# PMATH 440 Course Notes

## Analytic Number Theory

Wentang Kuo • Fall 2021 • University of Waterloo

## Table of Contents

# 1 Introduction to Prime Numbers and Their Counting Function

## 1.1 Primes

Definition 1.1. A **prime number** is a positive integer greater than 1 such that its only factors are 1 and itself. We denote by $\mathcal{P}$ the set of all prime numbers. For a positive real number $x$, we define the **prime counting function** by

$$\pi(x) = \#\{p \leq x : p \in \mathcal{P}\},$$

where $\#S$ denotes the cardinality of the set $S$.

We would like to know how the primes are distributed among the integers. Let $p_n$ denote the $n$-th prime. Is there a formula to obtain $p_n$? Is there a polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(n) = p_n$ for all $n \in \mathbb{N}$? The answer to the latter question is no, due to the following result.

Proposition 1.2. There is no non-constant polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(n)$ is prime for all $n \in \mathbb{N}$.

Proof. Suppose such a polynomial $f(x) \in \mathbb{Z}[x]$ existed, and write

$$f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Let $q$ be a prime with $f(n) = q$ for some $n \in \mathbb{N}$. Then $q \mid f(n + kq)$ for each $k \in \mathbb{N}$. In particular, notice that if $f(m)$ is prime for every positive integer $m$, then $f(x)$ must be constant with $f(x) = q$ for some prime $q$. □

Remark 1.3.

(1) There are examples of polynomials whose initial values are surprisingly often prime. For example, the polynomial $n^2 + n + 41$ is prime for all $0 \leq n \leq 39$, and the polynomial $(n - 40)^2 + (n - 40) + 41$ is prime for all $0 \leq n \leq 79$.

(2) In the 1970s, Matijasevic proved Hilbert's tenth problem, and in the process, he was able to show that tehre is a polynomial $f \in \mathbb{Z}[a, b, \ldots, z]$ such that the set of positive values in $f(\mathbb{N}^{26})$ is exactly the set of primes. In 1977, he showed that only 10 variables are needed.

Let us instead ask a weaker question. Can we find a non-constant polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(n)$ yields a prime for infinitely many $n \in \mathbb{N}$? Trivially, we see that $f(x) = x + k$ works for any $k \in \mathbb{Z}$. When the coefficient of $x$ is not equal to 1, we have the following result, which we will prove at the end of this course.

Theorem 1.4 (Dirichlet). Let $k$ and $\ell$ be coprime positive integers. Then $kn + \ell$ is prime for infinitely many positive integers $n$.

Remark 1.5.

(1) At the moment, there is no known polynomial of degree greater than 1 in one variable known to take prime values infinitely often. The best result known to date is that $n^2 + 1$ is a product of two primes for infinitely many $n$.

(2) If we instead consider polynomials of two variables, we can go further. It is known that an odd prime $p$ is the sum of two squares if and only if $p \equiv 1 \pmod 4$. In 1998, Friedlander and Iwaniec proved that there are infinitely many primes of the form $n^2 + m^4$. In 2001, Heath-Brown showed that there are infinitely many primes of the form $n^3 + 2m^3$.

Theorem 1.6 (Euclid). There are infinitely many prime numbers.

Proof. Assume that there are only finitely many primes, say $p_1, \ldots, p_n$, and consider

$$m = p_1 \cdots p_n + 1.$$

Then $m$ can be written as a product of primes by unique factorization, and $p_k \mid m$ for some $1 \leq k \leq n$. Hence, we see that $p_k \mid m - p_1 \cdots p_n$ and $p_k \mid 1$, which is a contradiction. □

We would like to estimate the prime counting function $\pi(x)$.

PROPOSITION 1.7. For all $n \in \mathbb{N}$, we have $p_n \leq 2^{2^n}$.

PROOF. We proceed by induction. For $n = 1$, we have $2 = p_1 \leq 2^{2^1} = 4$. Suppose the result holds for all $1 \leq k \leq n$. By Euclid's argument, we obtain $p_{n+1} \leq p_1 \cdots p_n + 1$. It follows from induction that

$$p_{n+1} \leq 2^{2^1} 2^{2^2} \cdots 2^{2^n} + 1 \leq 2^{2^{n+1}-2} + 1 \leq 2^{2^{n+1}},$$

which completes the proof. □

COROLLARY 1.8. For all $x \geq 2$, we have $\pi(x) > \log\log x$. (In this course, log denotes the natural logarithm.)

PROOF. Let $x \geq 2$, and let $s$ be the integer satisfying

$$2^{2^s} \leq x < 2^{2^{s+1}}.$$

By the previous proposition, we have $\pi(x) \geq s$. On the other hand, since $x < 2^{2^{s+1}}$, taking logarithms yields $\log_2(\log_2 x) < s + 1$, and hence

$$\frac{\log(\frac{\log x}{\log 2})}{\log 2} < s + 1.$$

It follows that

$$\pi(x) \geq s > \frac{\log(\frac{\log x}{\log 2})}{\log 2} - 1 \geq \log\log x.$$ □

There is an alternative way to prove Euclid's theorem, due to Euler, which is left as part of the homework. Using the same idea, we can derive a slightly better lower bound for $\pi(x)$.

PROPOSITION 1.9. For all $x \geq 2$, we have

$$\pi(x) \geq \frac{\log\log x}{\log 2}.$$

PROOF. Suppose that $x \geq 2$. Then we have

$$2^{\pi(x)} \geq \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \geq \sum_{n \leq x} \frac{1}{n} \geq \int_1^{\lfloor x \rfloor + 1} \frac{1}{u}\, \mathrm{d}u \geq \log x,$$

where the product $\prod_{p \leq x}$ means that $p$ runs through all primes at most $x$, and $\lfloor y \rfloor$ is the greatest integer less than or equal to $y$. We will will use this notation for the rest of the course. Taking logarithms yields the desired inequality. □

Fermat had conjectured that the numbers of the form $2^{2^n} + 1$ are prime for $n \in \mathbb{N}$. He had checked it for the values $0 \leq n \leq 4$. These are known as the **Fermat numbers** and are denoted by

$$F_n = 2^{2^n} + 1.$$

In 1732, Euler showed that $641 \mid F_5$. It is also known that $F_6, \ldots, F_{21}$ are composite. It is quite likely that only finitely many Fermat numbers are prime.

THEOREM 1.10 (Polyá). If $n$ and $m$ are positive integers with $1 \leq n < m$, then $(F_n, F_m) = 1$.

PROOF. Write $m = n + k$ with $k \geq 1$. First, we will show that $F_n \mid F_m - 2$. Observe that

$$F_m - 2 = (2^{2^{n+k}} + 1) - 2 = 2^{2^{n+k}} - 1.$$

The polynomial $x^{2^k} - 1$ is divisible by $x + 1$ in $\mathbb{Z}[x]$. Now, letting $x = 2^{2^n}$, we get

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1 \in \mathbb{Z}.$$

Hence, we have $F_n \mid F_m - 2$. Suppose now that $d \mid F_n$ and $d \mid F_m$. Then $d \mid 2$ and $2 \nmid F_n$, which implies that $d = \pm 1$. The result follows. □

This gives yet another proof of Euclid's theorem, as well as the bound $p_n \leq 2^{2^n} + 1$.

## 1.2 Elementary Approximations of $\pi(x)$

In 1896, Hadamand and de la Vallée Poussin each proved the Prime Number Theorem independently.

THEOREM 1.11 (Prime Number Theorem). We have

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

This was initially conjectured by Gauss. We will prove this theorem later in the course; for now, we will see how to approach this problem using elementary methods.

THEOREM 1.12. For all $x \geq 2$, we have

$$\pi(x) \geq \frac{\log x}{2\log 2}.$$

Moreover, for all $n \geq 1$, we have $p_n \leq 4^n$.

PROOF. Let $x \geq 2$ be an integer. Let $p_1, \ldots, p_j$ be the primes less than or equal to $x$. Note that we have $j = \pi(x)$ here. For every integer $n$ with $n \leq x$, we can write $n = n_1^2 m$ where $n_1$ is a positive integer and $m$ is squarefree. Then $m$ is of the form

$$m = p_1^{\varepsilon_1} \cdots p_j^{\varepsilon_j},$$

where $\varepsilon_i \in \{0,1\}$ for each $1 \leq i \leq j$. We see that there are at most $2^j$ possible values for $m$. Moreover, there are at most $\sqrt{x}$ possible values for $n_1$. Hence, we have $2^j\sqrt{x} \geq x$, which implies that $2^j \geq \sqrt{x}$. Denote this inequality by $(\star)$. Since $j = \pi(x)$, we see that

$$\pi(x)\log 2 \geq \frac{\log x}{2},$$

so the first equality follows. For the second equality, take $x = p_n$ so that $\pi(p_n) = n$. By $(\star)$, we obtain $2^n \geq \sqrt{p_n}$ and hence $4^n \geq p_n$. $\square$

Let $n$ be a positive integer and let $p$ be a prime. Recall that the exact power of $p$ dividing $n!$ is

$$\sum_{n=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{n=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

