

Proving the Prime Number Theorem *in an hour*

Curtis Bright

University of Waterloo

September 9, 2013

Abstract

A proof of the prime number theorem is presented, using nothing more advanced than the residue theorem from complex analysis. Based on the paper *Newman's Short Proof of the Prime Number Theorem* by Don Zagier.

The statement

- Let $\pi(x)$ count the primes $\leq x$, i.e., $\pi(x) := \sum_{p \leq x} 1$.
- The *Prime Number Theorem* states that

$$\lim_{x \rightarrow \infty} \left(\pi(x) / \frac{x}{\ln x} \right) = 1.$$

- The simplest proofs require the use of complex numbers!

Notation

- Throughout let $z = x + iy$ be a complex number with x, y real, and let p be prime.

Analytic functions

- Complex differentiable functions are known as *analytic*.
- We will be concerned with functions defined by well-behaved limiting processes.
 - Wherever the limit converges the functions will be analytic.
- Even if the limit doesn't converge, the function can sometimes still be defined using *analytic continuation*.

Zeros and poles

- Let $f(z)$ be analytic around $\alpha \in \mathbb{C}$. We can uniquely represent f around α by a *Laurent series*

$$f(z) = \sum_{n=-\infty}^{\infty} c_n (z - \alpha)^n.$$

- Let $\text{Ord}_f(\alpha)$ denote the minimal n such that $c_n \neq 0$.
 - When $\text{Ord}_f(\alpha) > 0$, α is known as a *zero*.
 - When $\text{Ord}_f(\alpha) < 0$, α is known as a *pole*, and if $\text{Ord}_f(\alpha) = -1$, α is known as a *simple pole*.
- $\text{Res}_f(\alpha) := c_{-1}$ is known as the *residue* of the pole at α .
- For simple poles, $\text{Res}_f(\alpha) = \lim_{z \rightarrow \alpha} (z - \alpha)f(z)$.

M-L inequality

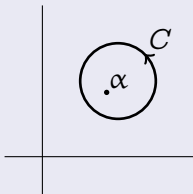
- The *maximum times length* (M-L) estimate is a simple way of bounding the absolute value of integrals:

$$\left| \int_C f(z) dz \right| \leq M \operatorname{len}(C)$$

where $|f(z)| \leq M$ for z on C .

Cauchy's residue theorem

- Let C be a counterclockwise circle containing α , and let $f(z)$ be analytic on and within C , except for a pole at α .



- Cauchy's residue theorem* states that

$$\int_C f(z) dz = 2\pi i \operatorname{Res}_f(\alpha).$$

- In addition, C can be freely deformed in the analytic region.

Absolute value of complex exponentials

- To compute the norm of n^z , replace z with its real part:

$$\begin{aligned} |n^z| &= |e^{(x+iy) \ln n}| \\ &= e^{x \ln n} |\cos(y \ln n) + i \sin(y \ln n)| \\ &= n^x \sqrt{\cos^2(y \ln n) + \sin^2(y \ln n)} \\ &= n^x \end{aligned}$$

Four important functions

$$\zeta(z) := \sum_{n=1}^{\infty} \frac{1}{n^z}$$

$$\Phi(z) := \sum_p \frac{\ln p}{p^z}$$

$$\vartheta(x) := \sum_{p \leq x} \ln p$$

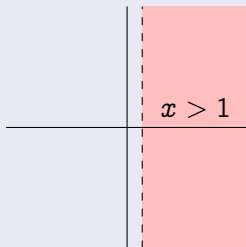
$$\pi(x) := \sum_{p \leq x} 1$$

Convergence of $\zeta(z)$ and $\Phi(z)$

- $\zeta(z)$ converges absolutely for $x > 1$ by the integral test:

$$\sum_{n=1}^{\infty} \left| \frac{1}{n^z} \right| = \sum_{n=1}^{\infty} \frac{1}{n^x} \leq 1 + \int_1^{\infty} \frac{du}{u^x} = \frac{x}{x-1}.$$

- Similarly, $\Phi(z)$ converges absolutely for $x > 1$.
- The region of convergence for $\zeta(z)$ and $\Phi(z)$:



