Math 782: Analytic Number Theory
(Instructor's Notes)*

Analytic Versus Elementary:

• Terminology (Analytic Number Theory makes use of Complex Analysis and Elementary Number Theory does not; but it isn't so simple to distinguish.)

• Writing an integer as a sum of two squares. This is the first of a few examples of how Complex Analysis can be used to answer a question seemingly unrelated to it: if a and b are sums of 2 squares, why must ab be also?

• Coverings. A *covering* of the integers is a system of congruences $x \equiv a_j \pmod{m_j}$ such that every integer satisfies at least one of these congruences. A *perfect covering* is one in which each integer satisfies exactly one of the congruences. Suppose we have a *finite* perfect covering of the integers with each modulus $m_j > 1$. Show that the largest modulus occurs twice. Use that

$$\frac{1}{1-z} = \sum_{j=1}^{r} \frac{z^{a_j}}{1-z^{m_j}} \qquad \text{for } |z| < 1,$$

where $1 < m_1 \le m_2 \le \cdots \le m_r$ and $0 \le a_j < m_j$. Suppose that $m_{r-1} \ne m_r$. Then the right-hand side, and not the left-hand side, gets large (in absolute value) as z approaches $\exp(2\pi i/m_r)$. The contradiction implies $m_{r-1} = m_r$.

• Preliminaries on exponentials. The following are useful formulas:

$$\sum_{j=0}^{n-1} e^{(i2\pi k/n)j} = \begin{cases} 0 & \text{if } k \ne 0 \\ n & \text{if } k = 0, \end{cases}$$

$$\int_0^1 e^{i2\pi k\theta}\, d\theta = \frac{1}{2\pi} \int_0^{2\pi} e^{ik\theta}\, d\theta = \begin{cases} 0 & \text{if } k \ne 0 \\ 1 & \text{if } k = 0. \end{cases}$$

• Putnam Problem A-6, 1985. If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ is a polynomial with real coefficients a_j, then set $\Gamma(p(x)) = a_0^2 + a_1^2 + \cdots + a_m^2$. Let $f(x) = 3x^2 + 7x + 2$. Find, with proof, a polynomial $g(x)$ with real coefficients such that (i) $g(0) = 1$, and (ii) $\Gamma(f(x)^n) = \Gamma(g(x)^n)$ for all positive integers n.

There are perhaps better ways to do this problem, but we use what we just learned to establish

$$\Gamma(p(x)) = \int_0^1 p\left(e^{2\pi i\theta}\right) p\left(e^{-2\pi i\theta}\right)\, d\theta.$$

Note that $f(x) = (3x+1)(x+2)$. That $g(x) = 6x^2 + 5x + 1 = (3x+1)(2x+1)$ provides a solution follows from

$$\Gamma\left(f(x)^n\right) = \int_0^1 f\left(e^{2\pi i\theta}\right)^n f\left(e^{-2\pi i\theta}\right)^n\, d\theta$$

*These notes are from a course taught by Michael Filaseta in the Fall of 1996.

$$= \int_0^1 \left(3e^{2\pi i\theta}+1\right)^n \left(e^{2\pi i\theta}+2\right)^n \left(3e^{-2\pi i\theta}+1\right)^n \left(e^{-2\pi i\theta}+2\right)^n \, d\theta$$

$$= \int_0^1 \left(3e^{2\pi i\theta}+1\right)^n \left(2e^{2\pi i\theta}+1\right)^n \left(3e^{-2\pi i\theta}+1\right)^n \left(2e^{-2\pi i\theta}+1\right)^n \, d\theta$$

$$= \int_0^1 g\left(e^{2\pi i\theta}\right)^n g\left(e^{-2\pi i\theta}\right)^n \, d\theta$$

$$= \Gamma\left(g(x)^n\right).$$

• A Geometric Problem. Let R be a rectangle, and suppose R can be expressed as a union of rectangles R_j with edges parallel to R and common points only along these edges. Suppose each R_j has at least one edge of integer length. Then R itself must have an edge of integer length.

Let R be positioned so that it is in the first quadrant of the xy-plane, with an edge on each of the x and y axes. Let R_j have bottom left-hand corner (u_j, v_j), and let α_j and β_j be the horizontal and vertical dimensions of R_j respectively. Observe that

$$\left| \int_w^{w+\gamma} e^{2\pi i t}\, dt \right| = \frac{1}{2\pi} \left| e^{2\pi i\gamma} - 1 \right| = 0 \qquad \Longleftrightarrow \qquad \gamma \in \mathbb{Z}.$$

One uses that one of α_j and β_j is an integer for each j and that

$$\left| \int\!\!\int_R e^{2\pi i(x+y)}\, dx\, dy \right| = \left| \sum_{j=1}^{r} \int\!\!\int_{R_j} e^{2\pi i(x+y)}\, dx\, dy \right|$$

to obtain the desired result.

Homework:

(1) (a) If a and b are integers which can each be expressed in the form x^2+5y^2 for some integers x and y, explain why it is possible to express ab in this form as well.

(b) Determine whether the following is true: *if a and b are integers and ab can be expressed in the form x^2+5y^2 with x and y integers, then either a or b can be as well.* Either prove the result or give a counterexample.

(2) (Putnam Problem A-5, 1985) For m a positive integer, define

$$I_m = \int_0^{2\pi} \cos x \cos(2x) \cos(3x) \cdots \cos(mx)\, dx.$$

(a) Use one of the preliminary results above (yes, you must to get credit for the problem) to determine with proof for which integers m with $1 \le m \le 10$ we have $I_m \neq 0$. (Hint: Use that $\cos x = (e^{ix} + e^{-ix})/2$.)

(b) Generalize part (a). In other words, determine which positive integers m are such that $I_m \neq 0$. The answer should be in the form: $I_m \neq 0$ if and only if $m \equiv u \pmod{v}$ where v is an integer and u is a list of integers. Justify your answer.

Elementary Aspects:

- The Fundamental Theorem of Arithmetic (the atoms of which the matter called integers is made are "primes")

- There are infinitely many primes (Give three proofs: (i) Euclid's, (ii) $2^{2^n}+1$ is divisible by a prime $> 2^{n+1}$, and (iii) $\prod_p (1-1/p^2)^{-1} = \pi^2/6$, an irrational number.)

- Explain the notion of rearranging the terms of a series as well as the following lemmas about absolute convergence.

Lemma 1. *If the terms of an absolutely converging series $\sum_{n=1}^{\infty} a_n$ with $a_n \in \mathbb{C}$ are rearranged, then the value of the series remains unchanged. On the other hand, if the series $\sum_{n=1}^{\infty} a_n$ with $a_n \in \mathbb{R}$ converges but not absolutely, then any real value can be obtained from an appropriate rearrangement of the series.*

Use the example of the alternating harmonic series $\sum_{n=1}^{\infty} (-1)^{n+1}/n$ to illustrate the second half of the lemma (and to give the first half more meaning). For the first half, let $S = \sum_{n=1}^{\infty} a_n$ and let $\sum_{n=1}^{\infty} a'_n$ be a rearrangement of it. Let $\varepsilon > 0$. Fix n_0 such that $\sum_{n>n_0} |a_n| < \varepsilon$. Let N be sufficiently large so that the terms $a_1, \ldots, a_{n_0}$ appear among $a'_1, \ldots, a'_N$. Then

$$\left| \sum_{n=1}^{N} a'_n - S \right| \leq \sum_{n>n_0} |a_n| < \varepsilon.$$

The first part of the lemma follows.

Lemma 2. *The product of two absolutely converging series converges absolutely.*

The product of $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ is $\sum_{n=2}^{\infty} c_n$ where $c_n = \sum_{k=1}^{n-1} a_k b_{n-k}$. The result follows since $\sum_{n=2}^{N} |c_n|$ is an increasing function of N bounded above by

$$\left(\sum_{n=1}^{N} |a_n| \right) \left(\sum_{n=1}^{N} |b_n| \right) \leq \left(\sum_{n=1}^{\infty} |a_n| \right) \left(\sum_{n=1}^{\infty} |b_n| \right).$$

In fact, $\sum_{k=1}^{\infty} \sum_{\ell=1}^{\infty} |a_k b_\ell|$ converges. Lemma 2 is of interest but is not really needed in what follows.

Homework:

(1) Let $f : (\mathbb{Z}^+)^2 \mapsto \mathbb{C}$. We say that the iterated series

$$\sum_{n=1}^{\infty} \sum_{m=1}^{\infty} f(m,n) = \sum_{n=1}^{\infty} \left(\sum_{m=1}^{\infty} f(m,n) \right)$$

converges if for each positive integer n, the series $\sum_{m=1}^{\infty} f(m,n)$ converges, and if

$$\lim_{N\to\infty} \sum_{n=1}^{N} \left(\sum_{m=1}^{\infty} f(m,n) \right)$$

exists. The value of this limit is called the value of the iterated series. We say that the double series

$$\sum_{\substack{1\le n<\infty \\ 1\le m<\infty}} f(m,n)$$

converges if there is an S such that for every $\varepsilon > 0$, there exists a $K = K(\varepsilon)$ such that if N and M are positive integers $\ge K$, then

$$\left| \left(\sum_{n=1}^{N} \sum_{m=1}^{M} f(m,n) \right) - S \right| < \varepsilon.$$

The number S is called the value of the double series. Suppose the double series is absolutely convergent, in other words that $\sum_{1\le n<\infty,\ 1\le m<\infty} |f(m,n)|$ converges. Prove that each of

$$\sum_{\substack{1\le n<\infty \\ 1\le m<\infty}} f(m,n), \quad \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} f(m,n), \quad \text{and} \quad \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} f(m,n)$$

converges and that their three values are equal.

- Euler's product identity, namely

$$\prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{for } s > 1.$$

Let $P(x)$ denote the product above restricted to primes $p \le x$. Use Lemma 1 to show

$$\sum_{n=1}^{[x]} \frac{1}{n^s} \le P(x) \le \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The identity follows.

- First proof that $\sum_p 1/p$ diverges.

Assume not. Fix N such that $\sum_{p>N} 1/p < 1/2$. Then

$$\prod_{p\le N} \left(1 - \frac{1}{p}\right)^{-1} \left(1 + \sum_{p>N} \frac{1}{p} + \left(\sum_{p>N} \frac{1}{p}\right)^2 + \cdots \right) \ge \sum_{n=1}^{M} \frac{1}{n}$$

for any $M > 0$. This is a contradiction (the left-hand side is finite).

- Logarithms and $\prod_{n=1}^{\infty}(1-a_n)$.

Suppose that $0 \le a_n \le 1/2$. This condition implies

$$(*) \qquad \sum_{k=2}^{\infty} \frac{a_n^k}{k} \le \sum_{k=2}^{\infty} a_n^k \le 2a_n^2 \le a_n.$$

We use

$$\log(1-x) = -\sum_{k=1}^{\infty} \frac{x^k}{k} \qquad \text{for } |x| < 1 \text{ (actually for } -1 \le x < 1).$$

Observe that

$$\log \prod_{n=1}^{N}(1-a_n) = \sum_{n=1}^{N} \log(1-a_n) \ge -2\sum_{n=1}^{N} a_n.$$

The left-hand side is decreasing so that if $\sum_{n=1}^{\infty} a_n$ converges, then so does $\prod_{n=1}^{\infty}(1-a_n)$. The inequality $\log\prod_{n=1}^{N}(1-a_n) \le -\sum_{n=1}^{N} a_n$ implies that if $\prod_{n=1}^{\infty}(1-a_n)$ converges, then so does $\sum_{n=1}^{\infty} a_n$.

- The estimate $\prod_{p\le x}\left(1-\dfrac{1}{p}\right) \le \dfrac{1}{\log x}$.

Use

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} \ge \sum_{n=1}^{[x]} \frac{1}{n} \ge \int_1^x \frac{1}{t}\,dt = \log x.$$

- Second proof that $\sum_p 1/p$ diverges.

Let $P(x) = \prod_{p\le x}(1-(1/p))^{-1}$ and $S(x) = \sum_{p\le x} 1/p$. Then by $(*)$

$$\log P(x) = S(x) + E \qquad \text{where} \qquad 0 \le E \le 2\sum_{p\le x}\frac{1}{p^2} \le 2.$$

The result follows since $P(x) \ge \log x$. (Note: we have found a "good" lower bound for $\sum_{p\le x} 1/p$.)

- A noteworthy example.

The product $\prod_p(1-(1/p))$ and $\sum_{n=1}^{\infty}\mu(n)/n$ are related (if you expand the product and rearrange the terms, you get the sum). The value of the product is 0 and the value of the sum is 0; however, it is considerably harder to show the latter. (It is equivalent to the Prime Number Theorem).

- The notation $\pi(x)$ and a proof that $\lim_{x\to\infty}\pi(x)/x = 0$.