THEOREM 1.13. For all $x \geq 2$, we have

$$\left(\frac{3\log 2}{8}\right)\frac{x}{\log x} < \pi(x) < (6\log 2)\frac{x}{\log x}.$$

PROOF. This argument was given by Erdős. First, we will prove the lower bound. Note that $\binom{2n}{n}$ is an integer, and

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \;\Big|\; \prod_{p\leq 2n} p^{r_p},$$

where $r_p$ is an integer satisfying $p^{r_p} \leq 2n < p^{r_p+1}$. Indeed, note that the exact power of $p$ dividing $(2n)!$ is

$$\sum_{k=1}^{r_p} \left\lfloor \frac{2n}{p^k} \right\rfloor,$$

and the exact power of $p$ dividing $n!$ is

$$\sum_{k=1}^{r_p} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Thus, the exact power of $p$ dividing $\binom{2n}{n}$ is

$$\sum_{k=1}^{r_p}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor-\left\lfloor\frac{n}{p^k}\right\rfloor\right)\le r_p,$$

since $\lfloor 2a\rfloor-2\lfloor a\rfloor\le 1$ for all $a\in\mathbb{R}$. In particular, we have

$$\binom{2n}{n}\le\prod_{p\le 2n}p^{r_p}\le(2n)^{\pi(2n)}.$$

Notice that

$$\binom{2n}{n}=\frac{2n\cdot(2n-1)\cdots(n+1)}{n\cdot(n-1)\cdots 1}=\frac{2n}{n}\cdots\frac{n+1}{1}\ge 2^n.$$

Hence, we get $2^n\le(2n)^{\pi(2n)}$. Now, we have

$$\pi(2n)\ge\left(\frac{\log 2}{2}\right)\frac{2n}{\log(2n)}.$$

Recall that $\frac{x}{\log x}$ is increasing for $x>e$. If $x\ge 6$, choose $n\in\mathbb{N}$ such that $3x/4\le 2n\le x$. We see that

$$\pi(x)\ge\pi(2n)\ge\left(\frac{\log 2}{2}\right)\frac{2n}{\log(2n)}\ge\left(\frac{\log 2}{2}\right)\frac{\frac{3}{4}x}{\log(\frac{3}{4}x)}>\frac{3\log 2}{8}\frac{x}{\log x}.$$

One can manually check that the result holds for $2\le x\le 6$, which finishes the proof of the lower bound.

We now turn to the upper bound. Observe that

$$\prod_{n<p\le 2n}p\;\Bigg|\;\binom{2n}{n},$$

so by the binomial theorem, we have

$$\prod_{n<p\le 2n}p\le\binom{2n}{n}\le(1+1)^{2n}=2^{2n}.$$

On the other hand, notice that

$$\prod_{n<p\le 2n}p\ge n^{\pi(2n)-\pi(n)},$$

so it follows that

$$\pi(2n)\log n-\pi(n)\log(n/2)<(\log 2)2n+(\log 2)\pi(n)<(3\log 2)n.$$

By taking $n=2^k,2^{k-1},\ldots,4$, we obtain a telescoping collection of inequalities, given by

$$\begin{aligned}\pi(2^{k+1})\log 2^k-\pi(2^k)\log 2^{k-1}&<(3\log 2)2^k,\\ \pi(2^k)\log 2^{k-1}-\pi(2^{k-1})\log 2^{k-2}&<(3\log 2)2^{k-1},\\ &\vdots\\ \pi(8)\log 4-\pi(4)\log 2&<(3\log 2)4.\end{aligned}$$

Putting these inequalities together, we have

$$\pi(2^{k+1})\log 2^k<(3\log 2)(2^k+2^{k+1}+\cdots+4)+\pi(4)\log 2<(3\log 2)2^{k+1},$$

and hence

$$\pi(2^{k+1})<(3\log 2)\left(\frac{2^{k+1}}{\log(2^k)}\right).$$

If $x > e$, choose $k$ such that $2^k \leq x \leq 2^{k+1}$. Then $\pi(x) \leq \pi(2^{k+1})$, and so

$$\pi(x) \leq (3\log 2)\left(\frac{2^{k+1}}{\log(2^k)}\right) \leq (6\log 2)\left(\frac{2^k}{\log(2^k)}\right) \leq (6\log 2)\left(\frac{x}{\log x}\right),$$

where in the last equality, we use the fact that $\frac{x}{\log x}$ is increasing for $x > e$. The values $2 \leq x \leq e$ can be checked manually, proving the lower bound. □

We should note that $\frac{3\log 2}{8}$ is in some sense arbitrary. In the proof, we could have picked $n \in \mathbb{N}$ such that $1 - \varepsilon \leq 2n \leq x$ instead of $3x/4 \leq 2n \leq x$ for $\varepsilon$ arbitrarily small. However, this comes at the cost that the bound may potentially fail for small $x$, and there is little purpose in a better lower bound for large $x$ as it is overshadowed by the Prime Number Theorem.

## 1.3 Bertrand's Postulate

In 1845, Bertrand showed that there is always a prime $p$ in the interval $[n, 2n]$ for $n \in \mathbb{Z}^+$ provided that $n < 6 \cdot 10^6$, and he had conjectured that this holds for all $n \in \mathbb{Z}^+$. Chebyshev proved that this was indeed the case in 1950. Note that this is not a trivial result; it doesn't occur for free just because $\pi(x) \sim x/\log x$.

Proposition 1.14. For all $n \in \mathbb{Z}^+$, we have

$$\prod_{p\leq n} p < 4^n.$$

Proof. The result is clearly true for $n = 1$ and $n = 2$. Suppose that it holds for all $1 \leq n \leq k-1$. Note that we can restrict our attention to the case where $n$ is odd, because if $n$ is even and $n > 2$, then

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p,$$

and the result will follow by induction. Write $n = 2m+1$ for some $m \in \mathbb{Z}^+$, and consider $\binom{2m+1}{m}$. In particular, we have

$$\prod_{m+1<p\leq 2m+1} p \;\Bigg|\; \binom{2m+1}{m}.$$

Since $\binom{2m+1}{m}$ and $\binom{2m+1}{m+1}$ both appear in the binomial expansion of $(1+1)^{2m+1}$ with $\binom{2m+1}{m} = \binom{2m+1}{m+1}$, we obtain

$$\binom{2m+1}{m} \leq \frac{1}{2}(2^{2m+1}) = 4^m.$$

By our inductive hypothesis and the previous inequality, it follows that

$$\prod_{p\leq 2m+1} p = \left(\prod_{p\leq m+1} p\right)\left(\prod_{m+1<p\leq 2m+1} p\right) \leq 4^{m+1}4^m = 4^{2m+1}.$$ □

Lemma 1.15. If $n \geq 3$ and $p$ is a prime with $\frac{2}{3}n < p \leq n$, then $p \nmid \binom{2n}{n}$.

Proof. Since $n \geq 3$, we see that if $p$ is in the range $\frac{2}{3}n < p \leq n$, then $p > 2$. Then $p$ and $2p$ are the only multiples of $p$ at most $2n$, and so

$$p^2 \parallel (2n)!,$$

where we write $p^k \parallel b$ to mean that $p^{k+1} \nmid b$ and $p^k \mid b$. Furthermore, since $\frac{2}{3}n < p \leq n$, we have $p \parallel n!$ and hence $p^2 \parallel (n!)^2$. Using the identity

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2},$$

we see that $p \nmid \binom{2n}{n}$. □

THEOREM 1.16 (Chebyshev). For every $n \in \mathbb{Z}^+$, there exists a prime satisfying $n < p \leq 2n$.

PROOF. This argument was given by Erdős. Note that the result holds for $1 \leq n \leq 3$. Assume that the result is false for some integer $n \geq 4$. By the previous lemma, every prime dividing $\binom{2n}{n}$ is at most $\frac{2}{3}n$.

Let $p$ be a prime divisor of $\binom{2n}{n}$ where we have $p \leq \frac{2}{3}n$. Suppose that $p^{\alpha_p} \parallel \binom{2n}{n}$ for some integer $\alpha_p$. Recall that in the proof of Theorem 1.13, we defined $r_p$ to be the integer satisfying $p^{r_p} \leq 2n < p^{r_p+1}$. Then we have $\alpha_p \leq r_p$, and hence $p^{\alpha_p} \leq p^{r_p} \leq 2n$.