Main steps of the proof

Setup

- I $\zeta(z) = \prod_p (1 - 1/p^z)^{-1}$ for $x > 1$
- II $\zeta(z)$ is analytic for $x \geq 1$, except for a simple pole at $z = 1$
- III $\Phi(z)$ is analytic for $x \geq 1$, except for a simple pole at $z = 1$
- IV $\vartheta(x) = O(x)$

Analytic Theorem

- V If $|f(t)|$ is bounded and $\int_0^\infty f(t)e^{-zt} dt$ can be analytically continued to $x = 0$ then $\int_0^\infty f(t) dt$ converges

Downhill

- VI $\int_1^\infty \frac{\vartheta(x) - x}{x^2} dx$ converges
- VII $\lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = 1$
- VIII $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1$

I. $\zeta(z) = \prod_p (1 - 1/p^z)^{-1}$ for $x > 1$

- Euler discovered a beautiful relation between $\zeta(z)$ and the primes:

$$\sum_{n=1}^{\infty} \frac{1}{n^z} = \prod_p \frac{1}{1 - 1/p^z}$$

I. $\zeta(z) = \prod_p (1 - 1/p^z)^{-1}$ for $x > 1$

- Use the geometric series formula with ratio $1/p^z$:

$$\prod_p \frac{1}{1 - 1/p^z} = \prod_p \sum_{k \geq 0} \frac{1}{p^{kz}}$$

- Multiplying the first two factors:

$$\sum_{k \geq 0} \frac{1}{2^{kz}} \cdot \sum_{k \geq 0} \frac{1}{3^{kz}} = \sum_{k_1, k_2 \geq 0} \frac{1}{(2^{k_1} 3^{k_2})^z}$$

- Continue multiplying together the factors to obtain:

$$\sum_{k_1, k_2, k_3, \dots \geq 0} \frac{1}{(2^{k_1} 3^{k_2} 5^{k_3} \dots)^z}$$

- By rearranging terms and using unique factorization, this is equal to $\sum_{n \geq 1} 1/n^z$.

II. $\zeta(z)$ is analytic for $x \geq 1$, except for a simple pole at $z = 1$

- We want to show that $\zeta(z)$ admits an analytic continuation to the line $x = 1$.
 - Actually, this isn't possible because of a pole at $z = 1$.
- However, by “subtracting off” the pole, as in

$$\zeta(z) - \frac{1}{z-1},$$

then the analytic continuation to $x = 1$ works.

II. $\zeta(z)$ is analytic for $x \geq 1$, except for a simple pole at $z = 1$

- For $x > 1$ we have

$$\zeta(z) - \frac{1}{z-1} = \sum_{n=1}^{\infty} \frac{1}{n^z} - \int_1^{\infty} \frac{du}{u^z} = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{1}{n^z} - \frac{1}{u^z} du.$$

- The absolute value of **this summand** is at most

$$\begin{aligned} \max_{u \in [n, n+1]} \left| \frac{1}{n^z} - \frac{1}{u^z} \right| &= \max_{u \in [n, n+1]} \left| \int_n^u \frac{z \, dv}{v^{z+1}} \right| \\ &\leq \max_{u \in [n, n+1]} \max_{v \in [n, u]} \left| \frac{z}{v^{z+1}} \right| \\ &= \frac{|z|}{n^{x+1}}. \end{aligned}$$

- Employing the M-L inequality twice.
- By comparison with $\sum_{n \geq 1} \frac{|z|}{n^{x+1}}$, **the sum on the right** converges absolutely for $x > 0$.

III. $\Phi(z)$ is analytic for $x \geq 1$, except for a simple pole at $z = 1$

- Taking the **logarithmic derivative** of the Euler product:

$$\frac{\zeta'(z)}{\zeta(z)} = \frac{d}{dz} \ln \zeta(z) = - \sum_p \frac{\ln p/p^z}{1 - 1/p^z} = -\Phi(z) - A(z)$$

where $A(z) := \sum_p \frac{\ln p}{p^z(p^z-1)}$ is analytic for $x > 1/2$.

