MAS430 - Analytic Number Theory

Daniel Fretwell

Semester 1 - Autumn 2014/15

Introduction

Number theory is considered one of the oldest branches of mathematics. Classically it aims to study certain explicit but interesting properties of the ring $\mathbb{Z}$ of integers.

Questions that were asked in MAS208/330 were typically about solutions of Diophantine equations (such as the Fermat equation $x^n + y^n = z^n$ or Pell's equation $x^2 - Ny^2 = 1$) or about certain types of special number (perfect numbers, Mersenne primes, Fermat primes, Fibonacci numbers). Tools such as modular arithmetic, Legendre symbols and continued fractions were developed to answer such questions.

From a modern point of view number theory splits into separate branches, the main two being algebraic and analytic.

In algebraic number theory we study the integers and certain algebraic analogues of them via methods from abstract algebra. This area of number theory grew out of various attempts to solve Fermat's Last Theorem and other special Diophantine equations by extending to fields such as $\mathbb{Q}(\sqrt{2})$ and cyclotomic fields $\mathbb{Q}(\zeta)$.

Algebraic number theorists ask questions such as; what are the units of my ring? Do I have unique factorisation? If not can I fix it or measure its failure? Some of these questions were answered for nice rings in MAS276.

Analytic number theory, the topic of this course, began as an attempt to use real and complex analysis to study the integers.

The majority of analytic number theory grew from 19th century mathematics but earlier mathematicians such as Euler considered (and often solved) questions which are now thought to belong to this branch of number theory.

Analytic number theory concerns itself with questions on a very large scale. Here we care about the overall distribution of a given set of numbers when we can't measure exactly. Typical questions are of the form; How many numbers exist with a given property? Roughly how many of them lie in an interval? How big should we expect the nth such number to be? Can I approximate the distribution of these numbers as we approach infinity? Questions of this flavour are possibly newer to you but are still interesting.

The two branches of number theory often help each other to advance!

Formalities

- Lectures will occur twice weekly.
- Homework will be announced in lectures.
- There will be **no** official office hours. However, if anyone requires any help then feel free to get in touch (preferably by email or by dropping into my office J14a) and we can arrange a time to meet and sort out your problems.
- ...and now the bit you have all been waiting for. The exam will be of the same format to previous years. You should **not** expect the questions to be exactly the same though. More details will be given near the end of the course.

How to use the notes

I always try and motivate every piece of maths I teach and try my best to make it as interesting as possible. After all, it really is!

That said, doing this comes with a price. You will probably have noticed that the notes are quite lengthy. Do not panic, not everything in these notes is examinable!

At times there will be extra tidbits thrown in that are connected to the course but lie outside the syllabus. I have decided to label these as "Interesting facts" rather than "Non-examinable", in order to try and deter mathematical discrimination (whether or not this works we shall see!).

Go on, read them if you dare...you might find out something interesting!

Either way, my intentions are to produce a second set of notes. These will simply contain any important definitions/theorems from the course and nothing else.

Finally, I will finish by giving a piece of advice that you have no doubt heard before. (Pure) Maths is **not** about memorizing definitions and proofs. It is a beautiful discipline and this should be respected.

Of course there is some amount of memory involved but you should always strive to **understand** the material to the best of your ability. This takes effort, but is worth it in the long run!

Here are some tips (most of these apply to any module):

- Never be happy reading a formal definition without knowing its purpose or getting some intuition behind it. Nothing in maths is ever created randomly!

  Formal definitions are usually the most concise way of capturing a given notion/behaviour and are often developed/refined over many years. However they aren't always the easiest to understand.

- Theorems have feelings too!

  Always try and pull the full potential out of a theorem. What does it **mean**? How can I **use** it to show other interesting stuff? Is it a **strong** theorem?

- In the notes I have included small exercises where possible. **Do them!** (They are not compulsory but will aid your thinking/understanding of what is going on).

- If something crops up from previous modules then make sure to go back and refresh your memory. Maths is not a collection of disjoint topics...different areas relate!

- If the notes/lectures are **not** to your liking then shop around! These are not the only analytic number theory resources in existence.

  Of course I welcome suggestions on how to improve things too.

- Some of the exercises are tough! However try not to depend on solutions. This is a hard habit to break if you have done this so far.

  In my experience I find that the more you rely on someone else to solve your problems the less you appreciate the solution or the effort that goes into producing it. More importantly the less you learn about what you haven't learnt.

  Of course noone can solve **every** problem by themselves but it can only do you some good to try (even if you don't get anywhere). For a module at this level I would recommend spending at least 30 mins on a problem before consulting solutions. This is not unreasonable...some mathematicians spend their whole lives trying to solve a single problem!

Reading list These notes/exercises were chiseled together via a mixture of A.F. Jarvis' notes, J. Manoharmayum's notes and various books.

It is not compulsory to read anything (not even these notes) but here are a few suggestions for books. However none of these books contain the entire course.

- T. Apostol - Analytic Number Theory (Springer, "Undergraduate Texts in Mathematics" series).

  This book is probably the closest to the course and is aimed at an advanced undergrad audience (so is written to be very accessible). There are plenty of exercises etc.

- J. Stopple - A Primer of Analytic Number Theory (Cambridge University Press).

  This is also a good introductory book. There are many down to earth discussions of concepts with lots of computational evidence. However the book doesn't approach Dirichlet's theorem beyond its statement, but replaces this with lots of other interesting topics.

- R. Murty - Problems in Analytic Number Theory (Springer, "Graduate Texts in Mathematics" series).

  This book is written as a textbook but in a problematic style. Half the book is about learning/discovering Analytic number theory through solving problems and the other half gives full solutions if you get stuck.

- H. Edwards - The Riemann Zeta Function (Dover publishing).

  This is an older book but is still regarded as one of the greats for getting to grips with the Riemann zeta function. The main aim is to discuss in detail what Riemann's amazing 1859 paper is about and how much it tells us about the distribution of primes.

- J. Derbyshire - Prime Obsession (Plume publishing).

  This book is intended to be written for the general public but is actually quite a pleasant and interesting read. It showcases in plain terms everything that we will see about the prime number theorem, the Riemann zeta function and more...getting towards the advanced theory and the Riemann Hypothesis.

  In alternating chapters the author chooses to change between maths and history, giving a bit of something for everyone.

Contents

1 Primes and their distribution

1.1 Primes

Recall that an integer $n \geq 2$ is **prime** if the only positive divisors of n are 1 and n.

Prime numbers are interesting, but why?

1. By virtue of the fundamental theorem of arithmetic we can write every positive integer $n \geq 2$ as a product of primes in a unique way. In some sense the primes are the "building blocks" of the integers.
2. Primes happen to exhibit quite a few extremely nice properties. Thus they appear in many applications of maths (consider all modern cryptosystems found in MAS328, for example the RSA cryptosystem).
3. A common belief in number theory folklore is that to prove/study something for all integers you should first prove/study it for primes. This is usually easier, something you have probably observed in previous modules.
4. Prime numbers are also mysterious. They are non-trivial to study and for every question we solve about them there are probably another ten that remain unsolved.

As mentioned in the introduction, analytic number theory typically asks questions about the distributional or asymptotic behaviour of number theoretic objects. In this section we will see some results of this kind for prime numbers.

1.1.1 Three proofs of the infinitude of primes

The first natural question to ask about the distribution of prime numbers is, "How many are there?".

It is likely that you have seen the answer to this question before. We will see the answer again, but we will see **three** proofs. This might seem like a silly thing to do but seeing the same result proved in different ways can sometimes help to develop different ways of thinking.

Theorem 1.1. *(Euclid) There are infinitely many primes.*

Proof 1 *(the proof you have probably seen before)*

Suppose there are only finitely many primes $p_1, p_2, ..., p_n$.

Form the number:

$$N = p_1 p_2 ... p_n + 1.$$

Then $N \geq 2$ and so by the fundamental theorem of arithmetic there must exist a prime p such that $p|N$.

