Number-theoretical theorems in LEAN

Ke Yu, Xiang Li

Imperial College London
University of Cambridge

16th February 2023

Outline

Euler's Totient Theorem

The Euler function $\phi(n)$ is defined as the number of natural numbers not exceeding n which are coprime with n, and we have $\phi(1) = 1$.

Theorem (Euler's theorem)

Let $n > 1$ be a natural number, and let $a \in \mathbb{N}$ such that n and a are coprime. Then $a^{\phi(n)} - 1 = 0 \mod n$.

Proof

Proof.

Using the ring $\mathbb{Z}_n$, for an integer i, we denote the coset of i in $\mathbb{Z}_n$ by $[i]$.
Then, the problem changes to proving $[a^{\phi(n)}] = [1]$.
Let $1 \leqslant k_1, k_2, ..., k_{\phi(n)} < n$ be all numbers coprime with n and list the corresponding elements of ring $\mathbb{Z}_n$:$[k_1], [k_2], ..., [k_{\phi(n)}]$. We claim that $[k_1 \cdot a], [k_2 \cdot a], ..., [k_{\phi(n)} \cdot a]$ are the same elements of ring $\mathbb{Z}_n$, possibly in a different order.
Then,

$$\begin{aligned}[k_1] \cdot [k_2] \cdot ... \cdot [k_{\phi(n)}] &= [k_1 \cdot a] \cdot [k_2 \cdot a] \cdot ... \cdot [k_{\phi(n)} \cdot a] \\ &= [k_1] \cdot [k_2] \cdots [k_{\phi(n)}] \cdot [a]^{\phi(n)}.\end{aligned}$$

Thus,

$$[a^{\phi(n)}] = [1].$$

$\square$

Lean Implementation

Let

$$M = [k_1] \cdot [k_2] \cdot ... \cdot [k_{\phi(n)}]$$
$$N = [k_1 \cdot a] \cdot [k_2 \cdot a] \cdot ... \cdot [k_{\phi(n)} \cdot a]$$

1. Proving two big products are equal: $M = N$
2. Taking out $[a]^{\phi(n)}$: $N = M * [a]^{\phi(n)}$
3. Cancelling M: $M = M * [a]^{\phi(n)} \rightarrow [1] = [a]^{\phi(n)}$

Prime Number Theorem

Let $\pi(x) := \sum_{p \leqslant x} 1$ be the prime-counting function, for any $x \in \mathbb{R}$.

Theorem (Prime Number Theorem)

We have the asymptotic formula

$$\pi(x) \sim x/\log x, \tag{1}$$

which is equivalent to the following: for every $c_1 < 1 < c_2$,

$$c_1 \frac{x}{\log x} \leqslant \pi(x) \leqslant c_2 \frac{x}{\log x}.$$

Outline of the proof

We prove this by showing a sequence of properties of the three functions:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \Phi(s) := \sum_{p} \frac{\log p}{p^s} \quad \theta(x) := \sum_{p \leqslant x} \log p \quad s \in \mathbb{C} \quad x \in \mathbb{N}.$$

1. Reduce $\pi(x) \sim x/\log x$ to $\theta(x) \sim x$.
2. Reduce $\theta(x) \sim x$ to showing $I := \int_1^\infty \frac{\theta(x)-x}{x^2} dx$ is convergent.
3. Prove an Analytic Theorem.
4. Apply the Analytic Theorem on I, then suffice to show $\zeta(s) \neq 0$ for $\Re(s) = 1$.

We focused on formalising (1) and (3).

Newman's Proof - First Reduction 1

Reduce the asymptotic formula $\pi(x) \sim x/\log x$ to $\theta(x) \sim x$, where

$$\theta(x) := \sum_{p \leqslant x} \log p.$$

Proof.

For any $0 < \epsilon \leqslant 1/2$ and $x > 1$, we have an upper bound for of $\theta(x)$:

$$\theta(x) = \sum_{p \leqslant x} \log p \leqslant \log x \sum_{p \leqslant x} 1 = \pi(x) \log x. \tag{2}$$

And a lower bound:

$$\theta(x) \geqslant \sum_{x^{1-\epsilon} < p \leqslant x} \log p \geqslant (1-\epsilon) \log x \sum_{x^{1-\epsilon} < p \leqslant x} 1 = (1-\epsilon)(\pi(x) - \pi(x^{1-\epsilon})) \log x \tag{3}$$

Hence,

$$(1-\epsilon)(\pi(x) - \pi(x^{1-\epsilon})) \log x \leqslant \theta(x) \leqslant \pi(x) \log x. \tag{4}$$

First Reduction 2

Proof.

Recall Chebyshev's bounds for $\pi(N)$: for sufficiently large x, there exists constants $a, b > 0$ such that

$$a\frac{x}{\log x} \leqslant \pi(x) \leqslant b\frac{x}{\log x}. \tag{5}$$

Hence for large $x > 1, 0 < \epsilon \leqslant 1/2$,

$$\pi(x^{1-\epsilon}) \leqslant b\frac{x^{1-\epsilon}}{\log x^{1-\epsilon}} \leqslant 2b\frac{x^{1-\epsilon}}{\log x}. \tag{6}$$

$\square$

First Reduction 3

Proof.