- The logarithmic derivative has an especially simple Laurent expansion around α :

$$\frac{\zeta'(z)}{\zeta(z)} = \frac{\text{Ord}_\zeta(\alpha)}{z - \alpha} + O(1)$$

- It follows $\text{Res}_\Phi(\alpha) = -\text{Ord}_\zeta(\alpha)$.
 - To show Φ is analytic at α , we show $\text{Ord}_\zeta(\alpha) = 0$.

III. $\Phi(z)$ is analytic for $x \geq 1$, except for a simple pole at $z = 1$

- From

$$\lim_{\epsilon \rightarrow 0^+} \epsilon \sum_p \frac{\ln p}{p^{z+\epsilon}} = \text{Res}_\Phi(z)$$

one gets that

$$\lim_{\epsilon \rightarrow 0^+} \epsilon \sum_p \frac{\ln p}{p^{x+\epsilon}} (p^{2yi} + 4p^{yi} + 6 + 4p^{-yi} + p^{-2yi})$$

$$= \text{Res}_\Phi(x - 2yi) + 4 \text{Res}_\Phi(x - yi) + 6 \text{Res}_\Phi(x) + 4 \text{Res}_\Phi(x + yi) + \text{Res}_\Phi(x + 2yi)$$

$$= 2 \text{Res}_\Phi(x + 2yi) + 8 \text{Res}_\Phi(x + yi) + 6 \text{Res}_\Phi(x)$$

- The residues of Φ being invariant under complex conjugation being a consequence of $\Phi(z) = \overline{\Phi(\bar{z})}$.
- **The ugly factor** simplifies to $(p^{yi/2} + p^{-yi/2})^4$.
- Nonnegative since its **inside** is real.

III. $\Phi(z)$ is analytic for $x \geq 1$, except for a simple pole at $z = 1$

- Then

$$\epsilon \sum_p \frac{\ln p}{p^{x+\epsilon}} (p^{yi/2} + p^{-yi/2})^4 \geq 0$$

and, taking the limit as $\epsilon \rightarrow 0^+$, we have

$$2 \operatorname{Res}_{\Phi}(x + 2yi) + 8 \operatorname{Res}_{\Phi}(x + yi) + 6 \operatorname{Res}_{\Phi}(x) \geq 0$$

$$2 \operatorname{Ord}_{\zeta}(x + 2iy) + 8 \operatorname{Ord}_{\zeta}(x + iy) + 6 \operatorname{Ord}_{\zeta}(x) \leq 0$$

- Making use of $\operatorname{Res}_{\Phi}(z) = -\operatorname{Ord}_{\zeta}(z)$.

III. $\Phi(z)$ is analytic for $x \geq 1$, except for a simple pole at $z = 1$

- Using $\text{Ord}_\zeta(z) \geq -1$, this becomes

$$2 \text{Ord}_\zeta(x + 2iy) + 8 \text{Ord}_\zeta(x + iy) \leq 6.$$

- For $x \geq 1$ and $z \neq 1$ we know $\zeta(z)$ has no poles, so

$$\text{Ord}_\zeta(z) \geq 0.$$

- Combining the above two inequalities, we have

$$\text{Ord}_\zeta(x + iy) = 0.$$

- Thus $\Phi(z)$ is analytic for $x \geq 1$ and $z \neq 1$.
 - $\Phi(1)$ is a simple pole with residue $-\text{Ord}_\zeta(1) = 1$.

IV. $\vartheta(x) = O(x)$

- The binomial theorem gives the following upper bound on the central binomial coefficient:

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

- But every prime $n < p \leq 2n$ is a factor of $(2n)!/(n!)^2$:

$$\begin{aligned} \binom{2n}{n} &\geq \prod_{n < p \leq 2n} p = \exp\left(\sum_{p \leq 2n} \ln p - \sum_{p \leq n} \ln p\right) \\ &= \exp(\vartheta(2n) - \vartheta(n)) \end{aligned}$$