Show that in fact $\pi(x) < Cx/\log\log x$ for some constant C by using the sieve of Eratosthenes. (Discuss sieves in general.)

Homework:

(1) (a) Modify the previous argument to show that almost all positive integers n have a prime factor $\le \log n$. More precisely (and moreover) show that

$$|\{n \le x : n \text{ does not have a prime factor } \le \log n\}|$$

is bounded above by $Cx/\log\log x$ for some constant C. (Hint: Most $n \le x$ which do not have a prime factor $\le \log n$ also do not have a prime factor $\le (\log x)/2$.)

(b) Suppose $w(n)$ is any function defined for $n \in \mathbb{Z}^+$ which tends to infinity with n. Prove that

$$\lim_{x\to\infty} \frac{|\{n \le x : n \text{ has a prime factor } \le w(n)\}|}{x} = 1.$$

(2) Give the analysis details to the second half of the proof of Lemma 1.

The Functions $\pi(x)$, $\vartheta(x)$, and $\psi(x)$, and Chebyshev's Estimate:

- Define $\vartheta(x) = \sum_{p\le x} \log p$ and $\psi(x) = \sum_{p^m \le x} \log p = \sum_{p \le x} \left[\frac{\log x}{\log p}\right] \log p$.
- The limit connection (with possibly infinite limits):

Theorem. *The following hold:*

$$\liminf_{x\to\infty} \frac{\vartheta(x)}{x} = \liminf_{x\to\infty} \frac{\psi(x)}{x} = \liminf_{x\to\infty} \frac{\pi(x)\log x}{x}$$

and

$$\limsup_{x\to\infty} \frac{\vartheta(x)}{x} = \limsup_{x\to\infty} \frac{\psi(x)}{x} = \limsup_{x\to\infty} \frac{\pi(x)\log x}{x}.$$

More generally, if x_n is such that $\lim_{n\to\infty} x_n = \infty$ and any of the limits $\lim_{n\to\infty} \vartheta(x_n)/x_n$, $\lim_{n\to\infty} \psi(x_n)/x_n$, $\lim_{n\to\infty} \pi(x_n)\log(x_n)/x_n$ exists, then they all exist and are equal.

Comment: This theorem follows fairly quickly from the fact that $\lim_{x\to\infty} \pi(x)/x = 0$ and Abel summation (to be discussed momentarily).

Proof of Theorem. We show that for every $\varepsilon > 0$ and for x sufficiently large ($x \ge x_0(\varepsilon)$),

$$(1-\varepsilon)\frac{\pi(x)\log x}{x} + o(1) \le \frac{\vartheta(x)}{x} \le \frac{\psi(x)}{x} \le \frac{\pi(x)\log x}{x},$$

from which the theorem follows. The second inequality is obvious. The last inequality is a consequence of

$$\psi(x) = \sum_{p\le x} \left[\frac{\log x}{\log p}\right] \log p \le \sum_{p \le x} \log x = \pi(x)\log x.$$

For the first inequality, suppose as we may that $\varepsilon < 1$ and take $w = 1 - \varepsilon$. From

$$\vartheta(x) = \sum_{p \le x} \log p \ge \sum_{x^w < p \le x} \log p \ge (w \log x)(\pi(x) - \pi(x^w)),$$

we deduce that

$$\frac{\vartheta(x)}{x} \ge w \frac{\pi(x) \log x}{x} - \frac{w \log x}{x^{1-w}},$$

and the first inequality follows.

- Chebyshev's Theorem (in a weaker form)

Theorem. *If x is sufficiently large, then*

$$0.69 \frac{x}{\log x} < \pi(x) < 2.78 \frac{x}{\log x}.$$

Lemma. *Let n be a positive integer, and let p be a prime. Then the non-negative integer k for which p^k exactly divides $n!$ is*

$$k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots .$$

Proof of Theorem. Let $N = \binom{2n}{n}$. Let k_p denote the integer k such that p^k exactly divides N. From the Lemma, we deduce that

$$k_p = \sum_{j=1}^{\infty} \left(\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right] \right).$$

The upper limit of summation could be replaced by $[(\log 2n)/(\log p)]$. Observe that $[2x] - 2[x]$ is 0 or 1 depending respectively on whether $x = [x] + \{x\}$ is such that $\{x\} < 1/2$ or not. It follows that $k_p \le [(\log 2n)/(\log p)]$. Using $\psi(x) = \sum_{p \le x} \big[(\log x)/(\log p)\big] \log p$ and that $N = \prod_{p \le 2n} p^{k_p}$, we deduce that $\log N \le \psi(2n)$.

Since N is the largest coefficient in $(x+1)^{2n}$ (to see this use that $\binom{m}{k} = \frac{m-k+1}{k}\binom{m}{k-1}$), we deduce that (i) $N < 2^{2n}$ and (ii) $(2n+1)N > 2^{2n}$. We are interested in (ii) for the moment which implies a lower bound on $\log N$. We deduce from the above that

$$\psi(2n) \ge 2n \log 2 - \log(2n+1).$$

For $x > 2$ and $n = [x/2]$, we obtain

$$\psi(x) \ge \psi(2n) > (x-2) \log 2 - \log(x+1).$$

Dividing by x, we deduce that $\liminf_{x \to \infty} \psi(x)/x \ge \log 2 > 0.69$. The previous theorem now implies the lower bound in Chebyshev's theorem.

The upper bound can be obtained by using $\prod_{n<p\le 2n} p \le N$ and (i) to deduce that

$$\vartheta(2n) - \vartheta(n) = \sum_{n<p\le 2n} \log p \le \log N < 2n \log 2.$$

Let $x > 1$ and denote by m the non-negative integer for which $2^m < x \le 2^{m+1}$. Letting $n = 1, 2, 4, \dots, 2^m$ above and summing, we obtain

$$\vartheta(x) \le \vartheta(2^{m+1}) = \sum_{j=0}^{m} \left(\vartheta\big(2^{j+1}\big) - \vartheta\big(2^j\big) \right) < 2^{m+2} \log 2 < (4 \log 2) x.$$

It follows that $\limsup_{x\to\infty} \vartheta(x)/x \le 4\log 2 < 2.78$. The upper bound in Chebyshev's theorem now follows from the previous theorem.

- Why did Chebyshev care?

Chebyshev was interested in proving Bertrand's hypothesis that for every positive integer n, there is a prime in the interval $(n, 2n]$. He did this by obtaining a stronger version of his theorem than we have stated here. He showed that

$$0.92 \frac{x}{\log x} < \pi(x) < 1.11 \frac{x}{\log x}$$

for x sufficiently large. It follows that for n sufficiently large

$$\pi(2n) - \pi(n) > 0.92 \frac{2n}{\log(2n)} - 1.11 \frac{n}{\log n} > 0$$

which establishes Bertrand's hypothesis (when n is sufficiently large). To complete the proof of Bertrand's hypothesis, one can determine what "sufficiently large" means here and then check the hypothesis directly for the n which are not sufficiently large.

Homework:

(1) (a) Using the ideas above and Chebyshev's theorem as we have established it, find a constant c as small as you can such that for every $\varepsilon > 0$ and for x sufficiently large (depending on ε), there is a prime in the interval $(x, (c+\varepsilon)x]$.

(b) Find a constant c' as small as you can such that for every $\varepsilon > 0$ and for x sufficiently large (depending on ε), there are at least 3 primes in the interval $(x, (c'+\varepsilon)x]$.

(2) (a) Show that for n sufficiently large, the nth prime is $\le 2n \log n$.

(b) Show that for n sufficiently large, the nth prime is $\ge n(\log n)/3$.

(3) Explain why the Chebyshev estimates established here imply that there are positive constants C_1 and C_2 such that

$$C_1 \frac{x}{\log x} < \pi(x) < C_2 \frac{x}{\log x} \qquad \text{for all } x \ge 2.$$

More Background Material:

- Abel's Summation Formula

Theorem. *For a function a with domain $\mathbb{Z}^+$, set $A(x) = \sum_{k \le x} a(k)$. Suppose f is a function with a continuous derivative on the interval $[u, v]$ where $0 < u < v$. Then*

$$\sum_{u<n\le v} a(n)f(n) = A(v)f(v) - A(u)f(u) - \int_u^v A(x)f'(x)\,dx.$$

Proof. Clearly, the left-hand side is not changed by replacing u with $[u]$ and v with $[v]$. One checks that the same is true of the right-hand side. It therefore suffices to consider u and v to be integers. Observe that $a(n) = A(n) - A(n-1)$. The theorem follows from

$$\begin{aligned}\sum_{u<n\le v} a(n)f(n) &= \sum_{n=u+1}^{v} (A(n) - A(n-1))f(n) \\ &= A(v)f(v) - A(u)f(u+1) - \sum_{n=u+1}^{v-1} (f(n+1) - f(n))A(n) \\ &= A(v)f(v) - A(u)f(u) - \sum_{n=u}^{v-1} A(n) \int_n^{n+1} f'(x)\,dx \\ &= A(v)f(v) - A(u)f(u) - \int_u^v A(x)f'(x)\,dx.\end{aligned}$$

Homework:

(1) Let A be a set of positive integers, and let

$$A(x) = |\{a \in A : a \le x\}|.$$

Suppose that there is a constant $c > 0$ such that

$$\sum_{\substack{a\in A\\ a\le x}} \frac{1}{a} > c\log\log x \qquad \text{for all } x \text{ sufficiently large.}$$

Prove that given any $t > 0$, there is an $x \ge t$ for which

$$A(x) > \frac{cx}{2\log x}.$$

(Note that I did not say that for all $x \ge t$ the last inequality holds.)

(2) Let n denote an arbitrary positive integer. Recall that

$$(*) \qquad e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \qquad \text{for all } x \in \mathbb{R}.$$

(a) Using $(*)$, show that $n! > (n/e)^n$.
(b) Let $x = n + 1$ in $(*)$ and show that the first $2n + 2$ terms are each $\leq (n+1)^n/n!$. Also, show that the remaining terms sum to a number $< (n+1)^n/n!$.
(c) Use (b) to show that $n! < \dfrac{(n+1)^n}{e^{n+1}}(2n+3)$.
(d) Modify the above to show that $n! < 2\left(\dfrac{n+1}{e}\right)^{n+1}$.

(3) (a) Let n be a positive integer. Using Abel summation, prove that

$$\sum_{k=1}^{n} \log k = n \log n - \int_1^n \frac{[x]}{x}\, dx.$$

(b) Using (a) and the inequality $[x] \leq x$, prove that $n! > (n/e)^n$.
(c) Do a similar argument to show that $n! < \dfrac{n^{n+1}}{e^n}$.
(d) Which upper bound on $n!$ is better when n is large: the one given in (2)(d) or the one given in (3)(c)? Explain.

- Derivatives of Sums and Sums of Derivatives

Theorem. *Let $\{f_n(x)\}_{n=1}^{\infty}$ be a sequence of differentiable functions such that $F(x) = \sum_{n=1}^{\infty} f_n(x)$ converges for $x > x_0$ and $G(x) = \sum_{n=1}^{\infty} f_n'(x)$ converges uniformly for $x > x_0$. Then $F'(x)$ exists and $F'(x) = G(x)$ for $x > x_0$.*

Proof. Let $\varepsilon > 0$. Let $F_N(x) = \sum_{n=1}^{N} f_n(x)$ and $G_N(x) = \sum_{n=1}^{N} f_n'(x)$. There is an $N_0 = N_0(\varepsilon)$ such that if $M \geq N_0$ and x is any real number $> x_0$, then

$$|G_M(x) - G(x)| < \frac{\varepsilon}{4}.$$

Let N and M be $\geq N_0$. Then

$$|G_N(t) - G_M(t)| < \frac{\varepsilon}{2} \quad \text{for all } t > x_0.$$

Fix $x > x_0$. Then there is a $\delta = \delta(M, x) \in (0, x - x_0)$ such that if $|h| < \delta$, then

$$\left| \frac{F_M(x+h) - F_M(x)}{h} - G_M(x) \right| < \frac{\varepsilon}{4}.$$

Fix $|h| < \delta$. Since $F_N - F_M$ is differentiable on (x_0, ∞), we deduce from the Mean Value Theorem that there is a t between x and $x + h$ such that

$$(F_N(x+h) - F_M(x+h)) - (F_N(x) - F_M(x)) = h(F_N'(t) - F_M'(t)) = h(G_N(t) - G_M(t)).$$

We deduce that

$$\left| \frac{F_N(x+h) - F_N(x)}{h} - \frac{F_M(x+h) - F_M(x)}{h} \right| < \frac{\varepsilon}{2}.$$

This is true independent of the choice of $N \ge N_0$ so by letting N tend to infinity, we obtain

$$\left| \frac{F(x+h) - F(x)}{h} - \frac{F_M(x+h) - F_M(x)}{h} \right| \le \frac{\varepsilon}{2}.$$

Combining the first, third, and fifth of the above displayed inequalities, we obtain that

$$\left| \frac{F(x+h) - F(x)}{h} - G(x) \right| < \varepsilon.$$

It follows that $F'(x)$ exists and $F'(x) = G(x)$ as desired.

