Elementary proof on the order of magnitude of the prime-counting function

Damien Lefebvre

November 17, 2016

Faculty supervisor: *John B. Garnett*.

Abstract

The purpose of this written document is to support a two (2) hour lecture intended as a final project for an individual studies class with Professor John B. Garnett from the Mathematics Department.

The presentation is based on the book "Introduction to Analytic Number Theory" written by Tom M. Apostol and covers concepts from the first four (4) chapters, to culminate in the proof of Theorem 4.6.

Said theorem presents an inequality that shows $n/\log n$ is the correct order of magnitude of $\pi(n)$, thus supporting the Prime Number Theorem.

Contents

1 Preliminary concepts

1.1 Logarithmic identities

1.1.1 Product, quotient, power

The logarithm of a product is the sum of the logarithms of the numbers being multiplied.

$$\log_b xy = \log_b x + \log_b y \tag{1}$$

The logarithm of the ratio of two numbers is the difference of the logarithms.

$$\log_b \frac{x}{y} = \log_b x - \log_b y \tag{2}$$

The logarithm of the p-th power of a number is p times the logarithm of the number itself.

$$\log_b x^p = p * \log_b x \tag{3}$$

1.1.2 Change of base

The logarithm of x base b can be computed from the logarithms of x and b with respect to an arbitrary base k.

$$\log_b x = \frac{\log_k x}{\log_k b} \tag{4}$$

Also note $\log x$ increases for all positive real numbers.

1.2 Floor function

1.2.1 Notation

$[x]$ denotes the largest integer less than or equal to x. Notice $[x] = x$ if x is an integer.

1.2.2 Identity

$$[2x] - 2[x] = \begin{cases} 0 & \text{if x is an integer,} \\ 1 & \text{otherwise.} \end{cases} \tag{5}$$

1.3 Dirichlet convolutions

1.3.1 Definition

If f and g are two arithmetical functions, we define their Dirichlet convolution to be the arithmetical function h defined by the equation with the following notation

$$h(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = (f * g)(n) \tag{6}$$

1.3.2 Commutative law

The commutative property is self-evident from this alternative expression

$$(f * g)(n) = \sum_{a \cdot b = n} f(a)g(b) \tag{7}$$

1.4 Generalized convolutions

1.4.1 Definition

Let F denote a real or complex-valued function defined on the positive real axis $(0, +\infty)$ such that $F(x) = 0$ for $0 < x < 1$ and α denote any arithmetical function. We define their generalized convolution to be the arithmetical function N defined by the equation with the following notation

$$H(x) = \sum_{n \leq x} \alpha(n)F(\frac{x}{n}) = (\alpha \circ F)(x). \tag{8}$$

1.4.2 Associative property relating Dirichlet and generalized convolutions

For any arithmetical functions α and β we have

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F \tag{9}$$

Proof. For $x > 0$ we have

$$\begin{aligned} \{\alpha \circ (\beta \circ F)\}(x) &= \sum_{n \leq x} \alpha(n)(\beta \circ F)(x/n) \\ &= \sum_{n \leq x} \alpha(n) \sum_{m \leq (x/n)} \beta(m)F(\frac{(x/n)}{m}) \\ &= \sum_{mn \leq x} \alpha(n)\beta(m)F(\frac{x}{mn}) \end{aligned} \tag{10}$$

Let $k = mn$, so $(k/n) = m$ implies $n \mid k$ and

$$\begin{aligned} \sum_{mn \leq x} \alpha(n)\beta(m)F(\frac{x}{mn}) &= \sum_{k \leq x} (\sum_{n|k} \alpha(n)\beta(\frac{k}{n}))F(\frac{x}{k}) \\ &= \sum_{k \leq x} (\alpha * \beta)(k)F(\frac{x}{k}) \\ &= \{(\alpha * \beta) \circ F\}(x) \end{aligned} \tag{11}$$