If $\alpha_p \geq 2$, then $p^2 \leq p^{\alpha_p} \leq 2n$ so that $p \leq \sqrt{2n}$. By Proposition 1.14, we have

$$\binom{2n}{n} \leq \left( \prod_{\substack{p \leq \frac{2}{3}n \\ \alpha_p \leq 1}} p \right) \left( \prod_{\substack{p \leq \frac{2}{3}n \\ \alpha_p \geq 2}} p \right) \leq 4^{2n/3} (2n)^{\pi(\sqrt{2n})} \leq 4^{2n/3} (2n)^{\sqrt{2n}}.$$

Note that $\binom{2n}{n}$ is the largest of the $2n+1$ terms in the binomial expansion of

$$(1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{2n},$$

so we get

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}.$$

Combining the above inequalities gives

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq 4^{2n/3} (2n)^{\sqrt{2n}},$$

which implies that

$$4^{n/3} \leq (2n)^{\sqrt{2n}} (2n+1) < (2n)^{\sqrt{2n}+2}.$$

One can check manually that the result holds for $4 \leq n \leq 16$, so assume that $n > 16$. Taking logarithms, we find that

$$\frac{n}{3} \log 4 < (\sqrt{2n} + 2) \log(2n) < 2\sqrt{n} \log(2n) < 2\sqrt{n} \log(n^{5/4}) < \frac{5}{2} \sqrt{n} \log n.$$

Notice that $\frac{\sqrt{n}}{\log n}$ is increasing for $n > e^2$. Putting this together with the fact that

$$\frac{\sqrt{1600}}{\log 1600} \approx 5.421 > 5.410 \approx \frac{15}{2 \log 4},$$

we have $n \leq 1600$. Finally, we know that $\{2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 557, 1109, 2207\}$ are all primes, where each number in the set is the largest prime less than twice the previous one. Thus, no counterexample exists, and the result holds for all $n \geq 4$. $\square$

## 1.4 Gaps Between Twin Primes

By Theorem 1.16, we have

$$p_{n+1} - p_n \leq p_n$$

as there is a prime between $p_n$ and $2p_n$. What more can we say about differences of consecutive primes?

By the Prime Number Theorem, there are about $x/\log x$ primes $p$ at most $x$. Therefore, the "average gap" between primes $p$ at most $x$ is $\log x$. However, the value of $p_{n+1} - p_n$ can vary widely.

Notice that for any $n \geq 2$, the numbers $n! + k$ for $2 \leq k \leq n$ are all composite. This implies that

$$\limsup_{n\to\infty} (p_{n+1} - p_n) = \infty.$$

In 1931, Weszynthius showed that

$$\limsup_{n\to\infty} \left( \frac{p_{n+1} - p_n}{\log p_n} \right) = \infty.$$

By probabilistic reasoning, Cramer had conjectured in 1936 that

$$\limsup_{n\to\infty} \left( \frac{p_{n+1} - p_n}{(\log p_n)^2} \right) \leq 1.$$

In the 1930s, Erdős proved that for infinitely many integers $n$, we have

$$p_{n+1} - p_n > c \log p_n \frac{\log\log p_n}{(\log\log\log p_n)^2}$$

for some positive constant $c$. In 1938, Rankin added a factor of $\log\log\log\log p_n$.

What about small gaps between consecutive primes? The famous Twin Prime Conjecture states that there are infinitely many $n \in \mathbb{Z}^+$ such that $p_{n+1} - p_n = 2$. Equivalently, it can be stated that

$$\liminf_{n\to\infty} (p_{n+1} - p_n) = 2.$$

If we assume that the primes are randomly distributed and an integer is prime with probability $1/\log x$, then we might expect $x$ and $x + 2$ to both be prime with probability $1/(\log x)^2$.

Therefore, we expect about $x/(\log x)^2$ primes $p$ such that $p + 2$ is also prime and $p \leq x$. A more careful heuristic suggests that there are about $Cx/(\log x)^2$ such primes $p$ where $C > 0$ and $C \neq 1$. In the 1960s, Chen proved that there are more than $0.6x/(\log x)^2$ primes $p$ with $p \leq x$ such that $p + 2$ is a product of at most two primes (called a $P_2$), provided that $x$ is sufficiently large.

In 2005, Goldston, Pintz, and Yildirim showed that

$$\liminf_{n\to\infty} \left( \frac{p_{n+1} - p_n}{\log p_n} \right) = 0.$$

However, this is still quite far from the Twin Prime Conjecture; the bound between consecutive primes can still go to infinity.

Astoundingly, Zhang made a breakthrough in 2013 and showed that

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \leq 7 \cdot 10^7.$$

This was independently improved by Tao and Maynard (via the Polymath Project) in the same year to get

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \leq 246.$$

# 2 Asymptotic Analysis for $\pi(x)$

## 2.1 The Möbius Function

DEFINITION 2.1. Let $f$ and $g$ be functions from $\mathbb{N}$ or $\mathbb{R}^+$ to $\mathbb{R}$, and suppose that $g$ maps to $\mathbb{R}^+$.

(1) We write $f = O(g)$ if there exist constants $c_1, c_2 > 0$ such that for all $x > c_1$, we have $|f(x)| \leq c_2 g(x)$.

(2) We write $f = o(g)$ if $\lim_{n\to\infty} f(n)/g(n) = 0$.

(3) We write $f \sim g$ if $\lim_{n\to\infty} f(n)/g(n) = 1$, and we say that $f$ is **asymptotic** to $g$.

By the Prime Number Theorem, we have $\pi(x) \sim x/\log x$, or equivalently,

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right). \tag{2.1}$$

REMARK 2.2. Let $\varepsilon > 0$. Then the number of primes in the interval $[x, (1+\varepsilon)x]$ is

$$\pi((1+\varepsilon)x) - \pi(x) = \frac{(1+\varepsilon)x}{\log((1+\varepsilon)x)} - \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Notice that

$$\frac{(1+\varepsilon)x}{\log((1+\varepsilon)x)} = \frac{(1+\varepsilon)x}{\log x + \log(1+\varepsilon)} = \frac{(1+\varepsilon)x}{(\log x)(1 + \log(1+\varepsilon)/\log x)} = \frac{(1+\varepsilon)x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Therefore, it follows that

$$\pi((1+\varepsilon)x) - \pi(x) = \frac{(1+\varepsilon)x}{\log x} - \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) = \frac{\varepsilon x}{\log x} + o\left(\frac{x}{\log x}\right).$$

By taking $\varepsilon = 1$, we have

$$\pi(2x) - \pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right). \tag{2.2}$$

Equation (2.2) might look odd together with equation (2.1). Nonetheless, the result is correct; it's just that the bounds in the notation $o$ are different.

DEFINITION 2.3. We define the **Möbius function** on $\mathbb{N}$ by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not squarefree}, \\ (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes.} \end{cases}$$

For example, we have $\mu(48) = \mu(2^4 \cdot 3) = 0$ and $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$.

PROPOSITION 2.4. We have

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where $\sum_{d|n}$ means that the summation runs through the positive divisors $d$ of $n$.

PROOF. The result is true for $n = 1$. For $n > 1$, let $n = p_1^{a_1} \cdots p_r^{a_r}$ be the unique factorization of $n$ into distinct prime numbers. Set $N = p_1 \cdots p_r$ (which is called the **radical** of $n$). Since $\mu(d) = 0$ when $d$ is not squarefree, we have

$$\sum_{d|n} \mu(d) = \sum_{d|N} \mu(d).$$

Note that the divisors of $N$ are in bijective correspondence with the subsets of $\{p_1, \dots, p_r\}$. Since the number of $k$ element subsets is $\binom{r}{k}$ and the corresponding divisor $d$ of such a set satisfies $\mu(d) = (-1)^k$, we have

$$\sum_{d|n} \mu(d) = \sum_{d|N} \mu(d) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1-1)^r = 0. \qquad \square$$

Proposition 2.5 (Möbius Inversion Formula).

(1) For two functions $f, g : \mathbb{R}^+ \to \mathbb{C}$, we have

$$g(x) = \sum_{1 \le n \le x} f(x/n)$$

if and only if

$$f(x) = \sum_{1 \le n \le x} \mu(n) g(x/n).$$

(2) For two functions $f, g : \mathbb{N} \to \mathbb{C}$, we have

$$f(n) = \sum_{d|n} g(d)$$

if and only if

$$g(n) = \sum_{d|n} \mu(d) f(n/d).$$

Proof. This is on Homework 1. $\square$

## 2.2 The von Mangoldt Function

Definition 2.6. We define the **von Mangoldt function** on $\mathbb{N}$ by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for } p \text{ prime and } k \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, for all $x \in \mathbb{R}$, we define the functions

$$\theta(x) = \sum_{p \le x} \log p = \log \prod_{p \le x} p,$$
$$\psi(x) = \sum_{p^k \le x} \log p = \sum_{n \le x} \Lambda(n).$$

Notice that

$$\psi(x) = \sum_{p \le x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p.$$

Since $p^2 \le x$ is equivalent to $p \le x^{1/2}$ and $p^3 \le x$ if and only if $p \le x^{1/3}$, we see that

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots.$$

Note that $\theta(x^{1/m}) = 0$ when $m > \frac{\log x}{\log 2}$. Therefore, we get

$$\psi(x) = \sum_{k=1}^{\left\lfloor \frac{\log x}{\log 2} \right\rfloor} \theta(x^{1/k}).$$

Observe that we have the inequality

$$\theta(x) = \sum_{p \le x} \log p \le x \log x,$$

so it follows that

$$\sum_{k \ge 2} \theta(x^{1/k}) = O\left(x^{1/2}(\log x)^2\right).$$

Therefore, we obtain

$$\psi(x) = \theta(x) + O\left(x^{1/2}(\log x)^2\right)$$

and so by Theorem 1.12, we get

$$\theta(x) = \sum_{p \le x} \log p \le \pi(x) \log x < c_1 x$$

for $x \ge 2$ and a constant $c_1 > 0$. Similarly, one finds that $\psi(x) < c_2 x$ for $x \ge 2$ and a positive constant $c_2$. Furthermore, from the proof of Theorem 1.12, we have $2^n \le \binom{2n}{n}$ and $\binom{2n}{n} \mid \prod_{p \le 2n} p^{r_p}$, where $r_p$ is the integer satisfying $p^{r_p} \le 2n < p^{r_p+1}$. It follows that

$$n \log 2 = \log(2^n) \le \log \binom{2n}{n} \le \sum_{p \le 2n} r_p \log p \le \sum_{p \le 2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log p \le \psi(2n).$$

For $x \ge 2$, choosing $n$ such that $2n \le x < 2n + 2$ gives

$$\psi(x) \ge \psi(2n) \ge n \log 2 > \frac{x-2}{2} \log 2.$$

Hence, we have $\psi(x) > c_3 x$ and $\theta(x) > c_4 x$ for positive constants $c_3$ and $c_4$.

