UNSW AUSTRALIA.
SCHOOL OF MATHEMATICS AND STATISTICS.

MATH5645: TOPICS IN NUMBER THEORY.

§0 INTRODUCTION:

Number Theory is essentially concerned with the properties of the natural numbers and the integers,

$$\mathbb{N} = \{0, 1, 2, 3, ...\}, \qquad \mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

The ancient Greeks studied some basic properties of numbers and Euclid describes some of these results in Book 10 of the *Elements.* Diophantus (c. 250 AD ??) studied certain equations (called *Diophantine Equations* in his honour) which may or may not have integer/rational solutions. Diophantus' work inspired Fermat (1601-1665), regarded as the 'founder' of modern number theory, to develop number theory as a systematic branch of learning. Major strides forward were taken by Euler and Gauss.
Nowadays, number theory is divided into a range of categories including:

- Algebraic Number Theory
- Analytic Number Theory
- Probabilistic Number Theory
- Geometric Number Theory

etc.

This course will deal with the rudiments of Classical and Analytic Number Theory.

§1 SOME CLASSICAL NUMBER THEORY:

Summary of basic facts

Notation:
For n a positive integer, we will use the notation $\mathbb{Z}_n$ to denote the ring of integers modulo n. In the case when n is a prime p, $\mathbb{Z}_p$ forms a field, and so each non-zero element has a multiplicative inverse. The invertible elements in the ring $\mathbb{Z}_n$ are those elements which are co-prime to n. These numbers are called the **units** in the ring, and the set of such elements is denoted by $\mathbb{U}_n$. Thus, $\mathbb{U}_{12} = \{1, 5, 7, 11\}$.

We will write (a, b) for $\gcd(a, b)$ and recall that if $d = (a, b)$ then $d = ax + by$ for some integers x, y.

Basic Theorems:

Linear Equations:

For n a positive integer and a, b integers, the linear congruence equation $ax \equiv b \mod n$ has solutions if and only if $d = (a, n)$ is a factor of b, in which case there are d mutually incongruent solutions modulo n.

The Chinese Remainder Theorem deals with simultaneous linear congruence equations. Thus, if $n_1, n_2, ..., n_k$ are pairwise coprime positive integers, then the system:

$$x \equiv a_1 \mod n_1$$

$$x \equiv a_2 \mod n_2$$

.....

$$x \equiv a_k \mod n_k$$

has a unique solution modulo $N = n_1 n_2 ... n_k$.

This result is very useful, since when dealing with a congruence equation of the form $f(x) \equiv 0 \mod n$, we can uniquely factor n into a product of prime powers and consider the congruence with respect to each prime power and finally recombine to obtain solutions if they exist.

Fermat's Little Theorem states that if p is prime and $p \not| a$ then

$$a^{p-1} \equiv 1 \mod p.$$

To generalise this we need Euler's phi function, $\phi(n)$, which equals the size of the set $\{x \in \mathbb{Z}^+ : 0 < x < n, (x, n) = 1\}$. Thus $\phi(12) = 4$.

For p prime, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Also, if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. These two facts allow us to find $\phi(n)$ for any positive integer n. For example:

$\phi(7878) =$

Euler's Theorem states that if $(a, m) = 1$, where $m \in \mathbb{Z}^+$, then

$$a^{\phi(m)} \equiv 1 \mod m.$$

The group $\mathbb{U}_n$ is cyclic if and only if $n = 1, 2, 4, p^\alpha, 2p^\alpha$, where p is an odd prime. In this case, there are $\phi(\phi(n))$ generators, often referred to as **primitive roots**. In the case when $n = p$, there are $\phi(p-1)$ primitive roots.

A number a has **order** k mod n means that k is the smallest positive integer such that $a^k \equiv 1 \mod n$. Thus a is a primitive root mod n if and only if a has order $\phi(n)$.

Wilson's Theorem.
p is prime iff $(p-1)! \equiv -1 \mod p$.

Corollary. Suppose p is a prime congruent to 1 mod 4. Then $x^2 \equiv -1$ has a solution.

Proof.

(Note that the converse is also true, i.e. with p an odd prime, $x^2 \equiv -1 \mod p$ has a solution only if $p \equiv 1 \mod 4$.)

The following two results are worth noting:

Theorem 1.1 Let n be an integer for which $\mathbb{U}_n$ admits primitive roots and suppose $(a, n) = 1$. Then the congruence $x^k \equiv a \mod n$ has a solution iff

$$a^{\frac{\phi(n)}{d}} \equiv 1 \mod n$$

where $d = \gcd(k, \phi(n))$. Furthermore, if it has solutions, then it has exactly d solutions in $\mathbb{U}_n$.

A special case, originally due to Euler, states:

Corollary: Suppose p is a prime and $(a, p) = 1$. Then the congruence $x^k \equiv a \mod p$ has solution iff $a^{(p-1)/d} \equiv 1 \mod p$, where $d = \gcd(k, p-1)$.

Quadratic Residues.

If $x^2 \equiv a \mod p$ has solution, that is, if a is a square in $\mathbb{Z}_p$, and $a \not\equiv 0$, then we say that a is a **quadratic residue** modulo p, q.r. for short, otherwise it is referred to as a **quadratic non-residue**, (q.n.r.).

For example, in $\mathbb{U}_{11}, \{1, 4, 9, 5, 3\}$ are the quadratic residues and $\{2, 6, 7, 8, 10\}$ are the non-residues.

Theorem 1.2:
For p a prime, exactly half of the numbers in $\mathbb{U}_p$ are quadratic residues.

Proof:
This is almost obvious, but the following proof contains a useful idea.

Euler's Criterion.

We want a simple test to determine when a given number a is a (non-zero) square in $\mathbb{Z}_p$. For example, is 3127 a square in $\mathbb{Z}_{12713}$?

Theorem 1.3:

If p is an odd prime, and $p \not| a$ then $x^2 \equiv a \mod p$ is solvable iff

$$a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

(Hence a is a non-residue if $a^{\frac{p-1}{2}} \equiv -1 \mod p$.)

Proof: This is a special case of Theorem 1.1.

Example: Is 3 a q.r. in $\mathbb{Z}_{23}$?

Euler's criterion is a useful theoretical tool (as you will see in the tutorial problems), but for large moduli it is not very practical.

Legendre's Symbol:

We define the Legendre symbol by:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a q.r.} \mod p \\ -1 & \text{if } a \text{ is a q.n.r.} \mod p \end{cases}$$

where $(a, p) = 1$.

we can now state Euler's theorem as $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

Trivially, for $(a, p) = 1$ we have $\left(\frac{1}{p}\right) = \left(\frac{a^2}{p}\right) = 1$ and for $p \equiv 1 \mod 4$, $\left(\frac{-1}{p}\right) = 1$.

Theorem 1.2 immediately implies that

$$\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0$$

for any odd prime p.

The Legendre symbol has a number of simple properties which assist in its calculation:

Theorem 1.4: If $(a, p) = (b, p) = 1$, p an odd prime, then

(i) $a \equiv b \mod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof: Simple exercise.

Examples: Find $\left(\frac{19}{5}\right), \left(\frac{47}{17}\right), \left(\frac{5}{17}\right)$.

Gauss' Lemma.

There are still computational difficulties, for example, how do we find $\left(\frac{127}{3499}\right)$?

The key to evaluating Legendre symbols is Gauss' famous reciprocity law. Gauss gave a number of proofs of this, but all of them, with one exception, relied on the following rather strange result, known as Gauss' Lemma. (There is a wonderful two line proof (!) but this requires the machinery of characters and Gauss sums, which we will not have time to cover.)

Theorem 1.5: Gauss' Lemma.
Suppose that p is an odd prime and $(a, p) = 1$. Consider the set $S = \{a, 2a, ..., \frac{1}{2}(p-1)a\}$ with elements reduced modulo p. Let k be the number of elements in the reduced set S that are greater than $\frac{p-1}{2}$, then $\left(\frac{a}{p}\right) = (-1)^k$.

Proof:

Example: Use Gauss' Lemma to find $\left(\frac{5}{13}\right)$.

Example: Use Gauss' Lemma to show that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

for any odd prime p.

Example. Suppose q is an odd integer such that $p = 12q + 1$ is prime.
(i) Evaluate $\left(\frac{2}{p}\right)$

(ii) Use Euler's Criterion to show that $2^{6q} \equiv -1 \bmod p$.

(iii) Find a prime factor of $2^{78} + 1$.

The Law of Quadratic Reciprocity.

Theorem 1.6:

Suppose p, q are **odd** primes, then

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if $p \equiv 1 \mod 4$ OR $q \equiv 1 \mod 4$

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p \equiv 3 \mod 4$ AND $q \equiv 3 \mod 4$.

Equivalently,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

Example: Evaluate $\left(\frac{521}{997}\right)$.

There are many proofs of the reciprocity theorem.

The following proof is due to Eisenstein, and attracted Gauss' high approval.

Lemma:
Let a be an **odd** integer and p a prime not dividing a.
Let

$$M = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + ... + \left[\frac{\frac{1}{2}(p-1)a}{p}\right],$$

then $\left(\frac{a}{p}\right) = (-1)^M$.

Proof: Applying the method in Gauss' Lemma, we divide the elements of the set $\{a, 2a, ..., \frac{1}{2}(p-1)a\}$ by p and write

$$a = p\left[\frac{a}{p}\right] + r_1$$

$$2a = p\left[\frac{2a}{p}\right] + r_2$$

$$.....$$

$$\frac{1}{2}(p-1)a = p\left[\frac{a(p-1)/2}{p}\right] + r_{\frac{1}{2}(p-1)}.$$

Now add both sides to get

$$\frac{1}{8}(p^2-1)a = pM + r_1 + r_2 + ... + r_{\frac{1}{2}(p-1)}.$$

Now the remainders are all different (since $p \not| a$) and (as in the proof of Gauss' Lemma) we let $a_1, ..., a_k$ be those remainders which are $> \frac{1}{2}(p-1)$ and $a_{k+1}, ..., a_{\frac{1}{2}(p-1)}$ be the rest. Hence we can write the above equation as:

$$\frac{1}{8}(p^2-1)a = pM + a_1 + a_2 + ... + a_k + a_{k+1} + ... + a_{\frac{1}{2}(p-1)}. \qquad (*).$$

Now $p - a_1, p - a_2, ..., p - a_k$ will be less than $\frac{1}{2}(p-1)$ and so the set of numbers

$$\{p - a_1, p - a_2, ..., p - a_k, a_{k+1}, ..., a_{\frac{1}{2}(p-1)}\}$$

will just be the numbers $\{1, 2, 3, ..., \frac{1}{2}(p-1)\}$ (in some order). So adding these numbers we have

$$\frac{1}{8}(p^2-1) = kp - (a_1 + a_2 + ... + a_k) + a_{k+1} + ... + a_{\frac{1}{2}(p-1)}.$$

Subtracting this from equation (*) we have:

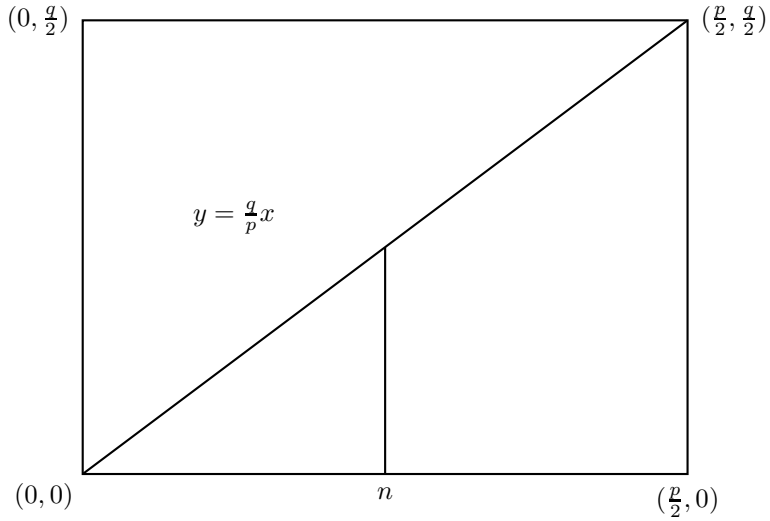
$$\frac{1}{8}(p^2-1)(a-1) = p(M-k) + 2a_1 + ... + 2a_k.$$

Since a is odd, $M - k$ is even so M and k are either both even or both odd and so $(-1)^k = (-1)^M$, and thus $\left(\frac{a}{p}\right) = (-1)^k = (-1)^M$.

Proof of Theorem 1.6:

Let $M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + ... + \left[\frac{\frac{1}{2}(p-1)q}{p}\right]$ and
$N = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + ... + \left[\frac{\frac{1}{2}(q-1)p}{q}\right]$, then by the Lemma, we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N}$ and so we need to show that $M + N = \frac{1}{2}(p-1)\frac{1}{2}(q-1)$.

Consider a rectangle R in the plane with vertices $(0,0), (\frac{p}{2}, 0), (0, \frac{q}{2}), (\frac{p}{2}, \frac{q}{2})$ as shown.



The rectangle R contains $\frac{1}{2}(p-1)\frac{1}{2}(q-1)$ lattice points excluding the boundary. The diagonal from $(0,0)$ to $(\frac{p}{2}, \frac{q}{2})$ has equation $y = \frac{q}{p}x$ and so for any positive integer $n < \frac{p}{2}$, $\left[\frac{nq}{p}\right]$ is the number of lattice points on the vertical line through the point $(n, 0)$ that lie on or below the diagonal. Now there are no lattice points on the diagonal since p, a prime, cannot cancel with any integer x less than $\frac{p}{2}$.

Thus M counts all the lattice points below that diagonal and similarly N counts all those above the diagonal and hence $N + M = \frac{1}{2}(p-1)\frac{1}{2}(q-1)$ as claimed.

Example: Show that 5 is a q.r. for all primes of the form $p \equiv \pm 1 \mod 10$.

Example: Find all the primes for which 3 is a q.r. modulo p.

Sums of Integer Squares:

The numbers 8 and 90 can be expressed as the sum of two squares,

$$8 = 2^2 + 2^2 \qquad 90 = 3^2 + 9^2,$$

while we need three squares to represent 35,

$$35 = 5^2 + 3^2 + 1^2$$

and even three squares is not enough for 28 which is

$$28 = 5^2 + 1^2 + 1^2 + 1^2 = 3^2 + 3^2 + 3^2 + 1^2.$$

In this section, we try to see what is happening here and how we might predict the minimal number of squares required to represent a given positive integer.

As usual, we begin by restricting ourselves to primes and since the squares modulo 4 are $0, 1$, we immediately see that a prime congruent to 3 mod 4 is NOT the sum of two squares, (this is, of course, true for any integer n, not just primes), while the situation for primes congruent to 1 mod 4 is covered by the following theorem:

Theorem 1.7: Suppose p is a prime congruent to 1 mod 4. Then p can be expressed as the sum of two integer squares.

Proof: By the corollary to Wilson's Theorem, there is an $x \in \mathbb{Z}_p$ such that $x^2 \equiv -1 \mod p$. Consider the set $S = \{0, 1, 2, ..., \lfloor \sqrt{p} \rfloor\}$ and all the numbers of the form $a + bx$ with $a, b \in S$.

There are $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$ choices for the a and b, so, modulo p, by the pigeon-hole principle,

$$a + bx \equiv A + Bx \mod p$$

for some $a, b, A, B \in S$, and the pair $(a, b) \neq (A, B)$. Hence

$$(a - A) \equiv (B - b)x \mod p \Rightarrow (a - A)^2 \equiv -(B - b)^2 \mod p \Rightarrow (a - A)^2 + (B - b)^2 = cp$$

for some integer c. But $|a - A| < \sqrt{p}$ and $|b - B| < \sqrt{p}$, so $(a - A)^2 + (B - b)^2 < 2p$ which gives $c = 1$ and the result follows.

Note, of course, that $2 = 1^2 + 1^2$, so this deals with all the primes.

The simple identity, $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$, which shows that the product of two numbers, each of which is the sum of two squares, is also the sum of two squares, enables us, (with a little extra work), to conclude that:

Theorem 1.8: Factor the positive integer n as

$$n = 2^{\epsilon} n_1^2 p_1 p_2 ... p_k$$

where $\epsilon \in \{1, -1\}$ and p_i is a prime.

Then, n is the sum of two squares iff $p_i \equiv 1 \mod 4$ for $i = 1, 2, ..., k$.

(Note that writing $(a^2 + b^2) = |a + ib|^2 = N(a + ib)$ proves the identity and gives us a simple way to produce a desired representation.)

Example: $n = 5525 = 5^2 \times 13 \times 17$.

The Number of Representations:

We now know exactly which numbers can be represented by the sum of two squares and so we turn to the question of the **number** of a such representations. We will count a representation such as $5 = 2^2 + 1^2$ as having 8 representations, since we can write

$$5 = (\pm 2)^2 + (\pm 1)^2 = (\pm 1)^2 + (\pm 2)^2.$$

We will write $N(n)$ to denote the number of representations of n as a sum of two squares, counting sign and order, so by the above, $N(5) = 8$.

We introduce the function $f(n) = D_1(n) - D_3(n)$, where $D_i(n)$ denotes the number of divisors of n of the form $4k + i$.

The following theorem, (which we state without proof), goes back to Jacobi.

Theorem 1.9:

With the above notation, for any positive integer $n > 1$, we have

$$N(n) = 4f(n).$$

Thus, if $n = p$, a prime of the form $4k + 1$, then $N(p) = D_1(p) = 8$ and so, ignoring order and signs, there is only one way to express such a prime as a sum of two squares.

Pythagorean Triples:

Before looking at sums of 3 and 4 squares, we digress briefly to look at Pythagorean triples.

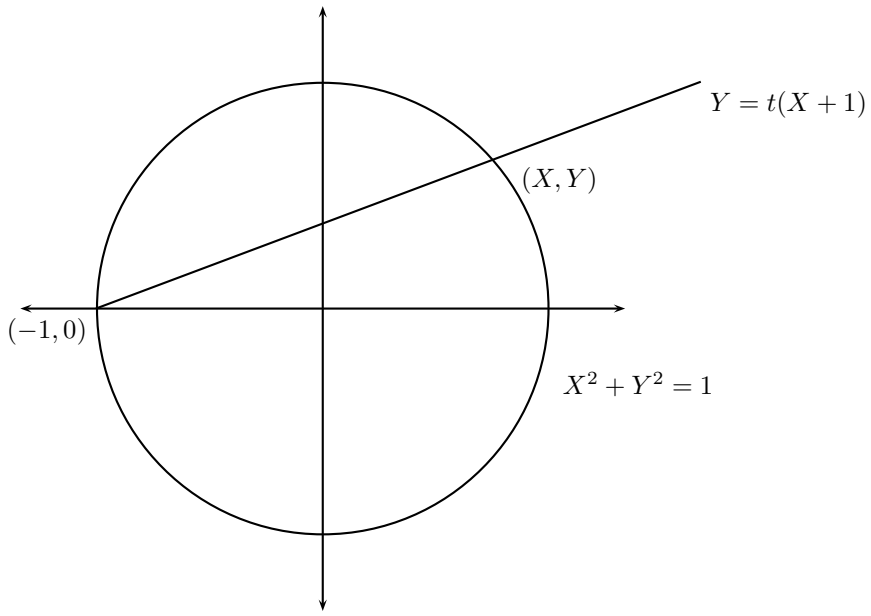
A triple (x, y, z) of positive integers such that $x^2 + y^2 = z^2$ is known as a **Pythagorean Triple.**

We wish to find all such triples.

Firstly, we take the equation $x^2 + y^2 = z^2$ and divide by z^2 to get $(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1$, so that if x, y, z are integers, then $\frac{x}{z}$ and $\frac{y}{z}$ are **rational** numbers. Put $X = \frac{x}{z}, Y = \frac{y}{z}$.

So, given integers x, y, z such that $x^2 + y^2 = z^2$, the equation $X^2 + Y^2 = 1$ has rational solutions, and conversely, if we can find rational solutions of $X^2 + Y^2 = 1$, we can express X and Y with a same denominator and thus get integers x, y, z with $x^2 + y^2 = z^2$.

Hence the problem of finding triads is equivalent to finding **rational** points on the circle $X^2 + Y^2 = 1$. (Note that the correspondence is NOT 1-1, since we can get $(3, 4, 5)$ and $(6, 8, 10)$ etc. from the same rational point $(\frac{3}{5}, \frac{4}{5})$. If however, we insist that $\gcd(x, y, z) = 1$ then the correspondence is 1-1.)



Consider the circle $X^2 + Y^2 = 1$ and draw a line passing through the point $(-1, 0)$ with slope t, which meets the circle at a point (X, Y). We restrict t between 0 and 1 so there will be an intersection point in the first

quadrant.

The equation of the line is $Y = t(X + 1)$.

Now observe that if (X, Y) is a rational point, then $t = \frac{Y}{X+1}$ is also rational. Conversely, if t is rational, solving the line $Y = t(X + 1)$ with the circle $X^2 + Y^2 = 1$, we have

$$(1 + t^2)X^2 + 2t^2X + (t^2 - 1) = 0.$$

We know that one of the roots is $X = -1$, so the other root is $X = \frac{1-t^2}{1+t^2}$ and so $Y = \frac{2t}{1+t^2}$. Thus, if t is rational, $(0 < t < 1)$, then (X, Y) will also be rational.

Example: $t = \frac{73}{91}$ gives $(X, Y) = (\frac{2952}{13610}, \frac{13286}{13610})$, hence $(2952, 13286, 13610)$ is a pythagorean triad.

We can now construct formulae to generate all the triads.

Put $t = \frac{u}{v}$, so $X = \frac{v^2-u^2}{v^2+u^2}, Y = \frac{2uv}{v^2+u^2}$. Thus

$$x = k(v^2 - u^2), \quad y = 2uvk, \quad z = k(u^2 + v^2)$$

where k is an integer, and $0 < u < v$.

Example: $k = 1, u = 5, v = 7$; gives the triad $(24, 70, 74)$

Note that the k is important if all triads are to be obtained. For example, if $k = 1$, the triad $(9, 12, 15)$ cannot be obtained.

Primitive triads:
If (a, b, c) is a triad and $\gcd(a, b, c) = 1$ then the triad is said to be *primitive*. A little thought will reveal that the conditions required on u, v and k to generate primitive triads are:

$k = 1$, $\gcd(u, v) = 1$ **and** u and v have opposite parity.

Example: $u = 5, v = 7$ does not yield a primitive triad (as seen in the above example) since the numbers are both odd.

$u = 2, v = 3$ gives the triad $(5, 12, 13)$ which is clearly primitive.

An Application to Fermat's Last Theorem for $n = 4$.

Fermat claimed that the equation $x^n + y^n = z^n$ has no positive integer solutions (x, y, z) for $n \geq 3$. He also claimed to have a proof, but never wrote it down. This result has only recently been proven using very advanced techniques. The problem is generally refered to as 'Fermat's Last Theorem' and was one of the 'holy grails' of mathematics.

We can use the ideas developed above to prove it true for the case $n = 4$.

Firstly note that if $x^4 + y^4 = z^4$ has integer solutions then so does $x^4 + y^4 = z^2$, so suppose (x, y, z) satisfy this last equation with z **as small as possible**. The idea is to find integers (X, Y, Z) such that $X^4 + Y^4 = Z^2$, with $Z < z$, thus contradicting the minimality of z.

(This technique is known as the "Method of Infinite Descent" and seems to have been first used by Fermat.)

We may suppose that x, y, z have no common factor and that $\gcd(x, y) = 1$. Therefore (x^2, y^2, z) forms a primitive pythagorean triad, and so $x^2 = p^2 - q^2, y^2 = 2pq, z = p^2 + q^2$, where p, q are relatively prime integers with opposite parity.

Now if p is even, q odd, then $x^2 \equiv 3 \bmod 4$ which is impossible, so p is odd and q even. Put $q = 2r$ giving

$$x^2 = p^2 - (2r)^2, \left(\frac{1}{2}y\right)^2 = pr \text{ with gcd } (p, r) = 1$$

The second of these equations implies that p and r are perfect squares, so put $p = Z^2, r = W^2$, hence

$$x^2 + (2W^2)^2 = Z^4$$

so $(x, 2W^2, Z^2)$ is a primitive triad, and thus we can write

$$x = P^2 - Q^2, 2W^2 = 2PQ, Z^2 = P^2 + Q^2 \text{ with } \gcd(P, Q) = 1.$$

(Check here that $2W^2 = P^2 - Q^2$ is not possible, since P and Q must have opposite parity.)

The second equation again gives P, Q squares, so put $X^2 = P, Y^2 = Q$, then from the third equation we have $X^4 + Y^4 = Z^2$ but

$Z^2 = p = \sqrt{z - q^2} < \sqrt{z} < z < z^2$, so $Z < z$, contradicting the minimality of z.

Sums of Three Squares:

We have seen that certain numbers cannot be written as the sum of two squares, and there are numbers, such as 15, which cannot be written as the sum of three squares. We would like to characterise when a number can be written as the sum of three squares.

Lemma: If $x \equiv 7 \bmod 8$ then x cannot be written as the sum of three squares.

Proof:

The full story is:

Theorem 1.10: An integer n can be expressed as the sum of (at most) three integer squares unless $n = 4^\alpha(8k + 7)$, for some integers α and k.

Proof:

Sums of Four Squares:

The following theorem, due to Lagrange, completes the story on sums of squares. We will not give the proof here, but it can be gotten from an interesting generalisation of complex numbers called quaternions, from which the following (amazing!) identity is derived.

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = (ax+by+cz+dw)^2 + (ay-bx-cw+dz)^2$$

$$+(az+bw-cx-dy)^2 + (aw-bz+cy-dx)^2.$$

This tells us that if X and Y are the sum of four squares, then so is their product. From this, one can (with a lot of work!) prove:

Theorem 1.11: (Lagrange) Every integer can be expressed as the sum of (at most) four squares.

Proof: Deleted.

Waring's Problem:

Having dealt with representations by sums of squares, it is natural to ask about higher powers. For example, it is known that every integer can be written as the sum of (at most) nine cubes. In fact only the numbers 23 and 239 actually require nine cubes,viz. $23 = 2^3+2^3+1^3+1^3+1^3+1^3+1^3+1^3+1^3$.

In 1970 it was shown that every integer can be written as the sum of 19 fourth powers.

For each positive integer k, let $G(k)$ be the minimum number of kth powers required to represent every integer, equivalently, we want the smallest number $G(k)$, such that $x = x_1^k + x_2^k + ... + x_{G(k)}^k$ has integer solutions $x_1, ..., x_{G(k)}$, for all integers x.

Can we find a formula for $G(k)$? No such formula is known and the problem is often refered to as Waring's problem.