IV. $\vartheta(x) = O(x)$

- Combining these and taking the logarithm,

$$\vartheta(2n) - \vartheta(n) \leq n \ln 4.$$

- If n is a power of 2, summing this over $n, n/2, \dots, 1$ the left side telescopes and the right side is a truncated geometric series:

$$\vartheta(2n) \leq (n + n/2 + \dots + 1) \ln 4 \leq 2n \ln 4$$

- For arbitrary x , let $n \leq x < 2n$ where n is a power of 2. Then:

$$\vartheta(x) \leq \vartheta(2n) \leq 2n \ln 4 \leq 2x \ln 4$$

V. Analytic Theorem - The statement

- If $|f(t)|$ is bounded (say by M) and its Laplace transform

$$\int_0^{\infty} f(t) e^{-zt} dt$$

defines an analytic function $g(z)$ for $x \geq 0$, then the integral converges for $z = 0$.

V. Analytic Theorem - Easy convergence

- Note the integral converges absolutely for $x > 0$ since

$$\int_0^{\infty} |f(t) e^{-zt}| dt \leq M \int_0^{\infty} e^{-xt} dt = \frac{M}{x}.$$

V. Analytic Theorem - Setup

- Define the ‘truncated’ Laplace transform,

$$g_T(z) := \int_0^T f(t) e^{-zt} dt.$$

This is analytic for all z by differentiation under the integral sign. As $T \rightarrow \infty$ this converges to $g(z)$ for $x > 0$.

- We will show this also occurs at $z = 0$, i.e.,

$$\lim_{T \rightarrow \infty} \int_0^T f(t) dt = g(0).$$

V. Analytic Theorem - A useful function

- Consider the function

$$(g(z) - g_T(z)) e^{zT} \left(\frac{1}{z} + \frac{z}{R^2} \right).$$

- This is analytic for $x \geq 0$ and $z \neq 0$, since:
 - $g(z) - g_T(z)$ is analytic for $x \geq 0$
 - e^{zT} is analytic for all z
 - $1/z + z/R^2$ is analytic for $z \neq 0$
- At $z = 0$, this has a simple pole with residue $g(0) - g_T(0)$.

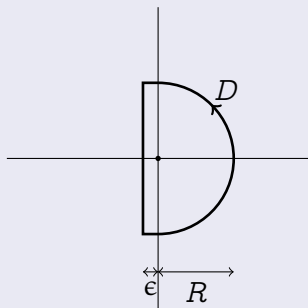
V. Analytic Theorem - A useful fact

- On the circle $|z| = R$, **the final factor** is equal to

$$\frac{x - yi}{x^2 + y^2} + \frac{x + yi}{x^2 + y^2} = \frac{2x}{R^2}.$$

V. Analytic Theorem - A useful contour

- Define the contour D in the complex plane by:



- Here ϵ (depending on R) is taken small enough so that $g(z)$ is analytic on and inside D .
- By Cauchy's residue theorem,

$$\int_D (g(z) - g_T(z)) e^{zT} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz = 2\pi i (g(0) - g_T(0)).$$

V. Analytic Theorem - A useful integral

- We split the integral

$$I := \int_D (g(z) - g_T(z)) e^{zT} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz$$

into three such that $I = I_1 - I_2 + I_3$:

$$I_1 := \int_{D_1} (g(z) - g_T(z)) e^{zT} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz$$



$$I_2 := \int_{D_2} g_T(z) e^{zT} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz$$



$$I_3 := \int_{D_3} g(z) e^{zT} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz$$



V. Analytic Theorem - The first integral

- For $x > 0$, we have that $|g(z) - g_T(z)|$ is equal to

$$\left| \int_T^\infty f(t) e^{-zt} dt \right| \leq M \int_T^\infty e^{-xt} dt = M \frac{e^{-xT}}{x}.$$

- Using M-L we can bound $|I_1|$:

$$\begin{aligned} & \left| \int_{D_1} (g(z) - g_T(z)) e^{zT} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz \right| \\ & \leq \max_{z \in D_1} \pi R \quad M \frac{e^{-xT}}{x} \quad e^{xT} \quad \frac{2x}{R^2} \quad = O\left(\frac{1}{R}\right) \end{aligned}$$