What is the relationship between $\theta(x)$, $\psi(x)$, and $\pi(x)$? We note that

$$\theta(x) = \sum_{p \le x} \log p \le x \log p \le \pi(x) \log x,$$

so it follows that

$$\pi(x) \ge \frac{\theta(x)}{\log x} > c_4 \frac{x}{\log x}.$$

Theorem 2.7. We have

$$\pi(x) \sim \frac{\theta(x)}{\log x} \sim \frac{\psi(x)}{\log x}.$$

Proof. Since $\psi(x) = \theta(x) + O(x^{1/2}(\log x)^2)$ and $\theta(x) > c_4 x$, we see that $\theta(x) \sim \psi(x)$. In particular, we have $\theta(x)/\log x \sim \psi(x)/\log x$, so it only remains to show that $\pi(x) \sim \theta(x)/\log x$.

We have already shown that $\pi(x) \ge \theta(x) \ge \log x$, so

$$\liminf_{n \to \infty} \frac{\pi(x) \log x}{\theta(x)} \ge 1.$$

We need an upper bound for $\pi(x)$ in terms of $\theta(x)$. Note that for any $\delta > 0$, we have

$$\theta(x) = \sum_{p \le x} \log p \ge \log(x^{1-\delta}) \sum_{x^{1-\delta} \le p \le x} 1 \ge (1-\delta)(\log x)\left(\pi(x) - \pi(x^{1-\delta})\right).$$

Since $\pi(y) \le y$ for all real numbers $y > 0$, we get

$$\theta(x) + (1-\delta)x^{1-\delta} \log x \ge (1-\delta)(\log x)\pi(x).$$

Rearranging the above gives

$$\frac{\theta(x)}{(1-\delta)\log x} + x^{1-\delta} \geq \pi(x),$$

and therefore

$$\frac{1}{1-\delta} + \frac{x^{1-\delta}\log x}{\theta(x)} \geq \frac{\pi(x)\log x}{\theta(x)}.$$

Given $\varepsilon > 0$, we can choose $\delta > 0$ such that $\frac{1}{1-\delta} < 1 + \frac{\varepsilon}{2}$, and then pick $x_0$ such that if $x > x_0$, then

$$\frac{x^{1-\delta}\log x}{\theta(x)} < \frac{\varepsilon}{2}$$

since $\theta(x) > c_1 x$ for $x \geq 2$. Then for all $x > x_0$, we have

$$1 \leq \frac{\pi(x)\log x}{\theta(x)} < 1 + \varepsilon,$$

which completes the proof. □

## 2.3 Abel's Summation Formula

We will prove Abel's summation formula and give some of its applications.

Lemma 2.8 (Abel's summation formula). Let $\{a_n\}_{n=1}^{\infty}$ be a sequence of complex numbers. Let $f : \{x \in \mathbb{R} : x \geq 1\} \to \mathbb{C}$ be a function. For all $x \geq 1$, we define

$$A(x) := \sum_{n \leq x} a_n,$$

where the summation runs through all positive integers up to $x$. If $f'$ is continuous at every $x \geq 1$, then

$$\sum_{n \leq x} a_n f(n) = A(x)f(x) - \int_1^x A(u)f'(u)\,\mathrm{d}u.$$

Proof. Set $N = \lfloor x \rfloor$. Note that $a_n = A(n) - A(n-1)$ for all $n \geq 2$, so we can write

$$\begin{aligned}\sum_{n \leq N} a_n f(n) &= A(1)f(1) + (A(2) - A(1))f(2) + \cdots + (A(N) - A(N-1))f(N)\\ &= A(1)(f(1) - f(2)) + \cdots + A(N-1)(f(N-1) - f(N)) + A(N)f(N).\end{aligned}$$

Observe that if $i \in \mathbb{Z}^+$ and $t \in \mathbb{R}$ with $i \leq t < i+1$, then $A(t) = A(i)$. It follows that

$$A(i)(f(i) - f(i+1)) = -\int_i^{i+1} A(u)f'(u)\,\mathrm{d}u.$$

Therefore, we have

$$\sum_{n \leq N} a_n f(n) = -\int_1^N A(u)f'(u)\,\mathrm{d}u + A(N)f(N),$$

so the result holds when $x$ is an integer. Now, notice that $A(t) = A(N)$ for all $x \geq t \geq N$, so we obtain

$$\int_N^x A(u)f'(u)\,\mathrm{d}u = A(x)(f(x) - f(N)) = A(x)f(x) - A(N)f(N).$$

Thus, the result holds for all $x \geq 1$. □

Definition 2.9. Given $x \in \mathbb{R}$, we denote the **fractional part** of $x$ by $\{x\}$; that is,

$$\{x\} := x - \lfloor x \rfloor.$$

We define **Euler's constant** by

$$\gamma := 1 - \int_1^\infty \frac{\{t\}}{t^2}\,\mathrm{d}t = 1 - \int_1^\infty \frac{t - \lfloor t \rfloor}{t^2}\,\mathrm{d}t.$$

Note that $\gamma \approx 0.55721$.

This has not been proven, but it has been conjectured that $\gamma$ is irrational and transcendental.

Theorem 2.10. We have

$$\sum_{n \le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right).$$

Proof. Taking $a_n = 1$ and $f(t) = 1/t$ in Abel's summation formula, we have

$$A(x) = \sum_{n \le x} a_n = \sum_{n \le x} 1 = \lfloor x \rfloor$$

so that

$$\begin{aligned}
\sum_{n \le x} \frac{1}{n} &= \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor u \rfloor}{u^2}\,\mathrm{d}u \\
&= \frac{x - (x - \lfloor x \rfloor)}{x} + \int_1^x \frac{u - (u - \lfloor u \rfloor)}{u^2}\,\mathrm{d}u \\
&= 1 + O\left(\frac{1}{x}\right) + \int_1^x \frac{\mathrm{d}u}{u} - \int_1^x \frac{u - \lfloor u \rfloor}{u^2}\,\mathrm{d}u \\
&= 1 + O\left(\frac{1}{x}\right) + \log x - \left(\int_1^\infty \frac{u - \lfloor u \rfloor}{u^2}\,\mathrm{d}u - \int_x^\infty \frac{u - \lfloor u \rfloor}{u^2}\,\mathrm{d}u\right) \\
&= \log x + \gamma + O\left(\frac{1}{x}\right) + \int_x^\infty \frac{u - \lfloor u \rfloor}{u^2}\,\mathrm{d}u \\
&= \log x + \gamma + O\left(\frac{1}{x}\right) + O\left(\int_x^\infty \frac{1}{u^2}\,\mathrm{d}u\right) \\
&= \log x + \gamma + O\left(\frac{1}{x}\right).
\end{aligned}$$

□

Theorem 2.11. We have

$$\sum_{n \le x} \frac{\Lambda(n)}{n} = \log x + O(1).$$

Proof. First, we apply Abel's summation formula with $a_n = 1$ and $f(n) = \log n$ to get

$$\begin{aligned}
\sum_{n \le x} \log n &= \lfloor x \rfloor \log x - \int_1^x \frac{\lfloor u \rfloor}{u}\,\mathrm{d}u \\
&= (x - (x - \lfloor x \rfloor)) \log x - \int_1^x \frac{u - (u - \lfloor u \rfloor)}{u}\,\mathrm{d}u \\
&= x \log x + O(\log x) - (x - 1) + \int_1^x \frac{u - \lfloor u \rfloor}{u}\,\mathrm{d}u \\
&= x \log x - x + O(\log x).
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
\sum_{n\le x}\log n = \log(\lfloor x\rfloor !) &= \sum_{p\le x}\left(\sum_{k=1}^{\infty}\left\lfloor \frac{x}{p^k}\right\rfloor\right)\log p \\
&= \sum_{p^m\le x}\left\lfloor \frac{x}{p^m}\right\rfloor \log p \\
&= \sum_{n\le x}\left\lfloor \frac{x}{n}\right\rfloor \Lambda(n) \\
&= \sum_{n\le x}\frac{x}{n}\Lambda(n) - \sum_{n\le x}\left(\frac{x}{n}-\left\lfloor\frac{x}{n}\right\rfloor\right)\Lambda(n) \\
&= x\sum_{n\le x}\frac{\Lambda(n)}{n} - O\left(\sum_{n\le x}\Lambda(n)\right).
\end{aligned}$$