However since $p_1, p_2..., p_n$ are assumed to be **all** of the primes it must be that $p = p_i$ for some i.

This gives a contradiction since

$$p_i|(N - p_1p_2...p_n) = 1$$

□

The above proof is the classical one but there are many different proofs. Before uncovering a new proof we need a lemma that will also be of use in proving certain other results.

Lemma 1.2. *Let $p_1, p_2, ..., p_n$ be the first n primes. For $x \in \mathbb{N}$ let $N_n(x)$ be the number of integers less than or equal to x that are divisible **only** by $p_1, p_2, ..., p_n$.*

Then:

$$N_n(x) \leq 2^n\sqrt{x}.$$

Proof. Let $k \in \mathbb{N}$ be such that $1 \leq k \leq x$. We may write $k = s^2k'$ for some (unique) square-free $k' \in \mathbb{N}$.

Assume now that k is only divisible by the primes $p_1, p_2, ..., p_n$.

Thus:

$$k' = p_1^{a_1}p_2^{a_2}...p_n^{a_n}$$

where $a_i \in \{0, 1\}$ for all i. There are clearly at most 2^n choices for the tuple $(a_1, a_2, ..., a_n)$, hence at most 2^n many choices for k'.

Also

$$s^2 \leq s^2k' = k \leq x$$

so that $s \leq \sqrt{x}$. So there are at most $\sqrt{x}$ choices for s.

Putting this together means there are at most $2^n\sqrt{x}$ choices for k. Thus $N_n(x) \leq 2^n\sqrt{x}$. □

We are now ready to see a second proof of Euclids theorem.

Proof 2

Suppose there are only finitely many primes $p_1, p_2, ..., p_n$. Then **every** $n \geq 2$ can only be divisible by the primes $p_1, p_2, ..., p_n$ so that $N_n(m) = m$ for every $m \in \mathbb{N}$.

However by the lemma we then see that for **all** $m \in \mathbb{N}$:

$$m \leq 2^n\sqrt{m}.$$

This is a contradiction since the inequality fails for $m > 2^{2n}$. □

The above proof conveniently followed by studying the function $N_n : \mathbb{N} \longrightarrow \mathbb{C}$. Later in the course we will study such "arithmetic functions" in more detail.

For the third proof we employ the use of infinite series. We first need another small (but important) corollary.

Corollary 1.3. *Let p_i be the ith prime. Then the series:*

$$S = \sum_{i=1}^{\infty} \frac{1}{p_i}$$

diverges.

Proof. Suppose the sum converges and let S_n be the nth partial sum, i.e.

$$S_n = \sum_{i=1}^{n} \frac{1}{p_n}.$$

Now by definition of convergence of infinite sums $S_n \longrightarrow S$ thus we may find $m \geq 1$ such that $|S - S_m| < 1/2$, in other words:

$$\frac{1}{p_{m+1}} + \frac{1}{p_{m+2}} + \frac{1}{p_{m+3}} + ... < \frac{1}{2}.$$

But now for any integer $x \geq 1$:

$$\frac{x}{p_{m+1}} + \frac{x}{p_{m+2}} + \frac{x}{p_{m+3}} + ... < \frac{x}{2}.$$

Now $\left\lfloor \frac{x}{p_{m+k}} \right\rfloor$ counts the number of integers less than or equal to x that are divisible by p_{m+k}. So we see that:

$$x - N_m(x) \leq \frac{x}{p_{m+1}} + \frac{x}{p_{m+2}} + \frac{x}{p_{m+3}} + ... < \frac{x}{2}$$

i.e.

$$\frac{x}{2} < N_m(x) \leq 2^m \sqrt{x}$$

an inequality which fails for $x \geq 2^{2m+2}$. □

Interesting fact - How little do we know?

Even though S diverges we are a long way from observing this experimentally since:

$$\sum_{\text{known primes}} \frac{1}{p} < 4.$$

The third proof of Euclid's theorem is now apparent.

Proof 3

Suppose there exist finitely many primes $p_1, p_2, ..., p_n$. Then the sum S mentioned above will converge (since it is a finite sum) and this contradicts the corollary. □

Hopefully the two new proofs illustrate how analytic methods can be used to tell us things about number theory. In fact later we will see a proof similar to Proof 3 by using the divergence properties of the Riemann zeta function.

More proofs of Euclid's result can be found on Exercise sheet 1.

1.1.2 Primes in arithmetic progressions

The original proof of Euclid's theorem dates back to antiquity, albeit not in the form we see it today. However since this result became widely known number theorists have continued to ask questions of the form, "How many primes exist with a given property?".

For example, how many even primes exist? This is an easy question, the answer being that there is only one. (Hopefully this didn't surprise you at all!)

But even simple, innocent sounding questions can be tough to solve. For example, how many primes are there of the form $k^2 + 1$? Examples are easily generated:

$$\begin{aligned} 2 &= 1^2 + 1 \\ 5 &= 2^2 + 1 \\ 17 &= 4^2 + 1 \\ 37 &= 6^2 + 1 \\ 101 &= 10^2 + 1 \end{aligned}$$

and after more experimentation it appears that there are infinitely many such primes, but how does one go about **proving** that?

Truth be told...noone knows! This is an unsolved problem about prime numbers.

However we **can** handle this question for linear forms $ak + b$ $(a, b \in \mathbb{Z})$. In fact Euclid's result can be viewed as any of the cases where $a = 2$ and b is odd (or any of the cases where $a = \pm 1$).

Here are some other examples taken from MAS208/330.

Theorem 1.4. *There are infinitely many primes of the form* $4k + 3$*, i.e. congruent to* 3 mod 4.

Proof. Suppose there are only finitely many primes congruent to 3 mod 4. Label these $p_1, p_2, ..., p_n$.

Form the number:

$$N = 4p_1p_2...p_n - 1.$$

Then $N \geq 2$ so must have prime divisors. We show that N must have a prime divisor that is 3 mod 4.

Suppose on the contrary that **all** odd prime divisors of N are congruent to 1 mod 4. Then N would be factorised as a product of numbers that are all 1 mod 4, hence $N \equiv 1 \bmod 4$. However looking at our choice of N, it is clear that $N \equiv 3 \bmod 4$, giving a contradiction.

Thus there exists odd prime $p|N$ such that $p \equiv 3 \bmod 4$. However, since we assumed $p_1, p_2, ..., p_n$ are **all** of the primes that are 3 mod 4 it must be that $p = p_i$ for some i.

But then:

$$p_i|(N - 4p_1p_2...p_n) = -1.$$

□

If you try a similar argument for primes of the form $4k + 1$ you become stuck at some point. (why? Do it!)

However we can modify the proof using our knowledge of quadratic residues.

Theorem 1.5. *There are infinitely many primes of the form* $4k + 1$*, i.e. congruent to* 1 mod 4.

Proof. Suppose there are only finitely many primes congruent to 1 mod 4. Label these $p_1, p_2, ..., p_n$.

Form the number:

$$N = (2p_1p_2...p_n)^2 + 1.$$

Then $N \geq 2$ so must have prime divisors. We show that N must have a prime divisor that is 1 mod 4.

Note that if $p|N$ we see that:

$$(2p_1p_2...p_n)^2 \equiv -1 \bmod p$$

so that -1 is a quadratic residue mod p. But by results from MAS208/330 we know this happens if and only if $p \equiv 1 \bmod 4$. Hence in fact all prime divisors of N must be congruent to 1 mod 4.

Choose such a $p|N$. Then since $p_1, p_2, ..., p_n$ are assumed to be **all** of the primes congruent to 1 mod 4 we have $p = p_i$ for some i.

But then:

$$p_i|(N-(2p_1p_2...p_n)^2)=1.$$

□

Exercise sheet 1 contains questions of a similar nature, demanding more subtle techniques than we used here.