□

1.5 The partial sums of a Dirichlet convolution

1.5.1 Theorem 3.10

If $h = f * g$, let

$$H(x) = \sum_{n \leq x} h(n) \tag{12}$$

$$F(x) = \sum_{n \leq x} f(n) \tag{13}$$

$$G(x) = \sum_{n \leq x} g(n) \tag{14}$$

Then

$$H(x) = \sum_{n \leq x} f(n) G(\frac{x}{n}) = \sum_{n \leq x} g(n) F(\frac{x}{n}) \tag{15}$$

Proof. Let

$$U(x) = \begin{cases} 0 & \text{if } 0 < x < 1, \\ 1 & \text{if } x \geq 1. \end{cases} \tag{16}$$

Then $F = f \circ U$, $G = g \circ U$, and

$$H = h \circ U = (f * g) \circ U \tag{17}$$

$$f \circ G = f \circ (g \circ U) = (f * g) \circ U = H \tag{18}$$

$$g \circ F = g \circ (f \circ U) = (g * f) \circ U = H \tag{19}$$

□

1.5.2 Theorem 3.11

If $g(n) = 1$ for all n, then

$$G(x) = \sum_{n \leq x} g(n) = \sum_{n \leq x} 1 = [x] \tag{20}$$

and

$$\sum_{n \leq x} \sum_{d|n} f(d) = \sum_{n \leq x} f(n)[\frac{x}{n}] = \sum_{n \leq x} F(\frac{x}{n}) \tag{21}$$

2 Von Mangoldt function

2.1 Definition

For every integer $n \geq 1$ we define

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime p and some } m \geq 1, \\ 0 & \text{otherwise.} \end{cases} \tag{22}$$

2.2 Theorem 2.10

If $n \geq 1$, then

$$\log n = \sum_{d|n} \Lambda(d) \tag{23}$$

Proof. The theorem is true if $n = 1$ since both members are 0. Therefore, we assume that $n > 1$.

Consider the sum on the right: the only nonzero terms come from those divisors d of the form p_k^m for $m = 1, \ldots, a_k$ and $k = 1, \ldots, r$. Hence

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k \tag{24}$$

Notice that from the fundamental theorem of arithmetic, we can write

$$n = \prod_{k=1}^{r} p_k^{a_k} \tag{25}$$

Taking logarithms, we find the same expression and thus complete the proof

$$\log n = \log \left(\prod_{k=1}^{r} p_k^{a_k}\right) = \sum_{k=1}^{r} \log p_k^{a_k} = \sum_{k=1}^{r} a_k \log p_k \tag{26}$$

□

2.3 Theorem 3.12

For $x \leq 1$ we have

$$\sum_{n \leq x} \Lambda(n)[\frac{x}{n}] = \log [x]! \tag{27}$$

Proof. Recall from generalized convolutions:

$$\sum_{n \leq x} \Lambda(n)[\frac{x}{n}] = \sum_{n \leq x} \sum_{d|n} \Lambda(d) = \sum_{n \leq x} \log n = \log [x]! \tag{28}$$

□

3 Legendre's identity

3.1 Definition

For $x \geq 1$ and p a prime, we have

$$[x]! = \prod_{p \leq x} p^{\alpha(p)} \tag{29}$$

where

$$\alpha(p) = \sum_{m=1}^{\infty} [\frac{x}{p^m}]. \tag{30}$$

Proof. Once again, since $\Lambda(n) = 0$ unless n is a prime power, let $n = p^m$ and

$$\begin{aligned} \log [x]! &= \sum_{n \leq x} \Lambda(n)[\frac{x}{n}] = \sum_{p \leq x} \sum_{m=1}^{\infty} \Lambda(p^m)[\frac{x}{p^m}] = \sum_{p \leq x} \sum_{m=1}^{\infty} \log p[\frac{x}{p^m}] \\ &= \sum_{p \leq x} \sum_{m=1}^{\infty} [\frac{x}{p^m}] \log p = \sum_{p \leq x} \alpha(p) \log p = \sum_{p \leq x} \log p^{\alpha(p)} \\ &= \log \prod_{p \leq x} p^{\alpha(p)} \end{aligned} \tag{31}$$