Since $\sum_{n\le x}\Lambda(n)=\psi(x)=O(x)$, we have

$$\sum_{n\le x}\log x = x\sum_{n\le x}\frac{\Lambda(n)}{n} - O(n).$$

By the asymptotic formula of $\sum_{n\le x}\log n$ above, we see that

$$x\log x - x + O(\log x) = x\sum_{n\le x}\frac{\Lambda(n)}{n} - O(x).$$

Rearranging and tucking some terms under $O(x)$ gives

$$x\sum_{n\le x}\frac{\Lambda(n)}{n} = x\log x + O(x).$$

Finally, dividing through by $x$ gives

$$\sum_{n\le x}\frac{\Lambda(n)}{n} = \log x + O(1).$$

□

Theorem 2.12. We have

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1).$$

Proof. Note that

$$\sum_{p\le x}\frac{\log p}{p} = \sum_{n\le x}\frac{\Lambda(n)}{n} - \sum_{m\ge 2}\sum_{p^m\le x}\frac{\log p}{p^m} = \log x + O(1) - \sum_{m\ge 2}\sum_{p^m\le x}\frac{\log p}{p^m}.$$

Moreover, we see that

$$\sum_{m\ge 2}\sum_{p^m\le x}\frac{\log p}{p^m} \le \sum_{p}\left(\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)\log p \le \sum_{p}\frac{\log p}{p(p-1)} \le \sum_{n=2}^{\infty}\frac{\log n}{n(n-1)} = O(1),$$

which completes the proof. □

Theorem 2.13 (Merten). There exists a real number $\beta$ such that

$$\sum_{p\le x}\frac{1}{p} = \log\log x + \beta + O\left(\frac{1}{\log x}\right).$$

Proof. We apply Abel's summation formula with

$$a_n = \begin{cases} \frac{\log p}{p} & \text{if } n = p \text{ for a prime } p \\ 0 & \text{otherwise} \end{cases}$$

and $f(n) = 1/\log n$. Setting $A(x) = \sum_{n \le x} a_n$, we have

$$\sum_{p \le x} \frac{1}{p} = \frac{A(x)}{\log x} + \int_1^x \frac{A(u)}{u(\log u)^2}\,\mathrm{d}u.$$

By the preceding theorem, we have

$$A(x) = \sum_{p \le x} \frac{\log p}{p} = \log x + O(1),$$

so we see that

$$\sum_{p \le x} \frac{1}{p} = 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{\log u + \tau(u)}{u(\log u)^2}\,\mathrm{d}u,$$

where $\tau(u) = A(u) - \log u = O(1)$. Therefore, we have

$$\begin{aligned} \sum_{p \le x} \frac{1}{p} &= 1 + O\left(\frac{1}{\log x}\right) + \log\log x - \log\log 2 + \int_2^x \frac{\tau(u)}{u(\log u)^2}\,\mathrm{d}u \\ &= \log\log x + 1 - \log\log 2 + \int_2^\infty \frac{\tau(u)}{u(\log u)^2}\,\mathrm{d}u - \int_x^\infty \frac{\tau(u)}{u(\log u)^2}\,\mathrm{d}u + O\left(\frac{1}{\log x}\right). \end{aligned}$$

By setting $\beta$ to the middle terms above, we are done. □

In fact, we have

$$\beta = \gamma + \sum_p \left[\log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right] \approx 0.261497,$$

and $\beta$ is called **Merten's constant**.

# 3 Riemann's Zeta Function and the Prime Number Theorem

## 3.1 The Riemann Zeta Function

In order to prove the Prime Number Theorem, we need to first introduce the Riemann zeta function.

DEFINITION 3.1. For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, we define the **Riemann zeta function** by

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

We will denote $s = \sigma + it$ where $\sigma, t \in \mathbb{R}$.

Note that the series $\sum_{n=1}^{\infty} n^{-s}$ converges absolutely when $\mathrm{Re}(s) > 1$.

Recall that the infinite product $\prod_n (1 + a_n)$ converges absolutely (that is, it is finite and non-zero) if and only if $\sum_n |a_n|$ converges. We have the **Euler product representation** of $\zeta(s)$ given in the following lemma.

LEMMA 3.2 (Euler product). For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, we have

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

PROOF. Note that

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right).$$

A typical term in the sum is of the form

$$\frac{1}{p_1^{\alpha_1 s} \cdots p_k^{\alpha_k s}} = \frac{1}{(p_1^{\alpha_1} \cdots p_k^{\alpha_k})^s}.$$

By the Fundamental Theorem of Arithmetic, every positive integer can be expressed uniquely as a product of primes, so the identity holds. □

THEOREM 3.3. $\zeta(s)$ can be analytically continued to $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 0$ and $s \neq 1$. It is analytic except at the point $s = 1$ where it has a simple pole with residue 1.

PROOF. For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, we have $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. By Abel's summation formula with $a_n = 1$ and $f(x) = x^{-s}$, we find that

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{\lfloor x \rfloor}{x^s} + s \int_1^x \frac{\lfloor u \rfloor}{u^{s+1}} \, \mathrm{d}u.$$

Letting $x \to \infty$, we obtain

$$\begin{aligned}
\zeta(s) &= 0 + s \int_1^{\infty} \frac{\lfloor u \rfloor}{u^{s+1}} \, \mathrm{d}u \\
&= s \int_1^{\infty} \frac{u - (u - \lfloor u \rfloor)}{u^{s+1}} \, \mathrm{d}u \\
&= s \int_1^{\infty} \frac{u}{u^{s+1}} \, \mathrm{d}u - s \int_1^{\infty} \frac{u - \lfloor u \rfloor}{u^{s+1}} \, \mathrm{d}u \\
&= s \left( \frac{u^{1-s}}{1-s} \bigg|_1^{\infty} \right) - s \int_1^{\infty} \frac{u - \lfloor u \rfloor}{u^{s+1}} \, \mathrm{d}u \\
&= \frac{s}{s-1} - s \int_1^{\infty} \frac{u - \lfloor u \rfloor}{u^{s+1}} \, \mathrm{d}u
\end{aligned}$$

for $\mathrm{Re}(s) > 1$. Note that
$$\int_1^\infty \frac{u - \lfloor u \rfloor}{u^{s+1}}\,\mathrm{d}u$$
converges for $\mathrm{Re}(s) > 0$ and represents an analytic function. Therefore, we see that
$$\frac{s}{s-1} - s\int_1^\infty \frac{u - \lfloor u \rfloor}{u^{s+1}}\,\mathrm{d}u$$
is an analytic function for $\mathrm{Re}(s) > 0$ with $s \neq 1$. This gives a meromorphic continuation of $\zeta(s)$ to the region $\{s \in \mathbb{C} : \mathrm{Re}(s) > 0\}$. Finally, note that $\frac{s}{s-1}$ has a simple pole with residue 1 at $s = 1$. $\square$

THEOREM 3.4. $\zeta(s)$ has no zeroes in the region $\{s \in \mathbb{C} : \mathrm{Re}(s) \geq 1\}$.

PROOF. If $\mathrm{Re}(s) > 1$, then $\prod_p (1 - \frac{1}{p^s})^{-1}$ converges, so $\zeta(s) \neq 0$.

It only remains to consider the case where $\mathrm{Re}(s) = 1$. We will first do some preliminary work.

Recall that we denote $s = \sigma + it$ where $\sigma, t \in \mathbb{R}$. Let $\sigma > 1$. Then for all $t \in \mathbb{R}$, we have
$$\log^*(\zeta(\sigma + it)) = \log\left(\prod_p \left(1 + \frac{1}{p^s}\right)^{-1}\right) = \sum_p \sum_{n=1}^\infty \frac{1}{n}\left(\frac{1}{p^{ns}}\right),$$
where log denotes the principal branch and $\log^*$ denotes some branch of the logarithm (we have to be careful here as we are considering complex numbers). Comparing the real parts of the above equality, we have
$$\log|\zeta(\sigma + it)| = \sum_p \sum_{n=1}^\infty \frac{p^{-\sigma n}\cos(nt\log p)}{n},$$
since we can write
$$p^{-int} = e^{-int\log p} = \cos(-nt\log p) + i\sin(-nt\log p) = \cos(nt\log p) - i\sin(nt\log p)$$
and therefore $\mathrm{Re}(p^{-int}) = \cos(nt\log p)$. Moreover, observe that we have the inequality
$$\begin{aligned} 0 \leq 2(1+\cos\theta)^2 &= 2(1 + 2\cos\theta + \cos^2\theta) \\ &= 2 + 4\cos\theta + 2\cos^2\theta \\ &= 3 + 4\cos\theta + (2\cos^2\theta - 1) \\ &= 3 + 4\cos\theta + \cos(2\theta). \end{aligned}$$
From this, we can deduce that
$$\sum_p \sum_{n=1}^\infty \frac{p^{-\sigma n}}{n}(3 + 4\cos(nt\log p) + \cos(2nt\log p)) \geq 0.$$
Therefore, we have
$$\log|\zeta(\sigma)|^3 + \log|\zeta(\sigma + it)|^4 + \log|\zeta(\sigma + 2it)| \geq 0.$$
In particular, we see that
$$|\zeta(\sigma)|^3 \cdot |\zeta(\sigma + it)|^4 \cdot |\zeta(\sigma + 2it)| \geq 1 \tag{3.1}$$
for $\sigma > 1$ and $t \in \mathbb{R}$.