In order to form a general conjecture for primes of the form $mk+a$ we really ought to be careful in our choice of m and a.

Exercise If $\text{hcf}(a,m)>1$ show there can only be at most one prime of the form $mk+a$.

We are now in a position to state the general result.

Conjecture 1.6. *(Dirichlet) Let $a,m\in\mathbb{N}$ be coprime. Then there are infinitely many primes of the form $mk+a$ (i.e. congruent to $a \bmod m$).*

The above result is referred to as *Dirichlet's theorem on primes in arithmetic progressions.*

It should be clear that proving this general result would be tough, if not impossible, using only elementary tools (we had to have two different proofs just to tackle the cases $4k+1$ and $4k+3$).

One of the major aims of this course is to prove this theorem by using analytic tools, the way that Dirichlet did it originally. In fact Dirichlet's work on this theorem can be considered one of the major starting points of analytic number theory.

The basic idea behind the proof is to consider certain nicely behaved functions $\chi:\mathbb{Z}\longrightarrow\mathbb{C}$ that come from complex-valued homomorphisms of $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

To each such χ we will associate an infinite series called a Dirichlet L-function. Via considering certain combinations of such functions we will essentially be able to show that series such as:

$$\sum_{p\equiv a \bmod m}\frac{1}{p}$$

diverge, giving a proof of Dirichlet's theorem similar to Proof 3 of Euclid's theorem.

1.1.3 The Green-Tao theorem

We have just considered arithmetic progressions that contain infinitely many primes but an alternative question asks, "How long can an arithmetic progression **of** primes be?". Call such a progression of length k, common difference d a (k,d)-primog (non-standard notation).

For example $3,5,7$ is a $(3,2)$-primog.

Exercise

1. Let d be odd. Show that there is at most one $(2,d)$-primog.

   Conclude that if there exists an (n,d)-primog for $n>2$ then d is even.

2. Prove that $(3,5,7)$ is the only $(3,2)$-primog.

   Show that if $d \not\equiv 0 \bmod 3$ then there can be at most **one** $(3,d)$-primog.

   Conclude that if there exists an (n,d)-primog for $n>3$ then $6|d$.

3. For $k \geq 1$ denote by $k\# = \prod_{\text{prime } q\leq k} q$ the primorial of k.

   Show that if there exists an (n,d)-primog for $n>k$,with all terms k or bigger, then $k\#|d$.

4. Can you find examples of (n,k)-primogs for $n=4,5,6$? (Hint: Use the previous part).

5. How many $(2,2)$-primogs exist? (Don't spend too long trying to prove your answer...you might want to google the twin prime conjecture when you begin to get bored!)

The following beautiful theorem was proved by Green/Tao in 2004:

Theorem 1.7. *Let $k\in\mathbb{N}$. Then there exists an arithmetic progression of length k consisting only of primes.*

This is certainly a tough theorem to prove and in fact earned Tao the fields medal in 2006 (the mathematical equivalent of the Nobel prize). Experimental evidence is also tough to find. The current record is of length 26:

$$43142746595714191 + 5283234035979900\,n \qquad \text{for } n = 0,1,2,...,25$$

and was found using a PlayStation 3 in 2010! (Well using a distributed project, although I still think an Xbox would have been a better choice...)

Note that $25\#|5283234035979900$ as expected.

Exercise - Show that, in comparison to the above, it is easy to write down an arithmetic progression of length k consisting of **composite** numbers (Hint: consider numbers of the form $n!+m$ for a suitable choice of n).

1.2 Distribution of primes

Now that we have answered questions about the quantity of certain primes we start to ask about the overall behaviour of sets of primes. For the rest of this section of the notes we will see some amazing theorems about the distribution of primes amongst certain intervals (Bertrand's postulate) and cumulative distribution (the prime number theorem).

1.2.1 Bertrand's postulate

Given any positive integer n a natural question to ask is how far away the next prime is, e.g. the next prime after 2 is 3 and the next prime after 3 is 5. Bertrand's postulate tells us the nice fact that we never have to go beyond $2n$ to find the next prime.

Theorem 1.8. *(Bertrand's postulate) For every $n > 1$ there exists a prime p such that $n < p < 2n$.*

In order to recover Erdös' proof of this result we will first observe a few nice properties of the binomial coefficients $\binom{2n}{n}$.

To get started, it is easy to see that the only primes that can divide the integer $\binom{2n}{n}$ must be between 2 and $2n$. Our first lemma says that a large amount of these primes certainly do not.

Lemma 1.9. *If $n \geq 3$ and p is a prime such that $\frac{2n}{3} < p \leq n$. Then $\binom{2n}{n}$ is not divisible by p.*

Proof. The inequality implies that $p \neq 2$. (why?)

Note that:

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

It is enough to prove that p divides the numerator and denominator to the same order (so that after cancellation p cannot divide this integer).

Now both $p \leq 2n$ and $2p \leq 2n$ and so $p^2 \mid (2n)!$.

Also $p \neq 2$ (so that $2p \neq p^2$) and $3p > 2n$ by the inequality, so $p^3 \nmid (2n)!$.

Thus the highest power of p arising in the numerator is p^2.

Turning to the denominator we see that $p \leq n$ and $2p > \frac{4n}{3} > n$ and so $p \mid n!$ but $p^2 \nmid n!$.

Hence the highest power of p to divide $n!n!$ is also p^2 as required. □

Now we consider what the factorisation of $\binom{2n}{n}$ can look like. Naively we first expect that any prime power appearing in the factorisation is less than $(2n)!$ (or even $\frac{(2n)!}{n!} = (2n)(2n-1)(2n-2)...(n+1)$).

Our second lemma improves this upper bound greatly.

Lemma 1.10. *Let $n \geq 1$ be a fixed integer and choose a prime p. Suppose p^{α_p} is the highest power of p to divide $\binom{2n}{n}$.*

Then $p^{\alpha_p} \leq 2n$.

Proof. Let r_p be the unique integer such that $p^{r_p} \leq 2n < p^{r_p+1}$.

It remains to prove that $\alpha_p \leq r_p$, since then $p^{\alpha_p} \leq p^{r_p} \leq 2n$.

Now:

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

(see Exercise sheet 1) and each term in this sum is 0 or 1, hence $\alpha_p \leq r_p$. □

Our third lemma gives a trivial lower bound on the size of $\binom{2n}{n}$.

Lemma 1.11. *For all $n \geq 1$ we have:*

$$\binom{2n}{n} \geq \frac{4^n}{2n+1}.$$

Proof. Consider the binomial expansion of $(1+1)^{2n}$:

$$2^{2n} = (1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + ... + \binom{2n}{n} + ... + \binom{2n}{2n-1} + \binom{2n}{2n}.$$

Then since $\binom{2n}{n}$ is the central coefficient, it must be the largest term in this sum, hence:

$$2^{2n} \leq (2n+1)\binom{2n}{n}$$

giving the required inequality. □

We are now almost in a position to prove Bertrand's postulate. First we need one more small lemma providing a bound on products of primes.

Lemma 1.12. *For all $n \geq 2$:*

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

Proof. See Exercise sheet 1. □

Proof of Bertrand's postulate

Clearly the result is true for $n = 1, 2, 3, 4$ so assume it is false for some $n \geq 5$. Then for this particular n there are no primes between n and $2n$.

Consider the binomial coefficient $\binom{2n}{n}$. Then by our assumption and by Lemma 1.9 the only primes to divide $\binom{2n}{n}$ must be ones that are less than or equal to $\frac{2n}{3}$.