And also by Chebyshev's bound,

$$(1-\epsilon)\pi(x) \leqslant \pi(x) - 2b\frac{x^{1-\epsilon}}{\log x} \leqslant \pi(x) - \pi(x^{1-\epsilon}). \tag{7}$$

Thus,

$$(1-\epsilon)^2\pi(x)\log x \leqslant \theta(x) \leqslant \pi(x)\log x, \tag{8}$$

Dividing the above by x, we get $\pi(x) \sim x/\log x$. □

Cauchy's Integral Formula: Why We Need It

Theorem (An Analytic Theorem)

Let $f : [0, \infty) \to \mathbb{R}$ be a bounded locally integrable function. Suppose that $g(z) := \int_0^\infty f(t)e^{-tz}dt$ (for $\{\mathrm{Re}(z) > 0\}$) extends to a holomorphic function over a neighborhood of $\{\mathrm{Re}(z) > 0\}$. Then $\int_0^\infty f(t)dt$ exists (i.e., f is integrable) and equal to $g(0)$.

Cauchy's Integral Formula

What's missing in the mathlib:

- The definition of contour integral for a general contour.
- Cauchy's Integral Theorem for a general curve.

We did the first part, and the second part for a rectangular path, which is sufficient to prove the analytic theorem.

Cauchy's Integral Formula

What's missing in the mathlib:

- The definition of contour integral for a general contour.
- Cauchy's Integral Theorem for a general curve.

We did the first part, and the second part for a rectangular path, which is sufficient to prove the analytic theorem.

Cauchy's Integral Formula: The First Part

Preparation:

- Type conversions
- Affine functions and their derivative (deriv.scomp)
- Operations of path

Cauchy's Integral Formula: The First Part

Definition (Contour Integral)

$$\int_L f := \int_0^1 L'(t) \cdot f(L(t))dt$$

Cauchy's Integral Formula: The First Part

The "hardest" part: prove

$$\int_L (f+g) = \int_L f + \int_L g$$

- continuity and integrability (interval_integrable.smul_continuous_on)
- integrability and addictivity (interval_integral.integral_add)
- change of variables (interval_integral.smul_integral_comp_add_mul)

Cauchy's Integral Formula: The First Part

The "hardest" part: prove

$$\int_L (f+g) = \int_L f + \int_L g$$

- continuity and integrability (interval_integrable.smul_continuous_on)
- integrability and addictivity (interval_integral.integral_add)
- change of variables (interval_integral.smul_integral_comp_add_mul)

Cauchy's Integral Formula: The Second Part

Preparation:

- Continuity and differentiability of some basic functions
- Definitions and properties of rectangles
- Turns the contour integral along a rectangle into the real integral

Cauchy's Integral Formula: The Second Part

Theorem (Cauchy's Integral Formula for A Rectangle)

Let $c \in \mathbb{C}$ be a point in the interior of a rectangle region D. If f is continuous on ∂D and holomorphic on $\mathrm{int}(D)$, then $\int_{\partial D} \frac{f(z)}{z-c} dz = 2\pi i f(c)$.

Cauchy's Integral Formula: The Second Part

Basic idea: Construct

$$g(z) := \begin{cases} \frac{f(z)-f(c)}{z-c} & \text{if } z \neq c \\ f'(c) & \text{otherwise} \end{cases}$$

1. Show that g is continuous on ∂D and holomorphic on $\mathrm{int}(D)$. (analysis.calculus.dslope)
2. Show $\int_{\partial D} g = 0$ (complex.integral_boundary_rect..._countable).
3. Show $\int_{\partial D} \frac{1}{z-c} = 2\pi i$ (winding number).

Cauchy's Integral Formula: The Second Part

computation of the winding number of a rectangle:
say $b \leqslant \mathrm{Im}(z) \leqslant t, l \leqslant \mathrm{Re}(z) \leqslant r$.

- bottom: $\int \frac{1}{z-c} = \log(r-c+bi) - \log(l-c+bi)$
- top: $\int \frac{1}{z-c} = \log(l-c+ti) - \log(r-c+ti)$
- right: $\int \frac{1}{z-c} = \log(r-c+ti) - \log(r-c+bi)$
- left: $\int \frac{1}{z-c} = 2\pi i + \log(l-c+bi) - \log(l-c+ti)$

Cauchy's Integral Formula: The Second Part

Computation of the left one is extremely hard!
Still need to spilt into two parts: the upper one and the lower one.

- logarithm near the branch cut (analysis.special_functions.complex.log)
- distinguish continuous/differentiable _ on/at/within_at

Cauchy's Integral Formula: The Second Part

Computation of the left one is extremely hard!
Still need to spilt into two parts: the upper one and the lower one.

- logarithm near the branch cut (analysis.special_functions.complex.log)
- distinguish continuous/differentiable _ on/at/within_at