Suppose now that $1 + it_0$ is a zero of $\zeta(s)$, and note that $t_0 \neq 0$ as $\zeta(s)$ has a pole at $s = 1$. By taking $t \to 1^+$ (that is, from the right), we observe tht
$$|\zeta(s)| = O((\sigma - 1)^{-1})$$

since 1 is a simple pole of $\zeta(s)$. Moreover, since $1+it_0$ is a zero of $\zeta(s)$, we have $|\zeta(\sigma+it_0)| = O(\sigma-1)$ as $\sigma \to 1^+$. Finally, we have $|\zeta(\sigma+2it_0)| = O(1)$ as $\sigma \to 1^+$ since $1+2it_0$ is not a simple pole of $\zeta(s)$. It follows that

$$|\zeta(\sigma)|^3 \cdot |\zeta(\sigma+it)|^4 \cdot |\zeta(\sigma+2it)| = O((\sigma-1)^{-3}) \cdot O((\sigma-1)^4) \cdot O(1) = O(\sigma-1).$$

Thus, $|\zeta(s)|^3 \cdot |\zeta(\sigma+it)|^4 \cdot |\zeta(\sigma+2it)|$ tends to 0 as $\sigma \to 1^+$. But this contradicts that the lower bound we found in (3.1), so we conclude that $\zeta(s)$ cannot have a zero when $\mathrm{Re}(s) = 1$. $\square$

## 3.2 Newman's Theorem

THEOREM 3.5 (Newman). Let $\{a_n\}_{n=1}^{\infty}$ be a sequence of complex numbers with $|a_n| \le 1$ for all $n \ge 1$. Consider the series $\sum_{n=1}^{\infty} a_n/n^s$, which converges to an analytic function $F(s)$ for $\mathrm{Re}(s) > 1$. If $F(s)$ can be analytically continued to $\mathrm{Re}(s) \ge 1$, then $\sum_{n=1}^{\infty} a_n/n^s$ converges to $F(s)$ for $\mathrm{Re}(s) \ge 1$.

PROOF. Let $w \in \mathbb{C}$ with $\mathrm{Re}(w) \ge 1$. Then $F(z+w)$ is analytic for $\mathrm{Re}(z) \ge 0$. Choose $R \ge 1$ and let $\delta = \delta(R) > 0$ so that $F(z+w)$ is analytic on the region

$$\tilde{\Gamma} := \{z \in \mathbb{C} : \mathrm{Re}(z) \ge -\delta \text{ and } |z| \le R\}.$$

To see why such a $\delta > 0$ exists, first note that $F(z+w)$ is analytic for $\mathrm{Re}(z) \ge 0$. Consider the line $L = \{z = iy : |y| \le R\}$. Every point in $L$ has an open cover such that $F(z+w)$ is analytic on that cover; call the union of these covers $U$. Since $L$ is compact[1], there exists a finite open subcover $\tilde{U}$ of $U$ such that $L \subseteq \tilde{U} \subseteq U$. Since the number of open sets in $\tilde{U}$ is finite, it follows that such a $\delta > 0$ exists.

Let $M$ denote the maximum of $|F(z+w)|$ on $\tilde{\Gamma}$, and let $\Gamma$ denote the contour obtained by following the outside of $\tilde{\Gamma}$ in a counterclockwise path. Let $A$ be the part of $\Gamma$ in $\mathrm{Re}(z) > 0$, and let $B = \Gamma \setminus A$. For $N \in \mathbb{N}$, consider the function

$$F(z+w)N^z \left(\frac{1}{z} + \frac{z}{R^2}\right),$$

which is analytic on $\tilde{\Gamma}$ except at $z = 0$ where there is a simple pole with residue $F(0+w)N^0 = F(w)$. By Cauchy's residue theorem, we obtain

$$\begin{aligned} 2\pi i F(w) &= \int_\Gamma F(z+w)N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) \mathrm{d}z \\ &= \int_A F(z+w)N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) \mathrm{d}z + \int_B F(z+w)N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) \mathrm{d}z. \end{aligned} \tag{3.2}$$

Observe that $F(z+w)$ is equal to its series on $A$. We split the series as

$$S_N(z+w) = \sum_{n=1}^{N} \frac{a_n}{n^{z+w}}$$

and $R_N(z+w) = F(z+w) - S_N(z+w)$. Note that $S_N(z+w)$ is analytic for all $z \in \mathbb{C}$. Let $C$ be the contour given by the path $|z| = R$ taken in the counterclockwise direction. By Cauchy's residue theorem, we obtain

$$2\pi i S_N(w) = \int_C S_N(z+w)N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) \mathrm{d}z$$

since the integrand has a simple pole at $z = 0$ with residue $S_N(0+w)N^0 = S_N(w)$. Note that

$$C = A \cup (-A) \cup \{iR, -iR\}.$$

[1]Recall that a set $X$ is compact if every open cover of $X$ has a finite subcover.

Therefore, we see that

$$2\pi i S_N(w) = \int_A S_N(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)\,\mathrm{d}z + \int_{-A} S_N(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)\,\mathrm{d}z.$$

Consider the second integral above. Using the change of variables $z \to -z$, we find that

$$\int_{-A} S_N(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)\,\mathrm{d}z = \int_A S_N(-z+w)N^{-z}\left(\frac{1}{z}+\frac{z}{R^2}\right)\,\mathrm{d}z.$$

Thus, we obtain

$$2\pi i S_N(w) = \int_A \left(S_N(z+w)N^z + S_N(-z+w)N^{-z}\right)\left(\frac{1}{z}+\frac{z}{R^2}\right)\,\mathrm{d}z.$$

Combining the above equality with (3.2), we have

$$\begin{aligned}2\pi i(F(w)-S_N(w)) &= \int_A \left(R_N(z+w)N^z - S_N(-z+w)N^{-z}\right)\left(\frac{1}{z}+\frac{z}{R^2}\right)\,\mathrm{d}z \\ &\quad + \int_B F(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)\,\mathrm{d}z. \qquad (3.3)\end{aligned}$$

Our goal is to show that $S_N(w)$ converges to $F(w)$ as $N\to\infty$. Write $z = x+iy$ where $x, y\in\mathbb{R}$. Then for $z\in A$, we have $x>0$ and $|z| = R$, so

$$\frac{1}{z}+\frac{z}{R^2} = \frac{x-iy}{R^2}+\frac{x+iy}{R^2} = \frac{2x}{R^2}.$$

Since $|n^z| = n^x$, we have

$$|R_N(z+w)| \le \sum_{n=N+1}^{\infty}\frac{1}{n^{\mathrm{Re}(z+w)}} \le \sum_{n=N+1}^{\infty}\frac{1}{n^{x+1}} \le \int_N^\infty \frac{1}{u^{x+1}}\,\mathrm{d}u = \frac{1}{xN^x}.$$

Also, we have

$$|S_N(-z+w)| \le \sum_{n=1}^{N}\frac{1}{n^{-x+1}} \le N^{x-1} + \int_1^N u^{x-1}\,\mathrm{d}u \le N^{x-1} + \frac{N^x}{x} = N^x\left(\frac{1}{N}+\frac{1}{x}\right).$$

Putting the above estimates together, we get

$$\begin{aligned}\left|\int_A \left(R_N(z+w)N^z - S_N(-z+w)N^{-z}\right)\left(\frac{1}{z}+\frac{z}{R^2}\right)\,\mathrm{d}z\right| &\le \int_A\left(\frac{1}{xN^x}N^x + N^x\left(\frac{1}{N}+\frac{1}{x}\right)N^{-x}\right)\frac{2x}{R^2}\,\mathrm{d}z \\ &= \int_A\left(\frac{2}{x}+\frac{1}{N}\right)\frac{2x}{R^2}\,\mathrm{d}z \\ &= \int_A\left(\frac{4}{R^2}+\frac{2x}{NR^2}\right)\mathrm{d}z \\ &\le \pi R\left(\frac{4}{R^2}+\frac{2}{NR}\right) \quad \text{(since } x\le R\text{)} \\ &\le \frac{4\pi}{R}+\frac{2\pi}{N}.\end{aligned}$$

We now estimate the integral along $B$. We can divide $B$ into two parts; one part with $\mathrm{Re}(z) = -\delta$, and the other with $-\delta < \mathrm{Re}(z) \le 0$. For $z\in B$ with $\mathrm{Re}(z) = -\delta$, we use the fact that $|z|\le R$ to find that

$$\left|\frac{1}{z}+\frac{z}{R^2}\right| = \left|\frac{1}{z}\right|\left|\frac{\bar{z}}{z}+\frac{z\bar{z}}{R^2}\right| \le \frac{1}{\delta}\left(1+\frac{|z|^2}{R^2}\right) \le \frac{2}{\delta}.$$