Now consider the factorisation:

$$\binom{2n}{n} = \prod_{p \leq \frac{2n}{3}} p^{\alpha_p}.$$

By Lemma 1.10 we have $p^{\alpha_p} \leq 2n$ for each such p. Now if $p > \sqrt{2n}$ then clearly we must have $\alpha_p = 0$ or 1. Thus:

$$\binom{2n}{n} \leq \left(\prod_{p \leq \frac{2n}{3}} p \right) \left(\prod_{p \leq \sqrt{2n}} p^{\alpha_p} \right) \leq \left(\prod_{p \leq \frac{2n}{3}} p \right) (2n)^{\sqrt{2n}},$$

where the final inequality uses Lemma 1.10 and the fact that there are at most $\sqrt{2n}$ primes less than or we equal to $\sqrt{2n}$.

Using Lemmas 1.12 and 1.11 we may now conclude that:

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

Thus:

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

After taking logs we see that:

$$\frac{2n \ln(2)}{3} < (2 + \sqrt{2n}) \ln(2n).$$

This inequality fails for $n = 507$ and since the function

$$f(x) = \frac{2x \ln(2)}{3} - (2 + \sqrt{2x}) \ln(2x)$$

is increasing for $x \geq 507$ the inequality must in fact fail for all $n \geq 507$.

It remains to show that there is no counterexample below 507 but this is a small amount of computation. In fact the primes $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 557$ cover all of these possibilities. □

Exercise - Check the claim about $f(x)$ by using calculus. (Of course $f(x)$ starts to increase much earlier but we didn't need to know exactly when).

1.2.2 The prime counting function

We now move on to study how the primes are distributed as a whole. The way we do this is by constructing a function that measures quantites of primes for finite bounds.

Definition 1.13. For real $x > 0$ define the **prime counting function**:

$$\pi(x) = \#\{1 < p \leq x \,|\, p \text{ is prime}\}.$$

For example, $\pi(3) = 2, \pi(30) = 10, \pi(6.5) = 3, \pi(\pi) = 2$.

Our main interests will be to study the behaviour of $\pi(x)$ as $x \to \infty$. However it will be easier to study bounds for this function first to get some sort of idea of how the function behaves.

First we notice that there is **no** upper bound.

Lemma 1.14. *$\pi(x) \to \infty$ as $x \to \infty$.*

Proof. This is another way of stating that there are infinitely many primes. We have proved this several ways so far. □

Important questions arise. Even though $\pi(x)$ diverges, how **fast** does it diverge? Can we **measure** its divergence relative to other functions? We will try and answer these questions soon.

For now we observe a simple lower bound for $\pi(x)$.

Proposition 1.15. *For any $x \geq 1$:*

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

Proof. Let $\pi(x) = n$ so that there are exactly n primes less than or equal to x.

Since $\pi(x) = \pi(\lfloor x \rfloor)$ we may assume that x is an integer. Hence $N_n(x) = x$, since integers that are k or less can only be divisible by primes that are k or less.

But then by use of the inequality for $N_n(x)$:

$$x \leq 2^n \sqrt{x}$$

giving $x \leq 2^{2n}$. Thus:

$$\pi(x) = n \geq \frac{\ln(x)}{2\ \ln(2)}.$$

□

Using the inequality we can get an upper bounds for the nth prime.

Corollary 1.16. *Let p_n be the nth prime. Then $p_n < 4^n$.*

Proof. Let $x = p_n$. Then $\pi(x) = n$ and so:

$$n \geq \frac{\ln(p_n)}{2\ln(2)}.$$

Rearranging and taking exponentials gives $p_n \leq 4^n$. Equality is not possible (why?) thus $p_n < 4^n$. □

These two results are incredibly weak.

x	$\pi(x)$	$\frac{\ln(x)}{2\ln(2)}$ (to 5 d.p)
10	4	1.66096
100	25	3.32193
1000	168	4.98289
10000	1229	6.64386
100000	9592	8.30482
1000000	78498	9.96578

n	p_n	4^n (to 5 s.f)
10	29	1048600
100	541	1.6069×10^{60}
1000	7919	1.1481×10^{602}
10000	104729	3.9803×10^{6020}
100000	1299709	9.9801×10^{60205}
1000000	15485863	$9.8023 \times 10^{602059}$

In fact using Bertrand's postulate we can already get a better estimate for the nth prime without much effort:

Corollary 1.17.

$$p_n < 2^n$$

Proof. We know that 2 is prime and so it remains to show that there are at least $n-1$ primes in the interval $(2, 2^n)$.

However this is easy since Bertrand's postulate says that there is a prime lying in the interval $(2^k, 2^{k+1})$ for any $k \geq 1$ and

$$(2, 2^n) \supseteq (2,4) \cup (4,8) \cup ... \cup (2^{n-1}, 2^n).$$

□

But even **this** bound is not very good (check it against the tables!). We will soon provide better estimates for $\pi(x)$ and the nth prime.

1.2.3 Chebyshev's inequalities

Now that we have defined $\pi(x)$ and observed roughly how the function behaves we start to get a handle on how we might go about approximating $\pi(x)$ and how we might measure its divergence.

Chebyshev's inequalities begin to do this by providing certain elegant bounds of the form:

$$A\frac{x}{\ln(x)} \leq \pi(x) \leq B\frac{x}{\ln(x)}$$

for x sufficiently large.

This is a big improvement on the previous bounds. We will see two results that give explicit values for A and B. Both proofs will rely again on properties of the binomial coefficients $\binom{2n}{n}$.

First two small lemmas to help us on our way.

Lemma 1.18. *The function $f(x) = \frac{x}{\ln(x)}$ is increasing on $[e, \infty)$.*

Exercise - Prove this using calculus. Specifically look at stationary points.

Lemma 1.19. *For all $n \geq 1$*

$$\prod_{n+1 \leq p \leq 2n} p \leq 2^{2n}$$

Exercise - Prove this in two stages. First notice that the LHS divides $\binom{2n}{n}$ and then prove that $\binom{2n}{n} \leq 2^{2n}$ by using the binomial expansion of $(1+1)^{2n}$.

We start with an upper bound.

Theorem 1.20. *For $x \geq 2$:*

$$\pi(x) \leq (6\ln(2))\frac{x}{\ln(x)}.$$

Proof. We first prove a similar result for x an integer power of 2. Let $n \in \mathbb{N}$.

By Lemma 1.19 we know that:

$$\prod_{n+1 \leq p \leq 2n} p \leq 2^{2n}$$

But clearly we also have:

$$\prod_{n+1 \leq p \leq 2n} p \geq n^{\pi(2n)-\pi(n)}.$$

Putting these together we see that:

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

Taking logs gives:

$$\begin{aligned}(\pi(2n)-\pi(n))\ \ln(n) &\leq 2n\ \ln(2)\\ \pi(2n)\ \ln(n)-\pi(n)\ \ln(n) &\leq 2n\ \ln(2).\end{aligned}$$

Clever trick alert: Replace the second $\ln(n)$ with $\ln(\frac{n}{2})+\ln(2)$.

Now we have:

$$\pi(2n)\ \ln(n)-\pi(n)(\ln\left(\frac{n}{2}\right)+\ln(2)) \leq 2n\ \ln(2)$$

Rearranging gives:

$$\pi(2n)\ \ln(n)-\pi(n)\ \ln\left(\frac{n}{2}\right) \leq (2n+\pi(n))\ \ln(2) \leq 3n\ \ln(2).$$

If we now insert $n=2^k$ for $k=2,...m$:

$$\begin{aligned}\pi(8)\ \ln(4)-\pi(4)\ \ln(2) &\leq (3\ \ln(2))2^2\\ \pi(16)\ \ln(8)-\pi(8)\ \ln(4) &\leq (3\ \ln(2))2^3\\ \pi(32)\ \ln(16)-\pi(16)\ \ln(8) &\leq (3\ \ln(2))2^4\\ &...\\ \pi(2^k)\ \ln(2^{k-1})-\pi(2^{k-1})\ \ln(2^{k-2}) &\leq (3\ \ln(2))2^{k-1}\\ \pi(2^{k+1})\ \ln(2^k)-\pi(2^k)\ \ln(2^{k-1}) &\leq (3\ \ln(2))2^k.\end{aligned}$$

It is now noticed that if we sum all of these inequalities then we get a telescoping sum on the LHS, in the end giving:

$$\pi(2^{k+1})\ \ln(2^k)-\pi(4)\ \ln(2) \leq (3\ \ln(2))(4+8+...+2^k)$$

So that:

$$\begin{aligned}\pi(2^{k+1}) &\leq \frac{(3\ \ln(2))(4+8+...+2^k)+2\ \ln(2)}{\ln(2^k)}\\ &< (3\ \ln(2))\frac{2^{k+1}}{\ln(2^k)}\\ &= (6\ \ln(2))\frac{2^k}{\ln(2^k)}.\end{aligned}$$

For now let's assume $x>4$ and choose $k\in\mathbb{N}$ such that $2^k\leq x<2^{k+1}$. Then

$$\pi(x)\leq\pi(2^{k+1})<(6\ \ln(2))\frac{2^k}{\ln(2^k)}\leq(6\ \ln(2))\frac{x}{\ln(x)},$$

where the last inequality comes from Lemma 2.22 (since $e < 4 \leq 2^k < x$ by construction).