Further Elementary Results:

- Comment on this material.

Following classical lines, we show shortly that if $\lim_{x\to\infty} \pi(x)(\log x)/x$ exists, then it is 1. The approach below is of some interest in itself, but we note if the goal is simply to establish this information about $\lim_{x\to\infty} \pi(x)(\log x)/x$, there is an easier way. One can skip the next two sections, and go to Merten's formulas. Then this result on $\lim_{x\to\infty} \pi(x)(\log x)/x$ follows as a consequence of Merten's formulas and an application of Abel summation (see the third homework problem below).

- The function $\zeta(s)$ and its derivative

We use Euler's identity discussed earlier and define the Riemann zeta function to be

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

We will also use the von Mangoldt function $\Lambda(n)$ which is defined to be $\log p$ if $n = p^k$ for some prime p and some positive integer k and to be 0 otherwise. In particular, $\psi(x) = \sum_{n\le x} \Lambda(n)$. Observe that (for $s > 1$)

$$\log \zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}.$$

By taking derivatives on both sides of this first equation (and recalling the preliminary results above), we deduce that

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{p^{-s}\log p}{1 - p^{-s}} = \sum_{p,m} \frac{\log p}{p^{ms}} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

By Abel summation, we now deduce that

$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(x)}{x^{s+1}}\,dx \quad \text{for } s > 1.$$

- If $\lim_{x\to\infty} \pi(x)\log x/x$ exists, it is 1.

Theorem. $\liminf_{x\to\infty} \dfrac{\pi(x)\log x}{x} \le 1 \le \limsup_{x\to\infty} \dfrac{\pi(x)\log x}{x}$.

Lemma. $\lim_{s\to 1^+}(s-1)\zeta(s) = 1$ *and* $\lim_{s\to 1^+}(s-1)^2\zeta'(s) = -1$.

Proof of Lemma. For the first limit, use that

$$\frac{1}{s-1} = \int_1^\infty \frac{1}{x^s}\,dx < \sum_{n=1}^\infty \frac{1}{n^s} < 1 + \int_1^\infty \frac{1}{x^s}\,dx = \frac{s}{s-1}.$$

For the second use an integration by parts to obtain

$$\zeta'(s) = -\sum_{n=1}^\infty \frac{\log n}{n^s} = -\int_1^\infty \frac{\log x}{x^s}\,dx + E = -\frac{1}{(s-1)^2} + E,$$

where $|E| \le 1$.

Proof of Theorem. Let $f(s) = -\zeta'(s)/\zeta(s)$. The lemma implies that $\lim_{s\to 1^+}(s-1)f(s)$ exists and is 1. It suffices to show

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \le 1 \le \limsup_{x\to\infty} \frac{\psi(x)}{x}.$$

Assume the first inequality is incorrect. Then there is a $K > 1$ and an x_0 such that if $x \ge x_0$, then $\psi(x)/x > K$. Hence, for $s > 1$,

$$f(s) = s\int_1^\infty \frac{\psi(x)}{x^{s+1}}dx > s\int_1^{x_0} \frac{\psi(x)-Kx}{x^{s+1}}dx + s\int_1^\infty \frac{K}{x^s}dx = s\int_1^{x_0} \frac{\psi(x)-Kx}{x^{s+1}}dx + \frac{sK}{s-1}.$$

Multiplying through by $s-1$ and letting $s \to 1^+$, we obtain a contradiction. In the same manner, one handles the possibility that $\psi(x)/x < L < 1$ for $x \ge x_0'$.

- Merten's Formulas

  The following results are due to Merten:

$$\sum_{n\le x} \frac{\Lambda(n)}{n} = \log x + O(1), \quad \sum_{p\le x} \frac{\log p}{p} = \log x + O(1), \quad \int_1^x \frac{\psi(t)}{t^2}\,dt = \log x + O(1),$$

$$\sum_{p\le x}\frac{1}{p} = \log\log x + A + O(1/\log x), \qquad \text{and} \qquad \prod_{p\le x}\left(1-\frac{1}{p}\right) \sim \frac{B}{\log x},$$

where A and B are constants. Discuss what these results mean (the notation).

Observe that for any positive integer m,

$$e^m = \sum_{j=0}^{\infty}\frac{m^j}{j!} > \frac{m^m}{m!}.$$

For $m \ge 1$, we easily deduce that

$$m\log m \ge \log(m!) \ge m\log m - m.$$

Also,

$$\log(m!) = \sum_{p\le m}\sum_{j=0}^{[\log m/\log p]}\left[\frac{m}{p^j}\right]\log p = \sum_{n\le m}\left[\frac{m}{n}\right]\Lambda(n) = \sum_{n\le m}\frac{m\Lambda(n)}{n} + O(m)$$

(where we have used that $\psi(m) = \sum_{n\le m}\Lambda(n) = O(m)$). Dividing through by m, we obtain

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

The first of Merten's formulas now follows (consider replacing x with $[x]$). The second formula follows from the first by observing

$$\sum_{p}\sum_{j=2}^{\infty}\frac{\log p}{p^j} = \sum_{p}\frac{\log p}{p(p-1)}$$

is a convergent series. The third formula follows from the first by using Abel summation (take $a(n) = \Lambda(n)$ and $f(t) = 1/t$) and using that $\psi(x) = O(x)$ (by Chebyshev's estimates). The fourth formula follows from the second by Abel summation (take $a(p) = (\log p)/p$, $a(n) = 0$ otherwise, and $f(t) = 1/\log t$). The fifth formula is left as a homework problem.

Homework:

(1) We showed that if $\{x_n\}_{n=1}^{\infty}$ is a sequence tending to infinity and $\lim_{n\to\infty}\vartheta(x_n)/x_n$ or $\lim_{n\to\infty}\pi(x_n)\log x_n/x_n$ exists, then they both do and are equal. Show that this follows from Abel summation (you may also use $\lim_{x\to\infty}\pi(x)/x = 0$, but this is not necessary).

(2) Prove the formula $\displaystyle\prod_{p\le x}\left(1-\frac{1}{p}\right) \sim \frac{B}{\log x}$ above. (Hints: Use the Maclaurin series for $\log(1-x)$ as discussed earlier. You will want to take advantage of another of Merten's formulas.)

(3) Use the fourth formula of Merten above and Abel summation to give an alternative proof of the result

$$\liminf_{x\to\infty} \frac{\pi(x)\log x}{x} \le 1 \le \limsup_{x\to\infty} \frac{\pi(x)\log x}{x}.$$

Complex Preliminaries:

- Analytic functions on a region Ω (non-empty, open, and connected)
  The derivative of $f(z)$ exists on Ω.
  All the derivatives of $f(z)$ exist on Ω.
  The function $f(x+iy) = u(x,y) + iv(x,y)$ is such that u and v satisfy the Cauchy-Riemann equations in Ω: $\dfrac{\partial u}{\partial x} = \dfrac{\partial v}{\partial y}$ and $\dfrac{\partial u}{\partial y} = -\dfrac{\partial v}{\partial x}$.
  The function $f(z)$ may be represented as a power series at each point in Ω.
- The Identity Theorem

If $S \subseteq \Omega$ has an accumulation point in Ω and f and g are analytic functions for which $f(z) = g(z)$ for all $z \in S$, then $f \equiv g$ on Ω.

- Weierstrass' Theorem (a version of it)

Let $f_x(s)$ denote an analytic function in Ω for each $x \ge 1$. Suppose, as x approaches infinity, $f_x(s)$ converges uniformly to $f(s)$ on every compact subset of Ω. Then $f(s)$ is analytic in Ω and $f_x'(s)$ converges uniformly to $f'(s)$ on every compact subset of Ω.

Homework:

(1) Fix $\sigma \in \mathbb{R}$. Let C be a compact set in the region $\mathrm{Re}(s) > \sigma$. Prove that there is a $\sigma' > \sigma$ such that C is in the region $\mathrm{Re}(s) > \sigma'$.

The Riemann Zeta Function in the Complex Plane:

- The function $\zeta(s)$ in the right-half plane

The definition $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ is well-defined for $s = \sigma + it$ (σ and t real) with $\sigma > 1$ and defines an analytic function in this region (here we interpret n^s as $e^{s \log n}$ where "log" refers to the principal branch of the logarithm). It converges uniformly for $\sigma \ge \sigma_0 > 1$. By Abel summation (with $a(n) = 1$ and $f(t) = 1/t^s$), we deduce that

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{s-1} - s\int_1^{\infty} \frac{\{u\}}{u^{s+1}}\,du \quad \text{for } \sigma > 1.$$

By considering Weierstrass' Theorem with $f_x(s) = \displaystyle\int_1^x \frac{\{u\}}{u^{s+1}}\,du$, we deduce that the right-hand side is analytic for $\sigma > 0$ except for a pole with residue 1 at $s = 1$. By the Identity Theorem, the right-hand side is the only possible continuation of $\zeta(s)$ to the right-half plane (as a meromorphic function). The Riemann zeta function $\zeta(s)$ refers to the right-hand side above when $\sigma > 0$.

Euler's identity $\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ holds for $\sigma > 1$. Observe that for $\sigma > 1$,

$$\left| \prod_{p \le x} \left(1 - \frac{1}{p^s}\right) \right| \le \prod_{p \le x} \left(1 + \frac{1}{p^\sigma}\right) \le \zeta(\sigma).$$

It follows that the absolute value of the product in Euler's identity is bounded below by $1/\zeta(\sigma)$. In particular, $\zeta(s)$ is non-zero for $\sigma > 1$.

Homework:

(1) Look at our argument for Euler's identity given for real $s > 1$. Explain how to modify it to show the identity holds for $\sigma > 1$ as stated above.

- The Riemann Hypothesis (with $\zeta(s)$ defined as above, $\zeta(s) = 0 \implies \sigma = 1/2$; discuss some partial results that are known and implications such as on the gap problem for primes)
- The line $\sigma = 1$

Theorem. *If $t \ne 0$, then $\zeta(1 + it) \ne 0$.*

Lemma 1. $\log |z| = \mathit{Re}(\log z)$.

Lemma 2. $3 + 4\cos\theta + \cos(2\theta) = 2(1 + \cos\theta)^2 \ge 0$.

Proof of Theorem. From Lemma 1, for $\sigma > 1$,

$$\log|\zeta(s)| = \mathrm{Re}(\log\zeta(s)) = \mathrm{Re}\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}\right) = \mathrm{Re}\left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right) = \sum_{n=1}^{\infty} \frac{a_n}{n^\sigma}\cos(t\log n),$$

where $a_n = 1/m$ if $n = p^m$ for some prime p and $a_n = 0$ otherwise. Hence,

$$\log|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + i2t)| = \sum_{n=1}^{\infty} \frac{a_n}{n^\sigma}(3 + 4\cos(t\log n) + \cos(2t\log n)).$$

The definition of a_n and Lemma 2 imply that the right-hand side is ≥ 0. It follows that, for $\sigma > 1$,

$$|(\sigma - 1)\zeta(\sigma)|^3 \left|\frac{\zeta(\sigma + it)}{\sigma - 1}\right|^4 |\zeta(\sigma + i2t)| = \frac{1}{|\sigma - 1|}|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + i2t)| \ge \frac{1}{|\sigma - 1|}.$$

Assume $\zeta(1+it) = 0$ with $t \ne 0$. We let σ approach 1 from the right above. We have already shown $(\sigma - 1)\zeta(\sigma)$ approaches 1 (also clear from the analytic continuation formulation of $\zeta(s)$). Observe that $\zeta(\sigma + it)/(\sigma - 1)$ approaches $\zeta'(1 + it)$. Thus, taking a limit of the left-hand side above, we obtain $|\zeta'(1 + it)|^4|\zeta(1 + i2t)|$. On the right-hand side, the limit approaches infinity. Thus, we obtain a contradiction, establishing the theorem.