V. Analytic Theorem - The second integral

- For $x < 0$, we have that $|g_T(z)|$ is equal to

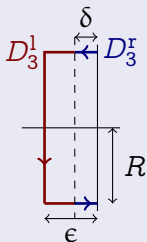
$$\left| \int_0^T f(t) e^{-zt} dt \right| \leq M \int_0^T e^{-xt} dt = M \frac{e^{-xT} - 1}{|x|}.$$

- Using M-L we can bound $|I_2|$:

$$\begin{aligned} & \left| \int_{D_2} g_T(z) e^{zT} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz \right| \\ & \leq \max_{z \in D_2} \pi R M \frac{e^{-xT}}{|x|} e^{xT} \frac{2|x|}{R^2} = O\left(\frac{1}{R}\right) \end{aligned}$$

V. Analytic Theorem - The third integral

- Since $g(z)\left(\frac{1}{z} + \frac{z}{R^2}\right)$ is analytic on D_3 , its absolute value must be bounded (say by B).
- We have $|e^{zT}| \leq 1$ for z on D_3 , but this is not sufficient for using M-L. Instead, we split D_3 into a **left** and **right** part based on a parameter $\delta \in (0, \epsilon)$:



V. Analytic Theorem - The third integral

- Using M-L on D_3^l and D_3^r separately we can bound $|I_3|$:

$$\left| \iint_C g(z) \left(\frac{1}{z} + \frac{z}{R^2} \right) e^{zT} dz \right|$$

for D_3^l :	$\leq 2(R + \epsilon)$	B	$e^{-\delta T}$	$= O(e^{-\delta T})$
for D_3^r :	$\leq 2\delta$	B	1	$= O(\delta)$

- Taking the limit as $T \rightarrow \infty$,

$$0 \leq \limsup_{T \rightarrow \infty} |I_3| \leq O(\delta).$$

- Taking the limit as $\delta \rightarrow 0^+$,

$$\lim_{T \rightarrow \infty} |I_3| = 0.$$

V. Analytic Theorem - Conclusion

- We have

$$|g(0) - g_T(0)| = \left| \frac{I}{2\pi i} \right| \leq |I_1| + |I_2| + |I_3|.$$

- Taking the limit as $T \rightarrow \infty$,

$$0 \leq \limsup_{T \rightarrow \infty} |g(0) - g_T(0)| \leq O\left(\frac{1}{R}\right).$$

- Taking the limit as $R \rightarrow \infty$,

$$\lim_{T \rightarrow \infty} |g(0) - g_T(0)| = 0.$$

- Therefore

$$\int_0^{\infty} f(t) dt = g(0).$$

VI. $\int_1^{\infty} \frac{\vartheta(x)-x}{x^2} dx$ converges

- Note the Laplace transform of $\vartheta(e^t)$ is $\Phi(z)/z$:

$$\frac{\Phi(z)}{z} = \int_0^{\infty} \vartheta(e^t) e^{-zt} dt$$

- This follows via summation by parts, algebra, and the substitution $u = e^t$:

$$\begin{aligned}\Phi(z) &= \sum_{n=1}^{\infty} \vartheta(n) \left(\frac{1}{n^z} - \frac{1}{(n+1)^z} \right) + \lim_{n \rightarrow \infty} \frac{\vartheta(n)}{n^z} \\ &= \sum_{n=1}^{\infty} \vartheta(n) \int_n^{n+1} \frac{z du}{u^{z+1}} \quad (x > 1) \\ &= z \int_1^{\infty} \frac{\vartheta(u)}{u^{z+1}} du\end{aligned}$$

VI. $\int_1^\infty \frac{\vartheta(x)-x}{x^2} dx$ converges

- Substituting $z \mapsto z + 1$ and subtracting $1/z = \int_0^\infty e^{-zt} dt$, this becomes:

$$\frac{\Phi(z+1)}{z+1} - \frac{1}{z} = \int_0^\infty \left(\frac{\vartheta(e^t)}{e^t} - 1 \right) e^{-zt} dt$$

- By III, the **left hand side** is analytic for $x \geq 0$, since $\frac{\Phi(z+1)}{z+1}$ is analytic there.
 - Except at $z = 0$, where it has a simple pole with residue $\lim_{z \rightarrow 0} z \frac{\Phi(z+1)}{z+1} = 1$.
- By IV, the **Laplace integrand** is $O(e^t)/e^t - 1 = O(1)$.