Since $|F(z+w)| \leq M$ for $z \in B$, we have

$$\begin{aligned}
\left|\int_B F(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)\mathrm{d}z\right| &\leq \int_{-R}^{R} MN^{-\delta}\frac{2}{\delta}\,\mathrm{d}z + 2\left|\int_{-\delta}^{0} MN^x\frac{2x}{R^2}\,\mathrm{d}x\right| \\
&= \frac{4MR}{\delta N^\delta} + \frac{4M}{R^2}\left|\int_{-\delta}^{0} xN^x\,\mathrm{d}x\right| \\
&\leq \frac{4MR}{\delta N^\delta} + \frac{4M\delta}{R^2}\left(\frac{1}{(\log N)^2} - \frac{\delta+1}{N^\delta \log N}\right) \\
&\leq \frac{4MR}{\delta N^\delta} + \frac{4M\delta}{R^2(\log N)^2}.
\end{aligned}$$

Combining this estimate with (3.2) and (3.3) yields

$$|2\pi i(F(w) - S_N(w))| \leq \frac{4\pi}{R} + \frac{2\pi}{N} + \frac{4MR}{\delta N^\delta} + \frac{4M\delta}{R^2(\log N)^2}.$$

That is, we have

$$|F(w) - S_N(w)| \leq \frac{2}{R} + \frac{1}{N} + \frac{MR}{\delta N^\delta} + \frac{M\delta}{R^2(\log N)^2}.$$

Given $\varepsilon > 0$, choose $R = 3/\varepsilon$. Then for sufficiently large $N$, we have

$$|F(w) - S_N(w)| < \varepsilon.$$

This implies that $S_N(w) \to F(w)$ as $N \to \infty$, which completes the proof. □

## 3.3 Revisiting the Möbius Function

Recall that we defined the Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not squarefree}, \\ (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes.} \end{cases}$$

We will show on Homework 2 that for $\mathrm{Re}(s) > 1$, we have

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

THEOREM 3.6. We have

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0.$$

PROOF. For all $\mathrm{Re}(s) > 1$, equation (3.4) holds. Moreover, we have shown that $(s-1)\zeta(s)$ is analytic and non-zero in $\mathrm{Re}(s) \geq 1$, so $1/\zeta(s)$ is analytic on $\mathrm{Re}(s) \geq 1$. Now, $\zeta(s)$ can be analytically continued up to $\mathrm{Re}(s) > 0$ and it is nonzero for $\mathrm{Re}(s) \geq 1$, so we see that the series

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

converges to $1/\zeta(s)$ for $\mathrm{Re}(s) \geq 1$. In particular, it converges at $s = 1$. But $\zeta(s)$ has a simple pole at $s = 1$, so $1/\zeta(1) = 0$. □

THEOREM 3.7. We have

$$\sum_{n\le x}\mu(n)=o(x).$$

PROOF. Applying Abel's summation formula with $a_n=\mu(n)/n$ and $f(x)=x$, we obtain

$$\sum_{n\le x}\mu(n)=A(x)x-\int_1^x A(u)\,\mathrm{d}u,$$

where we hae

$$A(t)=\sum_{n\le t}\frac{\mu(n)}{n}.$$

By Theorem 3.5, we know that $A(t)=o(1)$. It follows that $A(x)x=o(x)$ and

$$\int_1^x A(u)\,\mathrm{d}u=o(x),$$

so the result holds. □

## 3.4 Divisor Function

DEFINITION 3.8. For a positive integer $n\in\mathbb{N}$, let $d(n)$ be the number of positive integers that divide $n$.

For example, we have $d(1)=1$, $d(4)=3$, and $d(p)=2$ for all primes $p$.

THEOREM 3.9. We have

$$\sum_{m=1}^{n}d(m)=\sum_{m=1}^{n}\left\lfloor\frac{n}{m}\right\rfloor=n\log n+(2\gamma-1)n+O(n^{1/2}).$$

where $\gamma$ denotes Euler's constant.

PROOF. Let $D_n$ be the region in the upper right-hand quadrant not containing the $x$ or $y$ axes, which is under and includes the hyperbola $xy=n$. That is,

$$D_n:=\{(x,y)\in\mathbb{R}^2:x>0,\,y>0,\,xy\le n\}.$$

Define a **lattice point** to be a point in the plane with integer coordinates; that is, a point $(x,y)\in\mathbb{R}^2$ with $x,y\in\mathbb{Z}$. Notice that every lattice point in $D_n$ is contained in some hyperbola $xy=s$ where $s$ is an integer with $1\le s\le n$.

Therefore, $\sum_{s=1}^{n}d(s)$ is the number of lattice points in $D_n$; that is,

$$\sum_{s=1}^{n}d(s)=\#\{(x,y)\in\mathbb{R}^2:x,y\in\mathbb{N},\,xy\le n\}.$$

We now count the number of lattice points in a different way. Given $x\in\mathbb{N}$ with $1\le x\le n$, there are exactly $\lfloor\frac{x}{n}\rfloor$ many integers $y$ such that $xy\le n$. Thus, we see that

$$\#\{(x,y)\in\mathbb{R}^2:x,y\in\mathbb{N},\,xy\le n\}=\sum_{x=1}^{n}\left\lfloor\frac{n}{x}\right\rfloor.$$

Observe that the number of lattice points above the line $x=y$ inside $D_n$ is equal to the number of lattice points below it. Divide the lattice points in $D_n$ into three disjoint regions given by

$$\begin{aligned}D_{n,1}&=\{(x,y)\in\mathbb{N}^2:xy\le n,\,x<y\},\\D_{n,2}&=\{(x,y)\in\mathbb{N}^2:xy\le n,\,x>y\},\\D_{n,3}&=\{(x,y)\in\mathbb{N}^2:xy\le n,\,x=y\}.\end{aligned}$$

Our observation above shows that $|D_{n,1}| = |D_{n,2}|$. Suppose that $(x, y) \in D_{n,1}$. Then $x^2 < xy \leq n$, which implies that $x < \sqrt{n}$. Moreover, for a fixed integer $x$, the number of integers $y$ satisfying $xy \leq n$ and $y > x$ is $\lfloor \frac{n}{x} \rfloor - \lfloor x \rfloor$. We also see that $|D_{n,3}| = \lfloor \sqrt{n} \rfloor$, so we obtain

$$\begin{aligned}\sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor &= |D_{n,1}| + |D_{n,2}| + |D_{n,3}| \\ &= 2 \sum_{x=1}^{\lfloor \sqrt{n} \rfloor} \left( \left\lfloor \frac{n}{x} \right\rfloor - \lfloor x \rfloor \right) + \lfloor \sqrt{n} \rfloor \\ &= 2 \sum_{x=1}^{\lfloor \sqrt{n} \rfloor} \left( \frac{n}{x} - x + O(1) \right) + \lfloor \sqrt{n} \rfloor.\end{aligned}$$

By Theorem 2.10, we see that

$$\sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor = 2n \left( \log \lfloor \sqrt{n} \rfloor + \gamma + O\left( \frac{1}{\sqrt{n}} \right) \right) - \left( n + O(\sqrt{n}) \right) + O(\sqrt{n}).$$

Note that if we use the fact that $\log \lfloor \sqrt{n} \rfloor = \log \sqrt{n} + O(1)$, then the resulting error term $O(n)$ will be too large. Therefore, we need a finer estimate. Indeed, since $\lfloor \sqrt{n} \rfloor = \sqrt{n} - \{\sqrt{n}\}$ where $\{t\}$ denotes the fractional part of $t$ for $t \in \mathbb{R}$, we have

$$\begin{aligned}\log \lfloor \sqrt{n} \rfloor = \log \left( \sqrt{n} - \{\sqrt{n}\} \right) &= \log \left( \sqrt{n} \left( 1 - \frac{\{\sqrt{n}\}}{\sqrt{n}} \right) \right) \\ &= \log \sqrt{n} + \log \left( 1 - \frac{\{\sqrt{n}\}}{\sqrt{n}} \right) \\ &= \log \sqrt{n} + O\left( \frac{1}{\sqrt{n}} \right).\end{aligned}$$

Combining this with the previous equality gives

$$\sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor = n \log n + (2\gamma - 1)n + O(\sqrt{n}).$$

□

## 3.5 The Prime Number Theorem

We now have everything we need to prove the Prime Number Theorem.