Proof of the Prime Number Theorem:

• The Prime Number Theorem was first established independently by Hadamard and de la Vallée Poussin in 1896. It is the following:

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

Homework:

(1) Let p_n denote the nth prime. Using the Prime Number Theorem, prove that

$$\lim_{n\to\infty} \frac{p_n}{n\log n} = 1.$$

(2) Let $\varepsilon > 0$. Using the Prime Number Theorem, prove that there is an $x_0 = x_0(\varepsilon)$ such that

$$e^{(1-\varepsilon)x} < \prod_{p\le x} p < e^{(1+\varepsilon)x} \qquad \text{for all } x \ge x_0.$$

(3) Let p_j denote the jth prime, and suppose that $a_1, a_2, \ldots, a_m$ are positive integers. If p_r is the largest prime factor of $a_1 a_2 \cdots a_m$, then we can factor each a_k as

$$a_k = \prod_{j=1}^{r} p_j^{e_j(k)} \quad \text{where each } e_j(k) \ge 0.$$

The least common multiple of the integers $a_1, a_2, \ldots, a_m$, denoted $\operatorname{lcm}(a_1, a_2, \ldots, a_m)$, satisfies

$$\operatorname{lcm}(a_1, a_2, \ldots, a_m) = \prod_{j=1}^{r} p_j^{f_j} \quad \text{where} \quad f_j = \max\{e_j(k) : 1 \le k \le m\}.$$

Let c denote a constant. Using the Prime Number Theorem, prove that

$$\lim_{n\to\infty} \frac{\operatorname{lcm}(1,2,\ldots,n)}{e^{cn}} = \begin{cases} 0 & \text{if } c > 1 \\ \infty & \text{if } c < 1. \end{cases}$$

• For the proof of the Prime Number Theorem, we will make use of previous material together with the following result (the Wiener-Ikehara Theorem).

Theorem. *Let $A(x)$ be a non-negative, non-decreasing function of x, defined for $x \in [0,\infty)$. Suppose that the integral $\int_0^\infty A(x)e^{-xs}\,dx$ converges for $\sigma > 1$ to a function $f(s)$ which is analytic for $\sigma \ge 1$ except for a simple pole at $s = 1$ with residue 1. Then $\lim_{x\to\infty} e^{-x}A(x) = 1$.*

• The connection. We show here how the Wiener-Ikahara Theorem implies the Prime Number Theorem. Recall that we showed

$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(x)}{x^{s+1}}\,dx \quad \text{for } s>1.$$

For $\sigma > 1$, the right-hand side is analytic by Weierstrass' Theorem (consider $f_x(s) = s\int_1^x \frac{\psi(t)}{t^{s+1}}\,dt$). Since $\zeta(s)$ is a non-zero analytic function for $\sigma > 1$, we deduce that the left-hand side is analytic for $\sigma > 1$. The above equation for real $s > 1$ now implies by the Identity Theorem that the same equation holds for all complex $s = \sigma + it$ with $\sigma > 1$. Replacing x with e^x in the integral, we deduce that

$$(*) \qquad -\frac{\zeta'(s)}{s\zeta(s)} = \int_0^\infty \psi(e^x)e^{-xs}\,dx \quad \text{for } \sigma>1.$$

By our knowledge of $\zeta(s)$ on the line $s = 1 + it$, the left-hand side of $(*)$ is analytic for $\sigma \geq 1$ except for at $s = 1$. We have already seen $\lim_{s\to1}(s-1)\zeta(s) = 1$ and that $\lim_{s\to1} -(s-1)\zeta'(s)/\zeta(s) = 1$. It follows from the Wiener-Ikahara Theorem with $A(x) = \psi(e^x)$ that $\lim_{x\to\infty}\psi(x)/x = 1$ which as we have seen implies the Prime Number Theorem.

• Some preliminary analysis results:

Lemma 1. *Let $f : [a,b]\times[0,\infty)\to\mathbb{C}$ be a continuous function. Suppose that there are positive numbers C and ε such that $|f(t,x)| \leq Ce^{-\varepsilon x}$ for every pair $(t,x)\in[a,b]\times[0,\infty)$. Then*

$$\int_a^b\int_0^\infty f(t,x)\,dx\,dt = \int_0^\infty\int_a^b f(t,x)\,dt\,dx.$$

Comment: To prove the lemma, one can consider the double integral of $|f(t,x)|$. This integral is finite, and this justifies such an interchange.

Lemma 2. *Let $f(s)$ be analytic on $\sigma = Re(s) \geq 1$ (hence, in an open region containing such s). Let a and b be real numbers with $a < b$. Then as $w \to 0^+$, $f(1+w+iy)$ converges uniformly to $f(1+iy)$ for $y\in[a,b]$.*

Proof. Write $f(x+iy) = u(x,y) + iv(x,y)$. Since f is anaytic on $\sigma \geq 1$, each of u and v has continuous partial derivatives for (x,y) with $x \geq 1$. Let M be a bound on $|u_x(x,y)|$ and $|v_x(x,y)|$ in the set $[1,2]\times[a,b]$. Then with $z = 1+iy$ and $0 \leq w \leq 1$, the Mean Value Theorem gives

$$|f(z+w)-f(z)| \leq |u(1+w,y)-u(1,y)| + |v(1+w,y)-v(1,y)| \leq 2wM.$$

The lemma follows.

Lemma 3. *Let a and b be real numbers with $a < b$. Let $h(t,w) : [a,b]\times[0,\infty)\to\mathbb{C}$ be a continuous function such that $h(t,w)$ converges to $h(t,0)$ uniformly for $t\in[a,b]$. Then*

$$\lim_{w\to0^+}\int_a^b h(t,w)\,dt = \int_a^b h(t,0)\,dt.$$

Proof. Fix $\varepsilon > 0$. Choose $\delta > 0$ such that if $0 \le w < \delta$ and $t \in [a,b]$, then $|h(t,w) - h(t,0)| < \varepsilon/(b-a)$. Then

$$\left| \int_a^b h(t,w)\,dt - \int_a^b h(t,0)\,dt \right| \le \int_a^b |h(t,w) - h(t,0)|\,dt < \varepsilon.$$

The result follows.

Lemma 4. *Let $f : \mathbb{R} \to \mathbb{R}$ be a non-negative function for which $\int_0^\infty f(x)\,dx$ exists. Then $\lim_{w \to 0^+} \int_0^\infty f(x) e^{-wx}\,dx = \int_0^\infty f(x)\,dx$.*

Proof. Let $\varepsilon > 0$. Fix $t > 0$ such that $\int_t^\infty f(x)\,dx < \varepsilon/4$. Let $I = \int_0^t f(x)\,dx$. Fix $\delta > 0$ such that if $0 \le w < \delta$, then $1 - \dfrac{\varepsilon}{2I+1} < e^{-wt} \le 1$. Then

$$\left| \int_0^\infty f(x)e^{-wx}\,dx - \int_0^\infty f(x)\,dx \right| \le \frac{\varepsilon}{2I+1} \int_0^t f(x)\,dx + 2\int_t^\infty f(x)\,dx < \varepsilon.$$

The result follows.

Lemma 5. *Let $f : \mathbb{R} \to \mathbb{R}$ be a non-negative function for which $\lim_{w \to 0^+} \int_0^\infty f(x)e^{-wx}\,dx$ exists. Then $\lim_{w \to 0^+} \int_0^\infty f(x)e^{-wx}\,dx = \int_0^\infty f(x)\,dx$.*

Homework:

(1) Prove Lemma 5. (Do not assume $\int_0^\infty f(x)\,dx$ exists.)

We will use the following weak version of the Riemann-Lebesgue Lemma.

Lemma 6. *Let a and b be real numbers with $a < b$. Let $f : [a,b] \to \mathbb{C}$ be such that:*

(i) f' exists everywhere in $[a,b]$, and

(ii) $\int_a^b |f'(t)|\,dt$ is finite.

Then $\lim_{y \to \infty} \int_a^b f(t)e^{iyt}\,dt = 0$.

Comment: Observe that (ii) holds if f' is continuous on $[a,b]$. This will be the case for our use of the lemma.

Proof. Integration by parts gives

$$\int_a^b f(t)e^{iyt}dt = f(t)\frac{e^{iyt}}{iy}\bigg|_a^b - \frac{1}{iy}\int_a^b f'(t)e^{iyt}\,dt.$$

Thus,

$$\left|\int_a^b f(t)e^{iyt}dt\right| \le \frac{2(|f(a)|+|f(b)|)}{y} + \frac{1}{y}\int_a^b |f'(t)|\,dt.$$

The result follows.

We will also make use of

Lemma 7. $\displaystyle\int_{-\infty}^{\infty} \frac{\sin^2 x}{x^2}\,dx = \pi.$

There is no real need to discuss the proof as the value of the integral will not come into play; only its existence will (which is clear).

- A Proof of the Wiener-Ikehara Theorem

Set $B(x) = A(x)e^{-x}$. It follows that

$$f(s) - \frac{1}{s-1} = \int_0^\infty (B(x)-1)e^{-(s-1)x}\,dx \quad \text{for } \sigma > 1.$$

Define $g(s)$ to be the left-hand side. By the conditions on f, we deduce that g is analytic for $\sigma \ge 1$. Fix $\varepsilon > 0$, and let $h(t) = g(1+\varepsilon+it)$. Fix $\lambda > 0$. Then

$$\int_{-2\lambda}^{2\lambda} h(t)\left(1-\frac{|t|}{2\lambda}\right)e^{iyt}\,dt = \int_{-2\lambda}^{2\lambda}\left(1-\frac{|t|}{2\lambda}\right)e^{iyt}\left(\int_0^\infty (B(x)-1)e^{-(\varepsilon+it)x}\,dx\right)dt.$$

We justify that for $\sigma > 1$ we can interchange the order of integration by using Lemma 1. We consider $s = 1+(\varepsilon/2)$ and $x > 0$. Observe that

$$f(s) = \int_0^\infty A(u)e^{-us}du \ge A(x)\int_x^\infty e^{-us}du = \frac{A(x)e^{-xs}}{s}.$$

Thus, $B(x) = A(x)e^{-x} \le sf(s)e^{(\varepsilon/2)x}$. It follows that

$$\left|\left(1-\frac{|t|}{2\lambda}\right)e^{iyt}(B(x)-1)e^{-(\varepsilon+it)x}\right| \le Ce^{-(\varepsilon/2)x},$$

where $C = sf(s)+1$. Lemma 1 now justifies the interchange of the order of integration. A direct calculation gives

$$\frac{1}{2}\int_{-2\lambda}^{2\lambda}\left(1-\frac{|t|}{2\lambda}\right)e^{i(y-x)t}\,dt = \frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}.$$

We deduce that

$$(*) \qquad \frac{1}{2}\int_{-2\lambda}^{2\lambda} h(t)\left(1-\frac{|t|}{2\lambda}\right)e^{iyt}\,dt = \int_0^\infty (B(x)-1)e^{-\varepsilon x}\frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\,dx.$$

Since $g(s)$ is analytic for $\sigma \geq 1$, we deduce from Lemma 2 that $h(t)$ (see its definition) converges uniformly to $g(1+it)$ for $t \in [-2\lambda, 2\lambda]$ as ε approaches 0 from the right. It follows from Lemma 3 that

$$\lim_{\varepsilon \to 0^+} \int_{-2\lambda}^{2\lambda} h(t) \left(1 - \frac{|t|}{2\lambda}\right) e^{iyt}\, dt = \int_{-2\lambda}^{2\lambda} g(1+it) \left(1 - \frac{|t|}{2\lambda}\right) e^{iyt}\, dt.$$

By Lemma 4,

$$\lim_{\varepsilon \to 0^+} \int_0^\infty e^{-\varepsilon x} \frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\, dx = \int_0^\infty \frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\, dx = \int_{-\infty}^{\lambda y} \frac{\sin^2 v}{v^2}\, dv.$$

Since $B(x)$ is non-negative, Lemma 5 and $(*)$ now give

$$\begin{aligned}\lim_{\varepsilon \to 0^+} \int_0^\infty B(x) e^{-\varepsilon x} \frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\, dx &= \int_0^\infty B(x) \frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\, dx \\ &= \int_{-\infty}^{\lambda y} B\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv.\end{aligned}$$

We let $\varepsilon \to 0^+$ in $(*)$. Next, we let y tend to infinity. Observe that

$$\int_{-2\lambda}^{2\lambda} g(1+it) \left(1 - \frac{|t|}{2\lambda}\right) e^{iyt}\, dt = \int_{-2\lambda}^{0} g(1+it) \left(1 + \frac{t}{2\lambda}\right) e^{iyt}\, dt + \int_{0}^{2\lambda} g(1+it) \left(1 - \frac{t}{2\lambda}\right) e^{iyt}\, dt$$

and we can apply Lemma 6 to each of the integrals on the right. From this and Lemma 7, we obtain

$$(**) \qquad \lim_{y \to \infty} \int_{-\infty}^{\lambda y} B\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv = \pi.$$

Explain why intuitively $(**)$ implies we are through. Let a be such that $0 < a < \lambda y$. Since $A(x) = B(x)e^x$ is non-decreasing, we get for $-a \leq v \leq a$ that

$$e^{y-(a/\lambda)} B\left(y - \frac{a}{\lambda}\right) \leq e^{y-(v/\lambda)} B\left(y - \frac{v}{\lambda}\right) \leq e^{y+(a/\lambda)} B\left(y + \frac{a}{\lambda}\right)$$

so that

$$B\left(y - \frac{a}{\lambda}\right) e^{-2a/\lambda} \leq B\left(y - \frac{v}{\lambda}\right) \leq B\left(y + \frac{a}{\lambda}\right) e^{2a/\lambda}.$$