For $2 \leq x \leq 4$ note that $\pi(x) \leq \pi(4) = 2$ but that $(6\ \ln(2))\frac{x}{\ln(x)} \geq (6\ \ln(2))\frac{e}{\ln(e)} = 6e\ \ln(2) > 2$.

Thus the inequality holds for all $x \geq 2$.

□

One lower bound coming right up...

Theorem 1.21. *For $x \geq 2$:*

$$\pi(x) \geq \frac{3\ln(2)}{8}\frac{x}{\ln(x)}.$$

Proof. We first observe a similar result for $\pi(2n)$.

Consider the prime factorisation $\binom{2n}{n} = \prod_{p \leq 2n} p^{\alpha_p}$.

By Lemma 1.10 we know that each $p^{\alpha_p} \leq 2n$ hence:

$$\binom{2n}{n} \leq (2n)^{\pi(2n)}.$$

However also $\binom{2n}{n} \geq 2^n$ for all $n \geq 1$ (by induction).

Thus:

$$2^n \leq (2n)^{\pi(2n)}.$$

Taking logs gives:

$$\pi(2n) \geq \frac{n\ \ln(2)}{\ln(2n)} = \frac{\ln(2)}{2}\frac{2n}{\ln(2n)}.$$

For now assume that $x \geq 6$ and define n to be such that $2n \leq x < 2n + 2$.

Then:

$$\pi(x) \geq \pi(2n) \geq \frac{\ln(2)}{2}\frac{2n}{\ln(2n)}$$

By our choices we find that $e < \frac{3x}{4} \leq 2n$ and so by Lemma 2.22:

$$\frac{\ln(2)}{2}\frac{2n}{\ln(2n)} \geq \frac{\ln(2)}{2}\frac{\frac{3x}{4}}{\ln(\frac{3x}{4})} = \frac{3\ \ln(2)}{8}\frac{x}{\ln(\frac{3x}{4})} > \frac{3\ \ln(2)}{8}\frac{x}{\ln(x)}.$$

This proves the inequality for $x \geq 6$.

It is easily observed that for $2 \leq x \leq 6$ we have $\pi(x) \geq 1$ and $\frac{3\ln(2)}{8}\frac{x}{\ln(x)} < 1$. Thus the inequality holds for all $x \geq 2$.

□

Exercise - Why weren't we done by half way? What is wrong with the following:

Proof attempt

Starting from:

$$\pi(2n) \geq \frac{\ln(2)}{2}\frac{2n}{\ln(2n)}$$

choose n such that $x \geq 2n$. Then:

$$\pi(x) \geq \pi(2n) \geq \frac{\ln(2)}{2}\frac{2n}{\ln(2n)} \geq \frac{\ln(2)}{2}\frac{x}{\ln(x)} > \frac{3\ln(2)}{8}\frac{x}{\ln(x)}.$$

□

1.2.4 The prime number theorem and its applications

We wish to know the behaviour of $\pi(x)$ overall (for large x). More specifically we would like to know how **fast** it diverges.

In analytic number theory (and indeed in many other areas of maths) the correct way to measure this is by using **asymptotic analysis**. Basically the idea is we consider how the **proportions** of two functions behave as x gets large, rather than the differences. This should then give us a measure of how fast a function is diverging relative to another.

Definition 1.22. Let $f, g : \mathbb{R} \to \mathbb{R}$. Then f is **asymptotic to** g, written $f \sim g$, if $\frac{f(x)}{g(x)} \to 1$ as $x \to \infty$.

Knowing that $f \sim g$ tells you that both f, g approximate each other for large x but it doesn't tell you how **good** the approximation is. To know this you would have to know about the limiting behaviour of $f - g$ and this is not provided by asymptotic analysis.

In fact we will see examples of functions with $f \sim g$ but such that the difference $f - g$ diverges as $x \to \infty$. This behaviour is interpreted as f approximating g but the approximation getting worse as x increases (however still remaining good enough relative to the size of x).

Returning to the question at hand, given Chebyshev's inequalities we are led to conjecture the following:

Theorem 1.23. *(Prime number theorem)*

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

This is one of the biggest theorems in Analytic number theory, so big that it deserves the abbeviation PNT from now on.

It should be noted that Chebyshev's inequalities do **not** prove this theorem. However Chebyshev was able to prove the following partial result (which we will only state for simplicity).

Theorem 1.24. *Assuming*

$$\frac{\pi(x)}{x/\ln(x)} \longrightarrow L$$

then $L = 1$.

Note that this theorem doesn't prove the PNT either, since it assumes the limit exists beforehand. It is actually very difficult to show that the limit exists!

A proof of the prime number theorem can be found in any good book/website but beware...it is tough and requires tools that we develop later along with tools from complex analysis (Cauchy residue theorem etc).

Before we see some applications of the PNT we should discuss why this theorem is so great.

We **love** primes. I gave many reasons why at the beginning of this chapter. However even though we **do** have exact formulae that generate prime numbers they are generally useless and/or tough to work with in practice (some are even tautological).

The PNT gives one of the best known approximations of how many prime numbers we should have below a given bound (of course you can also use this information to estimate how many should be between **any** two given bounds). There are better approximations known but most of them diverge at the same rate as $\frac{x}{\ln(x)}$ asymptotically. The PNT was one of the first theorems predicting the rate of divergence of $\pi(x)$ and is still used to this day to study other things.

Interesting fact - A brief history of the PNT

We haven't worked chronologically over the last few sections. The discovery of the PNT actually **predates** Chebyshev's inequalities. In fact the inequalities were developed by Chebyshev as an attempt to try and **prove** the PNT.

A collection of mathematicians contributed to the formulation of the PNT.

Originally Legendre was the first to **publish** a result in 1798 stating that:

$$\pi(x) \sim \frac{x}{A\ \ln(x) + B}$$

for constants A, B.

This is a primitive version of the PNT. Of course by Chebyshev's contribution we now know that $A = 1$. Legendre was able to approximate $B \approx -1.08366...$

Originally Legendre was not the first to consider the behaviour of $\pi(x)$. Gauss, of the 14 year old variety, considered the same question in 1792 but did not publish his findings. However we do have documentary evidence of a letter to his friend (and mathematician) Encke which supports the claim.

We also have evidence that Gauss did in fact study $\pi(x)$ in some fashion. One of his favourite pastimes was to generate huge tables of prime counts. He would look in "chiliads" (blocks of size 1000) and compute the number of primes in such blocks **by hand**.