VI. $\int_1^\infty \frac{\vartheta(x) - x}{x^2} dx$ converges

- Using the analytic theorem with $f(t) := \vartheta(e^t)/e^t - 1$,

$$\int_0^\infty \frac{\vartheta(e^t)}{e^t} - 1 dt = \int_1^\infty \frac{\vartheta(x) - x}{x^2} dx$$

converges (the substitution $x = e^t$ was used).

- This is a strong condition; if $\vartheta(x) = (1 + \epsilon)x$ then this integral would be $\int_1^\infty \epsilon/x dx$, which diverges.

VII. $\lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = 1$

- Suppose otherwise. Then there is some $\epsilon > 0$ such that $\vartheta(x) > (1 + \epsilon)x$ or $\vartheta(x) < (1 - \epsilon)x$ for arbitrarily large x .
- In the first case, say $\{x_n\}$ is an increasing sequence with $\vartheta(x_n) > (1 + \epsilon)x_n$. Since $\vartheta(x)$ is non-decreasing,

$$\begin{aligned} \int_{x_n}^{(1+\epsilon)x_n} \frac{\vartheta(x) - x}{x^2} dx &> \int_{x_n}^{(1+\epsilon)x_n} \frac{(1 + \epsilon)x_n - x}{x^2} dx \\ &= \epsilon - \ln(1 + \epsilon) \end{aligned}$$

which is a positive number not depending on n .

- Since $\int_1^\infty \frac{\vartheta(x) - x}{x^2} dx$ converges, the above sequence of subintegrals should go to zero as $n \rightarrow \infty$.

VII. $\lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = 1$

- In the second case, say $\{x_n\}$ is an increasing sequence with $\vartheta(x_n) < (1 - \epsilon)x_n$. Since $\vartheta(x)$ is non-decreasing,

$$\begin{aligned} \int_{(1-\epsilon)x_n}^{x_n} \frac{\vartheta(x) - x}{x^2} dx &< \int_{(1-\epsilon)x_n}^{x_n} \frac{(1-\epsilon)x_n - x}{x^2} dx \\ &= \epsilon + \ln(1 - \epsilon) \end{aligned}$$

which is a negative number not depending on n .

- Since $\int_1^\infty \frac{\vartheta(x) - x}{x^2} dx$ converges, the above sequence of subintegrals should go to zero as $n \rightarrow \infty$.
- Either case leads to a contradiction, so we must in fact have $\lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = 1$.

$$\text{VIII. } \lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1$$

- By multiplying the **number of nonzero terms** with the **maximum or minimum term** one derives upper and lower bounds on $\vartheta(x)$ in terms of $\pi(x) \ln x$:

$$\vartheta(x) = \sum_{p \leq x} \ln p \leq \pi(x) \ln x$$

$$\vartheta(x) \geq \sum_{x^{1-\epsilon} < p \leq x} \ln p \geq (\pi(x) - \pi(x^{1-\epsilon})) \ln(x^{1-\epsilon})$$

- For the lower bound, we ignore primes less than $x^{1-\epsilon}$ for some constant parameter $\epsilon \in (0, 1)$.

VIII. $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1$

- Combining these,

$$\frac{\vartheta(x)}{x} \leq \frac{\pi(x)}{x/\ln x} \leq \frac{1}{1-\epsilon} \frac{\vartheta(x)}{x} + \frac{\ln x}{x^\epsilon}.$$

- Taking the limit as $x \rightarrow \infty$ and using $\lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = 1$,

$$1 \leq \limsup_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} \leq \frac{1}{1-\epsilon}.$$

- Similarly for the lim inf.
- Taking the limit as $\epsilon \rightarrow 0^+$,

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1.$$