Applying the exponential function to both sides will complete the proof. □

Notice from the use of the floor function, we must have

$$\frac{x}{p^m} \geq 1 \tag{32}$$

and since $p^m > 0$,

$$x \geq p^m. \tag{33}$$

Taking logarithms on both sides

$$\log x \geq m \cdot \log p \tag{34}$$

and since $\log p > 0$,

$$m \leq \frac{\log x}{\log p}. \tag{35}$$

Hence

$$\alpha(p) = \sum_{m=1}^{[\frac{\log x}{\log p}]} [\frac{x}{p^m}]. \tag{36}$$

4 Chebyshev's theta function

4.1 Definition

If $x \geq 0$ and p is prime, we define Chebyshev's θ-function by the equation

$$\theta(x) = \sum_{p \leq x} \log p \tag{37}$$

5 Prime-counting function inequality

5.1 Prime-counting function definition

If $x > 0$, let $\pi(x)$ denote the number of primes not exceeding x.

5.2 Inequality

For every integer $n > 2$ we have

$$\frac{1}{6}\frac{n}{\log n} < \pi(n) < 6\frac{n}{\log n} \tag{38}$$

Proof. We begin by finding an upper and lower bound for $\binom{2n}{n}$ in terms of powers of 2.

5.3 Binomial inequality

5.4 Binomial Theorem

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \tag{39}$$

where

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \tag{40}$$

5.4.1 Upper bound

Notice

$$4^n = (2)^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} = \binom{2n}{0} + \cdots + \binom{2n}{n} + \cdots + \binom{2n}{2n} \tag{41}$$

It follows that a sum is larger than one of its terms

$$\sum_{k=0}^{2n} \binom{2n}{k} > \binom{2n}{n} \tag{42}$$

Then we have

$$4^n > \binom{2n}{n} \tag{43}$$

5.4.2 Lower bound

Notice

$$\binom{2n}{n} = \frac{(2n)!}{n!\,n!} = \frac{1 \cdot \ldots (n) \cdot (n+1) \cdot \ldots (2n)}{n! \cdot n!} = \frac{n! \cdot (n+1) \cdot \ldots (2n)}{n! \cdot n!} \tag{44}$$

Cancel $n!$ from top and bottom to get

$$\frac{(n+1) \cdot (n+2) \ldots (2n)}{1 \cdot 2 \ldots n} \tag{45}$$

There are n factors on top and n factors on bottom and each top factor is greater than or equal to 2 times the corresponding bottom factor, hence