Gauss observed from these tables that the "density" of primes around the integer n was roughly $\frac{1}{\ln(n)}$ so that in the interval $[a, b)$ we would expect the number of primes to be:

$$\int_a^b \frac{dt}{\ln(t)}.$$

So he was able to predict from this that:

$$\pi(x) \sim \int_2^x \frac{dt}{\ln(t)}.$$

In fact by a result on Exercise sheet 1:

$$\frac{x}{\ln(x)} \sim \int_2^x \frac{dt}{\ln(t)},$$

so we get an alternative form of the PNT. However the function that Gauss predicted on the right looks to be a much better approximation to $\pi(x)$ than Legendre's $\frac{x}{\ln(x)}$ (a fact Gauss was able to demonstrate in writing). See the graph/tables below for evidence of this.

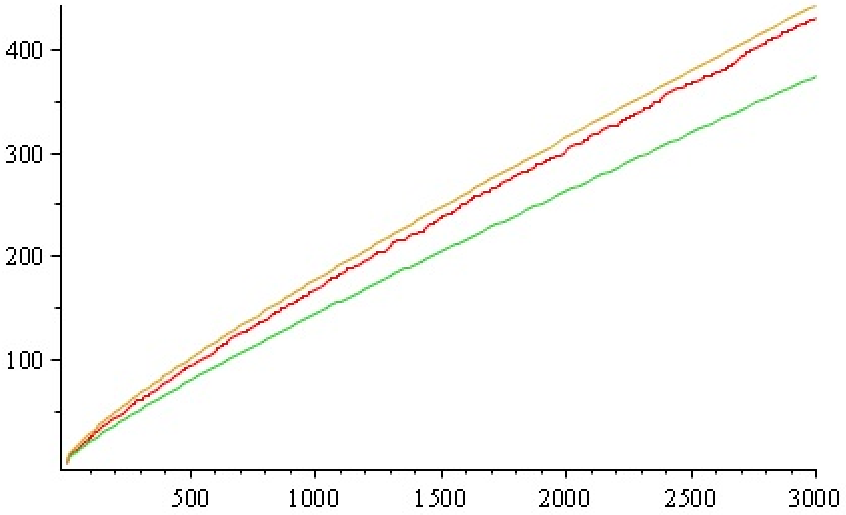
The Riemann hypothesis, discussed later, would make precise how good these approximations are. Unfortunately it is an unsolved problem!

Gauss' estimate is called the **logarithmic integral function** and is denoted $\text{Li}(x)$.

x	$\pi(x)$	$\frac{x}{\ln(x)}$	$\mathrm{Li}(x)$	$\frac{\pi(x)}{\frac{x}{\ln(x)}}$	$\frac{\pi(x)}{\mathrm{Li}(x)}$
10	4	4.34294	5.12044	0.92103	0.78118
100	25	21.71472	29.08098	1.15129	0.85967
1000	168	144.76483	176.56449	1.16050	0.95149
10000	1229	1085.73620	1245.09205	1.13195	0.98708
100000	9592	8685.88964	9628.76384	1.10432	0.99618
1000000	78498	72382.41365	78626.50400	1.08449	0.99837

x	$\left\lvert\pi(x) - \frac{x}{\ln(x)}\right\rvert$	$\lvert\pi(x) - \mathrm{Li}(x)\rvert$
10	0.34294	3.21076
100	3.28528	6.17131
1000	23.23517	10.65482
10000	143.26380	18.18238
100000	906.11036	38.85416
1000000	6115.58635	130.59432

Here is a graph of the three functions of interest to us (red is $\pi(x)$, green is $\frac{x}{\ln(x)}$, brown is $\mathrm{Li}(x)$):



From the graph it appears that $\mathrm{Li}(x) > \pi(x)$ for all $x \geq 1$. However it is known by a theorem of Littlewood that there are infinitely many overlaps $\pi(x) > \mathrm{Li}(x)$. But here is the interesting thing...noone has ever found one! The best we have is an upper bound for the first such **Littlewood violation**. Originally an upper bound was given by **Skewes number**, the astronomical:

$$10^{10^{10^{34}}}$$

During the previous century there has been an improvement of this bound to a number of the order of 10^{371} (which is still too huge to search up to).

The PNT was finally proved by Hadamard and de la Vallée-Poussin in 1896 but during the 20th century many easier/shorter proofs were found.

We now concern ourselves with three powerful applications of the PNT. See Exercise sheet 1 for other interesting applications.

Application 1 - Bertrand revisited

An interesting application of the PNT is that it provides a stronger version of Bertrand's postulate. Note that we may state Bertrand's postulate in an alternate form.

Theorem 1.25. *(Bertrand's postulate version 2) For all $x > 1$*

$$\pi(2x) - \pi(x) \geq 1$$

Exercise - Check carefully that the two versions are equivalent (one way is easier than the other).

One can prove this form of the result by using Chebyshev's inequalities.

Under this disguise we find an obvious generalization.

Theorem 1.26. *(Generalized Bertrand's postulate)*

*Let $a > 1$ be **any** real number. Then for x sufficiently large:*

$$\pi(ax) - \pi(x) \geq 1$$

*i.e. for large enough x there **always** exists a prime lying between x and ax.*

Of course the "sufficiently large" is really needed. The smaller a gets the bigger x will need to be to make the interval big enough to actually contain an integer (never mind a prime).

For example if we let $a = 1.0000000000000001$ then it would be silly to expect a number such as $x = 10$ to work (since $x = 10 < ax < 11$).

Exercise - For the above choice of a what values of x will the interval (x, ax) actually contain an integer? (Of course there is no guarantee that such integers are prime but it gives you some idea of how big "sufficiently large" should mean given a choice of a).

In order to prove this general theorem we remark that the PNT can be restated in a "Chebyshev" form.

Lemma 1.27. *Let A, B be **any** two real numbers such that $0 < A < 1 < B$. Then for x sufficiently large:*

$$A\frac{x}{\ln(x)} < \pi(x) < B\frac{x}{\ln(x)}.$$

Proof of the Generalized Bertrand's postulate

Choose B such that $1 < B < a$ and choose A such that $\frac{B}{a} < A < 1$.

Then by the above lemma we see that, there is some c such that for $x > c$:

$$\pi(ax) > A\frac{ax}{\ln(ax)}$$

and

$$\pi(x) < B\frac{x}{\ln(x)}.$$

Now $(Aa - B) > 0$ by construction and since log is an increasing function there will exist d such that for $x > d$:

$$(Aa - B)\ \ln(x) > B\ \ln(a)$$

(since the RHS is constant).

Notice this then proves that for $x > d$ we have:

$$A\frac{ax}{\ln(ax)} > B\frac{x}{\ln(x)}.$$

But now we are done since for $x > \max\{c, d\}$ we have that

$$\pi(ax) > A\frac{ax}{\ln(ax)} > B\frac{x}{\ln(x)} > \pi(x).$$

Since $\pi(ax), \pi(x) \in \mathbb{N}$ it must be that $\pi(ax) - \pi(x) \geq 1$ for $x > \max\{c, d\}$.

□

Note - In reality we do not know the value of $\max\{c, d\}$ but we can easily find the value of d (so do get a lower bound on "sufficiently large").

Application 2 - Estimating the nth prime

The PNT tells us something about the number of primes less than a number. Unsurprisingly we can use this information to tell us roughly how big the nth prime is. First we again provide an alternative statement of the PNT.