Theorem 3.10 (Prime Number Theorem). We have

$$\pi(x) \sim \frac{x}{\log x}.$$

Proof. In Theorem 2.7, we showed that

$$\pi(x) \sim \frac{\psi(x)}{\log x}.$$

Therefore, it suffices to show that $\psi(x) \sim x$. Define the function

$$F(x) = \sum_{n \leq x} \left( \psi\left( \frac{x}{n} \right) - \left\lfloor \frac{x}{n} \right\rfloor + 2\gamma \right),$$

where $\gamma$ denotes Euler's constant. By the Möbius inversion formula (Proposition 2.5), we have

$$\psi(x) - \lfloor x \rfloor + 2\gamma = \sum_{n \leq x} \mu(n) F\left( \frac{x}{n} \right).$$

In particular, we get
$$\psi(x) = x + O(1) + \sum_{n\le x} \mu(n) F\left(\frac{x}{n}\right).$$
Now, it is enough to show that $\sum_{n\le x} \mu(n)F(x/n) = o(x)$. First, we will estimate $F(x)$. Observe that
$$F(x) = \sum_{n\le x} \psi\left(\frac{x}{n}\right) - \sum_{n\le x}\left\lfloor \frac{x}{n}\right\rfloor + 2\gamma\lfloor x\rfloor. \tag{3.4}$$
Looking at the first sum in (3.4), we have
$$\begin{aligned}
\sum_{n\le x} \psi\left(\frac{x}{n}\right) &= \sum_{n\le x}\sum_{m\le \frac{x}{n}} \Lambda(m) \\
&= \sum_{n\le x} \Lambda(n) \sum_{m\le \frac{x}{n}} 1 \\
&= \sum_{n\le x} \Lambda(n)\left\lfloor \frac{x}{n}\right\rfloor \\
&= \sum_{p^k\le x} \log p \left\lfloor \frac{x}{p^k}\right\rfloor \\
&= \sum_{p\le x} \left(\left\lfloor \frac{x}{p}\right\rfloor + \left\lfloor \frac{x}{p^2}\right\rfloor + \cdots + \left\lfloor \frac{x}{p^k}\right\rfloor\right) \quad (\text{where } p^k \parallel \lfloor x\rfloor) \\
&= \log(\lfloor x\rfloor !) = \sum_{n\le x}\log n.
\end{aligned}$$
In the proof of Theorem 2.11, we showed that
$$\sum_{n\le x}\log n = x\log x - x + O(\log x).$$
Hence, we obtain
$$\sum_{n\le x} \psi\left(\frac{x}{n}\right) = x\log x - x + O(\log x). \tag{3.5}$$
Moreover, by Theorem 3.9, we have
$$\sum_{n=1}^{\lfloor x\rfloor}\left\lfloor \frac{\lfloor x\rfloor}{n}\right\rfloor = \lfloor x\rfloor \log\lfloor x\rfloor + (2\gamma - 1)\lfloor x\rfloor + O(x^{1/2}).$$
For all $y \in \mathbb{R}$, notice that $\lfloor y\rfloor \le y \le \lfloor y\rfloor + 1$. In particular, we obtain the inequalities
$$\sum_{n=1}^{\lfloor x\rfloor}\left\lfloor \frac{\lfloor x\rfloor}{n}\right\rfloor \le \sum_{n=1}^{\lfloor x\rfloor}\left\lfloor \frac{x}{n}\right\rfloor \le \sum_{n=1}^{\lfloor x\rfloor+1}\left\lfloor \frac{\lfloor x\rfloor + 1}{n}\right\rfloor,$$
and it follows that
$$\sum_{n=1}^{\lfloor x\rfloor}\left\lfloor \frac{x}{n}\right\rfloor = x\log x + (2\gamma - 1) + O(x^{1/2}). \tag{3.6}$$
Combining equations (3.4), (3.5), and (3.6) gives
$$F(x) = (x\log x - x + O(\log x)) - (x\log x + (2\gamma-1)x + O(x^{1/2})) + (2\gamma x + O(1)) = O(x^{1/2}).$$
Therefore, there exists a positive constant $c > 0$ such that
$$|F(x)| \le cx^{1/2}$$

for all $x \geq 1$. If $t > 1$ is an integer, then

$$\begin{aligned}
\left|\sum_{n \leq \frac{x}{t}} \mu(n) F\left(\frac{x}{n}\right)\right| &\leq \sum_{n \leq \frac{x}{t}} \left|F\left(\frac{x}{n}\right)\right| \\
&\leq \sum_{n \leq \frac{x}{t}} c\left(\frac{x}{n}\right)^{1/2} \\
&\leq cx^{1/2}\left(1 + \int_1^{x/t} \frac{1}{u^{1/2}}\, \mathrm{d}u\right) \\
&= cx^{1/2}\left(1 + 2\left(\frac{x}{t}\right)^{1/2} - 2\right) \\
&\leq 2 \cdot \frac{cx}{t^{1/2}}. \qquad (3.7)
\end{aligned}$$

Observe that $F$ is a step function. That is, if $a$ is an integer and $a \leq x < a+1$, then $F(x) = F(a)$. Therefore, we have

$$\sum_{\frac{x}{t} < n \leq x} \mu(n) F\left(\frac{x}{n}\right) = F(1) \sum_{\frac{x}{2} < n \leq x} \mu(n) + F(2) \sum_{\frac{x}{3} < n \leq \frac{x}{2}} \mu(n) + \cdots + F(t-1) \sum_{\frac{x}{t} < n \leq \frac{x}{t-1}} \mu(n).$$

We see that

$$\begin{aligned}
\left|\sum_{\frac{x}{t} < n \leq x} \mu(n) F\left(\frac{x}{n}\right)\right| &\leq |F(1)| \left|\sum_{\frac{x}{2} < n \leq x} \mu(n)\right| + |F(2)| \left|\sum_{\frac{x}{3} < n \leq \frac{x}{2}} \mu(n)\right| + \cdots + |F(t-1)| \left|\sum_{\frac{x}{t} < n \leq \frac{x}{t-1}} \mu(n)\right| \\
&\leq (|F(1)| + \cdots + |F(t-1)|) \max_{2 \leq i \leq t} \left|\sum_{\frac{x}{i} < n \leq \frac{x}{i-1}} \mu(n)\right| \\
&\leq \left(\sum_{i=1}^{t} ci^{1/2}\right) \max_{2 \leq i \leq t} \left|\sum_{\frac{x}{i} < n \leq \frac{x}{i-1}} \mu(n)\right|.
\end{aligned}$$

Notice that

$$\sum_{\frac{x}{i} < n \leq \frac{x}{i-1}} \mu(n) = \sum_{n \leq \frac{x}{i-1}} \mu(n) - \sum_{\frac{x}{i} < n} \mu(n) = o(x),$$

so we obtain

$$\left|\sum_{\frac{x}{t} < n \leq x} \mu(n) F\left(\frac{x}{n}\right)\right| = o(t^{3/2} x).$$

By Theorem 3.7, we have $\sum_{n \leq x} \mu(n) = o(x)$. Hence, for any $\varepsilon > 0$, we can find sufficiently large $x$ such that

$$-\varepsilon x \leq \sum_{n \leq x} \mu(n) \leq \varepsilon x.$$

In particular, when $x$ is sufficiently large, we get

$$-\frac{\varepsilon x}{i-1} - \frac{\varepsilon x}{i} \leq \sum_{\frac{x}{i} < n \leq \frac{x}{i-1}} \mu(n) \leq \frac{\varepsilon x}{i-1} + \frac{\varepsilon x}{i}.$$

For any given $\varepsilon > 0$, choose $t = t(\varepsilon)$ such that

$$\frac{2c}{t^{1/2}} < \frac{\varepsilon}{2}.$$

By equation (3.7), we have

$$\left|\sum_{n\le \frac{x}{t}} \mu(n)F\left(\frac{x}{n}\right)\right| \le 2\cdot\frac{cx}{t^{1/2}} < \frac{\varepsilon}{2}x. \tag{3.8}$$

For fixed $\varepsilon > 0$ and $t$ as above, we can choose $x$ sufficiently large so that $o(xt^{3/2}) \le \varepsilon x/2$. Indeed, we have $2c/t^{1/2} < \varepsilon/2$ if and only if $t > (4c)^2/\varepsilon^2$. In particular, we have $t = A^2\varepsilon^{-2}$ for some $A > 4c$, and we can pick $x$ large enough so that

$$o(x) \le \frac{\varepsilon^4}{2A^3}x.$$

Then we get

$$o(xt^{3/2}) \le \frac{\varepsilon^4}{2A^3}x\cdot A^3\varepsilon^{-3} = \frac{\varepsilon}{2}x.$$

It follows that

$$\left|\sum_{\frac{x}{t}<n\le x} \mu(n)F\left(\frac{x}{n}\right)\right| < \frac{\varepsilon}{2}. \tag{3.9}$$

Combining inequalities (3.8) and (3.9) yields

$$\left|\sum_{n\le x} \mu(n)F\left(\frac{x}{n}\right)\right| = o(x),$$

which completes the proof. □

Remark 3.11.

(1) In 1896, Hadamard and de la Vallée Poussin proved the Prime Number Theorem independently. Consider the logarithmic integral

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\,\mathrm{d}t \sim \frac{x}{\log x}\sum_{k=0}^{\infty}\frac{k!}{(\log x)^k}.$$

In 1899, de la Vallée Poussin proved that as $x \to \infty$, there exists some $a > 0$ such that

$$\pi(x) = \mathrm{Li}(x) + O(xe^{-a\sqrt{\log x}}).$$

(2) The main ingredient of our proof of the Prime Number Theorem is the fact that $\sum_{n\le x}\mu(n) = o(x)$, which is a consequence of the analytic continuation and non-vanishing of $\zeta(s)$ at $\mathrm{Re}(s) = 1$. The **Riemann hypothesis**, proposed by Riemann in 1859, states that the non-trivial zeros of $\zeta(s)$ all have real part $1/2$. (The trivial zeros of $\zeta(s)$ are of the form $2n$ for $n \in \mathbb{Z}$ and $n < 0$; these can be obtained by functional equations.) In 1901, Helge von Koch proved that the Riemann hypothesis is true if and only if

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x).$$