We now deduce from $(**)$ and the fact that $B(x)$ is non-negative that

$$\begin{aligned}e^{-2a/\lambda} \big(\limsup_{y \to \infty} B(y)\big) \int_{-a}^{a} \frac{\sin^2 v}{v^2}\, dv &= \limsup_{y \to \infty} B\left(y - \frac{a}{\lambda}\right) e^{-2a/\lambda} \int_{-a}^{a} \frac{\sin^2 v}{v^2}\, dv \\ &\leq \limsup_{y \to \infty} \int_{-a}^{a} B\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv \leq \pi.\end{aligned}$$

The above holds for any positive a and λ. Letting $a = \sqrt{\lambda}$ and letting λ tend to infinity gives that $\limsup_{x\to\infty} B(x) \le 1$. To finish the proof, we show $\liminf_{x\to\infty} B(x) \ge 1$. Observe that $\limsup_{x\to\infty} B(x) \le 1$ implies $B(x) \le c$ for some constant c and all $x \ge 0$. We take $a = \sqrt{\lambda}$ again and use that

$$\begin{aligned}
\pi &= \liminf_{y\to\infty} \int_{-\infty}^{\lambda y} B\Big(y - \frac{v}{\lambda}\Big) \frac{\sin^2 v}{v^2}\, dv \\
&\le c\bigg(\int_{-\infty}^{-a} \frac{\sin^2 v}{v^2}\, dv + \int_{a}^{\infty} \frac{\sin^2 v}{v^2}\, dv\bigg) + \liminf_{y\to\infty} \int_{-a}^{a} B\Big(y - \frac{v}{\lambda}\Big) \frac{\sin^2 v}{v^2}\, dv \\
&\le c\bigg(\int_{-\infty}^{-a} \frac{\sin^2 v}{v^2}\, dv + \int_{a}^{\infty} \frac{\sin^2 v}{v^2}\, dv\bigg) + e^{2a/\lambda}\big(\liminf_{y\to\infty} B(y)\big) \int_{-a}^{a} \frac{\sin^2 v}{v^2}\, dv.
\end{aligned}$$

The theorem follows now by letting λ tend to infinity.

Intermission:

- Question: Are there infinitely many primes whose decimal representation contains the digit 9? Answer: Yes.

Theorem. *Given any block of digits $d_1 d_2 \dots d_n$ base $b \ge 2$, there exist infinitely many primes whose base b representation contains the block of digits.*

We will specialize our arguments to the original question concerning the digit 9. We give three proofs that infinitely many such primes exist. One proof will use the main result of what is to come, one will use the main result of where we have been, and the other won't use much. Each of the arguments easily generalizes to give the above theorem. Before continuing, we note that it is unknown whether or not there exist infinitely many primes whose decimal representation does *not* contain the digit 9. (Actually, it is known; but no proof exists.)

- What is to come. The next main goal for the course is to establish Dirichlet's theorem that if a and b are relatively prime integers with $a > 0$, then there are infinitely many primes of the form $an + b$. Observe that with $a = 10$ and $b = 9$, we can deduce that there are infinitely many primes whose decimal representation contains (in fact, ends with) 9. (Note that the more general theorem stated above can be done the same way by considering $b = d_1 d_2 \dots d_n \times 10 + 1$.)

- Where we have been. We could instead use the Prime Number Theorem as follows.

Lemma. *Let $\epsilon > 0$. Then there is an $x_0 = x_0(\varepsilon)$ such that if $x \ge x_0$, then the interval $(x, x + \varepsilon x]$ contains a prime.*

Before proving the lemma, observe that it implies what we want by taking $\varepsilon = 1/9$ and $x = 9 \times 10^k \ge x_0$. (In fact, a similar argument shows there are infinitely many primes whose decimal representation begins with any given block of digits.)

Proof. We may suppose that $\varepsilon \le 1$ and do so. From the Prime Number Theorem, there is an $x_0' = x_0'(\varepsilon)$ such that if $x \ge x_0'$, then

$$\Big(1 - \frac{\varepsilon}{10}\Big)\frac{x}{\log x} < \pi(x) < \Big(1 + \frac{\varepsilon}{10}\Big)\frac{x}{\log x}.$$

Thus, $x \geq x_0'$ implies

$$\pi(x+\varepsilon x)-\pi(x) \geq \left(1-\frac{\varepsilon}{10}\right)\frac{x+\varepsilon x}{\log(2x)}-\left(1+\frac{\varepsilon}{10}\right)\frac{x}{\log x} \geq \frac{\varepsilon x}{\log(2x)}-\frac{x\log 2}{(\log x)(\log(2x))}-\frac{\varepsilon}{5}\frac{2x}{\log x}$$

(where the last term on the right is a bound on the contribution from the parts involving $\varepsilon/10$). We deduce that if x is sufficiently large, the interval $(x, x+\varepsilon x]$ contains a prime.

- An elementary argument. Let $n_1, n_2, \dots$ be the positive integers in increasing order whose decimal representations do *not* contain the digit 9. Then for $N \geq 1$

$$\sum_{n_k < 10^N} \frac{1}{n_k} = \sum_{j=1}^{N} \sum_{10^{j-1} \leq n_k < 10^j} \frac{1}{n_k} \leq \sum_{j=1}^{N} \frac{9^j}{10^{j-1}} < 90.$$

It follows that the partial sums of $\sum_{k=1}^{\infty} 1/n_k$ form a bounded increasing sequence, and hence the series converges. Since the sum of the reciprocals of the primes diverges, it follows that there are infinitely many primes not among the numbers n_k. Hence, there exist infinitely many primes whose decimal representation contains the digit 9.

Homework:

(1) An open problem of Erdős is to show that if $\{a_j\}_{j=1}^{\infty}$ is an arbitrary infinite sequence of integers such that (i) $1 \leq a_1 < a_2 < a_3 < \cdots$ and (ii) $\sum_{j=1}^{\infty} 1/a_j$ diverges, then there exist arbitrarily long arithmetic progressions among the a_j. More precisely, given a positive integer N, one can find N distinct a_j in an arithmetic progression. If true, this would imply there are arbitrarily long arithmetic progressions among the primes, something which as yet is unknown. One approach to resolving the problem might be to consider a sequence $\{a_j\}_{j=1}^{\infty}$ satisfying (i) and having no N term arithmetic progression and to show that $\sum_{j=1}^{\infty} 1/a_j$ must then converge. If one can show this is true regardless of the value of $N \geq 1$, then the problem of Erdős would be resolved. The case $N = 1$ and $N = 2$ are not interesting. Deal with the following special case with $N = 3$. Begin with $a_1 = 1$ and $a_2 = 2$. Let a_3 be as small as possible so that no 3 term arithmetic progression occurs among the a_j then selected. We get $a_3 = 4$. Choose a_4 now as small as possible avoiding again 3 term arithmetic progressions. Then $a_4 = 5$. Continue in this way. The next few a_j's are 10, 11, 13, and 14. Prove that $\sum_{j=1}^{\infty} 1/a_j$ converges. (Hint: Think base 3.)

Algebraic Preliminaries:

- A *group* is a set G of objects together with a binary operation $*$ satisfying:

(i) If a and b are in G, then so is $a * b$.
(ii) If a, b, and c are in G, then $(a * b) * c = a * (b * c)$.
(iii) There is an element e of G such that $a * e = e * a = a$ for every $a \in G$.
(iv) For every $a \in G$, there is a $b \in G$ such that $a * b = b * a = e$.

An *abelian group* is a group G such that $a * b = b * a$ for all a and b in G. A group is finite if G is finite. We will simply use ab to denote $a * b$ and refer to the binary operation as multiplication (unless noted otherwise).

• Examples. The set of integers under addtion, the set of non-zero rational numbers under multiplication, and the reduced residue system modulo n under multiplication are all abelian groups. Another example, is given by $\{\zeta^j : 0 \le j \le n-1\}$ where $\zeta = e^{2\pi i/n}$ and the binary operation is multiplication. Yet another example is given by $\{\phi_1, \phi_2, \phi_3\}$ under composition where the ϕ_j are defined multiplicatively on the elements of $\{\zeta, \zeta^2, \zeta^4\}$ where $\zeta = e^{2\pi i/7}$ with $\phi_1(\zeta) = \zeta$, $\phi_2(\zeta) = \zeta^2$, and $\phi_3(\zeta) = \zeta^4$. Finally, consider the multiplicative mappings from the reduced residue system modulo 7 to $\{\zeta^j : 0 \le j \le 5\}$ where $\zeta = e^{2\pi i/6}$; show that these mappings form a finite abelian group under multiplication.

• A simple theorem on finite groups. We will use the fact that if a is an element of a finite abelian group G, then $a^{|G|} = e$ where e is the identity element in G. Give a proof. Note that the same is true for any finite group.

• A theorem on finite abelian groups

Theorem. *Let H be a subgroup of a finite abelian group G. Let $a \in G$, and let k be the minimal positive integer for which $a^k \in H$. Let*

$$H' = \{a^j b : b \in H, 0 \le j < k\}.$$

Then H' is a subgroup of G and $|H'| = k|H|$.

Proof. Let $a^i b$ and $a^j b'$ be elements of H' with $0 \le i, j < k$ and b and b' in H. If $0 \le i+j < k$, then $bb' \in H$ implies $a^i a^j bb' = a^{i+j} bb' \in H'$. If $i+j \ge k$, then $0 \le i+j-k < k$. In this case, $a^k bb' \in H$ implies $a^i a^j bb' = a^{i+j-k} a^k bb' \in H'$. Thus, H' is closed under multiplication. One also checks that the inverse of $a^i b$ is $a^{k-i}(a^{-k} b^{-1}) \in H'$ (note that if $i = 0$, then $a^i b \in H \subseteq H'$). The other group properties of H' are easily determined to hold, and thus H' is a subgroup of G.

To prove $|H'| = k|H|$, it suffices to show that if $a^i b = a^j b'$, then $i = j$. Assume otherwise; we suppose as we may that $i > j$. Then $a^{i-j} = b' b^{-1} \in H$ contradicts the minimality condition on k. The contradiction completes the proof.

Characters:

• The definition. A *character* χ of a finite abelian group G is a multiplicative complex valued function, not identically zero, defined on the group. Thus, if a and b are elements of the group, then $\chi(ab) = \chi(a)\chi(b)$.

• Properties of characters:

(i) If e is the identity element of G and χ any character, then $\chi(e) = 1$. This follows from two observations. First, $\chi(e) \ne 0$; otherwise, $\chi(a) = \chi(a)\chi(e) = 0$ for all $a \in G$ contradicting the requirement in the definition that χ is not identically zero. Next, $\chi(e) = \chi(e)\chi(e)$, and we can deduce from our first observation that $\chi(e) = 1$.

(ii) If $|G| = n$, then $\chi(a)$ is an nth root of unity for every $a \in G$. This follows from $\chi(a)^n = \chi(a^{|G|}) = \chi(e) = 1$.

(iii) For every $a \in G$, $\chi(a) \ne 0$. (See (ii).)

(iv) If $|G| = n$, then there are exactly n distinct characters defined on G. Let $H_1 = \{e\}$ where e is the identity element of G. Thus, H_1 is a subgroup of G. If $G \neq H_1$, we apply the theorem of the previous section (on groups) to construct a new subgroup H_2 of G. Note that H_2 will be a cyclic subgroup of G generated by an element a different from e in G. How $a \neq e$ is chosen doesn't matter. If $G \neq H_2$, then we again apply the theorem to obtain a new subgroup H_3 of G. We continue defining for $i \geq 1$, as long as $G \neq H_i$, the subgroup $H_{i+1} = \{a_i^j b : b \in H_i, 0 \leq j < k_i\}$ where $a_i \notin H_i$ and k_i is the minimal positive integer for which $a_i^{k_i} \in H_i$. We show by induction on i that the number of distinct characters on H_i is $|H_i|$. The result will then follow.

We deduce from (i) that there is precisely one character defined on $H_1 = \{e\}$. Suppose there are precisely $|H_i|$ different characters defined on H_i for some $i \geq 1$. If $G = H_i$, then we are done (as there are no more subgroups to consider). Otherwise, we wish to show that there are precisely $|H_{i+1}| = k_i|H_i|$ different characters defined on H_{i+1}. Observe that any character on H_{i+1} is necessarily a character when restricted to H_i (make use of (i) or (iii)). We finish the argument by showing that each character χ of H_i extends to exactly k_i different characters on H_{i+1}. Fix χ. Observe first that the definition of H_{i+1} and the multiplicativity of χ imply that χ will be defined on H_{i+1} once the value of $\chi(a_i)$ is determined. On the other hand, the value of $\chi(a_i)^{k_i} = \chi(a_i^{k_i})$ is known (since $a_i^{k_i} \in H_i$). Call this number γ. Then $\chi(a_i)$ must be one of the k_i distinct k_ith roots of γ. This shows that there are at most k_i different extensions of χ to H_{i+1}. On the other hand, defining $\chi(a_i)$ to be such a k_ith root of γ is easily shown to produce an extension of χ to H_{i+1}. This completes the proof.