Lemma 1.28.

$$\pi(x) \sim \frac{x}{\ln(\pi(x))}$$

Alternatively

$$\pi(x)\ln(\pi(x)) \sim x.$$

Proof. The PNT tells us that:

$$\frac{\pi(x)\ln(x)}{x} \longrightarrow 1 \qquad \text{as } x \longrightarrow \infty.$$

Now $\ln(x)$ is continuous on $(0, \infty)$. Thus we may take logs in the above and find:

$$\ln(\pi(x)) + \ln(\ln(x)) - \ln(x) \longrightarrow 0 \qquad \text{as } x \longrightarrow \infty.$$

Dividing by $\ln(x)$ and using the fact that $\frac{\ln(\ln(x))}{\ln(x)} \longrightarrow 0$ as $x \longrightarrow \infty$ we see that:

$$\frac{\ln(\pi(x))}{\ln(x)} \longrightarrow 1 \qquad \text{as } x \longrightarrow \infty.$$

So we now know that $\ln(\pi(x)) \sim \ln(x)$. The lemma now follows. □

Corollary 1.29. *If p_n is the nth prime then $p_n \sim n \ln n$.*

Proof. Letting $x = p_n$ in the above lemma gives the result since $\pi(p_n) = n$. □

Let's see how good this approximation is.

n	p_n	$n\ln(n)$ (to 5 d.p)
10	29	23.02585
100	541	460.51702
1000	7919	6907.75528
10000	104729	92103.40372
100000	1299709	1151292.54650
1000000	15485863	13815510.55796

Application 3 - Primes in arithmetic progressions

We can also study the distribution of specific types of prime. For example given $x \geq 1$ (not necessarily an integer) define:

$$\pi_{m,a}(x) = \#\{\text{primes } p \leq x \,|\, p \equiv a \bmod m\}.$$

When Dirichlet proved his theorem on primes in arithmetic progressions he actually proved something stronger.

Theorem 1.30. *For any a, b coprime to m:*

$$\pi_{m,a}(x) \sim \pi_{m,b}(x).$$

Thus, given the PNT we have for any a coprime to m:

$$\pi_{m,a}(x) \sim \frac{x}{\phi(m)\ln(x)}.$$

Proof. The first claim is tough to prove. The second claim is proved from the first in Exercise sheet 1. □

This result is often referred to as the PNT for arithmetic progressions. Notice the independence of a on the RHS! This is telling us that the primes tend to be spread evenly amongst the $\phi(m)$ classes of $(\mathbb{Z}/m\mathbb{Z})^\times$ (ignoring the finitely many primes dividing m of course).

Heuristically, given this result we expect that for each a coprime to m a randomly chosen prime has probability $\frac{1}{\phi(m)}$ of being a mod m.

Interesting fact - Prime races.

Consider the functions $\pi_{4,1}(x)$ and $\pi_{4,3}(x)$.

x	$\pi_{4,1}(x)$	$\pi_{4,3}(x)$	$\pi_{4,3}(x) - \pi_{4,1}(x)$
10	1	2	1
100	11	13	2
1000	80	87	7
10000	609	619	10
100000	4783	4808	25
1000000	39175	39322	147

We know that both functions diverge at the same rate by the above result. It should be expected that both functions are roughly equal up to some small random error.

However in general we tend to find that $\pi_{4,3}(x) \geq \pi_{4,1}(x)$. This observation is known as **Chebyshev bias**. In fact the first x where $\pi_{4,3}(x) < \pi_{4,1}(x)$ occurs when $x = 26861$ (overtaking by exactly 1!).

It is now known by a theorem of Littlewood that there are infinitely such x for which $\pi_{4,1}(x)$ begins to overtake $\pi_{4,3}(x)$ but these values are quite rare!

Similar behaviour can be observed for **any** modulus. In particular whenever a is a quadratic non-residue mod m and b is a quadratic residue mod m we generally find Chebyshev bias $\pi_{m,a}(x) \geq \pi_{m,b}(x)$ (with overtaking happening rarely but infinitely many times as in Littlewood's result).

2 Arithmetic functions and Dirichlet series

2.1 Arithmetic functions

Throughout number theory you will have met functions that encode number theoretic properties of a given integer.

For example:

- Number of divisors:
$$\sigma_0(n) = \sum_{d|n} 1.$$
This function can be used to detect primes (since $\sigma_0(n) = 2$ if and only if n is prime).
- Sum of divisors:
$$\sigma(n) = \sum_{d|n} d.$$
This function is used to measure perfect/deficient/abundant numbers.
- Euler totient function:
$$\phi(n) = \#\{a \,|\, 1 \leq a \leq n,\ \operatorname{hcf}(a, n) = 1\}.$$
This function measures the size of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ and appears in Euler's generalisation of Fermat's little theorem.
- Legendre symbol:
$$\left(\frac{n}{p}\right) \in \{0, \pm 1\}.$$
This function measures the property of being a quadratic residue mod p.

Definition 2.1. An **arithmetic function** is a function $f : \mathbb{N} \to \mathbb{C}$.

Other important examples include:

- The **Dirichlet identity function**:
$$I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$
- The **power function** for $\alpha \in \mathbb{Z}$:
$$N_\alpha(n) = n^\alpha.$$
- The **unit function**:
$$u(n) = N_0(n) = 1$$

- The **constant function**:

$$N(n) = N_1(n) = n.$$

- The **power divisor sum** for $\alpha \in \mathbb{N}$:

$$\sigma_\alpha(n) = \sum_{d|n} N_\alpha(d) = \sum_{d|n} d^\alpha.$$

(Note: σ_0 and $\sigma = \sigma_1$ agree with earlier).

- The **Möbius μ function**:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 p_2 ... p_k \text{ for distinct primes } p_1, p_2, ..., p_k, \\ 0 & \text{otherwise.} \end{cases}$$

- The **Von-Mangoldt function**:

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

Soon we will observe ways of studying arithmetic functions using analytical tools. For now we will study arithmetic functions in more detail.

2.1.1 Dirichlet convolution and Möbius inversion

Let's consider the operations we can do with arithmetic functions:

- We can add:

$$(f + g)(n) := f(n) + g(n).$$

- We can scale by a complex number $\alpha \in \mathbb{C}$:

$$(\alpha f)(n) := \alpha f(n).$$

Lemma 2.2. *The set of arithmetic functions forms a $\mathbb{C}$-vector space under the above operations. The zero element is the arithmetic function given by $\boldsymbol{0}(n) = 0$.*

Exercise - Prove this by axiom bashing. What is the dimension of this vector space? Can you find a basis?

It is our interest to attach a multiplication to arithmetic functions. The most natural and obvious way to define it would be:

$$(fg)(n) := f(n)g(n).$$

However, for the purposes of studying arithmetic functions this definition is not going to help us much.

Many identities between arithmetic functions appear in the form:

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

We need a product that captures this.

Definition 2.3. Given f, g arithmetic functions we define their **Dirichlet convolution** to be the arithmetic function:

$$(f \star g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Note that this is similar to the usual convolution of real functions:

$$(f \star g)(t) := \int_a^b f(u) g(t-u) du.$$

Example 2.4. Here are some easy examples of Dirichlet convolutions:

- $\sigma_0 = u \star u$,
- $\sigma = N \star u$,
- $\sigma_\alpha = N_\alpha \star u$,
- $f = f \star I$ for any f,
- $\mathbf{0} = \mathbf{0} \star f$ for any f.

Some less obvious ones are:

- $N = \phi \star u$,
- $I = \mu \star u$,
- $N = \sigma \star \mu$,
- $\sigma = \phi \star \sigma_0$,
- $\ln = \Lambda \star u$.

Some of these will be proved on Exercise sheet 2.

Returning to the algebraic structure of arithmetic functions, we now have something stronger.

Theorem 2.5. *Under the operations of addition, scalar multiplication and Dirichlet convolution the set of all arithmetic functions forms a commutative $\mathbb{C}$-algebra (i.e.* ***both*** *a $\mathbb{C}$-vector space and a commutative ring). The multiplicative identity is given by the function I, defined earlier.*

Exercise - Prove this by axiom bashing.

We will not really have cause to use the full algebra structure in this course but will concern ourselves with the ring structure.

A simple fact from MAS276 is that the **units** of a commutative ring form an abelian group under multiplication. So really our next port of call should be to try and find these units (these are the arithmetic functions we can "divide" by, undoing the Dirichlet convolution operation).

Definition 2.6. Let f be an arithmetic function. Then an arithmetic function g is a **Dirichlet inverse** of f if $f \star g = I$.

Since inverses in a group are unique we will call g **the** Dirichlet inverse of f and denote it by $g = f^{-1}$ (note that this is **not** the same as the usual inverse function).