It is known that:

$G(2) = 4$ (Theorem 1.11)
$G(3) = 9$
$G(4) = 19$
$G(5) = 37.$

As we have seen, for fixed k only certain numbers actually need $G(k)$ terms, for example with $k=3$, only 23 and 239 need nine cubes.

Consider the number $n = 2^k\left[\left(\frac{3}{2}\right)^k\right] - 1$, where $[x]$ denotes the greatest integer less or equal to x. Observe that if $k=3, n=23$. This number n then, is an attempt to find the 'worst' case for each k.

Also note that $n < 2^k\left(\frac{3}{2}\right)^k - 1 < 2^k.\frac{3^k}{2^k} = 3^k$, so to represent n as the sum of kth powers, we need $x_i < 3$, i.e. $x_i \leq 2$. In fact we need $\left(\left[(\frac{3}{2})^k\right] - 1\right)$ lots of 2^k, leaving (2^k-1) lots of 1^k.

That is, we can write n as

$$n = \left(\left[\left(\frac{3}{2}\right)^k\right] - 1\right).\underline{2^k} + (2^k-1).\underline{1^k}$$

This would require $\left[\left(\frac{3}{2}\right)^k\right] - 1 + 2^k - 1 = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$ terms, so

$$G(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$$

which we will call $l(k)$.

Observe that

$$l(2) = 4 = G(2)$$
$$l(3) = 9 = G(3)$$
$$l(4) = 19 = G(4)$$
$$l(5) = 37 = G(5)$$

It is believed that $G(k) = l(k)$ but no proof has been found.

UNSW AUSTRALIA.
SCHOOL OF MATHEMATICS AND STATISTICS.

MATH5645: TOPICS IN NUMBER THEORY.
§2 SOME ELEMENTARY RESULTS ON THE DISTRIBUTION OF PRIMES:

The oldest result concerning the prime numbers is probably the fact that they increase without bound. This goes back to Euclid.

Theorem 2.1: There are infinitely many primes.

Proof 1: (Euclid) Suppose not, then we can write down the set S of **all** primes,

$$S = \{p_1, p_2, p_3, \cdots, p_n\}.$$

Now let $N = p_1 p_2 \cdots p_n + 1$. If N is prime we have a contradiction since clearly $N \notin S$. Hence N has a prime factor q, but $q \notin S$ and again we have a contradiction.

Proof 2: (Kummer). Again, suppose not and again let S be the set of all primes as above.

Proof 3:

(Proof 3 is constructive and not by contradiction. It allows you to explicitly write down a number with at least 1000 distinct prime factors!).

Definition: Let p_n denote the nth prime (so $p_1 = 2, p_2 = 3, p_4 = 5$ and so on) and let $\pi(n)$ denote the number of primes less or equal to n.

Thus $p_k = n \Leftrightarrow \pi(n) = k$.

Ex: $p_{10} = 29$ and $\pi(29) = 10$.

From Euclid's proof we can easily deduce that $p_n \leq p_1 p_2 \cdots p_{n-1} + 1$. Using this we can prove:

Theorem 2.2: $p_n \leq 2^{2^{(n-1)}}$, for $n \geq 1$.

Proof: (By induction).

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

Proof:

Note that this also shows there are infinitely many primes, but as a bound it is rather poor. For example, it says that $\pi(10^9) \geq \log\log 10^9 / \log 2 \approx 4$ (!)

Primes and Squares:

How do the primes compare with the squares? There are infinitely many of both, but since $\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$, in some sense there are not too many squares. Does $\sum_{n=1}^{\infty} \frac{1}{p_n}$ converge? We shall presently prove that this series diverges, so that in some sense, there are more primes than squares. It is interesting to note that if we take the above sum over all **known** primes, then the sum is relatively small!

Before we tackle the proof of this result, I want to introduce one of the key ideas (due to Euler) in the analysis of prime numbers.

Euler's Product:

Ignoring problems of convergence, let us see what we get when we expand

$$\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots\right)\left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots\right)\cdots$$

$$= \prod_{p \text{ prime}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right).$$

One the one hand, we have $\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=\left(1-\frac{1}{p}\right)^{-1}$ and so the product can be written as

$$\prod_{p \text{ prime}} \left(1-\frac{1}{p}\right)^{-1}.$$

On the other hand, Euler noted that by unique factorisation in the integers, the expansion of the left hand side above, produces the reciprocal of each positive integer **exactly** once. So

$$\prod_{p \text{ prime}} \left(1-\frac{1}{p}\right)^{-1} = \sum_{k=1}^{\infty} \frac{1}{k}.$$

Now at this stage, you will object that this is nonsense, since the right-hand side (and in fact the left hand side) diverges. Nonetheless, this 'equation' is really trying to say something important. We can use the same argument to prove that

$$\prod_{p \text{ prime}} \left(1-\frac{1}{p^s}\right)^{-1} = \sum_{k=1}^{\infty} \frac{1}{k^s},$$

which **is** valid for $s>1$. The function $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^s}$, denoted by $\zeta(s)$, plays a central role in analytic number theory and is known as the *Riemann Zeta Function.* We will study this function in much more detail later. For the moment, let us simply observe that

$$\prod_{i=1}^{\pi(n)} \left(1-\frac{1}{p_i}\right)^{-1} = 1+\frac{1}{2}+\cdots+\frac{1}{n}+\ldots > 1+\frac{1}{2}+\cdots+\frac{1}{n}.$$

The Sum $\displaystyle\sum_{p\leq x} \frac{1}{p}$.

We can now prove that the sum $\displaystyle\sum_{p\leq x} \frac{1}{p}$ diverges as $x\to\infty$ and furthermore, obtain a good estimation as to how fast it grows.

Theorem 2.3a: $\sum_{i=1}^{\infty} \frac{1}{p_i}$ diverges.

Proof: (There are many proofs of this. The proof given here, although slightly longer than some others contains a number of ideas which we will use again later.)

Although this series diverges, it does so very *slowly*. We would like to get some idea of the rate of growth. The following result gives a lower bound on $\sum_{p \leq x} \frac{1}{p}$, but from it, one can show that the true order of magnitude of this sum is $\log \log x$. As usual, in the statement $p \leq x$, it is assumed that p is prime.

As often, we need a simple Lemma:

Lemma:

(i) For $x \geq 1$, $\quad \sum_{n \leq x} \frac{1}{n} \geq \log x$.

(ii) For $x \geq 1$, $\quad 1 + \frac{1}{x} \leq e^{\frac{1}{x}}$.

Proof: (i) is left as an exercise - draw a diagram!

(ii) Follows immediately from the series expansion of the right-hand side.

Theorem 2.3b

For $x > 2$,

$$\sum_{p \leq x} \frac{1}{p} \geq \log \log x - \log \zeta(2).$$

Proof: (Again there are a number of proofs of this. I have chosen the one I think is the nicest.)

This, of course, gives yet another proof that the series $\sum_p \frac{1}{p}$ diverges. We will look again in more detail at this sum in Chapter 6.

Bertrand's Postulate:

We now state and prove an important result, known as *Bertand's Postulate*. (It is now a **Theorem**, but the name comes from the time when it was a conjecture.) It was first proven by Chebychev (1852) but the proof given here is a modification of a proof due to Erdös.

Lemma:
(a) For all real $x \geq 2$, $\prod_{p \leq x} p \leq 4^{x-1}$.
(b) (Legendre's Theorem) The number $n!$ contains the prime factor p exactly $\sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor$ times.
(c) For $n \geq 1$, $\binom{2n}{n} \geq \frac{4^n}{2n+1}$

Proof:
(a) See tutorial problems.

(b) Well known. (For example, find the number of zeros at the end of 1000!)

(c) $\binom{2n}{n}$ is the greatest among the co-efficients $\binom{2n}{0}, \binom{2n}{1}, \cdots, \binom{2n}{2n}$. Hence $\binom{2n}{n}$ cannot be less than their average which is $\frac{1}{2n+1} 2^{2n} = \frac{4^n}{2n+1}$.

Theorem 2.4: (Bertrand's Postulate).

If $n > 2$ then there exists a prime p satisfying $n < p \leq 2n$.

Proof:
If $n < 600$ then the result is true, since we only need to check that
$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 547$ are all primes.

We proceed by trying to find a bound on the size of $\binom{2n}{n}$, using its prime factors. These prime factors

fall into 4 regions. For example if $n = 39$,

$$\binom{78}{39} = \begin{array}{c|c|c|c} 2^4.5^2.7^2 & 11.23 & & 41.43.47.53.59.61.67.71.73 \\ \hline p \le \sqrt{2n} & \sqrt{2n} < p \le \frac{2}{3}n & \frac{2}{3}n < p \le n & n < p < 2n \end{array}$$

Let $r(p)$ denote the largest power of a prime p which divides $\binom{2n}{n}$. In the example above, with $n = 39$, we have $r(2) = 4, r(71) = 1$ and $r(29) = 0$

Using Legendre's theorem, $r(p) = \sum_{k\ge 1} \lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor$.

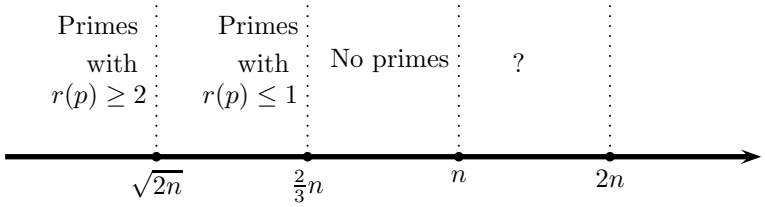
Each summand satisfies,

$$\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) = 2$$

and so is at most 1. Thus, $r(p) \le \max\{t : p^t \le 2n\}$, (since if $p^t > 2n$, the summand is vacuous). So in particular, in the region of all primes $p \le \sqrt{2n}$, the contribution to $\binom{2n}{n}$ is $\prod_{p\le\sqrt{2n}} p^{r(p)} \le \prod_{p\le\sqrt{2n}} 2n$.

Also if $r(p) \ge 2$, we have $p \le \sqrt{2n}$. Thus, primes p greater than $\sqrt{2n}$ appear at most once in the factorisation of $\binom{2n}{n}$.

Now for a rather striking observation (which is the key to the whole thing). Primes p, for which $\frac{2}{3}n < p \le n$, do NOT divide $\binom{2n}{n}$ at all! For if $3p > 2n$, p and $2p$ are the only multiples of p in the numerator of $\frac{(2n)!}{n!n!}$ while $p|n!$ (in fact $p||n!$) and so the two p's on the top cancel with the two p's on the bottom.



We can now estimate the size of $\binom{2n}{n}$. For $n \ge 3$, using the Lemma,

$$\frac{4^n}{2n+1} \le \binom{2n}{n} \le \prod_{p\le\sqrt{2n}} 2n \prod_{\sqrt{2n}<p\le\frac{2}{3}n} p \prod_{n<p\le 2n} p$$

Now suppose that the desired result is **false**, then the last product is 1, so we have

$$\frac{4^n}{2n+1} \le (2n)^{\sqrt{2n}} \prod_{\sqrt{2n}<p\le\frac{2}{3}n} p \le (2n)^{\sqrt{2n}} \prod_{p\le\frac{2}{3}n} p \le (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n-1} < (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n}$$

using part (a) of the Lemma.
This last inequality implies,

$$4^{\frac{1}{3}n} \le (2n+1)(2n)^{\sqrt{2n}} < (2n)^2(2n)^{\sqrt{2n}} = (2n)^{2+\sqrt{2n}}.$$

Taking logs this is equivalent to $\frac{1}{3}n\log 4 \le (\sqrt{2n}+2)\log(2n)$ which is false for sufficiently large n. In fact a MAPLE sketch indicates that it is false for $n > 600$.

Notes:

1. The above result can also be written as $\pi(2n) - \pi(n) \ge 1$ for $n \ge 2$. This can be generalised to show that $\pi(2n) - \pi(n) \ge 2$ for $n \ge 6$.

2. Using the same ideas above, it can be shown that $\prod_{n<p\leq 2n} p \geq 2^{\frac{n}{30}}$ for $n \geq 4000$, so there are at least $\log_{2n} 2^{\frac{n}{30}}$ primes between n and $2n$. The Prime Number Theorem gives the true order to be $\frac{n}{\log n}$.

3. Is there always a prime between n^2 and $(n+1)^2$? This is unsolved.

Primes in Arithmetic Sequences:

We saw earlier that the primes naturally split into those which are congruent to 1 mod 4 and those congruent to -1 mod 4. (For example the 1 mod 4 primes are the sum of two squares.)

Theorem 2.5a:

There are infinitely many primes congruent to -1 mod 4.

Proof: We model the proof on that of Theorem 2.1.

Note that the same kind of argument will NOT work for primes congruent to 1 mod 4.

Theorem 2.5b: There are infinitely many primes congruent to 1 mod 4.

Proof:

In the tutorial problems, you will be asked to prove similar special cases. All of these are special cases of the following key result due to Dirichlet, namely, if $(a, b) = 1$ then $\{a + bn : n = 1, 2, \cdots\}$ contains infinitely many primes. The *ad hoc* methods used above will not give the general result. We need a more sophisticated approach to the problem, and the proof of Dirichlet's Theorem will be covered in Chapter 4.

Chebychev's Bounds:

Let us return to the function $\pi(x)$. At the age of 14 (!!), Gauss guessed that this function can be asymptotically approximated by $\frac{x}{\log x}$ in the sense that $\frac{\pi(x)}{\frac{x}{\log x}} \to 1$ as $x \to \infty$. This is known as the **prime number theorem**. It will be the other main theorem we will prove in this course. Gauss could not prove it, but Chebychev was able to show that it was at least roughly correct. More precisely, he proved that **if** $\pi(x) \sim \frac{Cx}{\log x}$ then $C = 1$ and that there exist constants A and B such that

$$\frac{Ax}{\log x} \leq \pi(x) \leq \frac{Bx}{\log x}.$$

We will find such constants, but not quite as good as those which Chebychev found.

To progress to the result, we need a couple of technical facts about the binomial co-efficients.

Lemma:

(i) For $n \geq 1$, $2^n \leq \left(\begin{array}{c} 2n \\ n \end{array} \right) < 2^{2n}$

(ii) For $n \geq 1$, $p \left| \left(\begin{array}{c} 2n \\ n \end{array} \right) \right.$ for **every** prime p such that $n < p \leq 2n$.

Proof:

We can now see that Gauss' guess was in the right ballpark.

Theorem 2.6 (Chebychev)

$$\frac{2}{3}\frac{x}{\log x} < \pi(x) < 1.7\frac{x}{\log x}.$$

(Chebychev in fact was able to reduce the left hand constant to 0.921 and the right hand one to 1.105, but these can be further refined.)

Proof:

Firstly we note that $\pi(x) < 1.7\frac{x}{\log x}$ for $x < 1200$ by trial and error (or use MAPLE).

Now suppose the right-hand inequality is true for all $x \leq n$.
Consider $\left(\begin{array}{c} 2n \\ n \end{array} \right)$. From the Lemma, we have

$$\prod_{n<p\leq 2n} p \leq \left(\begin{array}{c} 2n \\ n \end{array} \right) < 2^{2n}.$$

Now there are $\pi(2n) - \pi(n)$ primes (strictly) between n and $2n$ each greater than n so

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p\leq 2n} p < 2^{2n}.$$

Taking logarithms and dividing by $\log n$ we have

$$\pi(2n) - \pi(n) < \frac{2n\log 2}{\log n} < 1.39\frac{n}{\log n}$$

(NB. $2\log 2 \approx 1.386$).
Now by assumption $\pi(n) < 1.7\frac{n}{\log n}$ so

$$\pi(2n) < 1.39\frac{n}{\log n} + \pi(n) < (1.39 + 1.7)\frac{n}{\log n} = 3.09\frac{n}{\log n}.$$

It is left as an exercise to show that $\frac{3.09n}{\log n} < 1.7 \times \frac{2n}{\log(2n)}$ if $n > 1200$. (In fact if $n > 1001$.)

Hence, if the inequality is true for n then is it true for $2n$. Also

$$\pi(2n+1) \leq \pi(2n) + 1 < 3.09\frac{n}{\log n} + 1 < 1.7 \times \frac{(2n+1)}{\log(2n+1)}$$

if $n > 1200$ (This last inequality is also left as an exercise but can be easily seen if we use MAPLE to draw the relevant graphs.)

Hence, if the inequality is true for n then it is true for $2n$ and $2n+1$, and so holds for all n.

Now for the left-hand side.

By Legendre's Theorem, (in the earlier Lemma), the highest power of p which divides $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$ is given by p^{ν_p} where

$$\nu_p = \sum_r \left(\lfloor \frac{n}{p^r} \rfloor - \lfloor \frac{k}{p^r} \rfloor - \lfloor \frac{n-k}{p^r} \rfloor \right).$$

Now it is an exercise to show that $\lfloor x \rfloor - \lfloor y \rfloor \leq \lfloor x - y \rfloor + 1$ and so each term in the sum is either 0 or 1. Furthermore, if $p^r > n$, i.e. if $r > \log_p n$, then each term of the sum is 0. Thus, $\nu_p \leq \log_p n$, and so $p^{\nu_p} \leq p^{\log_p n} = n$. Hence we have

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \prod_{p|\left(\begin{smallmatrix} n \\ k \end{smallmatrix} \right)} p^{\nu_p} \leq n^{\pi(n)},$$

since there are at most $\pi(n)$ terms in the product.
Also we note that $2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \leq (n+1)n^{\pi(n)}$ (there are $(n+1)$ terms in the sum) and so $n^{\pi(n)} \geq \frac{2^n}{n+1}$.
This gives

$$\pi(n) \geq \frac{1}{\log n}(n \log 2 - \log(n+1)) > \frac{2}{3}\frac{n}{\log n}$$

if $n > 220$. This last inequality is an exercise. (Note that $\log 2 \approx \frac{2}{3}$). (A MAPLE plot here is convincing).

Theorem 2.7: For $n \geq 1$, the nth prime, p_n, satisfies the inequalities

$$0.58n \log n < p_n < 3n(\log n + \frac{1}{2}).$$

Proof: If $k = p_n$ then $k \geq 2$ and $n = \pi(k)$.
Applying the previous theorem, we have

$$n = \pi(k) < \frac{1.7k}{\log k} = \frac{1.7p_n}{\log p_n}.$$

Hence $p_n > 0.58n \log p_n > 0.58n \log n$.

Also, $n = \pi(k) > \frac{2}{3}\frac{k}{\log k} = \frac{2}{3}\frac{p_n}{\log p_n}$, and hence

$$p_n < \frac{3}{2}n \log p_n \qquad (*).$$

Now $\log x < \sqrt{x}$, if $x > 1$, so $\log p_n \leq \sqrt{p_n}$. Thus, using (*), $p_n < \frac{3}{2}n\sqrt{p_n}$ giving $p_n < \frac{9}{4}n^2$. Taking logs, and using (*) again, we obtain

$$p_n < 3n(\log \frac{3}{2}n) < 3n(\log n + \frac{1}{2}), \quad (\text{ since } \log \frac{3}{2} \approx 0.4).$$

Ex:

n	$0.58n \log n$	p_n	$3n(\log n + \frac{1}{2})$
3	1.91	5	14.4
4	3.22	7	22.6
9	11.47	23	72.8
10	13.35	29	84.1

Notes:
1. The 'correct' order of magnitude of p_n is $n \log n$. (This is equivalent to the Prime Number Theorem.)

2. We obtain yet another proof that $\sum \frac{1}{p}$ diverges, since we can compare this series to $\sum \frac{1}{n \log n}$.

3. These difficult, but *ad hoc*, methods, do not produce particularly satisfying results. We need much better techniques.

UNSW AUSTRALIA.
SCHOOL OF MATHEMATICS AND STATISTICS.
MATH5645: TOPICS IN NUMBER THEORY.

§3 ARITHMETIC FUNCTIONS, DIRICHLET MULTIPLICATION:

A function $f : \mathbb{N} \to \mathbb{C}$ is called an *arithmetic* function.

If an arithmetic function f has the property that $f(ab) = f(a)f(b)$, whenever $(a, b) = 1$, then f is said to be *multiplicative*. If $f(ab) = f(a)f(b)$ for **any** positive integers a, b then f is said to be *completely multiplicative*. It is easy to see that $f(1) = 1$ for any multiplicative function f, provided $f \neq 0$.

A multiplicative function is completely determined by its values at prime powers.

In this section we are going to look at a number of important examples of multiplicative functions and define a special multiplication on the set of such functions. The function values of these functions tend to be rather spasmodic but we can *smooth* these out by averaging and then look at developing estimates of their average rate of growth.

Divisor Functions:

We define the well known *number of divisors* and *sum of divisor* functions τ and σ.

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d.$$

For example, $\tau(12) = 6, \sigma(12) = 28$.

Note that we may sometimes refer to $\sigma_0(n)$, which is the sum of the *aliquot* factors of n, i.e. $\sigma_0(n) = \sigma(n) - n$.

Also, $\sigma^k(n) = \sum_{d|n} d^k$ is the sum of the kth powers of the divisors.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ then clearly

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1),$$

since any divisor of n has the form $p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$, where $0 \leq \beta_i \leq \alpha_i$, and so there are $\alpha_i + 1$ choices for each exponent.

Similarly

$$\sigma(n) = \prod_{i=1}^{r} (1 + p_i + \dots + p_i^{\alpha_i}) = \prod_{i=1}^{r} \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right).$$

This becomes clear when we think of expanding out

$$(1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \cdots (1 + p_r + p_r^2 + \dots + p_r^{\alpha_r})$$

and using the Fundamental Theorem of Arithmetic.

Ex: $n = 1341648 = 2^4 \times 3^2 \times 7 \times 11^3$.

So $\tau(n) = 5 \times 3 \times 2 \times 4 = 120$
and $\sigma(n) = (1 + 2 + 4 + 8 + 16)(1 + 3 + 9)(1 + 7)(1 + 11 + 121 + 1331) = 4719936$.

It is easy to show that both σ and τ are multiplicative (but not completely multiplicative, since $3 = \tau(4) \neq$

$\tau(2)\tau(2) = 4$ and $7 = \sigma(4) \neq \sigma(2)\sigma(2) = 9$.)

The Möbius Function: $\mu(n)$.

This is a very important function in both number theory in general and in analytic number theory in particular.
To motivate the definition, recall that for $s > 1$,

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

Hence we define the Möbius function $\mu(n)$ by:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2|n \\ (-1)^r & \text{if } n = p_1 p_2 .... p_r \end{cases}$$

Thus $\mu(n)$ is zero if n has a square factor.

We can thus write $\dfrac{1}{\zeta(s)} = \displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$.

Ex: $\mu(12) = 0, \mu(30) = -1$.

The Möbius function is, in some sense, a discrete version of the Dirac δ function.

Theorem 3.1:

$$\sum_{d|n} \mu(d) = \lfloor \frac{1}{n} \rfloor = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Proof:

Euler's Totient Function: $\phi(n)$.

We previously defined the Euler *totient* function ϕ by $\phi(1) = 1$ and for $n > 1$,

$$\phi(n) = |\{x : (n, x) = 1\}| = \sum_{k=1}^{n}{}' 1,$$

where the $'$ denotes that the sum is taken over all positive integers k, that are less than and relatively prime to n. We also stated the result:

$$\phi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}) = \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

so ϕ is multiplicative.

Multiplicative Functions:

Theorem 3.2: If f is multiplicative then so is $F(n) = \sum_{d|n} f(d)$.

Proof: Let $(m, n) = 1$. A divisor d of mn can be uniquely expressed as $d = d_1 d_2$ where $d_1 | m$ and $d_2 | n$, with $(d_1, d_2) = 1$. Hence

(Here we have written a sum of products as a product of sums.)

We can use this important result to prove:

Theorem 3.3: For $n \geq 1$, $\sum_{d|n} \phi(d) = n$.

Proof:

Dirichlet Multiplication.

Sums of the form $\sum_{d|n} f(d)g(\frac{n}{d})$ or $\sum_{n=d_1 d_2} f(d_1)g(d_2)$ occur frequently.
Hence we define the *Dirichlet Product*, $f * g$ of two arithmetic functions f, g by:

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

Theorem 3.4:
(i) $f * g = g * f$
(ii) $(f * g) * h = f * (g * h)$

Proof: Tutorial Exercise.

We define two simple arithmetic functions, the *identity* function and the *unit* function by:

$I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$, and $u(n) = 1$ for all n.

These functions are trivially completely multiplicative. It is easy to show that $f * I = I * f = f$ and we can write Theorem 3.1 as: $\mu * u = I$, since if $n = 1$ the sum takes the value 1 and is zero otherwise.

Using these ideas we can state and easily prove the important relationship between the Dirichlet Product and the Möbius function.

Theorem 3.5: (Möbius Inversion Formula)

Let $F(n) = \sum_{d|n} f(d)$ then $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d})$.

Proof: The statement $F(n) = \sum_{d|n} f(d)$ can be translated into $F = f * u$ so $F * \mu = (f * u) * \mu = f * (u * \mu) = f * I = f$.

Translating back we have $f(n) = (F * \mu)(n) = (\mu * F)(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$.

As an immediate consequence we have:

Theorem 3.6: For $n \geq 1$,

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

Proof: Apply Theorem 3.5 to the result $\sum_{d|n} \phi(d) = n$.

Inverses:

We saw above that $\mu * u = I$. We can interpret this as saying that μ and u are **inverses** with respect to Dirichlet multiplication.
Is is true that any (arithmetic) function f has an inverse, f^{-1}, such that $(f * f^{-1})(n) = I(n)$? It can be shown (tutorial exercise), by induction on n, that such a function exists iff $f(1) \neq 0$, and that

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{d<n, d|n} f(\frac{n}{d}) f^{-1}(d).$$

Corollary: If f is completely multiplicative, then $f^{-1}(n) = \mu(n) f(n)$ for $n \geq 1$.

Proof: Let $g = \mu f$, then $(g * f)(n) = \sum_{d|n} \mu(d) f(d) f(\frac{n}{d}) = f(n) \sum_{d|n} \mu(d) = I(n)$. So $g = f^{-1}$.

Note that $(f * g)^{-1} = f^{-1} * g^{-1}$, whenever the inverses exist.

Introduce the completely multiplicative function N defined by $N(n) = n$ for all $n \geq 1$.

Then the result $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$ can be written as $\phi = \mu * N$.

Thus $\phi^{-1} =$

The Von Mangoldt Function: $\Lambda(n)$.

The Von Mangoldt function Λ plays an important role in the theory of the distribution of primes. For each integer $n \geq 1$, we define

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

For example $\Lambda(12) = 0, \qquad \Lambda(125) = \log 5.$

Observe that since $\Lambda(1) \neq 1$, Λ is not multiplicative.