(v) If $a \in G$ and $a \neq e$, then there is a character χ defined on G such that $\chi(a) \neq 1$. In our construction of the H_i above, we take $H_2 = \langle a \rangle$. The order of a given in the argument there is k_1. The construction gives a character χ of H_2 such that $\chi(a)$ is an arbitrary k_1th root of unity. We choose a k_1th root of unity other than 1. This character extends to a character of G with the desired property.

(vi) The characters of G form a finite abelian group under multiplication. If χ_1 and χ_2 are two characters defined on G, then $\chi = \chi_1\chi_2$ means $\chi(a) = \chi_1(a)\chi_2(a)$ for every a in G. One checks directly that χ is a multiplicative, complex valued function which is not identically zero; hence, the product of two characters is itself a character. Associativity and commutitivity follow from the same properties for multiplication in the set of complex numbers. The identity element, called the *principal character*, is defined by $\chi(a) = 1$ for every $a \in G$; and this is easily checked. One also checks that if χ is a character, then so is χ' defined by $\chi'(a) = (\chi(a))^{-1}$ and that χ' is the inverse of χ. From (iv), we now deduce that the characters form a finite abelian group. We note that the group G and the group of characters defined on G are isomorphic; we do not need this fact and so do not bother with the details of an explanation.

(vii) The following holds:

$$\sum_{a \in G} \chi(a) = \begin{cases} 0 & \text{if } \chi \text{ is not principal} \\ |G| & \text{if } \chi \text{ is principal.} \end{cases}$$

Observe that in the case that χ is principal, the result is trivial. If χ is not the principal character, then there is a $b \in G$ such that $\chi(b) \neq 1$. The proof follows by multiplying the sum, say S, by $\chi(b)$ and using that $\{ab : a \in G\} = G$. Thus, $\chi(b)S = S$ so that $S = 0$.

(viii) The following holds:

$$\sum_{\chi} \chi(a) = \begin{cases} 0 & \text{if } a \neq e \\ |G| & \text{if } a = e. \end{cases}$$

If $a = e$, the result follows from (iv). If $a \neq e$, then by (v) there is a character χ such that $\chi(a) \neq 1$. If the sum above is S, we obtain $\chi(a)S = S$ and the result follows along the same lines as (vii).

• Dirichlet characters. A Dirichlet character χ is a character on the reduced residue system modulo n extended to the complete system modulo n by defining $\chi(a) = 0$ whenever a and n are not relatively prime.

• Examples of Dirichlet characters. Discuss the two Dirichlet characters modulo 6, the four Dirichlet characters modulo 8, and the twelve Dirichlet characters modulo 36 by making Dirichlet character tables in the first two cases and explaining how to go about doing the same in the latter (by defining $\chi(5)$ to be a sixth root of unity and $\chi(35)$ to be ± 1).

Homework:

(1) (a) Make a Dirichlet character table of the eight characters modulo 15.
(b) Make a Dirichlet character table of the eight characters modulo 20.

Dirichlet Series:

• The definition. A *Dirichlet series* is a series of the form $\sum_{n=1}^{\infty} a_n/n^s$ where a_n and s denote complex numbers (we interpret n^s as $e^{s \log n}$ where "log" refers to the principal branch of the logarithm).

• Preliminary results.

Theorem 1. *Fix $\theta \in (0, \pi/2)$. If the series $\sum_{n=1}^{\infty} a_n/n^s$ converges for $s = s_0 \in \mathbb{C}$, then it converges uniformly in $\{s : |\arg(s - s_0)| \leq \theta\}$.*

Proof. By considering $b_n = a_n n^{-s_0}$ so that $\sum_{n=1}^{\infty} a_n/n^s = \sum_{n=1}^{\infty} b_n/n^{s-s_0}$, we see that it suffices to prove the theorem in the case that $s_0 = 0$. Thus, $\sum_{n=1}^{\infty} a_n$ converges and its partial sums form a Cauchy sequence. Fix $\varepsilon > 0$. Consider a positive integer M such that $|\sum_{M<n\leq x} a_n| < \varepsilon$ for all $x \geq M$. We definie $a'_n = a_n$ if $n > M$ and $a'_n = 0$ if $n \leq M$. Let $N > M$. We apply Abel summation with $A(x) = \sum_{n \leq x} a'_n$ and $f(x) = x^{-s}$ to obtain

$$(*) \qquad \sum_{M<n\leq N} \frac{a_n}{n^s} = A(N)f(N) - A(M)f(M) + s \int_M^N \frac{A(x)}{x^{s+1}}\, dx.$$

The definition of $A(x)$ implies that $|A(x)| < \varepsilon$ for all $x \geq M$. We write $s = \sigma + it$ and obtain

$$\left| \int_M^N \frac{A(x)}{x^{s+1}}\, dx \right| \leq \int_M^N \left| \frac{A(x)}{x^{s+1}} \right| dx \leq \varepsilon \int_M^N \frac{1}{x^{\sigma+1}}\, dx = \frac{\varepsilon}{\sigma}\left(\frac{1}{M^{\sigma}} - \frac{1}{N^{\sigma}} \right).$$

Note that
$$1 < \frac{|s|}{\sigma} \le \frac{1}{\cos\theta}.$$
From $(*)$, we deduce easily that
$$\left| \sum_{M<n\le N} \frac{a_n}{n^s} \right| \le \frac{4|s|\varepsilon}{\sigma M^\sigma} \le \frac{4|s|\varepsilon}{\sigma} \le \frac{4\varepsilon}{\cos\theta}.$$

Therefore, the partial sums of $\sum_{n=1}^\infty a_n/n^s$ form a Cauchy sequence and hence the series converges. The above inequality in fact implies uniform convergence.

Theorem 2. *If $\sum_{n=1}^\infty a_n/n^s$ converges for $s = s_0 = \sigma_0 + it_0$, then it converges in the half-plane $s = \sigma + it$ with $\sigma > \sigma_0$. Furthermore, in this case, the convergence is uniform on every compact subset of the half-plane with $\sigma > \sigma_0$.*

The proof of Theorem 2 is clear (given Theorem 1). The smallest value of σ_0 is called the *abscissa of convergence* for the Dirichlet series. Observe that if σ_0 is the abscissa of convergence for a Dirichlet series $\sum_{n=1}^\infty a_n/n^s$ and if σ_0 is finite, then the series converges if $\sigma = \mathrm{Re}(s) > \sigma_0$ and diverges if $\sigma < \sigma_0$. What happens on the line $\sigma = \sigma_0$ is unclear. It should be noted that σ_0 could be $+\infty$ or $-\infty$ (with, for example, $a_n = n!$ and $a_n = 1/n!$, respectively).

Theorem 3. *Let σ_0 be the abscissa of convergence for the Dirichlet series $\sum_{n=1}^\infty a_n/n^s$. Then the series represents an analytic function in the half-plane $\sigma > \sigma_0$ and its derivatives can be computed by termwise differentiation.*

In the complex preliminaries section of the notes, we introduced a theorem of Weierstrass. By considering $f_x(s) = \sum_{n\le x} a_n/n^s$ and applying Theorem 2, the above result follows.

Theorem 4. *Let $\sigma' \in \mathbb{R}$. Suppose $\sum_{n=1}^\infty a_n/n^s$ and $\sum_{n=1}^\infty b_n/n^s$ both converge for $\sigma > \sigma'$ and that they are equal on some non-empty open set in this half-plane. Then $a_n = b_n$ for all $n \ge 1$.*

Proof. Let $c_n = a_n - b_n$. The conditions in the theorem, Theorem 3, and the Identity Theorem imply that $\sum_{n=1}^\infty c_n/n^s$ is identically 0 in the half-plane $\sigma > \sigma'$. We wish to prove that $c_n = 0$ for all $n \ge 1$. Assume otherwise, and let M be minimal with $c_M \ne 0$. Fix for the moment $\sigma > \sigma'$. Observe that $\sum_{n=1}^\infty c_n/n^\sigma$ converges so that $|c_n|/n^\sigma < 1$ for n sufficiently large, say $n \ge N \ge M+2$. Now, for $u > 0$, $|c_n|/n^{\sigma+u} < 1/n^u$ for $n \ge N$. We obtain from $\sum_{n=M}^\infty c_n/n^{\sigma+u} = 0$ that
$$\frac{|c_M|}{M^{\sigma+u}} \le \sum_{n=M+1}^\infty \frac{|c_n|}{n^{\sigma+u}} \le \frac{1}{(M+1)^{\sigma+u}} \left(\sum_{n=M+1}^{N-1} |c_n| \right) + \sum_{n=N}^\infty \frac{1}{n^u} \le \frac{C}{(M+1)^u},$$
for some constant C. Multiplying through by $M^{\sigma+u}$ and letting u tend to infinity gives a contradiction and establishes the theorem.

Part I of the Proof of Dirichlet's Theorem:

- The Dirichlet series $L(s,\chi) = \sum_{n=1}^{\infty} \dfrac{\chi(n)}{n^s}$ where χ denotes a character modulo a positive integer m converges for $\sigma > 0$ if χ is not the principal character. To see this, observe that property (vii) of characters easily implies $\left|\sum_{n\le x} \chi(n)\right|$ is bounded as x goes to infinity. An application of Abel summation now shows that $L(s,\chi)$ converges for $\sigma > 0$. It is easy to see that $L(s,\chi)$ diverges for $\sigma < 0$. It follows that 0 is the abscissa of convergence. In particular, $L(s,\chi)$ is analytic in the region $\sigma > 0$.

- The connection between $L(s,\chi)$ and $\zeta(s)$ when χ is the principal character.

First, for an arbitrary Dirichlet character χ, a proof similar to that done before gives

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \qquad \text{for } \sigma > 1.$$

For the principal character χ_0 modulo m, we obtain

$$L(s,\chi_0) = \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \zeta(s).$$

It follows that $L(s,\chi_0)$ is analytic for $\sigma > 0$ except for a simple pole at $s = 1$ with residue $\prod_{p|m}(1 - (1/p))$.

- For every Dirichlet character χ, $L(s,\chi) \neq 0$ for $\sigma > 1$. A proof similar to that given for the analogous result for $\zeta(s)$ can be used here.

- The logarithm of $L(s,\chi)$.

For an arbitrary Dirichlet character χ modulo m, we define

$$w(L(s,\chi)) = \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} \qquad \text{for } \sigma > 1.$$

The right-hand side is what we would obtain from using the Maclaurin series for $\log(1-x)$ with the product formulation of $L(s,\chi)$ if we (incorrectly) assume $\log(z_1 z_2) = \log z_1 + \log z_2$ for complex numbers z_1 and z_2. Locally, w behaves like the logarithm of $L(s,\chi)$ but globally it may not correspond to any branch of the logarithm. In particular, since for the principal branch of the logarithm, $\log(1-z) = -z - z^2/2 - z^3/3 - \cdots$ for $|z| < 1$, it follows that $\exp(-z - z^2/2 - z^3/3 - \cdots) = 1 - z$ for $|z| < 1$ so that

$$\exp\left(\sum_{p\le x} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}\right) = \prod_{p\le x} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \qquad \text{for } \sigma > 1.$$

Thus,

$$\exp\big(w(L(s,\chi))\big) = L(s,\chi) \qquad \text{for } \sigma > 1.$$

Observe that w is defined as a Dirichlet series which is analytic for $\sigma > 1$. In particular, it is differentiable, and we have by taking derivatives above that

$$\frac{d}{ds}(L(s,\chi)) = \frac{L'(s,\chi)}{L(s,\chi)} \qquad \text{for } \sigma > 1.$$

Hence, for fixed $s = \sigma > 1$ and $c > \sigma$, we obtain

$$(*) \qquad w(L(s,\chi)) = -\int_s^c \frac{L'(u,\chi)}{L(u,\chi)}\,du + \log L(c,\chi).$$

Homework:

(1) (a) Let χ be a character on a group G. Let $\overline{\chi}$ be the function defined by $\overline{\chi}(g) = \overline{\chi(g)}$ (the complex conjugate of $\chi(g)$). Prove that $\overline{\chi}$ is a character on the group G.

