{\pi}\ `x) / (x / (\log\ `x)))) \rightsquigarrow_r 1$
pnt2	$\vdash (x \in \mathbb{R}^+ \mapsto ((\theta\ `x) / x)) \rightsquigarrow_r 1$
pnt3	$\vdash (x \in \mathbb{R}^+ \mapsto ((\psi\ `x) / x)) \rightsquigarrow_r 1$

Highlights

Theorem selberg 19263

Description: Selberg's symmetry formula. The statement has many forms, and this one is equivalent to the statement that $\Sigma n \leq x, \Lambda(n) \log n + \Sigma m \cdot n \leq x, \Lambda(m)\Lambda(n) = 2x \log x + O(x)$. Equation 10.4.10 of [Shapiro], p. 419. (Contributed by Mario Carneiro, 23-May-2016.)

Assertion

Ref	Expression
selberg	$\vdash (x \in \mathbb{R}^+ \mapsto ((\Sigma n \in (1...(\lfloor \text{‘}x))((\Lambda \text{‘}n) \cdot ((\log \text{‘}n) + (\psi \text{‘}(x / n)))) / x) - (2 \cdot (\log \text{‘}x)))) \in O(1)$
selberg2	$\vdash (x \in \mathbb{R}^+ \mapsto (((((\psi \text{‘}x) \cdot (\log \text{‘}x)) + \Sigma n \in (1...(\lfloor \text{‘}x))((\Lambda \text{‘}n) \cdot (\psi \text{‘}(x / n)))) / x) - (2 \cdot (\log \text{‘}x)))) \in O(1)$
selberg3	$\vdash (x \in (1(,) +\infty) \mapsto (((((\psi \text{‘}x) \cdot (\log \text{‘}x)) + ((2 / (\log \text{‘}x)) \cdot \Sigma n \in (1...(\lfloor \text{‘}x))(((\Lambda \text{‘}n) \cdot (\psi \text{‘}(x / n))) \cdot (\log \text{‘}n)))) / x) - (2 \cdot (\log \text{‘}x)))) \in O(1)$
selberg4	$\vdash (x \in (1(,) +\infty) \mapsto ((((\psi \text{‘}x) \cdot (\log \text{‘}x)) - ((2 / (\log \text{‘}x)) \cdot \Sigma n \in (1...(\lfloor \text{‘}x))((\Lambda \text{‘}n) \cdot \Sigma m \in (1...(\lfloor \text{‘}(x / n)))((\Lambda \text{‘}m) \cdot (\psi \text{‘}((x / n) / m)))))) / x)) \in O(1)$
selbergr	$\vdash (x \in \mathbb{R}^+ \mapsto ((((R \text{‘}x) \cdot (\log \text{‘}x)) + \Sigma d \in (1...(\lfloor \text{‘}x))((\Lambda \text{‘}d) \cdot (R \text{‘}(x / d)))) / x)) \in O(1)$
selberg3r	$\vdash (x \in (1(,) +\infty) \mapsto ((((R \text{‘}x) \cdot (\log \text{‘}x)) + ((2 / (\log \text{‘}x)) \cdot \Sigma n \in (1...(\lfloor \text{‘}x))(((\Lambda \text{‘}n) \cdot (R \text{‘}(x / n))) \cdot (\log \text{‘}n)))) / x)) \in O(1)$
selberg4r	$\vdash (x \in (1(,) +\infty) \mapsto ((((R \text{‘}x) \cdot (\log \text{‘}x)) - ((2 / (\log \text{‘}x)) \cdot \Sigma n \in (1...(\lfloor \text{‘}x))((\Lambda \text{‘}n) \cdot \Sigma m \in (1...(\lfloor \text{‘}(x / n)))((\Lambda \text{‘}m) \cdot (R \text{‘}((x / n) / m)))))) / x)) \in O(1)$
selberg34r	$\vdash (x \in (1(,) +\infty) \mapsto ((((R \text{‘}x) \cdot (\log \text{‘}x)) - (\Sigma n \in (1...(\lfloor \text{‘}x))((R \text{‘}(x / n)) \cdot (\Sigma m \in \{y \in \mathbb{N} \mid y \parallel n\} ((\Lambda \text{‘}m) \cdot (\Lambda \text{‘}(n / m))) - ((\Lambda \text{‘}n) \cdot (\log \text{‘}n)))) / (\log \text{‘}x))) / x)) \in O(1)$