Theorem 3.7: For $n \geq 1$, $\sum_{d|n} \Lambda(d) = \log n$.

Proof:

Note also that we can apply the Möbius Inversion Formula to obtain

$$\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu(d) \log n - \sum_{d|n} \mu(d) \log d$$

$$= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d = -\sum_{d|n} \mu(d) \log d, \quad \text{for } n > 1.$$

Derivatives of Arithmetic Functions:

Definition:
If f is an arithmetic function, we define its derivative f' by the formula

$$f'(n) = f(n) \log n.$$

Ex: $I'(n) = I(n)\log n = 0$ for all n, $\quad u'(n) = \log n$.

Thus the identity $\sum_{d|n} \Lambda(d) = \log n$ (Theorem 3.7) can be written as $\Lambda * u = u'$.

To see that this definition has some point to it, we note:

Theorem 3.8: If f and g are arithmetic functions then

(a) $(f+g)' = f' + g'$.

(b) $(f*g)' = f' * g + f * g'$.

(c) $(f^{-1})' = -f' * (f*f)^{-1}$ provided $f(1) \neq 0$.

Proof: (a) and (c) are left as exercises, (note that for (c) you should start from $f * f^{-1} = I$.)

(b)

$$(f*g)'(n) = \sum_{d|n} f(d)g(\frac{n}{d})\log n = \sum_{d|n} f(d)g(\frac{n}{d})\log(d.\frac{n}{d})$$

$$= \sum_{d|n}(f(d)\log d)g(\frac{n}{d}) + \sum_{d|n} f(d)(g(\frac{n}{d})\log(\frac{n}{d})) = (f'*g)(n) + (f*g')(n).$$

Using this we can prove the celebrated *Selberg Symmetry formula* which was the starting point for the so-called *elementary* proof of the PNT given 'independently' by Selberg and Erdös.

Theorem 3.9: If $n \geq 1$, we have

$$\Lambda(n)\log n + \sum_{d|n} \Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\left(\log\frac{n}{d})\right)^2.$$

Proof: We have $\Lambda * u = u'$ so applying the 'product rule', we can write

$$\Lambda' * u + \Lambda * u' = u''$$

Using the formula for u' above we write this as

$$\Lambda' * u + \Lambda * (\Lambda * u) = u''.$$

Recall that $\mu = u^{-1}$, so Dirichlet multiplying both sides by u^{-1} we obtain

$$\Lambda' + \Lambda * \Lambda = u'' * \mu$$

and translating back, we have the desired result.

Dirichlet Series:

In the next few chapters we will be looking in detail at functions defined by series of the form $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, where $f(n)$ is an arithmetic function. Such a series is called a *Dirichlet Series*, provided it converges. The following theorem relates Dirichlet series and Dirichlet Multiplication.

Theorem 3.10: Given two Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \qquad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

which converge absolutely for $s > \sigma_0$, then for $s > \sigma_0$ we have

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$$

where $h(n) = \sum_{d|n} f(d)g(\frac{n}{d})$, i.e. $h = f * g$.

Proof: For $s > \sigma_0$,

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \sum_{m=1}^{\infty} \frac{g(m)}{m^s} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{f(n)g(m)}{(nm)^s}.$$

Now collect the terms for which $mn = k$ for $k = 1, 2, \cdots$ and so

$$F(s)G(s) = \sum_{k=1}^{\infty} \left(\sum_{mn=k} f(n)g(m) \right) k^{-s} = \sum_{k=1}^{\infty} h(k)k^{-s}$$

where $h(k) = \sum_{mn=k} f(n)g(m) = (f * g)(k)$.

We can now prove the following Corollary which will be of importance in later work.

Let $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ for $s > 1$. Then since this series converges uniformly, (by Weierstrass M- test), we can differentiate to obtain $\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}$ and hence:

Corollary:

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

Proof:

Averages of Arithmetic Functions:

As mentioned in the introduction to this chapter, the values of the arithmetic functions behave very erratically. For example the function $\tau(n)$ takes the value 2 infinitely often. We can 'smooth out' these functions by looking at their average rate of growth. If f is an arithmetic function, then we will study the mean,

$$\tilde{f}(n) = \frac{1}{n}\sum_{k=1}^{n} f(k),$$

which we do by looking at $\sum_{k\leq x} f(k)$ for any positive real number x. It is understood that k varies from 1 to $\lfloor x \rfloor$.

To describe the growth rate of these functions, we introduce the (standard) notation $O(f(x))$, also known as Landau's notation.

Definition: Suppose $g(x) > 0$ for all $x \geq a$. If there is a constant M such that $\frac{|f(x)|}{g(x)} < M$ for all $x \geq a$, then we write $f(x) = O(g(x))$, which we read as 'f is of order g', or 'f is big-O g'.

Furthermore, if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$, then we say that f is asymptotic to g and write $f \sim g$.

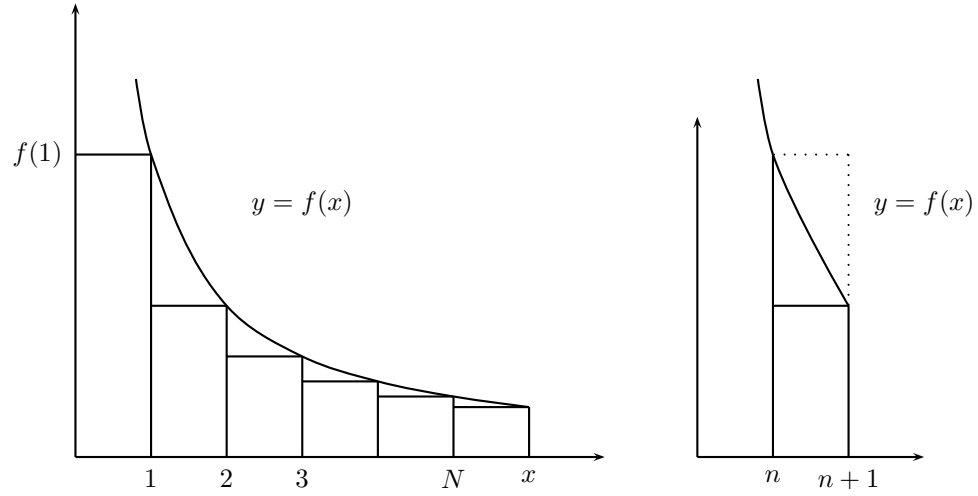
Examples:

In dealing with sums of the form $\sum_{k\leq x} f(k)$, we will frequently use the following result.

Theorem 3.11 If $f(x)$ is a positive decreasing function, then there is a constant k such that

$$\sum_{n\le x} f(n) = \int_1^x f(t)\,dt + k + O(f(x)).$$

Proof:



On $[n, n+1]$, since f is decreasing, $f(n+1) \le \int_n^{n+1} f(t)\,dt \le f(n)$,
so we define $a_n = f(n) - \int_n^{n+1} f(t)\,dt \le f(n) - f(n+1)$, noting that $a_n \ge 0$.

The number a_n is the area between the curve and rectangle from n to $n+1$.
Now, for positive integers, $0 < M < N$, we have

$$\sum_{n=M}^{N} a_n \le (f(M)-f(M+1))+(f(M+1)-f(M+2))+\ldots+(f(N)-f(N+1)) = f(M)-f(N+1) \le f(M),$$

since f is positive. Thus

$$0 \le \sum_{n=M}^{N} a_n \le f(M) \qquad (*).$$

In the case when $M = 1$, we have $\sum_{n=1}^{N} a_n \le f(1)$ and so the infinite series $\sum_{n=1}^{\infty} a_n$ converges since its partial sums are bounded and increasing. Let $k = \sum_{n=1}^{\infty} a_n$, then k is a constant determined solely by f and not N.

Now $k = \sum_{n=1}^{N} a_n + \sum_{n=N+1}^{\infty} a_n$, and by (*), $\sum_{n=N+1}^{\infty} a_n \le f(N+1)$. Hence $\sum_{n=N+1}^{\infty} a_n = O(f(N+1))$.
Now, referring back to the definition of a_n,

$$k = \sum_{n=1}^{N} a_n + O(f(N+1)) = \sum_{n=1}^{N} f(n) - \int_1^{N+1} f(t)\,dt + O(f(N+1)).$$

Re-arranging,

$$\sum_{n=1}^{N} f(n) = \int_1^{N+1} f(t)\,dt + k + O(f(N+1)).$$

Setting $N = \lfloor x \rfloor$,

$$\sum_{n \le x} f(n) = \int_1^{\lfloor x \rfloor + 1} f(t)\,dt + k + O(f(\lfloor x \rfloor + 1)).$$

Now f is decreasing, so $\displaystyle\int_x^{\lfloor x \rfloor + 1} f(t)\,dt \le f(x)$ and $0 \le f(\lfloor x \rfloor + 1) \le f(x)$ and so

$$\sum_{n \le x} f(n) = \int_1^x f(t)\,dt + \int_x^{\lfloor x \rfloor + 1} f(t)\,dt + k + O(f(x)) = \int_1^x f(t)\,dt + k + O(f(x)).$$

Dirichlet's Divisor Problem:

Lemma: $\displaystyle\sum_{n \le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$, where γ is Euler's constant.

Proof: This follows immediately from Theorem 3.11, noting that as $N \to \infty, \displaystyle\sum_{n=1}^{N} \frac{1}{n} - \log N \to \gamma$ and so the K above is Euler's constant.

Hence we have the rough approximation $\displaystyle\sum_{n \le x} \frac{1}{n} = O(\log x)$.

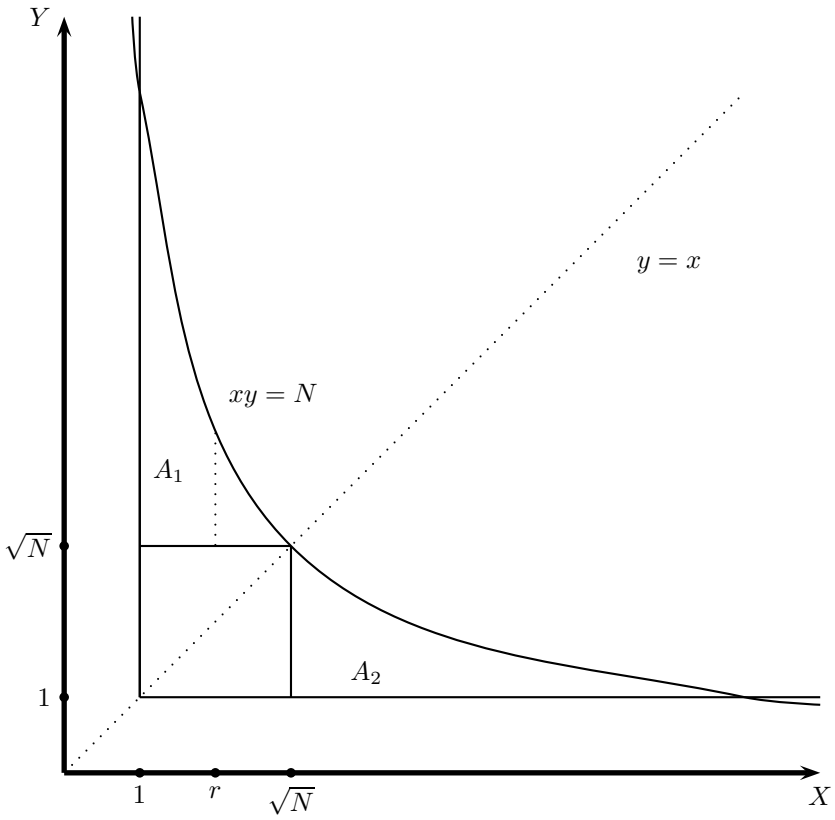
The following result goes back to Dirichlet (1838),

Theorem 3.12: For all $x \ge 1$, we have

$$\sum_{n \le x} \tau(n) = x \log x + (2\gamma - 1)x + O(\sqrt{x}).$$

(Note that this implies that $\tilde{\tau}(n) \sim \log n$.)

Proof:
The function $\tau(n)$ counts the number of lattice points of the form (x, y), lying on the hyperbola $xy = n$ in the first quadrant. Hence the sum $\displaystyle\sum_{n \le N} \tau(n)$ is simply the number of lattice points with positive co-ordinates lying under (and on if N is an integer) the hyperbola $xy = N$.



In the diagram, the number of lattice points lying in the square is $\lfloor\sqrt{N}\rfloor^2$. By symmetry, the number of lattice points in regions A_1 and A_2 are equal, so concentrate on A_1.

On any line $x = r$, $(1 \le r \le \sqrt{N})$, the number of lattice points in A_1 is clearly $\left\lfloor \frac{N}{r} \right\rfloor - \lfloor\sqrt{N}\rfloor$. Hence the total number of lattice points is

$$\sum_{n=1}^{N} \tau(n) = 2 \sum_{r=1}^{\lfloor\sqrt{N}\rfloor} \left(\left\lfloor \frac{N}{r} \right\rfloor - \lfloor\sqrt{N}\rfloor \right) + \lfloor\sqrt{N}\rfloor^2.$$

Using the estimate, $\lfloor y \rfloor = y + O(1)$, we can write this as

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

$$= 2N \sum_{n=1}^{\lfloor\sqrt{N}\rfloor} \frac{1}{n} - \lfloor\sqrt{N}\rfloor^2 + O(\sqrt{N})$$

$$= 2N \sum_{n=1}^{\lfloor\sqrt{N}\rfloor} \frac{1}{n} - N + O(\sqrt{N}).$$

Thus

$$\sum_{n \le x} \tau(n) = 2x \sum_{n=1}^{\lfloor\sqrt{x}\rfloor} \frac{1}{n} - x + O(\sqrt{x})$$

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

$$= x \log x + (2\gamma - 1)x + O(\sqrt{x}).$$

Notes: The error term $O(\sqrt{x})$ has been improved. The determination of the best possible error bound is known as the *Dirichlet Divisor Problem.* The most recent results (of which I am aware) are that $x^{\frac{1}{2}}$ can be replaced by $x^{\frac{7}{22}}$ (Iwaniec and Mossochi 1988, J. No. Th. 29(1), pp. 60-93) and in 1990 Van de Lune and Wattel conjectured $x^{\frac{1}{4}} \log x$. In 2003 Huxley reduced the power of x to $\frac{131}{416}$. Hardy and Landau showed (1915) that $\frac{1}{4}$ was a lower bound for this fraction and $x^{\frac{1}{4}}$ is widely believed to be the true order.

The order of σ:

Lemma 1:

a. $\displaystyle\sum_{n \le x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$ if $s > 1$.

b. $\displaystyle\sum_{n > x} \frac{1}{n^s} = O(x^{1-s})$ for $s > 1$.

Proof:

Dirichlet Sum Identities:

The following identities are extremely important in approximating sums over divisors.

Lemma 2: (Dirichlet Sum Identity, DSI)

a. If g is an arithmetic function, then

$$\sum_{n \le x} \sum_{d|n} g(d) = \sum_{n \le x} \sum_{d \le \frac{x}{n}} g(d), \qquad (DSI \quad 1).$$

b. If f, g are arithmetic functions, then

$$\sum_{n \le x} f(n) \sum_{d|n} g(d) = \sum_{d \le x} g(d) \sum_{j \le \frac{x}{d}} f(dj), \qquad (DSI \quad 2).$$

Proof:

We part (b) first and use it to do (a).

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

$$= f(1)g(1) + f(2)[g(1)+g(2)] + f(3)[g(1)+g(3)] + f(4)[g(1)+g(2)+g(4)] + ...$$

$$g(1)[f(1)+f(2)+...] + g(2)[f(2)+f(4)+...] + g(3)[f(3)+f(6)+...] + ...$$

$$= \sum_{d\le x} g(d) \sum_{dj\le x} f(dj) \qquad \text{(take all the multiples of } d \text{ less than } x\text{)}.$$

This gives the result.

For (a), take the result in (b) and let $f = 1$, then

$$\sum_{n\le x}\sum_{d|n} g(d) = \sum_{d\le x} g(d) \sum_{j\le \frac{x}{d}} 1.$$

Now the RHS of (a) says

$$\sum_{n\le x}\sum_{d\le \frac{x}{n}} g(d) = \sum_{\substack{n,d \\ nd\le x}} g(d) = \sum_{d\le x} g(d) \sum_{n\le \frac{x}{d}} 1 = \sum_{d\le x} g(d) \sum_{j\le \frac{x}{d}} 1.$$

The result follows.

Theorem 3.13:

$$\sum_{n\le x} \sigma(n) = \frac{\pi^2 x^2}{12} + O(x\log x).$$

Proof:

Thus the average value of $\sigma(x)$ is $\dfrac{\pi^2}{12}x + O(\log x)$, i.e. roughly linear(!).

The order of $\phi(n)$:

Recall that we defined $\mu(n)$ so that

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

for $s > 1$.

In particular we have

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} \text{ and } \sum_{n \le x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} - \sum_{n>x} \frac{\mu(n)}{n^2}$$

$$= \frac{6}{\pi^2} + O(\sum_{n>x} \frac{1}{n^2}) = \frac{6}{\pi^2} + O(\frac{1}{x})$$

by part (b) of Lemma 1 above.

Theorem 3.14: $\displaystyle\sum_{n \le x} \phi(n) = \frac{3x^2}{\pi^2} + O(x \log x)$.

(Hence the average order of $\phi(x)$ is $\dfrac{3}{\pi^2}x + O(\log x)$.)

Proof: Using the relation $\phi(n) = \displaystyle\sum_{d|n} \mu(d)\frac{n}{d}$, we have

$$\sum_{n \le x} \phi(n) = \sum_{n \le x} \sum_{d|n} \mu(d)\frac{n}{d}$$

$$= \sum_{n \le x} n \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d \le x} \frac{\mu(d)}{d} \sum_{q \le \frac{x}{d}} dq \qquad (DSI \quad 2)$$

$$= \sum_{d \le x} \mu(d) \sum_{q \le \frac{x}{d}} q$$

$$= \sum_{d \le x} \mu(d) \left\{ \frac{1}{2} \left(\frac{x}{d} \right)^2 + O\left(\frac{x}{d} \right) \right\}$$

$$= \frac{1}{2}x^2 \sum_{d \le x} \frac{\mu(d)}{d^2} + O\left(x \sum_{d \le x} \frac{1}{d} \right)$$

$$= \frac{1}{2}x^2 \left\{ \frac{6}{\pi^2} + O(\frac{1}{x}) \right\} + O(x \log x) = \frac{3x^2}{\pi^2} + O(x \log x).$$

Corollary: The probability that two positive integers chosen at random are coprime is $\frac{6}{\pi^2}$.

Proof: The number of pairs of positive integers $\{r, s\}$ satisfying $1 \leq r \leq s \leq n$ is $\binom{n+1}{2} = \frac{1}{2}n(n+1)$. (Choose 2 distinct numbers from the list $\{1, 2, ..., n+1\}$ and subtract 1 from the larger. Alternatively, the answer is $1 + 2 + ... + (n-1) + n = \frac{1}{2}n(n+1)$.)

Also $\sum_{i \leq n} \phi(i)$ equals the number of such pairs which are coprime (by the definition of ϕ). Hence we can define the probability of two integers being coprime to be

$$\lim_{n \to \infty} \frac{\sum_{i \leq n} \phi(i)}{\frac{1}{2}n(n+1)} = \frac{6}{\pi^2} \approx 0.608$$

by the previous theorem.

(Note: The answer above is simply $\frac{1}{\zeta(2)}$. It has been shown that the probability (as defined above) that N positive integers chosen at random are co-prime is $\frac{1}{\zeta(N)}$.)

Orders of μ and Λ:

The average orders of the Möbius and Von Mangoldt functions are more difficult to determine and are in fact quite deep results. We will show in a later section that

$$\text{(i)} \lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} \mu(n) = 0$$

and

$$\text{(ii)} \lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} \Lambda(n) = 1.$$

Each of these results is **equivalent** to the prime number theorem.

Furthermore, the sum $\sum_{n=1}^{\infty} \frac{\mu(n)}{n}$ converges and has a sum of zero, but this also is equivalent to the prime number theorem. Here we will show that this series has bounded partial sums.

Theorem 3.15: For all $x \geq 1$, we have

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1,$$

with equality only if $x < 2$.

Proof:

UNSW AUSTRALIA.
SCHOOL OF MATHEMATICS AND STATISTICS.
MATH5645: TOPICS IN NUMBER THEORY.

§4 CHARACTERS, L-SERIES and DIRICHLET'S THEOREM:

In Chapter 2 we used the properties of integers and primes to prove that certain arithmetic progressions contained infinitely many primes. These proofs relied on subtle observations and did not appear to generalise. We now seek to find a more general way of approaching such problems using analytic tools.

In order to accomplish this we need some way to *lift* the integers to the complex numbers. This is done via the notion of **characters** which are simply homomorphisms from a group G to $\mathbb{C}$. Although there is a general theory of characters for a general finite group, in what follows we will suppose that G is a finite **abelian** group.

Definition: A **character** is a function $\chi : G \to \mathbb{C}$, such that $\chi \neq 0$, and

$$\chi(xy) = \chi(x)\chi(y) \text{ for all } x, y \in G.$$

Ex: Suppose $G = C_n = \{1, x, \cdots, x^{n-1}\}$ with $x^n = 1$, and $\chi(x^a) = e^{\frac{2\pi i}{n}a}$.

Then $\chi(x^a)\chi(x^b) = e^{\frac{2\pi i(a+b)}{n}} = \chi(x^{a+b}) = \chi(x^a x^b)$. So χ is a character.

Ex: Given any finite abelian group G, define $\chi : G \to \mathbb{C}$ by $\chi(x) = 1$ for all $x \in G$.

χ is clearly a character and is called the **principal character** for G.

We usually write it as χ_1.

Theorem 4.1: If $\chi : G \to \mathbb{C}$ is a character then

(i) $\chi(1) = 1$

(ii) $\chi(x)$ is a root of unity and $(\chi(x))^{|G|} = 1$

(iii) $\chi(x^{-1}) = (\chi(x))^{-1} = \overline{\chi(x)}$.

Proof:

Theorem 4.2: If χ is a non-principal character then

$$\sum_{x \in G} \chi(x) = 0.$$

Proof:

Observe that for fixed G, the set of **all** characters on G is itself a finite abelian group under the operation

$$(\chi_1 . \chi_2)(x) = \chi_1(x)\chi_2(x) \quad \text{for} \quad x \in G.$$

The principal character χ_1 is the identity of the group and for each χ, we have $\chi^{-1} = \overline{\chi}$.

Note also that if G is cyclic of order n then there are exactly n characters for G, since once we have specified the value of χ for a generator α of G, then, for some k, we have $\chi(x) = \chi(\alpha^k) = (\chi(\alpha))^k$.

More generally, given any finite abelian group G of order n, there are precisely n characters on G. (For a proof of this see the Tutorial problems.)

We will write $\hat{G}$ for the group of characters on G.

Recall that $\mathbb{U}_n$ denotes the set of units in $\mathbb{Z}_n$, i.e.

$$\mathbb{U}_n = \{x \in \mathbb{Z}_n : (x, n) = 1\}.$$

You will recall that these are simply the invertible elements in $\mathbb{Z}_n$, that they form a group under multiplication and that $|\mathbb{U}_n| = \phi(n)$, where ϕ is Euler's totient function. You should also recall that $\mathbb{U}_n$ is cyclic precisely when $n = 1, 2, 4, p^\alpha, 2p^\alpha$, where p is an odd prime and $\alpha \geq 1$.

A character can be completely specified by drawing up a character table.

Examples:

1. $G = \mathbb{U}_4 = \{1, 3\}$. $\hat{G} = \{\chi_1, \chi_2\}$ with character table

	1	3
χ_1		
χ_2		

2. $G = \mathbb{U}_5 = \{1, 3, 4, 2\}$. $\hat{G} = \{\chi_1, \chi_2, \chi_3, \chi_4\}$.

Note that 3 is a generator (hence the order in which I have listed the elements).

Since the group is cyclic, if χ is not principal, then $\chi(3)$ is any of the 4 fourth roots of unity. Once $\chi(3)$ is decided, then the remainder of the row is determined.
The character table is

	1	3	4	2
χ_1				
χ_2				
χ_3				
χ_4				

3. $G = \mathbb{U}_8 = \{1, 3, 5, 7\} \cong C_2 \times C_2$. Each (non-identity) element is of order 2 and $3 \times 5 \equiv 7$. Hence the character table is:

	1	3	5	7
χ_1				
χ_2				
χ_3				
χ_4				

(The character tables for $\mathbb{U}_9$ and $\mathbb{U}_{16}$ are in the Tutorial problems.)

4. $G = \mathbb{U}_7 =< 3 >= \{1, 3, 2, 6, 4, 5\}$. 3 is a generator so $\chi(3)$ can be any 6th root of unity.
Let $\omega = e^{\frac{i\pi}{3}}$. The character table is:

	1	3	2	6	4	5
χ_1	1	1	1	1	1	1
χ_2	1	-1	1	-1	1	-1
χ_3	1	ω	ω^2	-1	$-\omega$	$-\omega^2$
χ_4	1	$-\omega$	ω^2	1	$-\omega$	ω^2
χ_5	1	ω^2	$-\omega$	1	ω^2	$-\omega$
χ_6	1	$-\omega^2$	$-\omega$	-1	ω^2	ω

Direct Products:

It is very easy to write down the character table for cyclic groups.

If G is a cyclic group of order m then $\hat{G}$ has exactly m characters given by

$$\chi_\rho(x^i) = \rho^i$$

where ρ is any m-th root of unity.

For non-cyclic abelian groups, we recall the Fundamental Theorem of Abelian groups which states that every finite abelian group is a direct product (or written additively, a direct sum) of cyclic groups.

Suppose $G = A_1 \otimes A_2 \otimes \cdots \otimes A_r$, where each A_i is a cyclic group of order n_i, and $A_i = \langle a_i \rangle$. For each i, select a complex n_i-th root of unity in $\mathbb{C}, \rho_i$.
Define $\chi_{\rho_i} : G \to \mathbb{C}$ by

$$\chi_{\rho_i}(a_1^{\alpha_1}, a_2^{\alpha_2}, \ldots, a_i^{\alpha_i}, \ldots, a_r^{\alpha_r}) = \rho_i^{\alpha_i}.$$

For each choice of ρ_i, for $i = 1, 2, \ldots, r$ we obtain a character

$$\chi = \chi_{\rho_1}\chi_{\rho_2}\cdots\chi_{\rho_r}$$

There are n_i choices for ρ_i and so this gives $n_1 n_2 \cdots n_r = |G|$ such characters.
The fact that there are no others requires a little proof. (Tutorial problem.)