(b) Let $L(s,\chi)$ be the Dirichlet L-series corresponding to a Dirichlet character χ modulo a positive integer m. Let χ_0 denote the principal character modulo m. Recall that $L(s,\chi)$ is analytic for $\sigma > 0$ if $\chi \neq \chi_0$ and that $L(s,\chi_0)$ is analytic for $\sigma > 0$ except for a simple pole at $s = 1$. Suppose

$$\prod_{\chi} L(1,\chi) \neq 0,$$

where the product is over all Dirichlet characters χ modulo m. Also, suppose χ is a character for which $\chi(a) \neq \pm 1$ for some integer a. Explain why $L(1,\chi) \neq 0$.

Part II of the Proof of Dirichlet's Theorem:

• We will show in the next section that $L(1,\chi) \neq 0$ if χ is a non-principal Dirichlet character. We use this fact for the remainder of this section to show how Dirichlet's theorem on primes in an arithmetic progression follows. Observe that from $(*)$ above, for χ a non-principal character, we deduce from the fact that $L(s,\chi)$ and $L'(s,\chi)$ are analytic for $\sigma > 0$ and $L(1,\chi) \neq 0$ that $w(L(s,\chi))$ remains bounded as $s \to 1^+$.

• The proof of Dirichlet's Theorem assuming $L(1,\chi) \neq 0$ if χ is a non-principal Dirichlet character.

Let a and m be integers with $m > 1$ (the case $m = 1$ is trivial) and $\gcd(a,m) = 1$. We prove there are infinitely many primes $p \equiv a \pmod{m}$ by showing that the sum of the reciprocals of such primes diverges. Let $b \in \mathbb{Z}$ with $ab \equiv 1 \pmod{m}$. Observe that $bx \equiv 1 \pmod{m}$ if and only if $x \equiv a \pmod{m}$. Consider the Dirichlet characters modulo m, and let $r \geq 1$ denote the number of them. By property (viii) of characters, it follows that

$$\sum_{\chi} \chi(pb) = \begin{cases} r & \text{if } p \equiv a \pmod{m} \\ 0 & \text{otherwise.} \end{cases}$$

We consider $s = \sigma > 1$ and define E by

$$(**) \qquad w(L(s,\chi)) = \sum_p \frac{\chi(p)}{p^s} + E$$

so that

$$E = \sum_p \sum_{k=2}^{\infty} \frac{\chi(p^k)}{kp^{ks}}.$$

A simple estimate gives that $|E| \le 1$. From $(**)$, we obtain for some E' bounded in absolute value by r that

$$\sum_{\chi} \chi(b) w(L(s,\chi)) = \sum_{\chi} \chi(b) \sum_p \frac{\chi(p)}{p^s} + E' = \sum_p \sum_{\chi} \frac{\chi(pb)}{p^s} + E' = r \sum_{p \equiv a \pmod{m}} \frac{1}{p^s} + E'.$$

We now let $s \to 1^+$ and observe that each term in the sum on the left remains bounded except for the summand involving the principal character and this summand increases in absolute value to infinity. This implies that the right-hand side must increase in absolute value to infinity so that the sum of the reciprocals of the primes $p \equiv a \pmod{m}$ diverges.

Part III of the Proof of Dirichlet's Theorem:

- We begin with some preliminaries:

Lemma 1. *Suppose $f(z)$ is analytic in a region Ω containing a point z_0. Suppose the disk $\mathcal{D} = \{z : |z - z_0| < r\}$ where $r > 0$ is in Ω. Then the series*

$$f(z_0) + \frac{f'(z_0)}{1!}(z - z_0) + \frac{f''(z_0)}{2!}(z - z_0)^2 + \frac{f'''(z_0)}{3!}(z - z_0)^3 + \cdots$$

converges in $\mathcal{D}$ to $f(z)$.

The lemma asserts that $f(z)$ is equal to its Taylor series representation about z_0 in any open disk centered at z_0 that is contained in Ω. We omit the proof of this lemma but use it to establish the following result of Landau (discuss the connection with $\zeta(s)$ as an example to help clarify the theorem).

Theorem 1. *Let $f(s)$ be analytic for $\sigma = Re(s) > 0$. Suppose that there is a Dirichlet series $\sum_{n=1}^{\infty} a_n/n^s$ with abscissa of convergence σ_0 that equals $f(s)$ for $\sigma > \max\{0, \sigma_0\}$. If $a_n \ge 0$ for every $n \ge 1$, then $\sigma_0 \le 0$.*

Proof. Assume $\sigma_0 > 0$. Since $f(s)$ is analytic for $\sigma > 0$, $f(s)$ can be represented as a Taylor series about $\sigma_0 + 1$ that (by Lemma 1) converges in a disk of radius $> 1 + \frac{1}{2}\sigma_0$ centered at $\sigma_0 + 1$. For k a positive integer, the Dirichlet series representation of $f(s)$ gives us

$$f^{(k)}(\sigma_0 + 1) = \sum_{n=1}^{\infty} \frac{a_n(-\log n)^k}{n^{1+\sigma_0}}.$$

Thus, inside this disk,

$$\begin{aligned}
f(s) &= \sum_{k=0}^{\infty} \frac{f^{(k)}(\sigma_0+1)}{k!}(s-\sigma_0-1)^k \\
&= \sum_{k=0}^{\infty} \frac{(s-\sigma_0-1)^k}{k!} \sum_{n=1}^{\infty} \frac{a_n(-\log n)^k}{n^{1+\sigma_0}} \\
&= \sum_{k=0}^{\infty} \frac{(1+\sigma_0-s)^k}{k!} \sum_{n=1}^{\infty} \frac{a_n(\log n)^k}{n^{1+\sigma_0}}.
\end{aligned}$$

Fix $s = u \in (\sigma_0/2, \sigma_0)$ (in the disk). Then the double sum converges and, since the terms are non-negative, it converges absolutely. We may therefore rearrange the order of the summations to obtain that

$$f(u) = \sum_{n=1}^{\infty} \frac{a_n}{n^{1+\sigma_0}} \sum_{k=0}^{\infty} \frac{(1+\sigma_0-u)^k(\log n)^k}{k!} = \sum_{n=1}^{\infty} \frac{a_n}{n^{1+\sigma_0}} e^{(1+\sigma_0-u)(\log n)} = \sum_{n=1}^{\infty} \frac{a_n}{n^u}.$$

This is impossible as u is to the left of the abscissa of convergence for $\sum_{n=1}^{\infty} a_n/n^s$. The theorem follows.

Lemma 2. *If a Dirichlet series* $\displaystyle\sum_{n=1}^{\infty} a_n/n^s$ *converges for* $s = s_0$, *then the series converges absolutely for* $\mathit{Re}(s) > \mathit{Re}(s_0) + 1$.

Proof. Let $\sigma_0 = \mathrm{Re}(s_0)$, and consider $s = \sigma + it$ with $\sigma > \sigma_0 + 1$. Convergence at s_0 implies that $\lim_{n\to\infty} |a_n/n^{\sigma_0}| = 0$. Thus, $|a_n/n^{\sigma_0}| < 1$ for n sufficiently large. Since $\sigma > \sigma_0 + 1$, it follows by comparison with $\sum_{n=1}^{\infty} 1/n^{\sigma-\sigma_0}$ that $\sum_{n=1}^{\infty} a_n/n^s = \sum_{n=1}^{\infty} a_n/(n^{\sigma_0} n^{s-\sigma_0})$ converges absolutely.

The product of two Dirichlet series $\sum_{n=1}^{\infty} a_n/n^s$ and $\sum_{n=1}^{\infty} b_n/n^s$ is defined to be the Dirichlet series $\sum_{n=1}^{\infty} c_n/n^s$ where $c_n = \sum_{k\ell=n} a_k b_\ell$ (here, k and ℓ represent positive integers). If the Dirichlet series involving a_n and b_n both converge for $s = \sigma + it$ with $\sigma > \sigma_0$, then they converge absolutely for $\sigma > \sigma_0 + 1$ by Lemma 2. It follows that the Dirichlet series representing their product will converge absolutely for $\sigma > \sigma_0 + 1$. The product will, therefore, converge in this same region (we view the product then as converging in a possibly smaller region then the initial two Dirichlet series). Observe also that if we consider $\left(\sum_{n=1}^{\infty} a_n/n^s\right)^k$ for k any positive integer (and expanding this product in the obvious way), it is easy to see that independent of k the resulting series converges (in fact, absolutely) for $\sigma > \sigma_0 + 1$. Note that the *values* of a series representing the product of two Dirichlet series is in fact equal to the product of the values of the two Dirichlet series if the series involved converge absolutely.

Homework:

(1) Prove that $\zeta(s)^2 = \sum_{n=1}^{\infty} \dfrac{d(n)}{n^s}$ for $\sigma > 1$ where $d(n)$ denotes the number of positive integer divisors of n.

(2) Recall that we showed $-\dfrac{\zeta'(s)}{\zeta(s)} = \displaystyle\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ for $s > 1$. Explain why this implies that $\sum_{d|n} \Lambda(d) = \log n$. (Hint: Write down the series representation for $\zeta'(s)$.)

(3) Prove that

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} = (2^{1-s} - 1)\zeta(s) \quad \text{for } s = \sigma + it \text{ with } \sigma > 0 \text{ (and } s \neq 1).$$

(Hint: It may help to consider the case $\sigma > 1$ first, but don't forget to address the case $\sigma > 0$.)

• We are now ready to complete the proof of Dirichlet's Theorem. As we saw before, we need only justify the following.

Theorem 2. *If χ is not the principal character modulo an integer $m > 1$, then $L(1, \chi) \neq 0$.*

Proof. Recalling the definition of $w(L(s, \chi))$ from the previous section (Part II of the Proof of Dirichlet's Theorem), we define for $\sigma > 1$,

$$Q(s) = \sum_{\chi} w(L(s, \chi)) = \sum_{\chi} \sum_{p} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}},$$

where the sum on χ is over all characters modulo m. The right-hand side converges absolutely for $\sigma > 1$ so that we can rearrange the order of summation. Let r denote the number of characters modulo m. Then by making the inner sum be over χ and using property (viii) of Dirichlet characters, we deduce that

$$Q(s) = \sum_{p} \sum_{\substack{1 \leq k < \infty \\ p^k \equiv 1 \pmod{m}}} \frac{r}{kp^{ks}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where $a_n = r/k$ if $n = p^k \equiv 1 \pmod{m}$ ($k \in \mathbb{Z}^+$) and $a_n = 0$ otherwise. This last series converges absolutely for $\sigma > 1$. Let d be such that $u^d \equiv 1 \pmod{m}$ for every integer u with $\gcd(u, m) = 1$ (so we may take $d = r = \phi(m)$, but we needn't be this precise). Then $a_n = r/d$ whenever $n = p^d$ and $p \nmid m$. It follows that the Dirichlet series $\sum_{n=1}^{\infty} a_n/n^s$ does not converge for $s = 1/d$ (use that the sum of the reciprocals of the primes diverges and that each $a_n \geq 0$). Hence the abscissa of convergence for $\sum_{n=1}^{\infty} a_n/n^s$ is in $[1/d, 1]$.

Now, consider

$$f(s) = e^{Q(s)} = 1 + Q(s) + \frac{Q(s)^2}{2!} + \frac{Q(s)^3}{3!} + \cdots.$$

The powers of $Q(s)$ are themselves Dirichlet series, and each power converges absolutely for $\sigma > 1$ since each $a_n \geq 0$. Also, $a_1 = 0$ implies that any given $1/n^s$ appears as a term with a non-zero coefficient for only finitely many of the powers of $Q(s)$. Since the expression on the right-hand side above converges for $\sigma > 1$, we obtain that the terms on the right-hand side can be rearranged to form a Dirichlet series representation for $f(s)$ that converges for $\sigma > 1$. This Dirichlet series will contain non-negative coefficients and the coefficient of $1/n^s$ will be at least a_n. Since the Dirichlet series $\sum_{n=1}^{\infty} a_n/n^s$ does not converge for $s = 1/d$, it follows that neither does the Dirichlet series representing $f(s)$. Thus, this Dirichlet series has abscissa of convergence $\sigma_0 \geq 1/d$.

Recall that $e^{w(L(s,\chi))} = L(s,\chi)$. The definition of $Q(s)$ implies that for $\sigma > 1$,

$$f(s) = e^{Q(s)} = \prod_{\chi} L(s,\chi).$$

Assume there is a non-principal character χ' such that $L(1,\chi') = 0$. Then (by considering the Taylor series for $L(s,\chi')$ about 1) we deduce that $L(s,\chi') = (s-1)g(s)$ for some analytic function $g(s)$. Recall that if χ_0 is the principal character, $L(s,\chi_0)$ is analytic for $\sigma > 0$ except for a simple pole at 1. It follows that $L(s,\chi')L(s,\chi_0)$ can be viewed as an analytic function in the region $\sigma > 0$. Therefore, we can view $f(s)$ as being analytic for $\sigma > 0$. But then $f(s)$ is an analytic function for $\sigma > 0$ which, for $\sigma > \sigma_0$, can be represented by a Dirichlet series with non-negative coefficients and with a positive abscissa of convergence. This contradicts Theorem 1, completing the proof.