Highlights

Theorem pntlemj 19323

Description: Lemma for pnt 19334. The induction step. Using pntibnd 19313, we find an interval in K↑J...K↑(J + 1) which is sufficiently large and has a much smaller value, R(z) / z ≤ E (instead of our original bound R(z) / z ≤ U). (Contributed by Mario Carneiro, 13-Apr-2016.)

Hypotheses

Ref	Expression
pntlem1.r	⊢ R = (a ∈ ℝ⁺ ↦ ((ψ ‘a) − a))
pntlem1.a	⊢ (φ → A ∈ ℝ⁺)
pntlem1.b	⊢ (φ → B ∈ ℝ⁺)
pntlem1.l	⊢ (φ → L ∈ (0(,)1))
pntlem1.d	⊢ D = (A + 1)
pntlem1.f	⊢ F = ((1 − (1 / D)) · ((L / (;32 · B)) / (D↑2)))
pntlem1.u	⊢ (φ → U ∈ ℝ⁺)
pntlem1.u2	⊢ (φ → U ≤ A)
pntlem1.e	⊢ E = (U / D)
pntlem1.k	⊢ K = (exp ‘(B / E))
pntlem1.y	⊢ (φ → (Y ∈ ℝ⁺ ∧ 1 ≤ Y))
pntlem1.x	⊢ (φ → (X ∈ ℝ⁺ ∧ Y < X))
pntlem1.c	⊢ (φ → C ∈ ℝ⁺)
pntlem1.w	⊢ W = (((Y + (4 / (L · E)))↑2) + (((X · (K↑2))↑4) + (exp ‘(((;32 · B) / ((U − E) · (L · (E↑2)))) · ((U · 3) + C)))))
pntlem1.z	⊢ (φ → Z ∈ (W[,) +∞))
pntlem1.m	⊢ M = ((⌊ ‘((log ‘X) / (log ‘K))) + 1)
pntlem1.n	⊢ N = (⌊ ‘(((log ‘Z) / (log ‘K)) / 2))
pntlem1.U	⊢ (φ → ∀z ∈ (Y[,) +∞)(abs ‘((R ‘z) / z)) ≤ U)
pntlem1.K	⊢ (φ → ∀y ∈ (X(,) +∞)∃z ∈ ℝ⁺ ((y < z ∧ ((1 + (L · E)) · z) < (K · y)) ∧ ∀u ∈ (z[,]((1 + (L · E)) · z))(abs ‘((R ‘u) / u)) ≤ E))
pntlem1.o	⊢ O = (((⌊ ‘(Z / (K↑(J + 1)))) + 1)...(⌊ ‘(Z / (K↑J))))
pntlem1.v	⊢ (φ → V ∈ ℝ⁺)
pntlem1.V	⊢ (φ → (((K↑J) < V ∧ ((1 + (L · E)) · V) < (K · (K↑J))) ∧ ∀u ∈ (V[,]((1 + (L · E)) · V))(abs ‘((R ‘u) / u)) ≤ E))
pntlem1.j	⊢ (φ → J ∈ (M..^N))
pntlem1.i	⊢ I = (((⌊ ‘(Z / ((1 + (L · E)) · V))) + 1)...(⌊ ‘(Z / V)))

Assertion

Ref	Expression
pntlemj	⊢ (φ → ((U − E) · (((L · E) / 8) · (log ‘Z))) ≤ Σn ∈ O (((U / n) − (abs ‘((R ‘(Z / n)) / Z))) · (log ‘n)))