The smallest 'interesting' example is:

5. $G = \mathbb{U}_{35} \cong \mathbb{U}_5 \otimes \mathbb{U}_7$.
Now $\mathbb{U}_5 = \langle 3 \rangle = \{1, 3, 4, 2\}$ and $\mathbf{U_7} = \langle 3 \rangle = \{1, 3, 2, 6, 4, 5\}$. Let ρ be a 4th root of unity (so $\rho \in \{1, -1, i, -i\}$), and σ be a 6th root of unity. We can write the valuations of the group as follows:

$\mathbb{U}_{35}$	$\cong \mathbb{U}_5 \otimes \mathbb{U}_7$	χ_ρ	ψ_σ	$\chi_\rho\psi_\sigma$
1	$(1,1)$	1	1	1
2	$(2,2)$	ρ^3	σ^2	$\rho^3\sigma^2$
3	$(3,3)$	ρ	σ	$\rho\sigma$
4	$(4,4)$	ρ^2	σ^4	$\rho^2\sigma^4$
6	$(1,6)$	1	σ^3	σ^3
8	$(3,1)$	ρ	1	ρ
9	$(4,2)$	ρ^2	σ^2	$\rho^2\sigma^2$
11	$(1,4)$	1	σ^4	σ^4
12	$(2,5)$	ρ^3	σ^5	$\rho^3\sigma^5$
13	$(3,6)$	ρ	σ^3	$\rho\sigma^3$
16	$(1,2)$	1	σ^2	σ^2
17	$(2,3)$	ρ^3	σ	$\rho^3\sigma$
18	$(3,4)$	ρ	σ^4	$\rho\sigma^4$
19	$(4,5)$	ρ^2	σ^5	$\rho^2\sigma^5$
22	$(2,1)$	ρ^3	1	ρ^3
23	$(3,1)$	ρ	σ^2	$\rho\sigma^2$
24	$(4,3)$	ρ^2	σ	$\rho^2\sigma$
26	$(1,5)$	1	σ^5	σ^5
27	$(2,6)$	ρ^3	σ^3	$\rho^3\sigma^3$
29	$(4,1)$	ρ^2	1	ρ^2
31	$(1,3)$	1	σ	σ
32	$(2,4)$	ρ^3	σ^4	$\rho^3\sigma^4$
33	$(3,5)$	ρ	σ^5	$\rho\sigma^5$
34	$(4,6)$	ρ^2	σ^3	$\rho^2\sigma^3$

There are 4 choices of ρ and 6 choices for σ giving 24= $\phi(35)$ characters.

Orthogonality Relations.

A quick glance at some of the smaller examples, suggests that the rows and columns satisfy some nice orthogonality relations.

Theorem 4.3:

(a) (Rows) If ϕ, χ are characters of G then

$$\sum_{x\in G} \phi(x)\overline{\chi(x)} = \begin{cases} |\mathrm{G}| & \text{if } \phi = \chi \\ 0 & \text{if } \phi \neq \chi \end{cases}$$

(b) (Columns) If $x, y \in G$ then

$$\sum_{\chi\in \hat{G}} \chi(x)\overline{\chi(y)} = \begin{cases} |\mathrm{G}| & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

Proof:

(a)

(b) Let $A = \sum_{\chi\in\hat{G}} \chi(x)\overline{\chi(y)} = \sum_{\chi\in\hat{G}} \chi(x)\chi(y^{-1}) = \sum_{\chi\in\hat{G}} \chi(xy^{-1})$.
Now if $x \neq y$ then $xy^{-1} \neq 1$ so there is a $\psi \in \hat{G}$ such that $\psi(xy^{-1}) \neq 1$. Hence

$$A\psi(xy^{-1}) = \sum_{\chi\in\hat{G}} \chi(xy^{-1})\psi(xy^{-1})$$

$$= \sum_{\chi\in\hat{G}} (\chi\psi)(xy^{-1}).$$

Now as χ runs through $\hat{G}$ so does $\chi\psi$, thus

$$A\psi(xy^{-1}) = \sum_{\chi\in\hat{G}} \chi(xy^{-1}) = A.$$

Now $\psi(xy^{-1}) \neq 1$ so $A = 0$.

Finally, if $x = y$ then $xy^{-1} = 1$ so $\chi(xy^{-1}) = 1$ giving $\sum_{\chi \in \hat{G}} \chi(xy^{-1}) = |\hat{G}| = |G|$.

Dirichlet Characters: We now try to lift the integers into $\mathbb{C}$ by using the fact that $\mathbb{Z}$ can be reduced to $\mathbb{Z}_n$ (by reading each integer modulo n) and then ignoring those x for which $(x, n) \neq 1$.

Definition: Suppose $\chi : \mathbb{U}_n \to \mathbb{C}$ is a character for the group $\mathbb{U}_n$.
We define a **Dirichlet character** χ^o modulo n, $\chi^o : \mathbb{Z} \to \mathbb{C}$, by

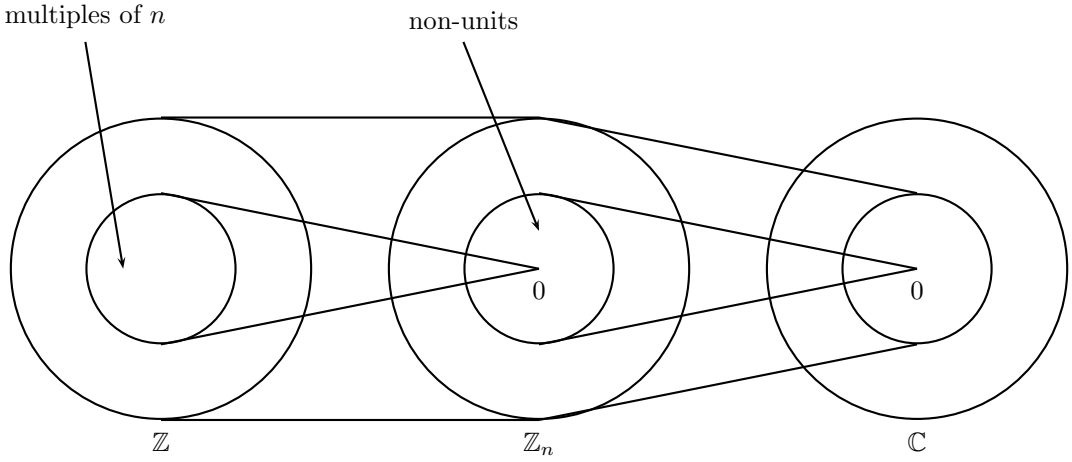
$$\chi^o(x) = \begin{cases} \chi(\hat{x}) & \text{if } (x, n) = 1 \\ 0 & \text{if } (x, n) \neq 1 \end{cases}$$

where $\hat{x} \in \mathbb{Z}_n$ and $\hat{x} \equiv x \bmod n$.

The **principal Dirichlet character**, χ_1^o is defined by

$$\chi_1^o(x) = \begin{cases} 1 & \text{if } (x, n) = 1 \\ 0 & \text{if } (x, n) \neq 1 \end{cases}$$

In simple terms χ^o maps $\mathbb{Z}$ into $\mathbb{Z}_n$, (in the usual way), kills all the non-units and maps the units into $\mathbb{C}$ via the character χ.



Note also that a Dirichlet character modulo n satisfies

$$(i) \quad \chi^o(xy) = \chi^o(x)\chi^o(y) \text{ for all } x, y \in \mathbb{Z}$$

$$(ii) \quad \chi^o(x + n) = \chi^o(x) \text{ for all integers } x.$$

Hence χ^o is completely multiplicative and periodic of period n.

Moreover, there are $\phi(n)$ distinct characters for $\mathbb{U}_n$, so it is clear that there will be $\phi(n)$ distinct Dirichlet characters modulo n.

At the risk of confusion, we will drop the ^{o} and refer to a Dirichlet character modulo n as simply a **character χ modulo n.**

Note that Theorem 4.3(b) can now be written as

$$\sum_{r=1}^{\phi(n)} \chi_r(x)\overline{\chi_r(y)} = \begin{cases} \phi(n) & \text{if } x \equiv y \bmod n \\ 0 & \text{otherwise.} \end{cases}$$

L- functions and the Generalised Euler Product:

Dirichlet generalised the zeta function and found an analogue to the Euler product,

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

From now on, we will take s to be a complex variable. Hence the above series converges for $\sigma = \Re(s) > 1$.

Using this, Dirichlet was able to generalise the proof of the divergence of $\sum_{p \text{ prime}} \frac{1}{p}$, from the set of all primes, to sets of primes of a certain shape.

Given a Dirichlet character χ modulo n, we define the function $L(s, \chi)$, called an L-function for χ, by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Now since $\left|\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}\right| \leq \sum_{n=1}^{\infty} \frac{1}{n^\sigma}$, the above series converges uniformly on any compact subset of the region $\Re(s) > 1$.

Now consider the product, for $\Re(s) > 1$,

$$\left(1 + \frac{\chi(2)}{2^s} + \frac{\chi(2^2)}{2^{2s}} + \cdots\right)\left(1 + \frac{\chi(3)}{3^s} + \frac{\chi(3^2)}{3^{2s}} + \cdots\right)\left(1 + \frac{\chi(5)}{5^s} + \cdots\right)\left(1 + \frac{\chi(7)}{7^s} + \cdots\right)\cdots$$

$$= \prod_{p \text{ prime}} \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Expanding out the brackets and using the fact that χ is complelely multiplicative, we obtain

$$1 + \frac{\chi(2)}{2^s} + \frac{\chi(3)}{3^s} + \frac{\chi(4)}{4^s} + \frac{\chi(5)}{5^s} + \cdots$$

$$= L(s, \chi).$$

Thus we have, for $\Re(s) > 1$,

$$L(s, \chi) = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

A Warm up to Dirichlet's Theorem:

Rather than launch into a proof of Dirichlet's theorem, let us take some time to see the key ideas displayed in some examples. In particular, we return to the problem of showing that there are infinitely many primes congruent to 1 mod 4 and infinitely many primes congruent to -1 mod 4.

Dirichlet Density:

Definition: A set of positive primes $\mathcal{P}$ is said to have Dirichlet density $d(\mathcal{P})$ if

$$\lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{P}} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)}$$

exists.

Notes:
1. This rather 'strange' definition is motivated by the fact that

$$\lim_{s\to 1^+} \frac{\log \zeta(s)}{\log\left(\frac{1}{s-1}\right)} = 1.$$

(see the assignment for the next chapter), so the set of all primes has Dirichlet density 1, as we would expect.

2. If $\mathcal{P}$ is any finite set of primes then $d(\mathcal{P}) = 0$ and if $\mathcal{P}$ contains all but a finite number of primes then $d(\mathcal{P}) = 1$.

3. The more natural definition of density would be to take the number of primes in $\mathcal{P}$ less than some number N, divide by $\pi(N)$ and take a limit as $N \to \infty$. This *natural* density, when it exists can be shown to be the same as the Dirichlet density, but there are sets which do not have natural density for which the Dirichlet density does exist. (For example, the set of all primes whose first digit is 1.)

4. Dirichlet proved that if $(a, b) = 1$ and $\mathcal{P} = \{$ primes $\equiv b \bmod a\}$, then $d(\mathcal{P}) = \frac{1}{\phi(a)}$. We will show this later on.

Hence in the above example, if $\mathcal{P} = \{$ primes $\equiv 1 \bmod 4\}$, then $d(\mathcal{P}) = \frac{1}{2}$.

To verify that this is correct, we note that (with χ_1 and χ_2 as in the above example),

$$L(s,\chi_1) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots = \zeta(s) - \left(\frac{1}{2^s} + \frac{1}{4^s} + \cdots\right)$$

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

Hence $\log L(s,\chi_1) = \log\left(1 - \frac{1}{2^s}\right) + \log\zeta(s)$.

We saw above that

$$\log L(s,\chi_2) + \log L(s,\chi_1) = 2 \sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} + R_3(s)$$

so

$$d(\mathcal{P}) = \frac{1}{2} \lim_{s\to 1^+} \frac{\log L(s,\chi_2) + \log L(s,\chi_1) - R_3(s)}{\log\left(\frac{1}{s-1}\right)}$$

$$= \frac{1}{2} \lim_{s\to 1^+} \frac{\log(1-\frac{1}{2^s}) + \log\zeta(s) + \log L(s,\chi_2) - R_3(s)}{\log\left(\frac{1}{s-1}\right)} = \frac{1}{2}.$$

Another Example:

We now look at the primes in the congruence classes modulo 8. The character table for $\mathbb{U}_8$ is

	1	3	5	7
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

We define a Dirichlet character mod 8 by

$$\chi_i^o(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ \chi_i(\hat{n}) & \text{if } n \text{ is odd} \end{cases}$$

and as usual we will immediately drop the ^{0}. Since the characters are real, we will take s real and $s > 1$.

As before, define $L(s, \chi_i) = \sum_{n=1}^{\infty} \frac{\chi_i(n)}{n^s}$ and as in the previous example

$$\log L(s, \chi_i) = \sum_{p \text{ odd prime}} \frac{\chi_i(p)}{p^s} + R_i(s)$$

for $i = 1, 2, 3, 4$, where $R_i(s)$ is bounded as $s \to 1^+$.

Now observe that

$$(\chi_1 + \chi_2 + \chi_3 + \chi_4)(n) = \begin{cases} 0 & \text{if } n \not\equiv 1 \bmod 8 \\ 4 & \text{if } n \equiv 1 \bmod 8 \end{cases}$$

$$(\chi_1 - \chi_2 + \chi_3 - \chi_4)(n) = \begin{cases} 0 & \text{if } n \not\equiv 3 \bmod 8 \\ 4 & \text{if } n \equiv 3 \bmod 8 \end{cases}$$

$$(\chi_1 + \chi_2 - \chi_3 - \chi_4)(n) = \begin{cases} 0 & \text{if } n \not\equiv 5 \bmod 8 \\ 4 & \text{if } n \equiv 5 \bmod 8 \end{cases}$$

$$(\chi_1 - \chi_2 - \chi_3 + \chi_4)(n) = \begin{cases} 0 & \text{if } n \not\equiv 7 \bmod 8 \\ 4 & \text{if } n \equiv 7 \bmod 8 \end{cases}$$

Thus,

$$\log L(s, \chi_1) + \log L(s, \chi_2) + \log L(s, \chi_3) + \log L(s, \chi_4) = 4 \sum_{p \equiv 1 \bmod 8} \frac{1}{p^s} + A(s)$$

where $A(s)$ is bounded as $s \to 1^+$,

$$\log L(s, \chi_1) - \log L(s, \chi_2) + \log L(s, \chi_3) - \log L(s, \chi_4) = 4 \sum_{p \equiv 3 \bmod 8} \frac{1}{p^s} + B(s)$$

where $B(s)$ is bounded as $s \to 1^+$, and so on for the other sums.

Now once again $L(s, \chi_1) = \sum_{n=0}^{\infty} \frac{1}{(2n+1)^s}$ diverges to ∞ as $s \to 1^+$. We need to show that all the other L-functions are bounded and away from 0 as $s \to 1^+$. This is left as an exercise. It then follows that there are infinitely many primes congruent to 1 mod 8, to 3 mod 8 etc.

Outline of the General Proof:

The general result, known as Dirichlet's theorem, states that there are infinitely many primes congruent to b mod a, whenever $(a, b) = 1$.

The key steps in proving this result are to show that:

- $L(s, \chi)$ is bounded away from 0 as $s \to 1^+$, for each non-principal character χ.

  This is done by showing that the series for $L(s, \chi)$ converges for $Re(s) > 0$, and (more difficult) also showing that $L(1, \chi) \neq 0$.

- $L(s, \chi_1)$ diverges as $s \to 1^+$.

  This is done by extending the zeta function to an analytic function, valid for $Re(s) > 0$, with a simple pole at $s = 1$, and relating $L(s, \chi_1)$ to this new function.

- For each b, $\sum_{p \equiv b \text{ mod a}} \frac{1}{p^s}$, where p is prime, is some linear combination of the logs of these L-functions.

  This is done using the orthogonality properties of characters.

Then, as $s \to 1^+$, it follows that this sum diverges, so there are infinitely many primes in the arithmetic progression $\{b + ka : k \in \mathbb{Z}\}$.

One may compare this idea with Euler's proof that $\sum \frac{1}{p}$ diverges, thus showing the infinitude of ordinary primes.

In the previous examples, the characters involved were real-valued. In general, this is, of course, not the case and so we will often need to think of s as a complex variable.

Some Notes on Complex Function Theory:

Since we will now regard s as a complex variable, we need a few results and ideas from complex function theory.

Weierstrass M-test and Uniform Convergence:

Recall from analysis the Weierstrass M-test.

Let $\{a_j(z)\}$ be a sequence of functions of a complex variable z.

Suppose $|a_j(z)| \leq M_j$ in some region G, where the M_j's are constants independent of z, and suppose

$$\sum_{j=1}^{\infty} M_j < \infty,$$

then the series $\sum_{j=1}^{\infty} a_j(z)$ converges uniformly in G.

Furthermore, if each $a_j(z)$ is analytic in G and the series $\sum_{j=1}^{\infty} a_j(z)$ converges uniformly in G, then this series represents an analytic function.

We can define the complex zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Note that if we write $s = \sigma + it$, then $\left|\frac{1}{n^s}\right| = \frac{1}{n^\sigma}$.

If we fix $\sigma, (\sigma > 1)$, then, for each fixed σ,

$$\sum_{n=1}^{\infty} \frac{1}{n^\sigma} < \infty.$$

It then follows, by the Weierstrass M test, that on any compact subset of the region $\sigma > 1$, the series converges uniformly and $\zeta(s)$ defines an analytic function in the complex plane which can be differentiated term by term as often as we please.

Analytic Continuation:

1. If two entire functions, f and g, agree on some open interval on the real axis, (no matter how small), then f and g agree everywhere in the complex plane.

This can be generalised as follows: Suppose two functions f and g are analytic in some domain D, which contains a portion of the real axis. If $f = g$ on the real axis then $f = g$ everywhere in D. We can use this to prove identities by specialising them to the real axis.

For example, since $\sin 2x = 2 \sin x \cos x$ for $x \in \mathbb{R}$, it follows that $\sin 2z = 2 \sin z \cos z$ for all $z \in \mathbb{C}$.

2. Consider the function $f(z) = 1 + z + z^2 + \cdots$.

This series converges (uniformly) in the open disc $|z| < 1$, but not outside this disc. However, for $|z| < 1$ we can sum this series to obtain $\frac{1}{1-z}$.

If we write $g(z) = \frac{1}{1-z}$, then g is a meromorphic function with a simple pole at $z = 1$ (and residue -1). Moreover, for $|z| < 1$, we have $f(z) = g(z)$.

We say that g is the **analytic continuation** of f with a simple pole at $z = 1$.

Given a function f which is analytic in some domain D, then if there is a meromorphic function g, defined on $E \supset D$, which agrees with f in D, then we say that g is the **analytic continuation** of f and such a g, if it exists, is unique.

In this section we will see how to analytically continue the zeta function from $\sigma > 1$ to $\sigma > 0$. In the next chapter, we will analytically continue ζ to the whole of the complex plane.

We now embark on the proof of Dirichlet's theorem, which requires a number of technical results.

The Proof of Dirichlet's Theorem:

Fix a, a positive integer greater than 1, once and for all. Let $\chi_i : \mathbb{Z}_a \to \mathbb{C}$ be a character and, as above, define the Dirichlet character $\chi_i^o : \mathbb{Z} \to \mathbb{C}$, for $i = 1, 2, \cdots, \phi(a)$ by

$$\chi_i^o(n) = \begin{cases} 0 & \text{if } (n,a) \neq 1 \\ \chi_i(\hat{n}) & \text{if } (n,a) = 1,\ \hat{n} \equiv n \bmod a \end{cases}$$

and as usual we will immediately drop the ^{o}.

As before, define the Dirichlet L-function by $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, where we will take s to be a complex variable whose real part is greater than 1. By the Weierstrass M-test, $L(s,\chi)$, converges absolutely and uniformly to an analytic function in this region.

Using the multiplicative property of χ we have, (as before):

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Abel's Summation Formulae:

a. Suppose $\{a_n\}$ and $\{b_n\}$ are sequences of complex numbers and let $A_n = a_1 + a_2 + \cdots + a_n$, then for $n \geq 0$, (setting $A_0 = 0$), and for $1 \leq M < N$, we have

$$\sum_{n=M}^{N} a_n b_n = \sum_{n=M}^{N-1} A_n(b_n - b_{n+1}) + A_N b_N - A_{M-1} b_M.$$

b. Suppose further that $\sum_{n=1}^{\infty} a_n b_n$ converges and that $A_n b_n \to 0$ as $n \to \infty$, then

$$\sum_{n=1}^{\infty} a_n b_n = \sum_{n=1}^{\infty} A_n(b_n - b_{n+1}).$$

Proof:
a. The steps are similar to the proof of (b) which follows.

b. Let $S_k = \sum_{n=1}^{k} a_n b_n$ and set $A_0 = 0$ then

$$\begin{aligned} S_k &= \sum_{n=1}^{k} (A_n - A_{n-1}) b_n = \sum_{n=1}^{k} A_n b_n - \sum_{n=1}^{k} A_{n-1} b_n \\ &= \sum_{n=1}^{k} A_n b_n - \sum_{n=1}^{k-1} A_n b_{n+1} \qquad (\text{since } A_0 = 0) \\ &= A_k b_k + \sum_{n=1}^{k-1} A_n(b_n - b_{n+1}) \to \sum_{n=1}^{\infty} A_n(b_n - b_{n+1}) \end{aligned}$$

as $k \to \infty$.
(Note that (a) is simply a form of 'summation by parts'.)

We now show that $\zeta(s) - \frac{1}{s-1}$ can be continued to an analytic function on the region $S = \{s \in \mathbb{C} : Re(s) > 0\}$.

This will follow from:

Theorem 4.4:

For $\Re(s) > 1$,

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{\{x\}}{x^{s+1}}\,dx$$

where $\{x\}$ denotes the fractional part of x.

Proof:

Now for $\sigma > 1$, $\zeta(s)$ agrees with $\frac{s}{s-1} - s\int_1^\infty \frac{\{x\}}{x^{s+1}}\,dx$ and so we can re-define $\zeta(s)$ to be $\frac{s}{s-1} - s\int_1^\infty \frac{\{x\}}{x^{s+1}}\,dx$ which is valid for $\sigma > 0, s \neq 1$.

In other words $\zeta(s)$ has an analytic continuation into the region $\sigma > 0$ and this new zeta function has a simple pole at $s = 1$.

We now try to do the same thing for $L(s, \chi)$, where $\chi \neq \chi_1$.

Lemma:
Let χ be a non-trivial character modulo a, then for all $N > 0$ we have

$$\left|\sum_{n=0}^{N} \chi(n)\right| \leq \phi(a).$$

Proof: For $\chi \neq \chi_1$, write $N = aq + r, 0 \leq r < a$, and note that $\chi(n + a) = \chi(n)$ for all positive integers n. Hence

$$\sum_{n=1}^{N} \chi(n) = q \sum_{n=0}^{a-1} \chi(n) + \sum_{n=1}^{r} \chi(n) = \sum_{n=1}^{r} \chi(n)$$

since the first sum is 0. Thus,

$$\left|\sum_{n=1}^{N} \chi(n)\right| = \left|\sum_{n=1}^{r} \chi(n)\right| \leq \sum_{n=1}^{a-1} |\chi(n)| = \phi(a).$$

Theorem 4.5:

If χ is not principal then the series for $L(s, \chi)$ is convergent for $Re(s) > 0$ and the sum is analytic in that region.

Thus, for $\chi \neq \chi_1$, $L(s, \chi)$ is bounded as $s \to 1^+$.

Proof:

Theorem 4.6:

For the principal character χ_1, $L(s, \chi_1)$ extends to a meromorphic function for $Re(s) > 0$, with a simple pole at $s = 1$, and

$$L(s, \chi_1) = \zeta(s) \prod_{p|a} \left(1 - \frac{1}{p^s}\right).$$

Hence, $L(s, \chi_1)$ **diverges** as $s \to 1^+$.

Proof:

The most difficult part of the proof of Dirichlet's theorem, is to show that for $\chi \neq \chi_1$, $L(1, \chi) \neq 0$ so its logarithm is finite. That is, $L(s, \chi)$ is bounded away from 0 as $s \to 1^+$.
We will assume this result for the time being and finish the proof of the theorem.

Theorem 4.7: If χ is not principal then $L(1, \chi) \neq 0$.

Theorem 4.8: (Dirichlet's Theorem.)
If a, b are relatively prime integers with $a > 0$ then there exist infinitely many primes of the form $ka + b$ with k a positive integer.

Proof: We need to show that for each non-principal Dirichlet character χ mod a, we have

$$\log L(s, \chi) = \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} + R(s, \chi)$$

where $R(s, \chi)$ is bounded as $s \to 1^+$.

Even if we restrict s to be real, the values of $L(s,\chi)$ are in general complex numbers so it is necessary to worry about the fact that $\log z$ is multivalued in the complex plane. One way around this is to define $\log L(s,\chi)$ by an infinite series.

Let χ be a Dirichlet character and s be real. We define $G(s,\chi)$ by

$$G(s,\chi) = \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}.$$

Note that this is simply the Taylor series of $\log \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$.

Since $\left|\frac{\chi(p^k)}{kp^{ks}}\right| \leq \frac{1}{p^{ks}}$, so $|G(s,\chi)| < \sum_p \frac{1}{p^s - 1} < 2\zeta(s)$ and since $\zeta(s)$ converges for $s > 1$, the same is true for $G(s,\chi)$. Thus $G(s,\chi)$ is continuous for $s > 1$.

Now if z is complex with $|z| < 1$ then $exp\left(\sum_{k=1}^{\infty} \frac{z^k}{k}\right) = \frac{1}{1-z}$.

Substituting $z = \chi(p)p^{-s}$ we have

$$\exp\left(\sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}\right) = \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Hence

$$exp\left(\sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}\right) = \prod_p exp\left(\sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}\right) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = L(s,\chi)$$

for $s > 1$.
Thus $G(s,\chi)$ provides an unambiguous definition for $\log L(s,\chi)$.

Moreover, for $\chi \neq \chi_1$, $L(s,\chi)$ is bounded as $s \to 1^+$ so $G(s,\chi)$ is bounded as $s \to 1^+$ and, $L(1,\chi) \neq 0$ tells us that $G(s,\chi)$ is defined at $s = 1$.