Homework:

(1) A stronger version of Dirichlet's Theorem and the Prime Number Theorem is as follows:

Theorem. *Let a and m be integers with $m \geq 1$ and $\gcd(a,m) = 1$. Let*

$$A(x) = |\{p \leq x : p \equiv a \pmod{m}\}|.$$

Then there are positive constants C_1 and C_2 such that for all $x \geq 2$

$$\left| A(x) - \frac{1}{\phi(m)} \int_2^x \frac{dt}{\log t} \right| < C_1 x e^{-C_2\sqrt{\log x}}.$$

In the theorem, $\phi(m)$ denotes the number of positive integers $k \leq m$ with $\gcd(k,m) = 1$.

(a) Show that $\left| \displaystyle\int_2^x \frac{dt}{\log t} - \frac{x}{\log x} \right| \leq \dfrac{5x}{\log^2 x}$ for x sufficiently large. (Suggestion: Integrate by parts and express the resulting integral as a sum of two integrals, one with limits of integration from $\sqrt{x}$ to x.)

(b) Show that $e^{-C_2\sqrt{\log x}} < \dfrac{1}{\log^2 x}$ for x sufficiently large. (Hint: Compare the logarithms of both sides.)

(c) Using the theorem above, show that there is a constant C' for which

$$\left| A(x) - \frac{x}{\phi(m)\log x} \right| < C' \frac{x}{\log^2 x} \qquad \text{for } x \text{ sufficiently large.}$$

(d) Using the theorem above or (c), show that there is a constant C'' for which

$$\left|\pi(x) - \frac{x}{\log x}\right| < C'' \frac{x}{\log^2 x} \qquad \text{for } x \text{ sufficiently large.}$$

(2) Using (1)(c) and Abel summation, prove that

$$\sum_{\substack{p \le x \\ p \equiv a \pmod{m}}} \frac{1}{p} = \frac{1}{\phi(m)} \log\log x + E,$$

where $|E| \le C$ for some constant C.

The Pure Brun Sieve:

• A quick review. Recall that we showed that $\pi(x)$ is small compared to x by estimating the size of

$$A(z,x) = |\{n \le x : p|n \implies p > z\}|.$$

We began with the identity

$$A(z,x) = [x] - \sum_{p \le z} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le z} \left[\frac{x}{p_1 p_2}\right] - \cdots .$$

We then obtained the estimate

$$A(z,x) \le \prod_{p \le z} \left(1 - \frac{1}{p}\right) x + 2^{\pi(z)}$$

by removing the brackets of the greatest integer function and estimating the resulting error. This is the basic idea of the Sieve of Eratosthenes. In this section, we give an alternative approach to bounding $A(z,x)$ called the Pure Brun Sieve. Unlike most of the material in this course, the approach here is elementary.

• A first estimate. To find an upper bound on $A(z,x)$, we first prove that

$$(*) \qquad A(z,x) \le [x] - \sum_{p \le z} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le z} \left[\frac{x}{p_1 p_2}\right] - \cdots + \sum_{p_1 < p_2 < \cdots < p_{2k} \le z} \left[\frac{x}{p_1 p_2 \cdots p_{2k}}\right],$$

where k is any positive integer. For this purpose, define

$$\alpha_n = 1 - \sum_{\substack{p \le z \\ p|n}} 1 + \sum_{\substack{p_1 < p_2 \le z \\ p_1 p_2 | n}} 1 - \cdots + \sum_{\substack{p_1 < p_2 < \cdots < p_{2k} \le z \\ p_1 p_2 \cdots p_{2k} | n}} 1.$$

To prove $(*)$, it suffices to show that

$$\alpha_n \text{ is } \begin{cases} = 1 & \text{if } p|n \implies p > z \\ \ge 0 & \text{otherwise} \end{cases}$$

(use that $A(z,x) \le \sum_{n\le x} \alpha_n$ and interchange summations). The first part is obvious for if every prime factor of n is $> z$, then all the sums in the definition of α_n are empty and only the term 1 is non-zero in this definition. Now, suppose $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$ where the p_j are distinct primes $\le z$, each of $r, e_1, \dots, e_r$ are positive integers, and every prime factor of m is $> z$. It follows that

$$(**) \qquad \alpha_n = 1 - \binom{r}{1} + \binom{r}{2} - \cdots + \binom{r}{2k},$$

where we interpret $\binom{a}{b}$ as 0 is $b > a$. To show that $\alpha_n \ge 0$, consider three cases: (i) $r \le 2k$, (ii) $2k < r \le 4k$, and (iii) $r > 4k$. Case (i) is dealt with by using $(1-1)^r = 0$ to show $\alpha_n = 0$. For Case (ii), use $(1-1)^r = 0$ to obtain

$$\begin{aligned}
\alpha_n &= \binom{r}{2k+1} - \binom{r}{2k+2} + \cdots \pm \binom{r}{r} \\
&\ge \left(\binom{r}{2k+1} - \binom{r}{2k+2}\right) + \left(\binom{r}{2k+3} - \binom{r}{2k+4}\right) + \cdots \ge 0.
\end{aligned}$$

For Case (iii), use $(**)$ directly to show that $\alpha_n \ge 1$ (by again grouping the binomial coefficients in pairs).

• Modifying the above. The above can be used to obtain an upper bound for $\pi(x)$ that is smaller than the estimate we made with the Sieve of Eratosthenes. However, our real goal is to find an upper bound for

$$\pi_a(x) = |\{n \le x : n \text{ and } n+a \text{ are primes }\}|,$$

where a is any fixed positive integer (which we will take to be even for obvious reasons). We define

$$A'(z,x) = |\{n \le x : p|n(n+a) \implies p > z\}|.$$

Observe that for any $z \ge 1$, $\pi_a(x) \le A'(z,x) + z$. Thus, we seek a good estimate for $A'(z,x)$. We use that

$$\begin{aligned}
A'(z,x) &\le \sum_{n\le x} \alpha_{n(n+a)} \\
&= \sum_{n\le x} 1 - \sum_{p\le z} \sum_{\substack{n\le x \\ p|n(n+a)}} 1 + \sum_{p_1<p_2\le z} \sum_{\substack{n\le x \\ p_1p_2|n(n+a)}} 1 \\
&\qquad - \cdots + \sum_{p_1<p_2<\cdots<p_{2k}\le z} \sum_{\substack{n\le x \\ p_1p_2\cdots p_{2k}|n(n+a)}} 1.
\end{aligned}$$

We fix momentarily $z \ge a$ so that if $p|a$, then $p \le z$. For a given $p \le z$, we consider two possibilities, $p|a$ and $p \nmid a$. If $p|a$, then the number of $n \le x$ for which $p|n(n+a)$ is $[x/p]$, which is within 1 of x/p. If $p \nmid a$, then the number of $n \le x$ for which $p|n(n+a)$ is within

2 of $2x/p$. In general, if $p_1, \ldots, p_u$ are distinct primes dividing a and $p_{u+1}, \ldots, p_{u+v}$ are distinct primes not dividing a, then the number of $n \le x$ for which $n(n+a)$ is divisible by $p_1 p_2 \cdots p_{u+v}$ is within 2^v of $2^v x / (p_1 p_2 \cdots p_{u+v})$ (this can be seen by using the Chinese Remainder Theorem and considering the number of such n in a complete system of residues modulo $p_1 p_2 \cdots p_{u+v}$). It follows that

$$\begin{aligned}
A'(z,x) &\le x - \sum_{\substack{p \le z \\ p \mid a}} \frac{x}{p} - \sum_{\substack{p \le z \\ p \nmid a}} \frac{2x}{p} \\
&\quad + \sum_{\substack{p_1 < p_2 \le z \\ p_1 p_2 \mid a}} \frac{x}{p_1 p_2} + \sum_{\substack{p_1 < p_2 \le z \\ p_1 \mid a, p_2 \nmid a}} \frac{2x}{p_1 p_2} + \sum_{\substack{p_1 < p_2 \le z \\ p_1 \nmid a, p_2 \nmid a}} \frac{4x}{p_1 p_2} \\
&\quad + \cdots + \sum_{\substack{p_1 < p_2 < \cdots < p_{2k} \le z \\ p_1 \nmid a, \ldots, p_{2k} \nmid a}} \frac{2^{2k} x}{p_1 \cdots p_{2k}} + E_1 \\
&= \prod_{p \mid a} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \le z \\ p \nmid a}} \left(1 - \frac{2}{p}\right) x + E_1 + E_2,
\end{aligned}$$

where

$$\begin{aligned}
E_1 &\le 1 + 2\binom{\pi(z)}{1} + 4\binom{\pi(z)}{2} + \cdots + 2^{2k}\binom{\pi(z)}{2k} \\
&\le \pi(z)^{2k}\left(1 + 2 + \frac{2^2}{2!} + \cdots + \frac{2^{2k}}{(2k)!}\right) \le e^2 \pi(z)^{2k}
\end{aligned}$$

and

$$E_2 \le \sum_{p_1 < p_2 < \cdots < p_{2k+1} \le z} \frac{2^{2k+1} x}{p_1 p_2 \cdots p_{2k+1}} + \sum_{p_1 < p_2 < \cdots < p_{2k+2} \le z} \frac{2^{2k+2} x}{p_1 p_2 \cdots p_{2k+2}} + \cdots .$$

We now find a bound for this last expression on the right to bound E_2 as follows:

$$E_2 \le x \sum_{u=2k+1}^{\infty} \frac{1}{u!} \left(\sum_{p \le z} \frac{2}{p} \right)^u \le x \sum_{u=2k+1}^{\infty} \frac{1}{u!} \big(2 \log\log z + 2C_1 \big)^u,$$

where C_1 is some appropriate constant. Using $e^u = \sum_{j=0}^{\infty} u^j / j! \ge u^u / u!$ and choosing $k = [6 \log\log z]$, we obtain

$$E_2 \le x \sum_{u=2k+1}^{\infty} \left(\frac{2e \log\log z + 2eC_1}{u} \right)^u \le x \sum_{u=2k+1}^{\infty} \left(\frac{1}{2}\right)^u = \frac{x}{2^{2k}} < \frac{x}{(\log z)^6}$$

for z sufficiently large. We also have

$$E_1 \le e^2 \pi(z)^{2k} \le z^{12 \log\log z}$$

for z sufficiently large. We now choose $z = x^{1/(24 \log\log x)}$ and consider x sufficiently large to deduce that

$$A'(z,x) \le \prod_{p|a}\left(1-\frac{1}{p}\right)\prod_{\substack{p\le z\\ p\nmid a}}\left(1-\frac{2}{p}\right)x + E,$$

where $|E| \le x/(\log x)^5$. Observe that, for some constants C_2 and C_3 depending on a,

$$\prod_{p|a}\left(1-\frac{1}{p}\right)\prod_{\substack{p\le z\\ p\nmid a}}\left(1-\frac{2}{p}\right)x \le C_2 x\left(\prod_{p\le z}\left(1-\frac{1}{p}\right)\right)^2 \le C_3\frac{x}{(\log x)^2}(\log\log x)^2.$$

Hence, we deduce the

Theorem. *Let a be any fixed positive integer. Then for x sufficiently large,*

$$\pi_a(x) \le C\frac{x}{(\log x)^2}(\log\log x)^2$$

for some constant C depending on a.

• Twin primes. A twin prime is a prime which differs from another prime by 2. Thus, the twin primes are $3, 5, 7, 11, 13, 17, 19, 29, 31, \ldots$. It is unknown whether or not there are infinitely many twin primes. Brun introduced what is now called the pure Brun sieve to establish that the sum of the reciprocals of the twin primes converges. Since $\pi_2(x)$ can be used to bound the number of twin primes up to x ($\pi_2(x)$ is not precisely the number of these twin primes, but clearly this number is $\le 2\pi_2(x)$ for $x \ge 1$), one can use the previous theorem and Abel summation to estimate the sum of the reciprocals of the twin primes. This shows the sum converges.

Homework:

(1) Let p_n denote the nth prime.

(a) Explain why the Prime Number Theorem implies that $\limsup_{n\to\infty}(p_{n+1}-p_n) = \infty$.

(b) Recall that we showed that

$$\pi_a(x) \le C\frac{x}{(\log x)^2}(\log\log x)^2$$

for some constant C, where

$$\pi_a(x) = |\{n \le x : n \text{ and } n+a \text{ are prime}\}|.$$

Use this to prove that for every positive integer k,

$$\limsup_{n\to\infty}\Big(\min\{p_{n+1}-p_n, p_{n+2}-p_{n+1}, \ldots, p_{n+k}-p_{n+k-1}\}\Big) = \infty.$$

(Note that this would follow from part (a) if "min" were replaced by "max"; the problem is to figure out how to handle the "min" situation.)