Highlights

Theorem dvfsumrlim 18035

Description: Compare a finite sum to an integral (the integral here is given as a function with a known derivative). The statement here says that if $x \in S \mapsto B$ is a decreasing function with antiderivative A converging to zero, then the difference between $\Sigma k \in (M...(\lfloor ` x))B(k)$ and $A(x) = \int u \in (M[,]x)B(u)\, du$ converges to a constant limit value, with the remainder term bounded by $B(x)$. (Contributed by Mario Carneiro, 18-May-2016.)

Hypotheses

Ref	Expression
dvfsum.s	$\vdash S = (T(,) +\infty)$
dvfsum.z	$\vdash Z = (\mathbb{Z}_{\geq} ` M)$
dvfsum.m	$\vdash (\varphi \to M \in \mathbb{Z})$
dvfsum.d	$\vdash (\varphi \to D \in \mathbb{R})$
dvfsum.md	$\vdash (\varphi \to M \leq (D + 1))$
dvfsum.t	$\vdash (\varphi \to T \in \mathbb{R})$
dvfsum.a	$\vdash ((\varphi \wedge x \in S) \to A \in \mathbb{R})$
dvfsum.b1	$\vdash ((\varphi \wedge x \in S) \to B \in V)$
dvfsum.b2	$\vdash ((\varphi \wedge x \in Z) \to B \in \mathbb{R})$
dvfsum.b3	$\vdash (\varphi \to (\mathbb{R}\mathrm{D}(x \in S \mapsto A)) = (x \in S \mapsto B))$
dvfsum.c	$\vdash (x = k \to B = C)$
dvfsumrlim.l	$\vdash ((\varphi \wedge (x \in S \wedge k \in S) \wedge (D \leq x \wedge x \leq k)) \to C \leq B)$
dvfsumrlim.g	$\vdash G = (x \in S \mapsto (\Sigma k \in (M...(\lfloor ` x))C - A))$
dvfsumrlim.k	$\vdash (\varphi \to (x \in S \mapsto B) \rightsquigarrow_r 0)$

Assertion

Ref	Expression
dvfsumrlim	$\vdash (\varphi \to G \in \mathrm{dom} \rightsquigarrow_r)$

Highlights

Theorem dchrmusum 19239

Description: The sum of the Möbius function multiplied by a non-principal Dirichlet character, divided by n, is bounded. Equation 9.4.16 of [Shapiro], p. 379. (Contributed by Mario Carneiro, 12-May-2016.)

Hypotheses

Ref	Expression
rpvmasum.z	$\vdash Z = (\mathbb{Z}/n\mathbb{Z}\ `N)$
rpvmasum.l	$\vdash L = (\mathbb{Z}\mathrm{RHom}\ `Z)$
rpvmasum.a	$\vdash (\varphi \to N \in \mathbb{N})$
dchrmusum.g	$\vdash G = (\mathrm{DChr}\ `N)$
dchrmusum.d	$\vdash D = (\mathrm{Base}\ `G)$
dchrmusum.1	$\vdash 1 = (0_g\ `G)$
dchrmusum.b	$\vdash (\varphi \to X \in D)$
dchrmusum.n1	$\vdash (\varphi \to X \neq 1)$

Assertion

Ref	Expression
dchrmusum	$\vdash (\varphi \to (x \in \mathbb{R}^+ \mapsto \Sigma n \in (1...(\lfloor\ `x))((X\ `(L\ `n)) \cdot ((\mu\ `n) / n))) \in O(1))$
dchrvmasum	$\vdash (\varphi \to (x \in \mathbb{R}^+ \mapsto \Sigma n \in (1...(\lfloor\ `x))((X\ `(L\ `n)) \cdot ((\Lambda\ `n) / n))) \in O(1))$

Questions