Now for any character χ, each of the terms in the inner sum of $G(s,\chi)$ satisfies,

$$\sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} = \frac{\chi(p)}{p^s} + \frac{1}{2}\frac{\chi(p^2)}{p^{2s}} + \cdots$$

$$= \frac{\chi(p)}{p^s} + r(s,p,\chi).$$

where,

$$|r(s,p,\chi)| = \left|\frac{1}{2}\frac{\chi(p^2)}{p^{2s}} + \frac{1}{3}\frac{\chi(p^3)}{p^{3s}} \cdots\right|$$

$$\leq \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \cdots$$

$$\leq \frac{1}{2p^{2s}}\left(1 + \frac{1}{p^s} + \cdots\right)$$

$$= \frac{1}{2p^s(p^s - 1)}.$$

Hence,

$$|R(s,\chi)| = \left|\sum_p r(s,p,\chi)\right| \leq \sum_p \frac{1}{2p^s(p^s-1)} \leq \frac{1}{2}\sum_p \frac{1}{p(p-1)} < \frac{1}{2}\sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \frac{1}{2}.$$

Thus $R(s,\chi)$ is bounded as $s \to 1^+$.

We can thus write $G(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + R(s,\chi)$, with the last term bounded as $s \to 1^+$.

The next step in the proof is to pick out the primes congruent to b mod a.

Multiplying the above formula for $G(s,\chi)$ by $\overline{\chi(b)}$ and summing over χ, we obtain

$$\sum_\chi \sum_{p \text{ prime}} \frac{\chi(p)\overline{\chi(b)}}{p^s} = \sum_\chi \overline{\chi(b)} G(s,\chi) - \sum_\chi \overline{\chi(b)} R(s,\chi).$$

Now reversing the order of summation on the left hand side and using the orthogonality relation in Theorem 4.3b, we have

$$\phi(a) \sum_{\substack{p \text{ prime} \\ p \equiv b \bmod a}} \frac{1}{p^s} = \sum_\chi \overline{\chi(b)} G(s,\chi) - \sum_\chi \overline{\chi(b)} R(s,\chi).$$

We have shown that the (finite) sum $\sum_\chi \overline{\chi(b)} R(s,\chi)$ is bounded as $s \to 1^+$.

Now $\sum_\chi \overline{\chi(b)} G(s,\chi) = \sum_{\chi \neq \chi_1} \overline{\chi(b)} G(s,\chi) + G(s,\chi_1)$ with the first sum defined and bounded as $s \to 1^+$. Also by Theorem 4.6, $\log L(s,\chi_1)$ is unbounded as $s \to 1^+$, thus $G(s,\chi_1)$ is unbounded as $s \to 1^+$ and it follows that the series

$$\sum_{\substack{p \text{ prime} \\ p \equiv b \bmod a}} \frac{1}{p^s}$$

diverges as $s \to 1^+$, giving the desired result.

Dirichlet's Density Formula:

Recall that we defined the Dirichlet density for a set of primes $\mathcal{P}$ as

$$\lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{P}} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)}$$

whenever it exists. Take s real.
From the above, if we take $\mathcal{P} = \{ \text{ primes } \equiv b \bmod a\}$, and recall that $L(s,\chi_1) = \zeta(s) \prod_{p|a} \left(1 - \frac{1}{p^s}\right)$ so that $\log L(s,\chi_1) = \log \zeta(s) + \log \prod_{p|a} \left(1 - \frac{1}{p^s}\right)$ then

$$d(\mathcal{P}) = \lim_{s \to 1^+} \frac{\sum_{p \equiv b \bmod a} \frac{1}{p^s}}{\log(\frac{1}{s-1})}$$

$$= \frac{1}{\phi(a)} \lim_{s \to 1^+} \frac{\log \zeta(s) + \log \prod_{p|a} \left(1 - \frac{1}{p^s}\right) + \sum_{\chi \neq \chi_1} \overline{\chi(b)} G(s,\chi) - \sum_\chi \overline{\chi(b)} R(s,\chi)}{\log(\frac{1}{s-1})}$$

$$= \frac{1}{\phi(a)},$$

since the last three terms in the numerator above are bounded as $s \to 1^+$.

Proof of Theorem 4.7:

Dirichlet used some deep results from the theory of quadratic forms to prove this result. These results were connected with the class numbers for quadratic extensions of $\mathbb{Q}$. Given a quadratic form $ax^2 + bxy + cy^2$, where a, b, c are integers, we define the discriminant by $d = b^2 - 4ac$. For fixed d, we take all the possible quadratic forms and look at the set of integers generated by these forms as x, y take all integer values. This partitions the forms into equivalence classes, and the number of such equivalence classes is called the *class number* corresponding to d. It is not at all obvious *a priori* that the class number is even finite, but this was shown to be true by Gauss. For example, the quadratics $x^2 + y^2$ and $x^2 + 2xy + 2y^2$ both have discriminant -4, and they represent the same integers, while $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ both have discriminant -20, but are inequivalent since the latter represents and 3 and 7, which are not representable by the first. Hence the class number of -20 is at least 2. Dirichlet showed that if $p > 3$ is a prime then the class number is a multiple of $L(1, \chi)$ and since the class number is at least one, then $L(1, \chi)$ is not zero.

Case 1: χ is real:

All known proofs of this are difficult. The proof given here is the easiest one to follow and is taken from Jamieson's book *The Prime Number Theorem*. Another proof is given in the Appendix at the end of this chapter.

We begin with some Lemmas.

Lemma 1: Let χ be a real character. Then for all n,

$$(\chi * u)(n) \geq 0 \qquad \text{and } (\chi * u)(n^2) \geq 1.$$

Proof: Since χ and u are multiplicative, so is $\chi * u$. Hence it suffices to show that if p is prime, then $(\chi * u)(p^n) \geq 0$ for all n and that $(\chi * u)(p^n) \geq 1$ if n is even. Now

$$(\chi * u)(p^n) = \sum_{d|p^n} \chi(d) u\left(\frac{p^n}{d}\right) = 1 + \sum_{r=1}^{n} (\chi(p))^r .$$

Hence $(\chi * u)(p^n) = n + 1$ if $\chi(p) = 1$ and 1 if $\chi(p) = 0$, while if $\chi(p) = -1$, the Dirichlet product takes the value 0 when n is odd and 1 when n is even.

Lemma 2: Let $g(x) = \dfrac{1}{x} - \dfrac{1}{e^x - 1}$.

Then $g(x)$ is decreasing and $0 < g(x) < \frac{1}{2}$ for $x > 0$.

Proof: A MAPLE plot is convincing, but a formal proof is in the Tutorial problems.

Given a non-principal character χ, defined on $\mathbb{U}_k$, we will write, for $x \geq 1$,

$$S_\chi(x) = \sum_{1 \leq r \leq x} \chi(r) \text{ and } M_\chi = \sup_{x \geq 1} |S_\chi(x)|.$$

That such an M_χ exists follows from the bound $M_\chi \leq \frac{\phi(k)}{2}$.
This is done in the Tutorial problems.

Main result:

If χ is a real non-principal character then

$$L(1, \chi) \geq \frac{\pi}{8M_\chi + 16}.$$

So in particular, $L(1, \chi) > 0$.

Proof:

For any $\alpha > 0$, let $F(\alpha) = \sum_{n=1}^{\infty} (\chi * u)(n) e^{-\alpha n}$.

By Lemma 1,

$$F(\alpha) \geq \sum_{n=1}^{\infty} e^{-\alpha n^2} = \sum_{n=0}^{\infty} e^{-\alpha n^2} - 1$$

$$\geq \int_0^{\infty} e^{-\alpha x^2}\, dx - 1 = \frac{1}{2}\left(\frac{\pi}{\alpha}\right)^{\frac{1}{2}} - 1.$$

Also, reversing summation, and putting $n = mj$,

$$F(\alpha) = \sum_{n=1}^{\infty} e^{-\alpha n} \sum_{j|n} \chi(j) = \sum_{j=1}^{\infty} \chi(j) \sum_{m=1}^{\infty} e^{-\alpha m j} = \sum_{j=1}^{\infty} \chi(j) \frac{1}{e^{\alpha j} - 1}. \quad \text{(G. Series.)}$$

Now in the notation of Lemma 2, $g(\alpha x) = \dfrac{1}{\alpha x} - \dfrac{1}{e^{\alpha x} - 1}$ so $\dfrac{1}{e^{\alpha j} - 1} = \dfrac{1}{\alpha j} - g(\alpha j) := \dfrac{1}{\alpha j} - h(j)$. Hence

$$F(\alpha) = \sum_{j=1}^{\infty} \frac{\chi(j)}{\alpha j} - \sum_{j=1}^{\infty} \chi(j) h(j)$$

$$= \frac{1}{\alpha} L(1, \chi) - \sum_{j=1}^{\infty} \chi(j) h(j).$$

Writing M for M_χ and noting that $h(j)$ is decreasing (Lemma 2), we can use the Abel Summation formula to write:

$$\left| \sum_{j=1}^{\infty} \chi(j) h(j) \right| \leq \sum_{j=1}^{\infty} M \left(h(j) - h(j+1) \right) = M h(1) = M g(\alpha) \leq \frac{1}{2} M$$

from Lemma 2.

Thus,

$$\frac{1}{\alpha} L(1, \chi) = \left| \frac{1}{\alpha} L(1, \chi) \right| = \left| F(\alpha) + \sum_{j=1}^{\infty} \chi(j) h(j) \right| \geq |F(\alpha)| - \left| \sum_{j=1}^{\infty} \chi(j) h(j) \right|$$

$$\geq \frac{1}{2}\left(\frac{\pi}{\alpha}\right)^{\frac{1}{2}} - 1 - \frac{1}{2} M.$$

Thus we can write $L(1, \chi) \geq a\alpha^{\frac{1}{2}} - b\alpha$, where $a = \dfrac{1}{2}\pi^{\frac{1}{2}}$ and $b = 1 + \frac{1}{2} M$.

The right-hand side, (essentially a quadratic in $\alpha^{\frac{1}{2}}$), has a maximum if we choose $\alpha^{\frac{1}{2}} = \dfrac{a}{2b}$, which gives

$$L(1, \chi) \geq \frac{a^2}{4b} = \frac{\pi}{8M + 16}.$$

Case 2: χ is complex: (i.e. $\overline{\chi} \neq \chi$).

Let $F(s) = \prod_{\chi} L(s,\chi)$, where the product is over all Dirichlet characters modulo m. Assume s is real and $s > 1$ and recall the function

$$G(s,\chi) = \sum_{p} \sum_{k=1}^{\infty} \frac{1}{k} \chi(p^k) p^{-ks}.$$

Recall also that $\sum_{\chi} \chi(p^k) = 0$ unless $p^k = 1$ in which case the sum is $\phi(m)$.

Hence summing over χ and changing the order of summation, we have

$$\sum_{\chi} G(s,\chi) = \phi(m) \sum_{\substack{p^k \equiv 1 \bmod m \\ p \text{ prime}, k \geq 1}} \frac{1}{k} p^{-ks}.$$

Now the righthand side is non-negative and so taking the exponential of both sides and recalling that $exp(G(s,\chi) = L(s,\chi)$, we see that $F(s) = \prod_{\chi} L(s,\chi) \geq 1$.

Now since s is real, $\overline{L(s,\chi)} = L(s,\overline{\chi})$ and so if $L(1,\chi) = 0$ then $L(1,\overline{\chi}) = 0$.

Assume then that $L(1,\chi) = 0$, where χ is a complex character, then the product $L(s,\chi)L(s,\overline{\chi})$ has a zero of order (at least) 2 at $s = 1$. Also $L(s,\chi_1)$ has a pole of order 1 at $s = 1$.

Thus the product $F(s)$ is analytic at $s = 1$ and has a zero there, since one zero cancels with the simple pole, leaving a zero. That is, $F(1) = 0$ which contradicts the above lower bound on F.

Thus $L(1,\chi) \neq 0$ in this case.

Evaluation of $L(1, \chi)$.

If χ is a non-principal character modulo k, then for any positive integer N, we have

Examples: If χ_3 is the (unique) non-principal character modulo 3, then

$$L(1,\chi_3) = \int_0^1 \frac{1-t}{1-t^3}\,dt = \frac{\pi}{3\sqrt{3}}.$$

Similarly, if χ is the real non-principal Dirichlet character modulo 5, then

$$L(1,\chi_5) = \int_0^1 \frac{1-x-x^2+x^3}{1-x^5}\,dx = \int_0^1 \frac{1-x^2}{1+x+x^2+x^3+x^4}\,dx.$$

Putting $y = x + \frac{1}{x}$ we obtain $L(1,\chi_5) = \displaystyle\int_2^\infty \frac{dy}{y^2+y-1} = \frac{2}{\sqrt{5}} \log\left(\frac{1+\sqrt{5}}{2}\right)$.

It is an exercise to show that if χ_4 and χ_6 are (unique) non-principal characters modulo 4 and 6 respectively, then $L(1,\chi_4) = \frac{\pi}{4}$ and $L(1,\chi_6) = \frac{\pi}{2\sqrt{3}}$.

More of these are given in the Tutorial problems. There are very surprising connections here between the evaluations of these L functions and the fundamental units in the rings $\mathbb{Z}(\sqrt{k})$. Alas, we do not have time to explore any further in that direction.

Appendix:

Here is another proof proof given by Shapiro (1950) that $L(1,\chi) \neq 0$ when χ is a real non-principal character. Since it appears in many books, I have included it here.

It is easy to show that

$$\sum_{n\leq x} \frac{1}{\sqrt{n}} \leq 2\sqrt{x} + C \qquad (1)$$

where C is a constant. (Draw diagram and over-approximate the area.)

We need now to get a bound on the tail of $L(s,\chi)$.

Set $S(n) = \sum_{k=1}^{n} \chi(k)$, then by the Lemma just prior to Theorem 4.5, we have $|S(n)| \leq \phi(a)$. Using summation by parts, for integers $M \leq N$, we can write

$$\left| \sum_{n=M}^{N} \frac{\chi(n)}{n^s} \right| = \left| \sum_{n=M}^{N} (S(n) - S(n-1)) \frac{1}{n^s} \right|$$

$$\left| -\frac{S(M-1)}{M^s} + \sum_{n=M}^{N-1} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + S(N)\frac{1}{N^s} \right|$$

$$\leq \phi(a) \left(\frac{1}{M^s} + \sum_{n=M}^{N-1} \left(\frac{1}{n^s} - \frac{1}{(n+1)} \right) + \frac{1}{N^s} \right) \leq \frac{2\phi(a)}{M^s}.$$

Thus,

$$\left| L(s,\chi) - \sum_{n\leq x} \frac{\chi(n)}{n^s} \right| = \left| \sum_{n>x} \frac{\chi(n)}{n^s} \right| \leq \frac{2\phi(a)}{x^s} = \frac{2c}{x^s}. \qquad (2)$$

Now fix χ, a real, non-trivial character, and let

$$F(n) = \sum_{d|n} \chi(d).$$

Note that F is multiplicative and since χ is real, it is easy to show that for any prime p and positive integer α,

$$F(p^\alpha) = \begin{cases} \alpha+1 & \text{if } \chi(p) = 1 \\ 0 & \text{if } \chi(p) = -1 \text{ and } \alpha \text{ is odd} \\ 1 & \text{if } \chi(p) = 0 \\ 1 & \text{if } \chi(p) = -1 \text{ and } \alpha \text{ is even} \end{cases}.$$

Hence $F(n) \geq 0$ for all n and $F(n) \geq 1$ if n is a square.

So

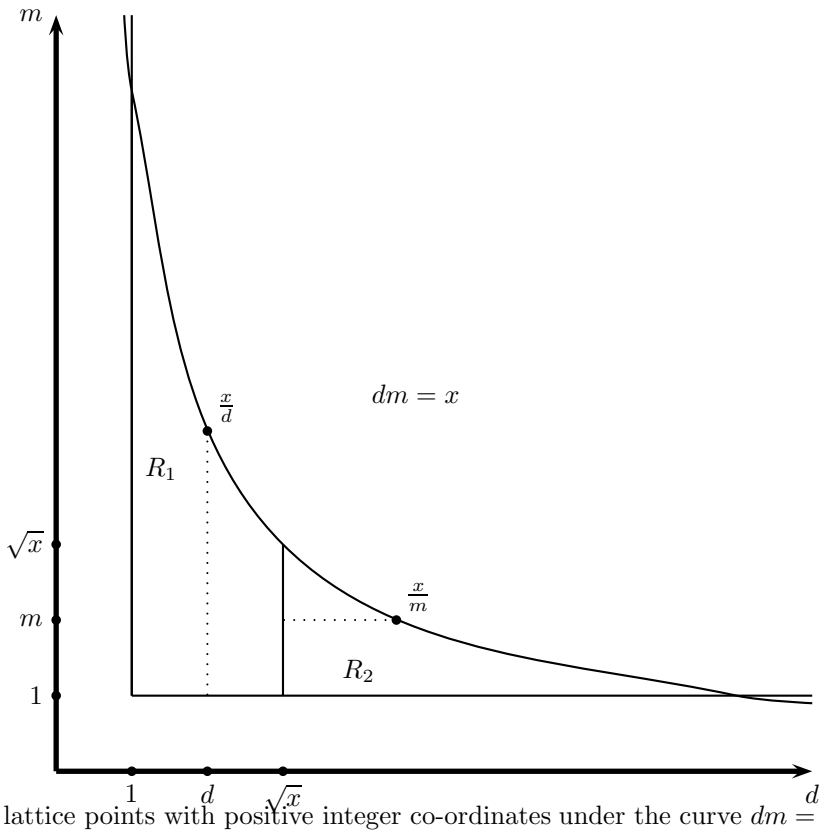
$$\sum_{n\leq x} \frac{F(n)}{\sqrt{n}} \geq \sum_{m^2\leq x} \frac{1}{m^2} \geq \sum_{m\leq\sqrt{x}} \frac{1}{m}.$$

Thus $S(x) = \sum_{n\leq x} \frac{F(n)}{\sqrt{n}}$ **diverges** as $x \to \infty$ (3).

Now

$$S(x) = \sum_{n\leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{d\leq x} \sum_{m\leq \frac{x}{d}} \frac{\chi(d)}{\sqrt{dm}} \text{ using DSI 2}$$

$$= \sum_{\substack{m,d \\ md \le x}} \frac{\chi(d)}{\sqrt{dm}}$$



The sum is over lattice points with positive integer co-ordinates under the curve $dm = x$. We split this into two regions R_1, R_2 where

$$R_1 = \{(d,m) : d \le \sqrt{x}, m \le \frac{x}{d}\}, R_2 = \{(d,m) : m \le \sqrt{x}, \sqrt{x} < d \le \frac{x}{m}\}.$$

Hence

$$S(x) = \sum_{d \le \sqrt{x}} \sum_{m \le \frac{x}{d}} \frac{\chi(d)}{\sqrt{dm}} + \sum_{m \le \sqrt{x}} \sum_{\sqrt{x} < d \le \frac{x}{m}} \frac{\chi(d)}{\sqrt{dm}} = S_1 + S_2.$$

Using (1), we have

$$S_1 \le \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \left(\frac{2\sqrt{x}}{\sqrt{d}} + C \right) = 2\sqrt{x} \sum_{d \le \sqrt{x}} \frac{\chi(d)}{d} + C \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}},$$

so for large x, the right-hand side approaches $2\sqrt{x}L(1,\chi) + CL(\frac{1}{2},\chi)$. Now if $L(1,\chi)$ were equal to 0, then S_1 would be bounded as $x \to \infty$.

Finally,

$$S_2 = \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}} \sum_{\sqrt{x} < d \le \frac{x}{m}} \frac{\chi(d)}{\sqrt{d}}$$

$$= \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}} \left(\sum_{d=1}^{\infty} \frac{\chi(d)}{\sqrt{d}} - \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} + \sum_{d \le \frac{x}{m}} \frac{\chi(d)}{\sqrt{d}} - \sum_{d=1}^{\infty} \frac{\chi(d)}{\sqrt{d}} \right)$$

$$= \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}} \left(L(\frac{1}{2},\chi) - \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} - L(\frac{1}{2},\chi) + \sum_{d \le \frac{x}{m}} \frac{\chi(d)}{\sqrt{d}} \right)$$

$$\leq \sum_{m \leq \sqrt{x}} \frac{1}{\sqrt{m}} \left(\frac{2c_1}{x^{\frac{1}{4}}} - \frac{2c_2}{x^{\frac{1}{2}}} \right) \quad \text{by (2)}$$

$$\leq (2x^{\frac{1}{4}} + C) \left(\frac{2c_1}{x^{\frac{1}{4}}} - \frac{2c_2}{x^{\frac{1}{2}}} \right) = O\left(\frac{1}{x^{\frac{1}{2}}} + O(1) \right)$$

and so is bounded. Thus S is bounded, which contradicts (3).

UNSW AUSTRALIA.
SCHOOL OF MATHEMATICS AND STATISTICS.
MATH5645: TOPICS IN NUMBER THEORY.

§5 THE RIEMANN ZETA FUNCTION:

ζ and the Arithmetic Functions:

We have previously seen that, for $s > 1$,

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

These can be extended to s complex as long as $\Re(s) > 1$.
We will write once and for all $s = \sigma + it$. The first series converges uniformly for $\sigma > 1$ and so defines a analytic function $\zeta(s)$ which we have previously called the *Riemann Zeta Function*. We have also seen a relationship between the Riemann Zeta function and $\Lambda(n)$, viz:

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

The Riemann Zeta function is intimately related to many of the arithmetic functions we have previously encountered.
Here are some examples of this:

$$(1) \qquad \frac{\zeta(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s}$$

$$(2) \qquad \frac{\zeta^3(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{\tau(n^2)}{n^s}$$

$$(3) \qquad \frac{\zeta^4(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{(\tau(n))^2}{n^s}.$$

Here are the proofs of (1) and (2). They rely on the general fact that if $f(n)$ is multiplicative then

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right).$$

Formula 3 and the corresponding sum for $\displaystyle\sum_{n=1}^{\infty} \frac{\zeta^2(s)}{\zeta(2s)}$ are in the tutorial problems.

For (1),

The zeta function is also related to the arithmetic functions ϕ and σ. For example, for $s > 2$,

$$1 + \frac{\sigma(p)}{p^s} + \frac{\sigma(p^2)}{p^{2s}} + \ldots = 1 + \frac{1}{p^s}(1+p) + \frac{1}{p^{2s}}(1+p+p^2) + \ldots$$

$$= \frac{p-1}{p-1} + \frac{1}{p^s}\frac{p^2-1}{p-1} + \frac{1}{p^{2s}}\frac{p^3-1}{p-1} + \ldots$$

$$= \frac{1}{p-1}\left[p + \frac{1}{p^{s-2}} + \frac{1}{p^{2s-3}} + \ldots\right] - \frac{1}{p-1}\left[1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right]$$

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

Thus for $s > 2$,

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

Similarly, $\displaystyle\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$, whence we can write $\displaystyle\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta^2(s) \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}$.

A more interesting result, is

$$\log \zeta(s) = s \int_2^{\infty} \frac{\pi(x)}{x(x^s-1)}\, dx.$$

(These last few results are tutorial exercises).
There are proofs of the Prime Number Theorem which begin from this equation and 'solve' for $\pi(x)$ using a version of the Mellin Transform. (eg. Grosswald 1984).

Extending the Domain:

Notice that for $\sigma > 1$, we can re-arrange the terms of the zeta function as follows:

This gives another proof that $s = 1$ is a simple pole with residue 1. (Compare with Theorem 4.4 of Chapter 4.)

The Gamma Function:

We seek to extend the ζ function further, so that is has an analytic continuation on the whole of the complex plane. To this end we will need to introduce the *Gamma Function* which is defined for $\Re(s) > 0$ by

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x}\, dx,$$

where the integration is carried out along the positive real axis in the x-plane. (It requires checking (tutorial exercise) that the improper integral does in fact converge for $\Re(s) > 0$.)

The notation Γ goes back to Legendre.
This function has the following properties:

(a) $\Gamma(s+1) = s\Gamma(s), \qquad \Gamma(1) = 1.$

(b) $\Gamma(n+1) = n!$, for n a non-negative integer.

(c) $\Gamma(\frac{1}{2}) = \sqrt{\pi}$

(d) $\Gamma(s)\Gamma(1-s) = \dfrac{\pi}{\sin \pi s}.$

(a) and (b) are easy to show, and (c) follows from (d). Result (d) is more difficult to show and is left as a tutorial problem. It is in fact this functional equation (d) which enables us to extend Γ analytically to a meromorphic function on $\mathbb{C}$, with simple poles at $s = -n, n = 0, 1, 2, \cdots$ and corresponding residues $\dfrac{(-1)^n}{n!}$.

(This is also left as a tutorial exercise).

The Re-Duplication Formula: The following formula was discovered by Legendre and generalised by Gauss, and will be of use later.

Lemma: For $s, t > 0$

$$\Gamma(s)\Gamma(t) = \Gamma(s+t) \times 2 \int_0^{\frac{\pi}{2}} \cos^{2s-1}\theta \sin^{2t-1}\theta \, d\theta.$$

(Note this is often written as

$$\frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)} = B(s,t) = 2 \int_0^{\frac{\pi}{2}} \cos^{2s-1}\theta \sin^{2t-1}\theta \, d\theta$$

where $B(s,t)$ is known as the beta function, $B(s,t)$.)

Proof:

Theorem 5.1: (Legendre)
For $\Re(s) > 0$,

$$2\sqrt{\pi}2^{-2s}\Gamma(2s) = \Gamma(s)\Gamma(s+\frac{1}{2}).$$

Proof: As usual, we prove that this for s real, and $s > 0$ and invoke analytic continuation.

Write the previous lemma as

$$\frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)} = 2\int_0^{\frac{\pi}{2}} \cos^{2s-1}\theta \sin^{2t-1}\theta \, d\theta = B(s,t)$$

then $\frac{1}{2}B(\frac{1}{2}, s+\frac{1}{2}) = \int_0^{\frac{\pi}{2}} \sin^{2s}\theta \, d\theta$.

Now let $J = \int_0^{\frac{\pi}{2}} \sin^{2s} 2\theta \, d\theta = \frac{1}{2}\int_0^{\pi} \sin^{2s} u \, du = \int_0^{\frac{\pi}{2}} \sin^{2s} u \, du$, by putting $u = 2\theta$ and using symmetry. Hence $J = \frac{1}{2}B(\frac{1}{2}, s+\frac{1}{2})$. But

$$J = \int_0^{\frac{\pi}{2}} (2\sin\theta\cos\theta)^{2s} \, d\theta = 2^{2s}\int_0^{\frac{\pi}{2}} \sin^{2s}\theta \cos^{2s}\theta \, d\theta = 2^{2s-1}B(s+\frac{1}{2}, s+\frac{1}{2}).$$

Hence

$$\frac{1}{2}B(\frac{1}{2}, s+\frac{1}{2}) = 2^{2s-1}B(s+\frac{1}{2}, s+\frac{1}{2}).$$

Re-writing these in terms of Γ and using properties (a) and (c) above, the result follows.