$$\frac{(n+1) \cdot (n+2) \ldots (2n)}{1 \cdot 2 \ldots n} > 2^n \tag{46}$$

5.4.3 Conclusion

$$2^n < \binom{2n}{n} < 4^n \tag{47}$$

5.5 Applying Legendre's identity

This binomial inequality can be rewritten as

$$2^n < \frac{(2n)!}{(n!\,)^2} < 4^n \tag{48}$$

Taking logarithms on each side

$$n \cdot \log 2 < \log 2n! - 2 \cdot \log n! < n \cdot \log 4 \tag{49}$$

Applying Legendre's identity on both logarithms

$$\log 2n! = \sum_{p \le 2n} \alpha(p) \log p \tag{50}$$

$$2 \cdot \log n! = 2 \cdot \sum_{p \le n} \alpha'(p) \log p \tag{51}$$

Subtracting them

$$
\begin{aligned}
\log 2n! - 2\cdot\log n! &= \sum_{p\le 2n}\alpha(p)\log p - 2\cdot\sum_{p\le n}\alpha'(p)\log p \\
&= \sum_{p\le 2n}(\alpha(p) - 2\alpha'(p))\log p \\
&= \sum_{p\le 2n}\Big(\sum_{m=1}^{[\frac{\log 2n}{\log p}]}[\frac{2n}{p^m}] - 2\sum_{m=1}^{[\frac{\log n}{\log p}]}[\frac{n}{p^m}]\Big)\log p \\
&= \sum_{p\le 2n}\sum_{m=1}^{[\frac{\log 2n}{\log p}]}\Big([\frac{2n}{p^m}] - 2[\frac{n}{p^m}]\Big)\log p \\
&= \sum_{p\le 2n}\sum_{m=1}^{[\frac{\log 2n}{\log p}]}(1)\log p = \sum_{p\le 2n}[\frac{\log 2n}{\log p}]\log p \\
&= \sum_{p\le 2n}\log 2n = \log 2n\sum_{p\le 2n}1 \\
&= \log 2n\cdot\pi(2n)
\end{aligned}
\tag{52}
$$

5.6 Finding the lower bound

Thus for even integers we have

$$\pi(2n) \ge \frac{n\log 2}{\log 2n} = \frac{2n}{\log 2n}\frac{\log 2}{2} \tag{53}$$

Since $\log 2 > 1/2$ and $\frac{\log 2}{2} > 1/4$

$$\pi(2n) > \frac{1}{4}\frac{2n}{\log 2n} \tag{54}$$

For odd integers we have

$$\pi(2n+1) \ge \pi(2n) > \frac{1}{4}\frac{2n}{\log 2n} > \frac{1}{4}\frac{2n}{2n+1}\frac{2n+1}{\log 2n+1} \tag{55}$$

Since $2n/(2n+1) \ge 2/3$

$$\pi(2n+1) > \frac{1}{6}\frac{2n+1}{\log 2n} \tag{56}$$

Thus we can generalize to both even and odd integers

$$\pi(n) > \frac{1}{6}\frac{n}{\log n} \tag{57}$$

5.7 Finding the upper bound

Recall

$$\log 2n! - 2 \cdot \log n! = \sum_{p \le 2n} \sum_{m=1}^{[\frac{\log 2n}{\log p}]} ([\frac{2n}{p^m}] - 2[\frac{n}{p^m}]) \log p \tag{58}$$

This sum will be greater or equal than the first term corresponding to $m = 1$, hence

$$\log 2n! - 2 \cdot \log n! \ge \sum_{p \le 2n} ([\frac{2n}{p}] - 2[\frac{n}{p}]) \log p \tag{59}$$

If we further restrict the interval for p, the inequality still holds. Hence, choosing $n < p < 2n$ gives $n/p < 1$ and $[2(n/p)] - 2[n/p] = 1$ so

$$\log 2n! - 2 \cdot \log n! \ge \sum_{n < p \le 2n} \log p \tag{60}$$

Using Chebyshev's θ-function,

$$\theta(2n) = \sum_{p \le 2n} \log p \tag{61}$$

$$\theta(n) = \sum_{p \le n} \log p \tag{62}$$

We can subtract both functions to retrieve the interval

$$\theta(2n) - \theta(n) = \sum_{n \le p \le 2n} \log p \tag{63}$$

Hence from (49),

$$\theta(2n) - \theta(n) < n \log 4 \tag{64}$$

In particular, if $n = 2^r$, this gives

$$\theta(2^{r+1}) - \theta(2^r) < 2^r \log 4 = 2^{r+1} \log 2 \tag{65}$$

Summing on $r = 0, 1, \ldots, k$ and knowing $\theta(1) = 0$ gives

$$\sum_{r=0}^{k} (\theta(2^{r+1}) - \theta(2^r)) = \theta(2^{k+1}) - \theta(2^0) = \theta(2^{k+1}) < \sum_{r=0}^{k} 2^{r+1} \log 2 \tag{66}$$