The following theorem shows the close relationship between the zeta and gamma functions:

Theorem 5.2: For $\Re(s) > 1$,

$$\zeta(s)\Gamma(s) = \int_0^{\infty} (e^t - 1)^{-1} t^{s-1} \, dt. \qquad (*)$$

Proof:

(N.B. The interchange of limit and integral can be justified by invoking the dominated convergence theorem from integration theory. This says that if $\int g < \infty$ and $|f_n| \leq g$ for all n, then $\int f_n \to \int f$ under the assumption that $f_n(x) \to f(x)$ for (almost) all x.
Here we take $f_n = \sum_{k=1}^{n+1} e^{-kt} t^{x-1}$ and $|f_n| = t^{x-1} e^{-t} \frac{(1 - e^{-(n+1)t})}{1 - e^{-t}} < t^{x-1} \frac{e^{-t}}{1 - e^{-t}}$ for all n.)

This integral arises in statistical mechanics and is known as the *Bose-Einstein Integral*.

For example, $\int_0^\infty (e^t - 1)^{-1} t^3 \, dt = \frac{\pi^4}{15}$.

The Functional Equation:

Our initial aim is to extend the definition of ζ to include the region $-1 < \Re(s) < 0$.

We now proceed by observing that $\frac{1}{e^t - 1}$ has a simple pole at $t = 0$ with residue 1 and using L'Hopital's rule, we find that $\frac{1}{e^t - 1} - \frac{1}{t} \to -\frac{1}{2}$ as $t \to 0$. Hence we can write

$$\frac{1}{e^t - 1} = \frac{1}{t} - \frac{1}{2} + \sum_{n=1}^{\infty} a_n t^n \qquad \text{for all } t \neq 0.$$

It is left as an exercise to show $a_{2n} = 0$.

Thus, for $\Re(s) > 0$, $\int_0^1 \left(\frac{1}{e^t - 1} - \frac{1}{t} \right) t^{s-1} \, dt$ is analytic and for $\Re(s) > 1$ we can write $\int_0^1 t^{s-2} \, dt = \frac{1}{s-1}$.

Write (*) above as

$$\zeta(s)\Gamma(s) = \int_0^1 \frac{1}{e^t - 1} t^{s-1} \, dt + \int_1^\infty \frac{1}{e^t - 1} t^{s-1} \, dt$$

which implies

$$\zeta(s) = \frac{1}{\Gamma(s)} \left[\int_0^1 \left(\frac{1}{e^t - 1} - \frac{1}{t} \right) t^{s-1} \, dt + \frac{1}{s-1} + \int_1^\infty \frac{1}{e^t - 1} t^{s-1} \, dt \right]$$

and so we can (once again) extend the definition of ζ from $\Re(s) > 1$ to $\Re(s) > 0$.

Now suppose that $0 < \Re(s) < 1$, then $\frac{1}{s-1} = -\int_1^\infty t^{s-2} \, dt$ so taking the $\frac{1}{s-1}$ term into the second integral and combining we can write (*) as

$$\zeta(s)\Gamma(s) = \int_0^\infty \left[\frac{1}{e^t - 1} - \frac{1}{t} \right] t^{s-1} \, dt$$

and hence as

$$\zeta(s)\Gamma(s) = \int_0^1 \left[(e^t-1)^{-1} - t^{-1} + \frac{1}{2}\right] t^{s-1}\,dt - \frac{1}{2s} + \int_1^\infty \left[(e^t-1)^{-1} - \frac{1}{t}\right] t^{s-1}\,dt$$

Both of the integrals are convergent for $-1 < \Re(s) < 0$ whilst the function $\dfrac{1}{s\Gamma(s)} = \dfrac{1}{\Gamma(s+1)}$ is analytic at 0. Consequently, we can extend $\zeta(s)$ to a meromorphic function defined on $Re(s) > -1$.
Now observe that for $-1 < \Re(s) < 0$, $\displaystyle\int_1^\infty t^{s-1}\,dt = -\frac{1}{s}$. Hence we can again take the $-\frac{1}{2s}$ term into the second integral and re-combine to obtain

$$\zeta(s)\Gamma(s) = \int_0^\infty \left[\frac{1}{e^t-1} - \frac{1}{t} + \frac{1}{2}\right] t^{s-1}\,dt$$

Now recall that $\pi\cot(\pi z) = \dfrac{1}{z} + \displaystyle\sum_{n=1}^{\infty} \frac{2z}{z^2-n^2}$ which is a standard result obtained using residues (tutorial exercise), whence $\cot z = \dfrac{1}{z} + \displaystyle\sum_{n=1}^{\infty} \frac{2z}{z^2-n^2\pi^2}$. Then

$$\frac{1}{e^t-1} - \frac{1}{t} + \frac{1}{2} = \frac{1}{2}\left(\frac{e^t+1}{e^t-1}\right) - \frac{1}{t} = \frac{i}{2}\cot(\frac{it}{2}) - \frac{1}{t}$$

$$= \frac{i}{2}(\frac{2}{it}) - \frac{1}{t} + \sum_{n=1}^{\infty} \frac{2i(\frac{it}{2})}{2\left((\frac{it}{2})^2 - n^2\pi^2\right)}$$

$$= \sum_{n=1}^{\infty} \frac{2t}{t^2+4n^2\pi^2}.$$

Hence for $-1 < \Re(s) < 0$ we can write

$$\zeta(s)\Gamma(s) = 2\int_0^\infty \left(\sum_{n=1}^{\infty} \frac{1}{t^2+4n^2\pi^2}\right) t^s\,dt = 2\sum_{n=1}^{\infty}\int_0^\infty \frac{t^s}{t^2+4n^2\pi^2}\,dt.$$

Now let $t = 2\pi n u$, then

$$\zeta(s)\Gamma(s) = 2\sum_{n=1}^{\infty}\int_0^\infty \frac{(2n\pi)^s u^s}{4n^2\pi^2(u^2+1)} 2n\pi\,du = 2\sum_{n=1}^{\infty}(2n\pi)^{s-1}\int_0^\infty \frac{u^s}{u^2+1}\,du$$

$$= 2(2\pi)^{s-1}\sum_{n=1}^{\infty}\frac{1}{n^{1-s}}\int_0^\infty \frac{u^s}{u^2+1}\,du = 2(2\pi)^{s-1}\zeta(1-s)\int_0^\infty \frac{u^s}{u^2+1}\,du.$$

If we again look at the case $s = x$, where $0 < x < 1$ is real, then it can be shown using complex anaylsis (exercise), that the last integral is equal to $\frac{\pi}{2}\sec(\frac{\pi s}{2})$ and so

$$\zeta(x)\Gamma(x) = 2(2\pi)^{x-1}\zeta(1-x)\frac{\pi}{2\cos(\frac{\pi x}{2})} = 2(2\pi)^{x-1}\zeta(1-x)\frac{\pi\sin(\frac{1}{2}\pi x)}{\sin(\pi x)}$$

(using double angle formula)

$$= 2(2\pi)^{x-1}\zeta(1-x)\Gamma(x)\Gamma(1-x)\sin(\frac{1}{2}\pi x)$$

by the functional equation for the Gamma function above.
'Thus' we have the so-called *Functional Equation* of Riemann, which states:

$$\zeta(s) = 2(2\pi)^{s-1}\Gamma(1-s)\zeta(1-s)\sin\left(\frac{\pi s}{2}\right).$$

We have established the functional equation for $-1 < \Re(s) < 0$. Now the right-hand side is defined and analytic for

(i) $1 - s \neq 0, -1, -2, \cdots$ (these are the singularities of Γ).

(ii) $\Re(1 - s) > -1$ (since this is the domain of ζ at this stage) and for $1 - s \neq 1$ (which is the singularity of ζ.)
So it is analytic provided $\Re(s) < 2$ and $s \neq 0, 1$. Thus both sides are analytic for
$-1 < \Re(s) < 1$, (provided $s \neq 0$). Thus this gives us an analytic continuation of ζ to the whole of the complex plane, with only a simple pole at $s = 1$ as we have seen before.

Ex: $\zeta(-1) = -\frac{1}{12}, \zeta(-2) = 0$.

To find $\zeta(0)$, we use the functional equation to write

$$\zeta(0) = \lim_{s\to 0^+} 2(2\pi)^{s-1}\Gamma(1-s)\zeta(1-s)\sin(\frac{\pi s}{2}) = \lim_{s\to 0^+} \frac{1}{\pi}\zeta(1-s)\sin(\frac{\pi s}{2})$$

$$= \lim_{s\to 0^+} \frac{1}{\pi}\left(\frac{-1}{s} + G(1-s)\right)\left(\frac{\pi}{2}s + O(s^3)\right) = -\frac{1}{2},$$

since $\zeta(s) = \frac{1}{s-1} + G(s)$ with $G(s)$ bounded as $s \to 1$.

The Zeros of Zeta:

We will firstly investigate $\zeta(s)$ for $\Re(s) > 1$.

Lemma: If $a_n \neq -1$ for all n and $\sum_{n=1}^{\infty} |a_n|$ converges, then $\prod_{n=1}^{\infty}(1 + a_n)$ converges and is not equal to zero.

Proof: Let $P_n = \prod_{k=1}^{n}(1 + a_k)$.

For $n \geq 2, P_n = (1 + a_n)P_{n-1}$ so

$$P_n - P_{n-1} = a_n P_{n-1} \qquad (*).$$

Suppose $\sum_{n=1}^{\infty} |a_n| = S$. Now

$$|1 + a_n| \leq 1 + |a_n| \leq e^{|a_n|}$$

so

$$|P_n| \leq e^S.$$

Hence $|a_n P_{n-1}| \leq e^S |a_n|$ so $\sum_{n=2}^{\infty} |a_n P_{n-1}| < \infty$ by the comparison test.

By (*), this implies that $\sum_{n=2}^{\infty}(P_n - P_{n-1}) < \infty$ so

$$\sum_{r=2}^{n}(P_r - P_{r-1}) = P_n - P_1$$

tends to a limit as $n \to \infty$. Hence $P_n \to$ a limit P say, as $n \to \infty$.

To show that $P \neq 0$, we show that the product $\prod_{n=1}^{\infty}(1 + a_n)^{-1}$ also converges to some limit Q and that $PQ = 1$ so that neither P nor Q can be zero.

Write $\frac{1}{1+a_n} = 1 - b_n$ then $b_n = \frac{a_n}{1+a_n}$. Now $1 + a_n \to 1$ as $n \to \infty$ so for sufficiently large n, $|1 + a_n| > \frac{1}{2}$ and hence $|b_n| < 2|a_n|$ - thus $\sum |b_n| < \infty$ and so $\prod_{n=1}^{\infty}(1 - b_n)$ converges to Q say. Finally, it is obvious that $PQ = 1$ and the result follows.

Specialising to $a_n = -\frac{1}{p^s}$, if $n = p$ is a prime and zero otherwise, tells us that the Euler product $\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ does not equal zero for any s in the half plane $\Re(s) > 1$, which in turn implies that $\zeta(s) \neq 0$ for $\Re(s) > 1$.

The Riemann Hypothesis:

We can see from the functional equation that $\zeta(-2n) = 0$ for $n = 1, 2, \cdots$.
These are the so-called *trivial zeros* for $\zeta(s)$. We know that from the above discussion that $\zeta(s) \neq 0$ if $\sigma > 1$. Also the functional equation shows that $\zeta(s) \neq 0$ if $\sigma \leq 0$, except for the trivial zeros.

Moreover we showed earlier that if s is real and $s > 0$, $\zeta(s) = \dfrac{s}{s-1} - s\displaystyle\int_1^\infty \frac{\{x\}}{x^{s+1}}\,dx$ so $\left|\zeta(s) - \dfrac{s}{s-1}\right| < s\displaystyle\int_1^\infty \frac{dx}{x^{s+1}} = 1$. Thus

$$-1 + \frac{s}{s-1} < \zeta(s) < 1 + \frac{s}{s-1} = \frac{2s-1}{s-1}.$$

Now for $\frac{1}{2} < s < 1$, both the left and right-hand sides are negative, so $\zeta(s) \neq 0$ for $\frac{1}{2} < s < 1$ and using the functional equation (and $\zeta(\frac{1}{2}) \neq 0$), we have $\zeta(s) < 0$ if s is real and $0 < s < 1$. We shall soon show that ζ is not zero on the line $1 + it$ for any real t. Hence $\zeta(s)$ is no-where zero outside the critical strip except for the trivial zeros, nor is it zero on the real line in the critical strip.

The functional equation can be written more compactly by using the Reduplication formula (Theorem 5.1), which says

$$2\sqrt{\pi}2^{-2s}\Gamma(2s) = \Gamma(s)\Gamma(s + \frac{1}{2}).$$

We replace s by $\frac{1-s}{2}$ giving

$$2^s\sqrt{\pi}\Gamma(1-s) = \Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1 - \frac{s}{2}\right).$$

Now since $\Gamma(\frac{s}{2})\Gamma(1 - \frac{s}{2}) = \dfrac{\pi}{\sin(\frac{\pi s}{2})}$, this gives us

$$\Gamma(1-s)\sin(\frac{\pi s}{2}) = \frac{2^{-s}\sqrt{\pi}\Gamma\left(\frac{1-s}{2}\right)}{\Gamma(\frac{s}{2})}.$$

Substituting this into the functional equation we obtain

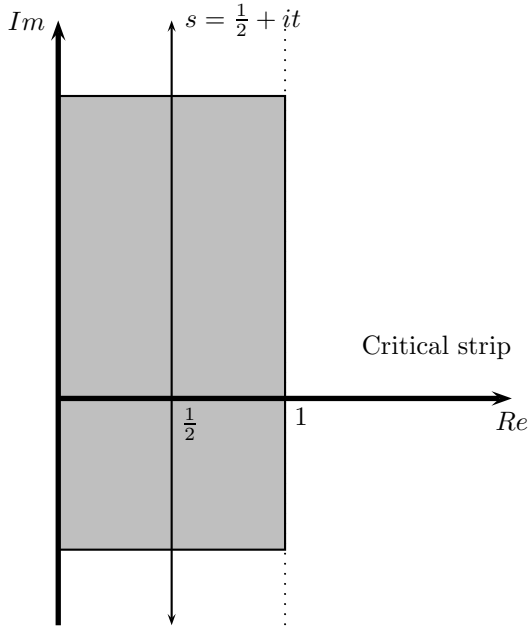
$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

This can now be written as

$$\Phi(s) = \Phi(1-s)$$

where $\Phi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$, which has simple poles at $s = 0$ and $s = 1$. To remove these, Riemann wrote $\xi(s) = \frac{1}{2}s(s-1)\Phi(s)$ giving the entire function $\xi(s)$, which satisfies the functional equation $\xi(s) = \xi(1-s) = \overline{\xi(\overline{s})}$ and so is real on the line $s = \frac{1}{2} + it$. (See Tutorial exercise).
It is clear that in the critical strip $\zeta(s) = 0 \Leftrightarrow \xi(s) = 0$ and it is also clear (tutorial exercise) that if ξ has any zeros in the critical strip they lie symmetrically about the line $\sigma = \frac{1}{2}$.
We shall presently see that $\xi(s)$ has infinitely many zeros in the critical strip.

At $s = \frac{1}{2}$, the functional equation collapses trivially. Riemann conjectured that in the critical strip, the only zeros are on the line $\Re(s) = \frac{1}{2}$. This conjecture has never been proven and is known as the *Riemann Hypothesis*. Both it and generalisations of it have important rameifications in many branches of Mathematics. Hardy proved that $\zeta(s)$ has infinitely many zeros on the above line and indeed millions of such zeros have been calculated.



Generalisations of the Zeta Function:

There are a number of different ways to generalise the zeta function.

(i) As we have seen, if χ is a Dirichlet character, then $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ defines an analytic function for $\Re(s) > 1$. This function can also be analytically extended and the case when χ is a non-principal character leads to another version of the Riemann Hypothesis, (the so-called Generalised Hypothesis).

(ii) The Hurwitz Zeta function, $\zeta(s, a)$ is defined by

$$\zeta(s, a) = \sum_{n=1}^{\infty} \frac{1}{(n+a)^s}$$

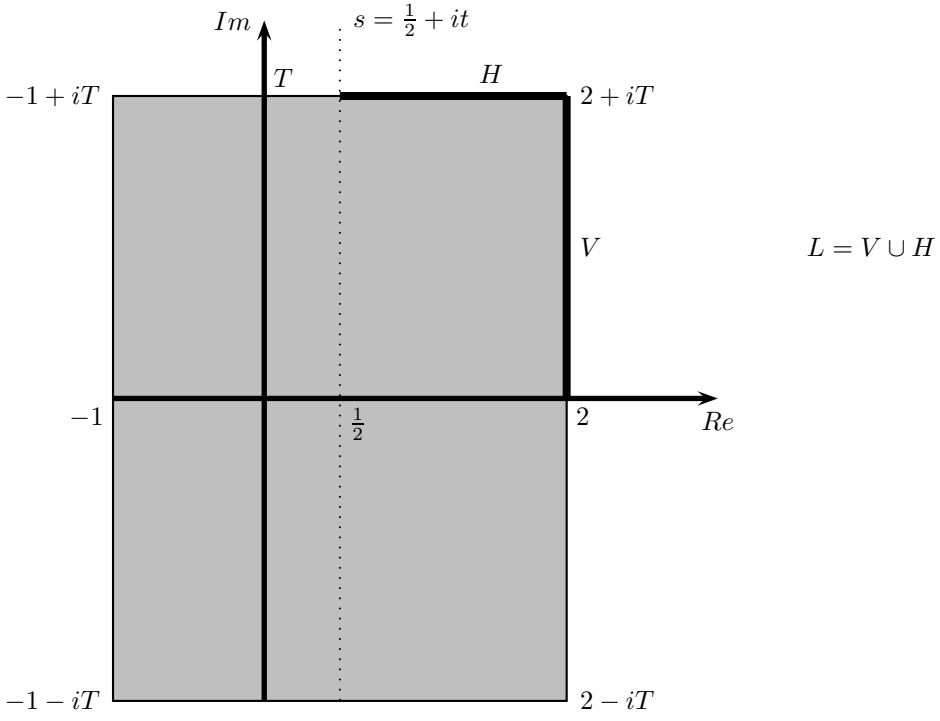
for $\sigma > 1$. As you would expect, results analogous to those for $\zeta(s)$ (including the functional equation) can be obtained for this function.

(iii) There are other generalisations involving the norms of ideals in number fields.

Number of Zeros of $\zeta(s)$ in the Critical Strip:

Since ξ is real on the line $s = \frac{1}{2} + it$, we can use the Intermediate Value Theorem to locate zeros. For example, $\xi(\frac{1}{2} + 14i) = 2 \times 10^{-4}$ and $\xi(\frac{1}{2} + 15i) = -7 \times 10^{-4}$, so there is a zero in this interval. In fact the 'first' zero is at $\frac{1}{2} + i14.134725...$. The next is somewhere between $\frac{1}{2} + 21i$ and $\frac{1}{2} + 22i$.

We will thus look at the number of zeros of $\xi(s)$ rather than those of $\zeta(s)$. We let $N(s)$ denote the number of zeros of $\xi(s)$ in the **upper half plane** intersected with the region R, where R denotes the rectangle with vertices $2 \pm iT$ and $-1 \pm iT$.



Recall that

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s).$$

Now we know from Complex Analysis that the number N of zeros of a function f, which is analytic in and on a closed contour γ, is given by

$$N = \frac{1}{2\pi i}\oint_\gamma \frac{f'(z)}{f(z)}\,dz = \frac{1}{2\pi}\left[argf(z)\right]_\gamma = \frac{1}{2\pi}\left[Im(\log f(z))\right]_\gamma,$$

where $[arg(f)]_\gamma$ denotes the change in the argument of f as z moves around the contour γ. Let L be the contour $V \cup H$ as shown in the above diagram.

We state without proof, the following results.

Lemma: (a) For any $\delta > 0$,

$$\log\Gamma(z+\alpha) = (z+\alpha-\frac{1}{2})\log z - z + \frac{1}{2}\log 2\pi + O(\frac{1}{|z|}),$$

uniformly for $-\pi + \delta \le arg(z) \le \pi - \delta$, and for any bounded α.

This can be obtained using a generalisation of Stirling's formula, $\Gamma(x+1) \sim e^{-x}x^{x-\frac{1}{2}}\sqrt{2\pi}$.

(b) $[arg(\zeta(s)]_L = O(\log T)$, where L is defined above.

Theorem 5.3: For $T \ge 2$, (and T not equal to any of the zeros of $\xi(s)$), we have

$$N(T) = \frac{T}{2\pi}\log\left(\frac{T}{2\pi}\right) - \frac{T}{2\pi} + O(\log T),$$

where the constant implied in the error term is absolute.

Proof: From the above comments, we have

$$2N(T) = \frac{1}{2\pi}\left[arg(\xi(s))\right]_R = \frac{1}{2\pi}\left[arg(\frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s))\right]_R$$

$$= \frac{1}{2\pi}\left[arg(\frac{1}{2}s(s-1))\right]_R + \frac{1}{2\pi}\left[arg(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s))\right]_R.$$

Clearly $\left[arg(\frac{1}{2}s(s-1))\right]_R = 4\pi$.
Now since $\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ takes equal values at the points s and $1-s$ and conjugate values at the points $\sigma \pm it$, it follows that

$$\left[arg(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s))\right]_R = 4\left[arg(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s))\right]_L,$$

where $L = V \cup H$ as shown in the diagram.

So far then, we have

$$N(T) = 1 + \frac{1}{\pi}\left[arg(\pi^{-\frac{s}{2}})\right]_L + \frac{1}{\pi}\left[arg(\Gamma\left(\frac{s}{2}\right))\right]_L + \frac{1}{\pi}\left[arg(\zeta(s))\right]_L.$$

Clearly, $\left[arg(\pi^{-\frac{s}{2}})\right]_L = \left[Im(\log(\pi^{-\frac{s}{2}}))\right]_L = \left[-\frac{t}{2}\log\pi\right]_0^T = -\frac{1}{2}T\log\pi.$

Also,

$$\left[arg\Gamma(\frac{s}{2})\right]_L = \left[Im(\log\Gamma(\frac{s}{2}))\right]_{s=2}^{s=\frac{1}{2}+iT} = Im(\log\Gamma(\frac{1}{4}+i\frac{T}{2})) - \log\Gamma(1))$$

$$= Im\left\{(-\frac{1}{4}+i\frac{T}{2})\log(\frac{iT}{2}) - i\frac{T}{2} + \frac{1}{2}\log 2\pi\right\} + O\left(\frac{1}{T}\right),$$

using the Lemma (a), with $z = i\frac{T}{2}, \alpha = \frac{1}{4}$.

Simplifying this, we have $\frac{1}{2}T\log\frac{T}{2} - \frac{T}{2} - \frac{\pi}{8} + O(\frac{1}{T})$.

Thus $N(T) = \frac{T}{2\pi}\log(\frac{T}{2\pi}) - \frac{T}{2\pi} + \frac{7}{8} + \frac{1}{\pi}\left[arg\zeta(s)\right]_L + O(\frac{1}{T})$. Using the above Lemma, part (b) gives the desired result.

This shows that there are infinitely many zeros in the critical strip. Furthermore, Selberg was able to show that there is a constant $c > 0$ such that for all sufficiently large T, the number of zeros on the line $\Re(s) = \frac{1}{2}$, with $0 < t < T$ is at least $c\frac{T}{2\pi}\log\frac{T}{2\pi}$. This means that a positive proportion of the zeros are on the critical line. Also, all the *known* zeros are simple and in 1970 it was shown by Montgomery that if the RH is true, then the proportion of simple zeros on the critical line is at least $\frac{2}{3}$.

Merten's Conjecture:

Let $M(x) = \sum_{n\leq x}\mu(n)$, where μ is the Möbius function. By definition $|\mu(n)| \leq 1$ for all n so $M(x) = O(x)$.
In 1897 Mertens conjectured that $|M(x)| \leq \sqrt{x}$, but this was shown to be false in 1985 by Odlyzko and te Riele. A weaker conjecture is that for all $\epsilon > 0$ and $x > 0$,

$$M(x) = o(x^{\frac{1}{2}+\epsilon})$$

in the sense that $\frac{M(x)}{x^{\frac{1}{2}+\epsilon}} \to 0$ as $x \to \infty$. This is, in fact, equivalent to the Riemann Hypothesis.
It is probably false that $M(x) = O(\sqrt{x})$, (Stieltjes claimed this in 1885) but no proof has been found.

Furthermore, it can be shown that the Prime Number Theorem is equivalent to the statement $M(x) = o(x)$ and so the Riemann Hypothesis implies the Prime Number Theorem, (but not, of course, conversely.)

The Line $1 + it$.

In this section we show that $\zeta(1 + it) \neq 0$ for any real t.

Lemma: For $\sigma > 1$, we have

$$\zeta^3(\sigma)|\zeta(\sigma + it)|^4|\zeta(\sigma + 2it)| \geq 1.$$

Proof:
For $\Re(s) > 1$, we have the representation

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}.$$

So for $\sigma > 1$, we can take logarithms and write

$$\log\{\zeta(\sigma + it)\} = -\sum_p \log(1 - p^{-\sigma - it})$$

$$= \sum_p \sum_{k=1}^{\infty} \frac{1}{k} p^{-k(\sigma + it)}.$$

Now equating the real parts

$$\log|\zeta(\sigma + it)| = \sum_p \sum_{k=1}^{\infty} \frac{1}{k} p^{-k\sigma} \cos(kt \log p).$$

Now it is easy to show that $3 + 4\cos\phi + \cos 2\phi = 2(1 + \cos\phi)^2 \geq 0$ and so using $\phi = kt \log p$, multiplying by $\frac{1}{k} p^{-k\sigma}$ and summing, we can write

$$\sum_p \sum_{k=1}^{\infty} \frac{1}{k} p^{-k\sigma}[3 + 4\cos(kt \log p) + \cos(2kt \log p)] \geq 0.$$

Writing this in terms of logs of zeta, we have

$$3 \log \zeta(\sigma) + 4 \log|\zeta(\sigma + it)| + \log|\zeta(\sigma + 2it)| \geq 0$$

and exponentiating, for $\sigma > 1$ and all real t, it follows that

$$\zeta^3(\sigma)|\zeta(\sigma + it)|^4|\zeta(\sigma + 2it)| \geq 1.$$

Theorem 5.4: $\zeta(1 + it) \neq 0$ for all real t.

Proof:

Rewrite the formula from the preceeding lemma as

$$[(\sigma - 1)\zeta(\sigma)]^3 \left| \frac{\zeta(\sigma + it)}{\sigma - 1} \right|^4 |\zeta(\sigma + 2it)| \geq \frac{1}{\sigma - 1}, \qquad (\#)$$

which is valid for $\sigma > 1$.

Now let $\sigma \to 1^+$. For $t = 0$, $\zeta(\sigma) \to \infty$ as $\sigma \to 1^+$, so we may suppose that $t \neq 0$.

Since ζ has a simple pole with residue 1 at $s = 1$, the first factor tends to 1. The third factor tends to $|\zeta(1 + 2it)|$ which is finite (the only pole is at $s = 1$). Now IF $\zeta(1 + it) = 0$, then we can write

$$\frac{\zeta(\sigma + it)}{\sigma - 1} = \frac{\zeta(\sigma + it) - \zeta(1 + it)}{\sigma - 1} \to \zeta'(1 + it) \text{ as } \sigma \to 1^+.$$

Thus the LHS of (#) is bounded (for $t \neq 0$) as $\sigma \to 1^+$, while the RHS tends to infinity. This is a contradiction.

Bounds on ζ and its derivative:

We now proceed to find some bounds on $\zeta(s)$ and its derivative which we will need in our proof of the Prime Number Theorem.

We begin with the following summation formula due to Euler.

Lemma: (*Euler-Summation Formula*).

If f has a continuous derivative on the interval $[0, N]$, where N is a positive integer, then

$$\sum_{n=1}^{N} f(n) = \int_0^N f(t)\,dt + \int_0^N (t - \lfloor t \rfloor) f'(t)\,dt.$$

Proof: Clearly,

$$\int_{n-1}^{n} \lfloor t \rfloor f'(t)\,dt = \int_{n-1}^{n} (n-1) f'(t)\,dt$$

$$= (n-1)[f(n) - f(n-1)] = [nf(n) - (n-1)f(n-1)] - f(n).$$

Summing from $n = 1$ to N,

$$\int_0^N \lfloor t \rfloor f'(t)\,dt = \sum_{n=1}^{N} \int_{n-1}^{n} \lfloor t \rfloor f'(t)\,dt$$

$$= \sum_{n=1}^{N} [nf(n) - (n-1)f(n-1)] - \sum_{n=1}^{N} f(n)$$

$$= Nf(N) - \sum_{n=1}^{N} f(n).$$

Thus

$$\sum_{n=1}^{N} f(n) = Nf(N) - \int_0^N \lfloor t \rfloor f'(t)\,dt.$$

Now, using integration by parts,

$$\int_0^N tf'(t)\,dt = Nf(N) - \int_0^N f(t)\,dt$$

and substituting back we have the desired result.

Now assuming the necessary integrals and series converge, we can change variables and take limits to obtain:

$$\sum_{n=M+1}^{\infty} f(n) = \int_M^\infty f(t)\,dt + \int_M^\infty (t - \lfloor t \rfloor) f'(t)\,dt.$$

Hence for $\sigma > 1$,

$$\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} + \sum_{n=N+1}^{\infty} \frac{1}{n^s}$$

$$= \sum_{n=1}^{N} \frac{1}{n^s} + \int_N^\infty \frac{1}{x^s}\,dx - s\int_N^\infty \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx$$

$$\text{so} \qquad \zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} + \frac{N^{1-s}}{s-1} - s\int_N^\infty \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx. \qquad \dagger$$

We can now state some bounds on ζ and its derivative.

Theorem 5.5:

A: When $\sigma \geq 1$ and $t \geq 2$ we have

$$|\zeta(\sigma + it)| \leq \log t + 4 \qquad (\leq M \log t).$$

B: When $\sigma \geq 1$ and $t \geq 2$ we have

$$|\zeta'(\sigma + it)| \leq \frac{1}{2}(\log t + 3)^2 \qquad (\leq M(\log t)^2).$$

Proof: We prove only part A. Part B is similar but more intricate.

From the above formula (†),

$$\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} + \frac{N^{1-s}}{s-1} - s\int_N^\infty \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx$$

$$= \sum_{n=1}^{N} \frac{1}{n^s} + \frac{N^{1-s}}{s-1} + r_N(s).$$

Let $N = \lfloor t \rfloor$, then $N \leq t < N+1$, hence $N \geq 2$. Recall also that $\sigma \geq 1, t \geq 2$.

Then

$$|r_N(s)| = \left| -s\int_N^\infty \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx \right| \leq |s| \int_N^\infty \frac{1}{x^{\sigma+1}}\,dx \leq \frac{|s|}{\sigma N^\sigma}$$

$$\leq \left(\frac{\sigma + t}{\sigma}\right)\frac{1}{N^\sigma} \leq (1+t)\frac{1}{N} \leq \frac{N+2}{N} \leq 2.$$

Also,

$$\left|\sum_{n=1}^{N} \frac{1}{n^s}\right| \leq \sum_{n=1}^{N} \frac{1}{n} \leq \log N + 1 \leq \log t + 1.$$

And finally,

$$\left|\frac{N^{1-s}}{s-1}\right| \leq \frac{1}{t} \leq \frac{1}{2}$$

since $|s-1| \geq t$.

Thus, $|\zeta(s)| = |\zeta(\sigma+it)| \leq (\log t + 1) + 2 + \frac{1}{2} \leq \log t + 4$.

Theorem 5.6: There is a constant M such that

$$\frac{1}{|\zeta(s)|} < M(\log t)^7 \quad \text{and} \quad \left|\frac{\zeta'(s)}{\zeta(s)}\right| < M(\log t)^9,$$

whenever $\sigma \geq 1$ and $t \geq e$.

The proof of this is rather long, see Apostol pp. 287-9, or Jamieson p. 108. The logarithmic derivative of $\zeta(s)$ plays an important role in the proof of the PNT.

Laurent Series for $\zeta(s)$.

Since $\zeta(s)$ has a simple pole at $s = 1$ with residue 1, we have

$$\zeta(s) = \frac{1}{s-1} + a_0 + a_1(s-1) + ...$$

What is the value of a_0?

Lemma
The expression $\sum_{r=1}^{n} \frac{1}{r} - \log n$ tends to the limit γ as $n \to \infty$.
The number γ may be written as

$$\gamma = 1 - \int_1^\infty \frac{t - [t]}{t^2}\, dt.$$

Proof: The existence of γ as the limit of $\sum_{r=1}^{n} \frac{1}{r} - \log n$ is well-known. Using the euler-summation formula with $f(t) = \frac{1}{t}$,

$$\sum_{n=2}^{N} \frac{1}{n} = \int_1^N \frac{1}{t}\, dt - \int_1^N \frac{(t - [t])}{t^2}\, dt$$

so

$$\sum_{n=1}^{N} \frac{1}{n} - \log N = 1 - \int_1^N \frac{(t - [t])}{t^2}\, dt.$$

As $N \to \infty$, the LHS approaches γ and the result follows.

Theorem 5.7: $\zeta(s) - \frac{1}{s-1} \to \gamma$ as $s \to 1$.

Hence $\zeta(s)$ has Laurent expansion

$$\zeta(s) = \frac{1}{s-1} + \gamma + \sum_{n=1}^{\infty} c_n (s-1)^n.$$

The constants c_n are called the Stieltjes Constants. It can be shown using CIF that

$$c_n = \frac{1}{2\pi} \int_0^{2\pi} e^{-inx} \zeta(e^{ix} + 1)\, dx.$$

Proof: This follows from equation † above Theorem 5.5.

Corollary: On some punctured disc with centre $s = 1$, we have

$$\frac{1}{\zeta(s)} = (s-1) - \gamma(s-1)^2 + ...$$

$$\frac{\zeta'(s)}{\zeta(s)} = -\frac{1}{s-1} + \gamma + a_1(s-1) + ...$$

Proof:

Bernoulli Numbers:

In this final section we will develop a nice connection between the values of the zeta function at even integer arguments and the Bernoulli numbers.

There are a number of ways to motivate the definition of the Bernoulli numbers. For our purposes we define them by

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty}\frac{B_n t^n}{n!}=B_0+B_1 t+\frac{B_2 t^2}{2!}+\cdots$$

Observe that multiplying by e^t-1 gives

$$t=\sum_{m=1}^{\infty}\frac{t^m}{m!}\sum_{n=0}^{\infty}\frac{B_n t^n}{n!}$$

and equating co-efficients, we have $B_0=1$ and (if $k+1=m+n$), the co-efficient of t^{k+1} on both sides gives:

$$0=\frac{B_0}{(k+1)!}+\frac{B_1}{k!1!}+\frac{B_2}{(k-1)!2!}+\cdots+\frac{B_k}{(k)!1!}$$

$$=\frac{1}{(k+1)!}\left[\frac{(k+1)!B_0}{(k+1)!}+\frac{(k+1)!B_1}{k!1!}+\cdots+\frac{B_k(k+1)!}{k!1!}\right]$$

$$=\frac{1}{(k+1)!}\sum_{j=0}^{k}B_j\left(\begin{array}{c}k+1\\ j\end{array}\right).$$

So, with $B_0=1$, and, for $k\geq 1$, $\displaystyle\sum_{j=0}^{k}B_j\left(\begin{array}{c}k+1\\ j\end{array}\right)=0$, we can compute $B_1=-\frac{1}{2}, B_2=\frac{1}{6}, B_3=0, B_4=-\frac{1}{30}, B_5=0, B_6=\frac{1}{42},\cdots$.

From these we surmise that:

Corollary: If $n>0$ then $B_{2n+1}=0$.

Proof: $B_1=-\frac{1}{2}$ so

$$\frac{t}{e^t-1}+\frac{t}{2}=1+\sum_{n=2}^{\infty}\frac{B_n t^n}{n!}.$$

Now $f(t)=\frac{t}{e^t-1}+\frac{t}{2}$ is an even function (!) and the result follows.

Our main reason for introducing the Bernoulli numbers here is to show their connection with the Riemann zeta function.

Theorem 5.8: (Euler). If t is a positive integer,

$$2(2t)!\zeta(2t)=(-1)^{t+1}(2\pi)^{2t}B_{2t}.$$

Proof: As before, we use the standard result, for $x\neq k\pi$, $k\in\mathbb{Z}$,

$$\cot x=\frac{1}{x}-2\sum_{n=1}^{\infty}\frac{x}{n^2\pi^2-x^2}.$$

Multiplying by x and using geometric series, we have

$$x\cot x=1-2\sum_{n=1}^{\infty}\frac{x^2}{n^2\pi^2-x^2}$$

$$= 1 - 2\sum_{n=1}^{\infty}\sum_{t=1}^{\infty}\left(\frac{x}{n\pi}\right)^{2t} = 1 - 2\sum_{t=1}^{\infty}\zeta(2t)\left(\frac{x}{\pi}\right)^{2t}.$$

Now $\cot x = i\dfrac{(e^{ix}+e^{-ix})}{(e^{ix}-e^{-ix})}$ so

$$x\cot x = ix\left(\frac{e^{2ix}+1}{e^{2xi}-1}\right) = \frac{1}{2}2ix + \frac{2ix}{e^{2ix}-1} = 1 + \sum_{s=2}^{\infty}\frac{B_s(2ix)^s}{s!} = 1 + \sum_{t=1}^{\infty}\frac{B_{2t}(2ix)^{2t}}{(2t)!},$$

since $B_s = 0$ for s odd $(s \neq 1)$.
Equating the coefficients of $x^{2t}, (t > 0)$ in these expressions for $x\cot x$, yields,
$-2\zeta(2t)\dfrac{1}{\pi^{2t}} = \dfrac{B_{2t}(2i)^{2t}}{(2t)!}$ and the result follows.

Hence $\zeta(2n)$ may be determined for positive integers n,
viz: $\zeta(2) = \dfrac{\pi^2}{6}, \qquad \zeta(4) = \dfrac{\pi^4}{90}, \qquad \zeta(6) = \dfrac{\pi^6}{945}, \qquad ....$

It can also be shown (tutorial problem) that for $n \geq 1$, $\zeta(1-2n) = -\dfrac{B_{2n}}{2n}$.

Little is known about $\zeta(2n+1)$. Apery (1979) proved that $\zeta(3)$ is irrational and more recently Rivoal (2001) proved that $\zeta(2n+1)$ is irrational for infinitely many n and that at least one of $\zeta(5), \zeta(7), \zeta(9), \cdots, \zeta(21)$, is irrational.

Asymptotic Formula for B_{2n}.

Theorem 5.8 can be written as

$$|B_{2n}| = \frac{2(2n)!}{(2\pi)^{2n}}\zeta(2n).$$

Now recall Stirling's approximation formula for $n!$, which says $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$.
Thus for large n,

$$|B_{2n}| \approx \frac{2}{(2\pi)^{2n}}\zeta(2n)\sqrt{4n\pi}\left(\frac{2n}{e}\right)^{2n}.$$

So

$$\frac{|B_{2n}|}{4\sqrt{n\pi}\left(\frac{n}{e\pi}\right)^{2n}} \sim \zeta(2n).$$

Now since $\zeta(2n) = \displaystyle\sum_{k=1}^{\infty}\frac{1}{k^{2n}} \to 1$ as $n \to \infty$, it follows that

$$|B_{2n}| \sim 4\sqrt{n\pi}\left(\frac{n}{e\pi}\right)^{2n}.$$

It was shown (by D.J. Leeming in 1989) that $|B_{2n}| < 5\sqrt{n\pi}\left(\dfrac{n}{e\pi}\right)^{2n}$ for $n \geq 2$.

Notes:

1. A prime p is said to be *regular* if p does not divide the numerators of $B_2, B_4, \cdots, B_{p-3}$. In his attempt to prove FLT, E. Kummer showed that the result was true for all regular primes.

2. It can be shown that $\displaystyle\sum_{x=1}^{k-1}x^n = \frac{1}{n+1}\sum_{j=0}^{n}B_j\binom{n+1}{j}k^{n+1-j}$.
So for example, we obtain $\displaystyle\sum_{x=1}^{k-1}x^2 = \frac{1}{3}(B_0k^3 + 3B_1k^2 + 3B_2k) = \frac{1}{6}k(k-1)(2k-1),$

$\sum_{x=1}^{k-1} x^3 = \frac{1}{4}k^2(k-1)^2$ and so on.

UNSW AUSTRALIA.
SCHOOL OF MATHEMATICS AND STATISTICS.
MATH5645: TOPICS IN NUMBER THEORY.

§6 THE PRIME NUMBER THEOREM:

This section will be devoted to studying the proof of the Prime Number Theorem (PNT), using analytic methods. In 1949 Selberg and Erdös independently found *elementary* (but certainly not *easy*) proofs of the PNT starting with the so-called *Selberg* identity

$$\psi(x)\log x + \sum_{n\leq x}\Lambda(n)\psi(\frac{x}{n}) = 2x\log x + O(x)$$

where $\Lambda(x)$ is the von Mangoldt function and $\psi(x) = \sum_{n\leq x}\Lambda(x)$.

The other known proofs are analytic in nature.

The original proof, given by de la Vallée Poussin (and independently by Hadamard), was modified by Ingham. It is rather long and is given as an Appendix to this chapter. It uses the Riemann-Lebesque Lemma.

A second proof, similar to but simpler than the above, invokes a result known as the Wiener-Ikehara theorem, in place of the Riemann-Lebesque Lemma. The proof of the Wiener-Ikehara theorem, which is technical, will not be given.

The most recent analytic proof is due to Newman (1980). It will appear as an Appendix, but we may go through it briefly, skipping over the more technical parts.

All analytic versions of the proof require some kind of *Tauberian* theorem from Measure Theory in the final step.

As is often the case in Mathematics, we try to write the problem in terms of an equivalent problem and solve the latter. This *equivalent probem* will involve the function $\psi(x)$ so we define:

The Chebyshev Functions:

In this section we introduce the Chebyshev functions ψ and ϑ.

Let $\psi(x) = \sum_{n\leq x}\Lambda(x)$ for $x > 0$, where $\Lambda(n)$ is the Von Mangoldt function which takes the value zero unless $n = p^m$ for some prime p, whereat it takes the value $\log p$.
Noting that $\Lambda(n) = 0$ unless n is a prime power, we have

$$\psi(x) = \sum_{n\leq x}\Lambda(n) = \sum_{m=1}^{\infty}\sum_{p^m\leq x}^{p}\Lambda(p^m) = \sum_{m=1}^{\infty}\sum_{p\leq x^{\frac{1}{m}}}\log p.$$

Now the sum on m is, in fact, finite, since it is empty if $x^{\frac{1}{m}} < 2$, i.e. if $m > \log_2 x$. Thus we can write

$$\psi(x) = \sum_{m\leq\log_2 x}\sum_{p\leq x^{\frac{1}{m}}}\log p.$$

This form motivates:

Definition: If $x > 0$, define $\vartheta(x)$ by

$$\vartheta(x) = \sum_{p\leq x}\log p,$$

where the sum is taken over all **primes** p less or equal to x.
Thus we can write

$$\psi(x) = \sum_{m \leq \log_2 x} \vartheta(x^{\frac{1}{m}}). \qquad (1)$$

Lemma 6.1: For $x > 0$, we have

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x}\log 2}.$$

Proof:

Note that this implies the equivalence:

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1 \Longleftrightarrow \lim_{x\to\infty} \frac{\psi(x)}{x} = 1.$$

Statements Equivalent to the PNT:

We now develop a sequence of statements which are equivalent to the PNT.

To proceed, we need the following technical result, which is also referred to as *Abel's Identity.*

Theorem 6.1: Suppose $a(n)$ is any arithmetic function and let $A(x) = \sum_{n\leq x} a(n)$, where we take $A(x) = 0$ if $x < 1$.
Suppose further that $f \in C^1[y, x]$ where $0 \leq y < x$. Then we have

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,dt.$$

Proof: I will prove a slightly easier version with $y = 0$. Let $k = \lfloor x \rfloor$. Then

$$\sum_{n\leq x} a(n)f(n) = \sum_{n=1}^{k} (A(n) - A(n-1))f(n)$$

$$= \sum_{n=1}^{k-1} A(n)(f(n) - f(n+1)) + A(k)f(k)$$

$$= -\sum_{n=0}^{k-1} A(n) \int_n^{n+1} f'(t)\,dt + A(k)f(k) \qquad \text{since } A(0) = 0,$$

$$= -\int_0^k A(t)f'(t)\,dt + A(k)f(k).$$

Hence

$$\sum_{n\le x} a(n)f(n) = A(x)f(x) - \int_0^x A(t)f'(t)\,dt.$$

This enables us to express the Chebychev function $\vartheta(x)$ in terms of an integral and relate it to the function $\pi(x)$.

Theorem 6.2: For $x \ge 2$, we have

$$\text{(a)} \qquad \vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\,dt$$

$$\text{(b)} \qquad \pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t(\log t)^2}\,dt.$$

Proof:

(a) Define $a(n) = \begin{cases} 1 & \text{if } n \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$ then

$$\pi(x) = \sum_{p\le x} 1 = \sum_{1<n\le x} a(n)$$

and

$$\vartheta(x) = \sum_{p\le x} \log p = \sum_{1<n\le x} a(n)\log n.$$

Applying Abel's identity, with $A(x) = \pi(x), f(x) = \log x$ and $y = 1$, we have part (a) of the theorem. (Note that $\pi(x) = 0$ for $x < 2$.)

For (b), let $b(n) = a(n)\log n$ then

$$\pi(x) = \sum_{\frac{3}{2}<n\le x} \frac{b(n)}{\log n}, \qquad \vartheta(x) = \sum_{n\le x} b(n)$$

so taking $f(x) = \frac{1}{\log x}, y = \frac{3}{2}$ and $A(x) = \vartheta(x) = \sum_{n\le x} b(n)$ a second application of Abel's identity yields

$$\pi(x) = \frac{\vartheta(x)}{\log x} - \frac{\vartheta(\frac{3}{2})}{\log \frac{3}{2}} + \int_{\frac{3}{2}}^x \frac{\vartheta(t)}{t(\log t)^2}\,dt$$

$$= \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t(\log t)^2}\,dt$$

since $\vartheta(t) = 0$ for $t < 2$.

We can now prove some equivalent forms of the prime number theorem, one of which will be used to prove the PNT.

Theorem 6.3: As $x \to \infty$

$$\frac{\pi(x)\log x}{x} \to 1 \iff \frac{\vartheta(x)}{x} \to 1 \iff \frac{\psi(x)}{x} \to 1.$$

$$\text{((a)} \qquad \iff \qquad \text{(b)} \qquad \iff \qquad \text{(c))}$$

Proof: We have already shown that (b) $\iff$ (c), so we suppose (a) holds.
Recall from Theorem 6.2 (a) that

$$\frac{\vartheta(x)}{x} = \frac{\pi(x)\log x}{x} - \frac{1}{x}\int_2^x \frac{\pi(t)}{t}\,dt$$

and so we need to show that $\dfrac{1}{x}\displaystyle\int_2^x \frac{\pi(t)}{t}\,dt \to 0$ as $x \to \infty$.

Now (a) implies that $\frac{\pi(t)}{t} = O(\frac{1}{\log t})$ for $t \geq 2$, so

$$\frac{1}{x}\int_2^x \frac{\pi(t)}{t}\,dt = O\left(\frac{1}{x}\int_2^x \frac{dt}{\log t}\right)$$

and

$$\frac{1}{x}\int_2^x \frac{dt}{\log t} = \frac{1}{x}\int_2^{\sqrt{x}} \frac{dt}{\log t} + \frac{1}{x}\int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{1}{x}\left(\frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}}\right)$$

and so $\dfrac{1}{x}\displaystyle\int_2^x \frac{\pi(t)}{t}\,dt \to 0$ as $x \to \infty$.

Now suppose (b), then by a similar argument we need to show that

$$\frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t(\log t)^2}\,dt \to 0$$

as $x \to \infty$. This is left as exercise 3 on the problem sheet.

We now have a number of equivalent forms for the PNT (there are many others as well) and it is (c) that we will use in our proof.

Proof that $\psi(x) \sim x$.

Recall from the Corollary to Theorem 2.8 that $-\dfrac{\zeta'(s)}{\zeta(s)} = \displaystyle\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$, where $\Lambda(n)$ is the Von Mangold function.

Theorem 6.4: For $s > 1$ and real,

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

Proof:

We now extend the above formula, by analytic continuation to the complex plane for $\Re(s) > 1$.

Put $x = e^u$, then we have

$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_0^\infty \psi(e^u)e^{-us}\,du$$

for $\sigma > 1, s = \sigma + it$.

By Theorem 4.4, we know that $\zeta(1+it) \neq 0$ for all $t \neq 0$ and by Theorem 4.5 both ζ and ζ' are bounded for $\sigma \geq 1$. Thus $-\dfrac{\zeta'(s)}{\zeta(s)}$ represents an analytic function for $\sigma \geq 1$ except at $s = 1$ where we have a simple pole with residue 1.

Theorem 6.5: (Wiener-Ikehara Theorem)

Let $A(x)$ be a non-negative non-decreasing function of x, $(0 \leq x < \infty)$ and suppose $A(0) \leq 1$. Suppose further that $\displaystyle\int_0^\infty A(x)e^{-sx}\,dx$, $s = \sigma + it$, converges for $\sigma > 1$ to the function $f(s)$ which is analytic for $\sigma \geq 1$ except for a simple pole at $s = 1$ with residue 1, then

$$\lim_{x\to\infty} e^{-x}A(x) = 1.$$

Proof: Very long and technical. It will not be given here.

Theorem 6.6: $\dfrac{\psi(x)}{x} \to 1$ as $x \to \infty$.

Proof:

Applying Theorem 6.5 to $-\dfrac{\zeta'(s)}{\zeta(s)} = s\displaystyle\int_0^\infty \psi(e^u)e^{-us}\,du$ with $A(u) = \psi(e^u)$ and $f(s) = -\frac{\zeta'(s)}{\zeta(s)}$, which satisfy the required conditions, we conclude that $\dfrac{\psi(e^u)}{e^u} \to 1$ as $u \to \infty$ and hence the result follows.

The PNT now follows from Theorem 6.3.

The Error Term:

We have thus proven that $\psi(x) = x + o(x)$. If we write $\psi(x) = x + r(x)$, what can be said about $r(x)$? De la Vallée Poussin showed that $r(x) = O(xe^{-\alpha\sqrt{\log x}})$, for a certain positive constant α, by finding a zero free region in the critical strip. The best known (to me) estimate is $r(x) = xexp\left(-\alpha\dfrac{\log x^{\frac{4}{7}}}{\log\log x^{\frac{3}{7}}}\right)$ which goes back to Vinogradov and Korobov (1958). On the other hand, if the Riemann Hypothesis is true, then it can be shown that $\psi_1(x) = \displaystyle\int_1^x \psi(t)\,dt = \frac{1}{2}x^2 + O(x^{\frac{3}{2}})$. Despite this, the exact order of magnitude of $\psi(x)$ is unknown, even assuming the Riemann Hypothesis.

Merten's Theorems:

We proved back in the first chapter that $\sum_p \frac{1}{p}$ diverges. We now state and prove a number of theorems, due to Mertens, which culminate in finding the true order of the sum $\sum_{p \leq x} \frac{1}{p}$.

We will assume the following two results which were tutorial problems. The first is from the problems from Chapter 2.

Result (1): Define $u(n) = 1$ for all n, then for $x > 1$, $\sum_{n \leq x} (f * u)(n) = \sum_{j \leq x} f(j) \left[\frac{x}{j}\right]$

Result (2): From the problems from this section, $\psi(x) \leq 2x$.

Theorem 6.7:
For $x > 1$,

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

Proof:

Theorem 6.8:

For $x > 1$, and p always prime,

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

Proof:

We now finally have:

Theorem 6.9:
For $x > 2$, and p always prime,

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

where C is a constant.

Proof:
Define

$$a(n) = \begin{cases} \frac{\log n}{n} & \text{if } n \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$$

then $\displaystyle\sum_{p \le x} \frac{\log p}{p} = \sum_{n \le x} a(n) = A(x)$.
From Theorem 6.9 above, $A(x) = \log x + O(1) = \log x + R(x)$, where $R(x) = O(1)$.