For $r \ne 1$, the sum of the first n terms of a geometric series is

$$ar^0 + ar^1 + \cdots + ar^{n-1} = \sum_{k=0}^{n-1} ar^k = a\frac{1 - r^n}{1 - r} \tag{67}$$

where a is the first term of the series, and r is the common ratio.

$$\sum_{r=0}^{k} 2^{r+1} = \sum_{r=1}^{k+1} 2^{r} = \frac{1-2^{k+2}}{1-2} = -(1-2^{k+2}) = 2^{k+2} - 1 < 2^{k+2} \tag{68}$$

Hence

$$\theta(2^{k+1}) < 2^{k+2} \log 2 \tag{69}$$

Choosing k so that $2^k \leq n < 2^{k+1}$, we apply the theta function to n and the upper bound

$$\theta(n) \leq \theta(2^{k+1}) < 2^{k+2} \log 2, \tag{70}$$

and quadruple n and the lower bound

$$4 \cdot 2^k = 2^{k+2} \leq 4n. \tag{71}$$

We multiply by $\log 2$

$$2^{k+2} \log 2 \leq 4n \log 2, \tag{72}$$

hence

$$\theta(n) < 4n \log 2. \tag{73}$$

Now we modify the interval for p in the logarithmic summation, in order to make the prime-counting function appear.

Choose $0 < \alpha < 1$. Notice $\pi(n) - \pi(n^\alpha)$ is the number of primes p such that $n^\alpha < p \leq n$.

For each such prime we have $\log n^\alpha < \log p$. Comparing this to the theta function, we have

$$(\pi(n) - \pi(n^\alpha)) \log n^\alpha < \sum_{n^\alpha < p \leq n} \log p \leq \theta(n) < 4n \log 2, \tag{74}$$

$$\pi(n) - \pi(n^\alpha) < \frac{4n \log 2}{\log n^\alpha} \tag{75}$$

$$\begin{aligned} \pi(n) < \pi(n^\alpha) + \frac{4n \log 2}{\alpha \log n} &< \frac{4n \log 2}{\alpha \log n} + n^\alpha \\ &= \frac{n}{\log n}\left(\frac{4 \log 2}{\alpha} + \frac{\log n}{n^{1-\alpha}}\right) \end{aligned} \tag{76}$$

Now if $c > 0$ and $x \geq 1$, we define the following function and find its first derivative

$$f(x) = x^{-c} \log x \tag{77}$$

$$f'(x) = x^{-c-1}(1 - c\log x) \tag{78}$$

$x^{-c-1} > 0$ for all x and $1-c\log a = 0$ yields $a = e^{1/c}$ as a critical point. Since the function increases then decreases, the unique critical point is a maximum. So $n^{-c}\log n \leq 1/(ce)$ for $n \geq 1$.

Taking $\alpha = 2/3$ in (76), we find

$$\frac{4}{\alpha}\log 2 = \frac{4}{2/3}\log 2 = 6\log 2 \tag{79}$$

and

$$\frac{\log n}{n^{1-\alpha}} = \frac{\log n}{n^{1-(2/3)}} = \frac{\log n}{n^{1/3}} = n^{-(1/3)}\log n \leq \frac{1}{\frac{1}{3}e} = \frac{3}{e} \tag{80}$$

so

$$\pi(n) < \frac{n}{\log n}(6\log 2 + \frac{3}{e}) = 6\frac{n}{\log n}(\log 2 + \frac{1}{2e}). \tag{81}$$

Since $\log 2 + \frac{1}{2e} > 0$, we conclude

$$\pi(n) < 6\frac{n}{\log n}. \tag{82}$$

□

6 Conclusion

If we divide the inequality by x, we find the density of the prime-counting function, which is $\frac{\log x}{x}$.

In 1896, two proofs of the asymptotic law of the distribution of prime numbers were obtained independently by Jacques Hadamard and Charles Jean de la Vallée-Poussin.