We now write

$$\sum_{p \le x} \frac{1}{p} = \sum_{2 \le n \le x} \frac{a(n)}{\log n}$$

and apply Abel's identity (Theorem 6.1) with $f(n) = \dfrac{1}{\log n}$ and $y = 1$, noting that $a(1) = 0$. Thus,

$$\sum_{p \le x} \frac{1}{p} = \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t(\log t)^2}\,dt = 1 + \frac{R(x)}{\log x} + \int_2^x \frac{\log t + R(t)}{t(\log t)^2}\,dt$$

$$= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{1}{t\log t}\,dt + \int_2^x \frac{R(t)}{t(\log t)^2}\,dt = 1 + O\left(\frac{1}{\log x}\right) + \log\log x - \log\log 2 + \int_2^x \frac{R(t)}{t(\log t)^2}\,dt.$$

Now since $R(t) = O(1)$ and $\displaystyle\int_2^x \frac{1}{t(\log t)^2}\,dt$ converges (by the integral test), $\displaystyle\int_2^x \frac{R(t)}{t(\log t)^2}\,dt$ has a finite limit as $x \to \infty$. Hence

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

where $C = 1 - \log\log 2 + \displaystyle\int_2^\infty \frac{R(t)}{t(\log t)^2}\,dt$.

Notes: The proof does not give much idea about the value of C, but it can be shown that $C \approx 0.26150$.

As a numerical example, MAPLE reports that

$$\sum_{p \leq 1000} \frac{1}{p} \approx 2.1980801, \qquad \log\log 1000 + C \approx 2.194145.$$

The Logarithmic Integral:

The approximation $\pi(x) \sim \frac{x}{\log x}$ is, of course, asymptotic and so does not really give a particularly good approximation to the actual value of $\pi(x)$. Gauss suggested that, to get a better estimate, one should 'average out', i.e. look at

$$Li(x) = \int_2^x \frac{1}{\log t}\, dt.$$

This (non-elementary) integral is called the *Logarithmic integral*.

The following table shows that Gauss had the right idea (as usual!). (In the table the values are rounded to the nearest integer).

n	$\pi(n)$	$\frac{n}{logn}$	$\mathrm{Li}(n)$
1,000	168	145	177
10,000	1,229	1,068	1,246
50,000	5,133	4,621	5,166
100,000	9,592	8,686	9,630
500,000	41,538	38,103	41,607
1,000,000	78,498	72,382	78,628
10,000,000	664,579	620,421	664,918

In this section we will show that $Li(x) \sim \frac{x}{\log x}$ and so $Li(x) \sim \pi(x)$.

Integration by parts gives:

$$Li(x) = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{1}{(\log t)^2}\, dt.$$

This suggests two things. Firstly, replace 2 by e to make the constants easier and secondly, look at the family of integrals:

$$I_n(x) = \int_e^x \frac{1}{(\log t)^n}\, dt.$$

A simple integration by parts gives

$$I_n(x) = \frac{x}{(\log x)^n} - e + nI_{n+1}(x).$$

Using this idea, it can be shown (tutorial problem) that

$$Li(x) = \frac{x}{\log x} + \frac{x}{(\log x)^2} + ... + (n-1)!\frac{x}{(\log x)^n} + r_{n+1}(x)$$

where $r_{n+1}(x) \sim n!\frac{x}{(\log x)^{n+1}}$ as $x \to \infty$.

Lemma: As $x \to \infty$,

$$I_n(x) \sim \frac{x}{(\log x)^n}.$$

Proof:
By the above recurrence, our desired result is equivalent to

$$I_{n+1}(x)\frac{(\log x)^n}{x} \to 0$$

as $x \to \infty$.

Divide the interval $[e, x]$ into $[e, \sqrt{x}] \cup [\sqrt{x}, x] = A \cup B$. Then for $t \in A$, $\log t \geq 1$ and for $t \in B$, $\log t \geq \frac{1}{2} \log x$.

Hence,

$$I_{n+1}(x) = \int_e^{\sqrt{x}} \frac{1}{(\log t)^{n+1}}\, dt + \int_{\sqrt{x}}^{x} \frac{1}{(\log t)^{n+1}}\, dt$$

$$\leq \int_e^{\sqrt{x}} 1\ dt + \int_{\sqrt{x}}^{x} \left(\frac{2}{\log x}\right)^{n+1} dt = \sqrt{x} - e + \left(\frac{2}{\log x}\right)^{n+1} (x - \sqrt{x})$$

$$\leq \sqrt{x} + x \left(\frac{2}{\log x}\right)^{n+1}.$$

Hence

$$I_{n+1}(x) \frac{(\log x)^n}{x} \leq \frac{(\log x)^n}{\sqrt{x}} + \frac{2^{n+1}}{\log x} \to 0$$

as $x \to \infty$.

Theorem 6.10:

$$Li(x) \sim \frac{x}{\log x}$$

as $\to \infty$. More precisely,

$$Li(x) = \frac{x}{\log x} + r(x)$$

where $r(x) \sim \dfrac{x}{(\log(x))^2}$ as $x \to \infty$.

Proof: It suffices to prove the equivalent statement for $I_1(x)$ instead of $Li(x)$.

Now $I_1(x) = \dfrac{x}{\log x} + I_2(x) - e$. By the Lemma, $I_2(x) - e \sim \frac{x}{(\log x)^2}$ as $x \to \infty$ and the result follows.

There are many deep connections between $Li(x)$ and $\pi(x)$. For example, it was proven a long time ago that

$$|\pi(x) - Li(x)| \leq Kxe^{-c(\log x)^{\frac{1}{2}}}$$

for some constants K and c. This result has not been bettered, but it is known that

$$|\pi(x) - Li(x)| \leq \sqrt{x}\log x$$

(for $x \geq 3$) is equivalent to the Riemann Hypothesis!! Hence the nature of the zeros of the zeta function in the critical strip impose a limitation on the accuracy with which $Li(x)$ can represent $\pi(x)$.

Riemann (and others) believed that $\pi(x) > Li(x)$ for all x (as the table above suggests). This was proven to be false. Indeed the two curves cross infinitely often (!) (Littlewood). The smallest x at which the curves cross is known as *Skewes number* but is not explicity known. Its size (given initially by Skewes in 1933) was shown to be less than $e^{e^{e^{79}}} \approx 10^{10^{10^{34}}}$. The Skewes number has since been reduced to 1.165×10^{1165} by Lehman in 1966, $e^{e^{27/4}} \approx 8.185 \times 10^{370}$ by te Riele (1987), and less than 1.39822×10^{316} (Bay and Hudson 2000.)

More recent work (2005) by Demichel establishes that the first crossover occurs around $1.397162914 \times 10^{316}$.

Hence we have come from the astronomical to the merely 'ginormous'.

Appendix 1: Newman's Proof.

This proof was given by D.J. Newman in 1980. If uses the equivalence between the PNT and $\frac{\vartheta(x)}{x} \to 1$. The Wiener-Ikehara Theorem is replaced by the so-called *Analytic Theorem* which has the advantage that it can be proven using only a simple contour integral.

Define $\Phi(s) = \sum_p \frac{\log p}{p^s}$.

Theorem 1: $\Phi(s) - \frac{1}{s-1}$ is holomorphic for $Re(s) \geq 1$.

Proof: For s real and $s > 1$, $-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p}{p^s - 1}$ (exercise).

The right-hand side of this is also equal to $\Phi(s) + \sum_p \frac{\log p}{p^s(p^s-1)}$. The latter sum converges for $s > \frac{1}{2}$ and so by analytic continuation it converges for complex s, provided $Re(s) > \frac{1}{2}$. Now since $-\frac{\zeta'(s)}{\zeta(s)}$ has a simple pole at $s = 1$ with residue 1, the result follows.

Theorem 2: (Analytic Theorem).

Let $f(t)$, $(t \geq 0)$, be a bounded integrable function and suppose that

$$g(z) = \int_0^\infty f(t)e^{-zt}\,dt,$$

for $Re(z) > 0$, extends holomorphically for $Re(z) \geq 0$, Then $\int_0^\infty f(t)\,dt$ exists and is equal to $g(0)$.

(Notice that g is simply the Laplace transform of f.)

Theorem 3:

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

Proof: Let $b(n) = 1$ if n is prime and zero otherwise, then $\vartheta(x) = \sum_{n \leq x} b(n)\log n$ and $\Phi(s) = \sum_p \frac{\log p}{p^s} = \sum_n \frac{b(n)\log n}{n^s}$.

Now for s real and $s > 1$, $\frac{\vartheta(x)}{x^2} \leq \frac{x \log x}{x^s} \to 0$ as $x \to \infty$. Again using Abel's lemma with $a(n) = b(n)\log n$, so $A(x) = \vartheta(x)$, and $f(n) = \frac{1}{n^s}$ and putting $x = e^t$, we have, (for $Re(s) > 1$),

$$\Phi(s) = \sum_p \frac{\log p}{p^s} = \lim_{x\to\infty} \frac{\vartheta(x)}{x^s} + s\int_1^\infty \frac{\vartheta(x)}{x^{s+1}}\,dx = s\int_0^\infty e^{-st}\vartheta(e^t)\,dt.$$

Now putting $f(t) = \vartheta(e^t)e^{-t} - 1$ and $g(z) = \frac{\Phi(z+1)}{z+1} - \frac{1}{z}$, then the conditions of Theorem 2 are satisfied and so $\int_0^\infty f(t)\,dt$ exists. Replacing e^t with x we arrive at the required integral.

Theorem 4: $\vartheta(x) \sim x$.

Proof: Suppose $\lambda > 1$ and there exist arbitrarily large x such that $\vartheta(x) \geq \lambda x$,. For $t \geq x$ we have $\vartheta(t) \geq \vartheta(x) \geq \lambda x$ so,

$$\int_x^{\lambda x} \frac{\vartheta(t) - t}{t^2}\,dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\,dt = \int_1^\lambda \frac{\lambda - t}{t^2}\,dt = \lambda + 1 - \log\lambda > 0.$$

(where we put $u = \frac{t}{x}$). Hence the tail of the integral is not going to zero, but this implies that the improper integral diverges contradicting Theorem 3.

Similarly, the inequality $\vartheta(x) \leq \lambda x$ with $\lambda < 1$ would imply that

$$\int_{\lambda x}^{x} \frac{\vartheta(t) - t}{t^2}\, dt < 0$$

again contradicting Theorem 3. The conclusion is that $\vartheta(x) \sim x$ so the PNT follows.

Appendix 2: The Ingham version of the first proof.

We introduce the function ψ_1 and get yet another equivalence to the PNT.

The function $\psi(x)$ is a step function, so as usual we will smooth it out by integrating and define

$$\psi_1(x) = \int_1^x \psi(t)\,dt.$$

We need to show that

$$\psi_1(x) \sim \frac{1}{2}x^2 \Longrightarrow \psi(x) \sim x$$

so that we can then concentrate on showing the left hand side of this implication.

To obtain this result, we need to following lemma:

Lemma 1. Let $A(x) = \sum_{n\le x} a(n)$, and $A_1(x) = \int_1^x A(t)\,dt$.
Assume that $a(n) \ge 0$ for all n, then if $A_1(x) \sim Lx^c$ as $x \to \infty$ for some $c > 0$ and $L > 0$, then $A(x) \sim cLx^{c-1}$ as $x \to \infty$.

(In other words, formal differentiation of the first asymptotic formula gives a correct asymptotic result.)

Proof: $A(x)$ is increasing since $a(n) \ge 0$. Now choose $\beta > 1$ and consider

$$A_1(\beta x) - A_1(x) = \int_x^{\beta x} A(u)\,du \ge A(x)(\beta x - x) = x(\beta - 1)A(x).$$

Thus

$$xA(x) \le \frac{1}{\beta - 1}\left\{A_1(\beta x) - A_1(x)\right\}$$

so

$$\frac{A(x)}{x^{c-1}} \le \frac{1}{\beta - 1}\left\{\frac{A_1(\beta x)}{(\beta x)^c}\beta^c - \frac{A_1(x)}{x^c}\right\}.$$

Now fix β and let $x \to \infty$, so using the asymptotic approximation to $A_1(x)$ we have

$$\limsup_{x\to\infty} \frac{A(x)}{x^{c-1}} \le \frac{1}{\beta - 1}(L\beta^c - L) = L\frac{\beta^c - 1}{\beta - 1}.$$

Now let $\beta \to 1^+$ then $\dfrac{\beta^c - 1}{\beta - 1} \to c$ and so

$$\limsup_{x\to\infty} \frac{A(x)}{x^{c-1}} \le cL.$$

Now consider any α strictly between 0 and 1, then a similar argument applied to $A_1(x) - A_1(\alpha x)$ gives

$$\liminf_{x\to\infty} \frac{A(x)}{x^{c-1}} \ge L\frac{(1 - \alpha^c)}{1 - \alpha}$$

and as $\alpha \to 1^-$, the righthand side tends to cL and hence $\dfrac{A(x)}{x^{c-1}} \to cL$ as $x \to \infty$.
Thus we have

Theorem 1:
$\psi_1(x) \sim \dfrac{x^2}{2} \Longrightarrow \psi(x) \sim x$ as $x \to \infty$.

Proof: This follows immediately from the Lemma.

Our next step is to represent $\psi_1(x)$ in terms of a complex contour integral involving the Riemann Zeta function. For this task we will need the following Lemmata. (Note that the first Lemma can be generalised, but we only require the simplest cases which are given here.) We use the (standard) notation

$$\int_{c-\infty i}^{c+\infty i} f(t)\,dt = \lim_{L\to\infty} \int_{c-Li}^{c+Li} f(t)\,dt$$

assuming the limit exists.

Lemma 2 Suppose $c > 0$ and $u > 0$ then

$$\text{a)} \qquad \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{u^{-z}}{z(z+1)}\,dz = \begin{cases} 1-u & \text{if } 0 < u \le 1 \\ 0 & \text{if } u > 1 \end{cases}$$

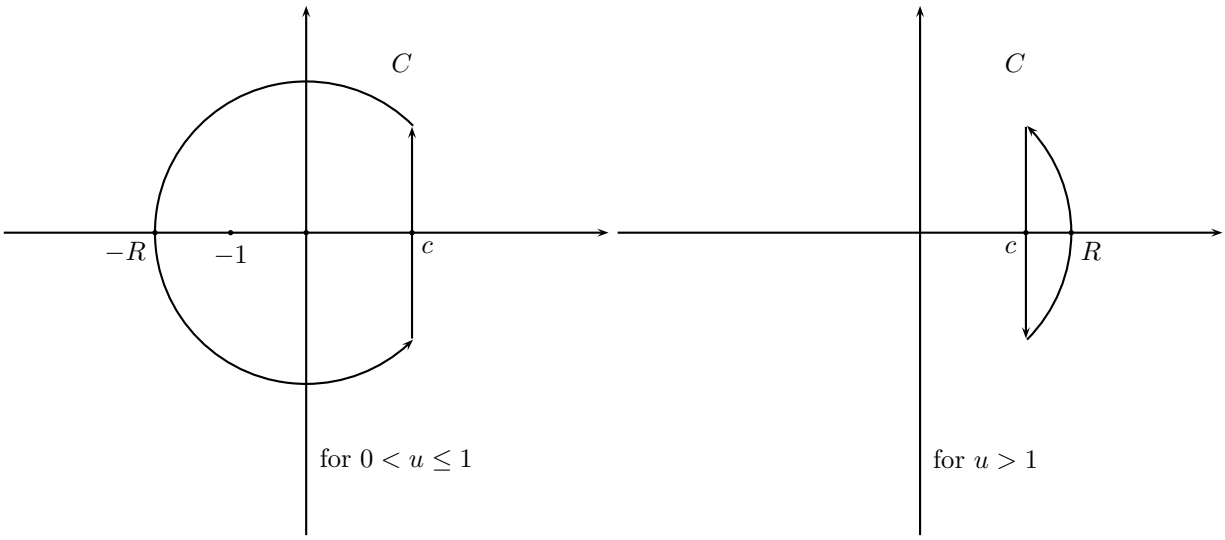
$$\text{b)} \qquad \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{u^{-z}}{z(z+1)(z+2)}\,dz = \begin{cases} \frac{1}{2}(1-u)^2 & \text{if } 0 < u \le 1 \\ 0 & \text{if } u > 1 \end{cases}$$

Proof: We will only prove (a) here, and note that (b) is done similarly.

Consider the integral

$$I = \frac{1}{2\pi i}\int_C \frac{u^{-z}}{z(z+1)}\,dz$$

where C is the appropriate contour shown below according as $0 < u \le 1$ or $u \ge 1$.



The segments shown are of radius $R > 2$ and we let C' refer to the curved section of either contour. Also let $f(z) = \frac{u^{-z}}{z(z+1)}$.

Now in either diagram, for $z \in C'$, we can estimate:

$$\left|\frac{u^{-z}}{z(z+1)}\right| \le \frac{u^{-x}}{|z||z+1|} \le \frac{u^{-c}}{R|z+1|}$$

since u^{-x} is increasing for $0 < u \le 1$ and decreasing for $u > 1$. Now again for $z \in C'$, $|z+1| \ge |z| - 1 = R - 1 \ge \frac{R}{2}$ and so

$$\left|\frac{1}{2\pi i}\int_{C'} \frac{u^{-z}}{z(z+1)}\,dz\right| \le \frac{1}{2\pi}.2\pi R.\frac{2u^{-c}}{R^2} \to 0$$

as $R \to \infty$.

Now for $u > 1$, $f(z)$ is analytic in C so the integral is zero.

For $0 < u \leq 1$, there are simple poles in C at $z = 0, z = -1$. The corresponding residues are clearly 1 and $-u$ and so, in this case

$$\frac{1}{2\pi i}\int_C \frac{u^{-z}}{z(z+1)}\,dz = (1-u)$$

by the residue theorem. Letting $R \to \infty$ we have the desired result.

Lemma 3.

a) For any arithmetic function $a(n)$, let $A(x) = \sum_{n\leq x} a(n)$, where $A(x) = 0$ for $x < 1$, then

$$\sum_{n\leq x}(x-n)a(n) = \int_1^x A(t)\,dt.$$

b) $\psi_1(x) = \sum_{n\leq x}(x-n)\Lambda(n)$

Proof: (a) Using Abel's identity (Theorem 6.1), with $f(t) = t$ we have

$$\sum_{n\leq x} a(n)f(n) = \sum_{n\leq x} na(n) = xA(x) - \int_1^x A(t)f'(t)\,dt$$

and so

$$-\sum_{n\leq x} na(n) + x\sum_{n\leq x} a(n) = \int_1^x A(t)\,dt$$

and the result follows.

(b) Put $a(n) = \Lambda(n)$ and $A(x) = \psi(x)$ in (a).

Recall from the Corollary to Theorem 2.8 that

$$\text{(a)} \qquad \zeta'(s) = -\sum_{n=1}^{\infty}\frac{\log n}{n^s}$$

$$\text{(b)} \qquad -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

We can now state and prove the following key result:

Theorem 2: If $c > 1$ and $x \geq 1$ then

$$\frac{\psi_1(x)}{x^2} = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)ds.$$

Proof: From Lemma 3(b), we know that $\dfrac{\psi_1(x)}{x} = \sum_{n\leq x}(1-\dfrac{n}{x})\Lambda(n)$ and from Lemma 2(a) above, with $u = \frac{n}{x}$, we obtain

$$1 - \frac{n}{x} = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{\left(\frac{x}{n}\right)^s}{s(s+1)}\,ds.$$

Multiplying by $\Lambda(n)$ and summing over all $n \leq x$, we have

$$\frac{\psi_1(x)}{x} = \sum_{n\leq x}\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{\Lambda(n)\left(\frac{x}{n}\right)^s}{s(s+1)}\,ds$$

$$= \sum_{n=1}^{\infty} \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{\Lambda(n)\left(\frac{x}{n}\right)^s}{s(s+1)}\, ds$$

since if $n > x$ then $u = \frac{n}{x} > 1$ and so by Lemma 3 the integral vanishes.

We now wish to interchange the summation and the integral which is allowable, by the dominated convergence theorem, provided $\sum_{n=1}^{\infty} \int_{c-\infty i}^{c+\infty i} \left| \frac{\Lambda(n)\left(\frac{x}{n}\right)^s}{s(s+1)} \right| ds$ converges. It is left as an exercise to show that the partial sums of the above series are bounded by $A \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^c}$, where A is a constant. (See Apostol p.283 for details). Hence

$$\frac{\psi_1(x)}{x} = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \sum_{n=1}^{\infty} \frac{\Lambda(n)\left(\frac{x}{n}\right)^s}{s(s+1)}\, ds = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{x^s}{s(s+1)} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}\, ds$$

$$= \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{x^s}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) ds.$$

Dividing by x gives the desired result.

We now use the above integral representation to show that

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi} \int_{-\infty}^{\infty} h(1+it) e^{it \log x}\, dt,$$

where $\int_{-\infty}^{\infty} |h(1+it)|\, dt$ converges.

Once again we need a succession of technical lemmata to achieve this.

Lemma 4: If $f(s)$ has a pole of order k at $s = \alpha$ then $\frac{f'(s)}{f(s)}$ has a simple pole at $s = \alpha$ with residue $-k$.

Proof: Tutorial Exercise

Lemma 6: The function $F(s) = \frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1}$ is analytic at $s = 1$.

Proof: Exercise. (Follows from Lemma 4).

Theorem 3: For $x \geq 1$ we have

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}(1 - \frac{1}{x})^2 = \frac{1}{2\pi} \int_{-\infty}^{\infty} h(1+it) e^{it \log x}\, dt,$$

where $\int_{-\infty}^{\infty} |h(1+it)|\, dt$ converges.

Proof:
From Lemma 3(b), with $u = \frac{1}{x}$, we have

$$\frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} \frac{x^s}{s(s+1)(s+2)}\, ds$$

where $c > 0$.

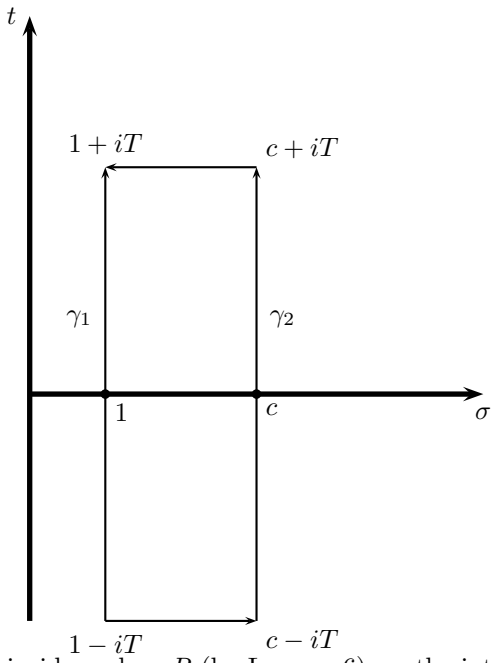
Replacing s by $s-1$ and subtracting the result from the formula in Theorem 2 gives

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{1}{2i\pi} \int_{c'-i\infty}^{c'+i\infty} \frac{x^{s-1}}{s(s+1)} \left[\frac{-1}{s-1} - \frac{\zeta'(s)}{\zeta(s)} \right] ds, \text{ where } c' > 1,$$

$$= \frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty} x^{s-1}h(s)\,ds \qquad \text{(relabelling } c' = c\text{)}$$

where $h(s) = \dfrac{-1}{s(s+1)}\left(\dfrac{1}{s-1} + \dfrac{\zeta'(s)}{\zeta(s)}\right)$.

We now use Cauchy's theorem to move the path of integration to the line $\sigma = 1$.
Consider the rectangular contour R shown with $T > e$ (recalling that $c > 1$).



Now $x^{s-1}h(s)$ is analytic inside and on R (by Lemma 6), so the integral around R is zero.
Now consider the integral along the top horizontal segment $-\gamma_3$, where $t = T$. For $s \in -\gamma_3$, clearly, $|s| \geq T, |s+1| \geq |s|$ and $|s-1| \geq T$, so

$$\left|\frac{1}{s(s+1)}\right| \leq \frac{1}{T^2} \quad \text{and} \quad \left|\frac{1}{s(s+1)(s-1)}\right| \leq \frac{1}{T^3} \leq \frac{1}{T^2}.$$

Recall now, from Theorem 4.6, that $\left|\dfrac{\zeta'(s)}{\zeta(s)}\right| \leq M(\log t)^9$, provided $\sigma \geq 1$ and $t \geq e$. Hence for $T \geq e$,

$$|h(s)| \leq \frac{2M(\log T)^9}{T^2} \qquad \text{for sufficiently large} T$$

so, on the top horizontal segment $-\gamma_3$, $s = t + iT$, $1 \leq t \leq c$,

$$\left|\int_{-\gamma_3} x^{s-1}h(s)\,ds\right| \leq \int_1^c x^{t-1}\,|h(t+iT)|\,dt \leq \frac{2Mx^{c-1}(\log T)^9}{T^2}(c-1) \to 0$$

as $T \to \infty$.
The same argument holds for the lower horizontal segment.

Hence, as $T \to \infty$,

$$\int_{\gamma_2} x^{s-1}h(s)\,ds = \int_{-\gamma_1} x^{s-1}h(s)\,ds$$

in other words

$$\int_{c-i\infty}^{c+i\infty} x^{s-1}h(s)\,ds = \int_{1-i\infty}^{1+i\infty} x^{s-1}h(s)\,ds.$$

Now on the line $\sigma = 1$, put $s = 1 + it$, then $x^{s-1} = x^{it} = e^{it \log x}$, so

$$\frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} x^{s-1} h(s)\, ds = \frac{1}{2\pi} \int_{-\infty}^{\infty} h(1+it) e^{it \log x}\, dt.$$

We can split this integral into the three parts

$$\int_{e}^{\infty} + \int_{-\infty}^{-e} + \int_{-e}^{e}.$$

Now for $e \leq t < \infty$, $|h(1+it)| \leq \frac{M(\log t)^9}{t^2}$ so $\displaystyle\int_e^{\infty} |h(1+it)|\, dt$ converges.

Similarly, $\displaystyle\int_{-\infty}^{-e} |h(1+it)|\, dt$ converges, and the third integral is finite. Thus $\displaystyle\int_{-\infty}^{\infty} |h(1+it)|\, dt$ converges.

The final piece in the puzzle is to show that the integral on the right in Theorem 3 goes to zero as $x \to \infty$ and this will complete the proof. To do this we need the follow result from Fourier Analysis.

Lemma 6: (Riemann-Lebesque Lemma).

If $\displaystyle\int_{-\infty}^{\infty} |f(t)|\, dt$ converges then $\displaystyle\int_{-\infty}^{\infty} f(t) e^{itx}\, dt \to 0$ as $x \to \infty$.

Proof: See Analysis 2 course.

Note that we can replace the x in the above by $\log x$.

Applying the Riemann Lebesque lemma to the formula in Theorem 3, we have

$$\int_{-\infty}^{\infty} h(1+it) e^{it \log x}\, dt \to 0 \quad \text{as} \quad x \to \infty$$

and so $\frac{\psi_1(x)}{x^2} \to \frac{1}{2}$ giving $\psi_1(x) \sim \frac{1}{2} x^2$ which implies the PNT.