Exercise - Does **0** have a Dirichlet inverse? Can you find an **algebraic** proof of this? (Think about the relationship between zero divisors and units).

Since not all arithmetic functions have a Dirichlet inverse we wish to find a condition on f that guarantees the existence of one.

Let us first suppose that f^{-1} exists. Then $(f \star f^{-1})(1) = I(1) = 1$. But $(f \star f^{-1})(1) = \sum_{d|1} f(d) f^{-1}\left(\frac{1}{d}\right) = f(1)f^{-1}(1)$.

It is now clear that we must have $f(1) \neq 0$ so that $f^{-1}(1) = \frac{1}{f(1)}$ is defined. What is perhaps less clear is that this is sufficient.

Lemma 2.7. *Let f be an arithmetic function. Then f^{-1} exists if and only if $f(1) \neq 0$.*

Proof. We have already seen that if f^{-1} exists then $f(1) \neq 0$.

We prove the converse by constructing f^{-1} given $f(1) \neq 0$. This will be easier than imagined, we will simply observe that we can **always** solve the equation $(f \star g) = I$ if $f(1) \neq 0$.

We have already seen that we are forced to define $g(1) = \frac{1}{f(1)}$ and this exists by our assumption that $f(1) \neq 0$.

Now for $n \geq 2$ if $(f \star g)(n) = 0$ then:

$$g(n)f(1) = -\sum_{d|n, d\neq 1} f(d) g\left(\frac{n}{d}\right).$$

giving:

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d\neq 1} f(d) g\left(\frac{n}{d}\right).$$

Inductively these values exist (to calculate the RHS you only need to know values of f^{-1} for **smaller** inputs). □

We now have the following theorem:

Theorem 2.8. *The set of arithmetic functions f with $f(1) \neq 0$ forms an abelian group under Dirichlet convolution.*

Proof. As mentioned earlier the set of such functions forms the unit group of the commutative ring of all arithmetic functions (under addition and Dirichlet convolution). Hence it must be an abelian group. □

The algebraic proof above is concise. In Exercise sheet 2 we will prove this result from scratch axiomatically.

Example 2.9. Let's see some examples of Dirichlet inverses.

- We saw earlier that $u \star \mu = I$ and so we have Dirichlet inverses $u^{-1} = \mu$ and $\mu^{-1} = u$.
- The Dirichlet inverse of N_α is $N_\alpha^{-1} = \mu N_\alpha$. To see this note that:

$$\begin{aligned}(\mu N_\alpha \star N_\alpha)(n) &= \sum_{d|n} (\mu N_\alpha)(d)\, N_\alpha\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) n^\alpha \\ &= n^\alpha (\mu \star u)(n) \\ &= n^\alpha I(n) \\ &= I(n).\end{aligned}$$

  In fact it is true in general that if f is completely multiplicative (defined soon) then $f^{-1} = \mu f$ (see Exercise sheet 2).

As mentioned earlier many arithmetic functions are defined via:

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

We now know we may interpret this as $f = g \star u$.

Naturally we wonder if from this we may recover the arithmetic function g as defined in terms of f. The Möbius inversion formula achieves this:

Theorem 2.10. *(Möbius Inversion) If f, g are arithmetic functions such that:*

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

then:

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Proof. We know that $f = g \star u$. We also know that the Dirichlet inverse of u is $u^{-1} = \mu$ and so

$$\mu \star f = f \star \mu = (g \star u) \star \mu = g \star (u \star \mu) = g \star I = g.$$

This is a concise version of the theorem. □

The Mobius inversion formula is extremely helpful in proving identities between arithmetic functions. Exercise sheet 2 contains many examples of this. Here is a simple example showing the power of the result.

Example 2.11. As mentioned earlier (and proved in Example sheet 2) we have the identity $N = \phi \star u$,

i.e. for $n \geq 1$ we have:

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

But using the Möbius inversion formula we now observe a formula for ϕ:

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

Exercise - Show (using the above) that the following well known formula holds:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Check the formula holds for n prime.

2.1.2 Muliplicativity

In MAS208/330 you observed that a few arithmetic functions have a particularly nice property. For example:

$$\phi(mn) = \phi(m)\phi(n) \qquad \text{if hcf}(m,n) = 1$$

$$\sigma(mn) = \sigma(m)\sigma(n) \qquad \text{if hcf}(m,n) = 1.$$

Definition 2.12. An arithmetic function f is **multiplicative** if it has the property that $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever $\text{hcf}(m,n) = 1$.

Further f is **completely multiplicative** if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for **all** m, n.

Exercise - Show that any arithmetic function satisfying $f(mn) = f(m)f(n)$ for all m, n is either the zero map or is completely multiplicative (so satisfies $f(1) = 1$ automatically).

Lemma 2.13. *Let f be an arithmetic function. Then:*

1. *f is multiplicative if and only if $f(1) = 1$ and*

$$f(p_1^{k_1} p_2^{k_2} ... p_m^{k_m}) = f(p_1^{k_1}) f(p_2^{k_2}) ... f(p_m^{k_m})$$

for all choices of primes $p_1, p_2, ..., p_m$ and $k_1, k_2, ..., k_m \in \mathbb{N}$.

2. *f is completely multiplicative if and only if f is multiplicative and*

$$f(p^k) = f(p)^k,$$

for all primes p and $k \in \mathbb{N}$.

Exercise - Prove this.

This lemma tells us that to test for multiplicativity/complete multiplicativity we need only test the property for prime powers/primes. In practice this is often much easier to do.

The lemma also tells us that in order to completely describe a multiplicative function we only need to know its values on prime powers. In order to describe a completely multiplicative function we actually only know its values on primes.

Clearly there are arithmetic functions that are multiplicative but **not** completely multiplicative. For example $\phi(4) = 2 \neq \phi(2)\phi(2)$ and $\sigma(4) = 7 \neq \sigma(2)\sigma(2)$.

Example 2.14. There are many examples of multiplicative and completely multiplicative functions.

- Completely multiplicative: $\left(\frac{n}{p}\right), I, N_\alpha, u$.
- Multiplicative but not completely multiplicative: ϕ, σ_α, μ.

Lemma 2.15. *Suppose f, g are arithmetic functions. If g and $h = f \star g$ are multiplicative then so is f.*

Proof. Suppose f is not multiplicative. Then there exists m, n such that m, n are coprime and $f(mn) \neq f(m)f(n)$. Choose m, n so that mn is the smallest value for which this happens.

Case 1 - If $mn = 1$ then we must have $m = n = 1$ and so $f(1) \neq f(1)f(1)$. But then $h(1) = f(1)g(1) = f(1) \neq 1$ so that h is not multiplicative. This is a contradiction.

Case 2 - If $mn > 1$ then by minimality of mn we see that $f(ab) = f(a)f(b)$ for all coprime $a \mid m, b \mid n$ with $ab < mn$.

But now:

$$\begin{aligned}
h(mn) &= \sum_{a,b} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) \\
&= \sum_{a,b} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) + f(mn) \\
&= \left(\sum_{a<m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b<n} f(b)g\left(\frac{n}{b}\right)\right) - (f(m)g(1))(f(n)g(1)) + f(mn) \\
&= h(m)h(n) - f(m)f(n) + f(mn).
\end{aligned}$$

Then $h(mn) \neq h(m)h(n)$, giving a contradiction. □

Lemma 2.16. *The Dirichlet convolution of two multiplicative functions is multiplicative. The Dirichlet inverse of a multiplicative function is also multiplicative.*

Thus the set of ***multiplicative*** *functions with $f(1) \neq 0$ forms a subgroup of the group in Theorem 2.8.*

Proof. Let f, g be multiplicative. If m, n are coprime then every divisor of mn can be factorised as ab where $a \mid m$ and $b \mid n$ (note that automatically a, b must be coprime).

Thus:

$$\begin{aligned}
(f \star g)(mn) &= \sum_{d \mid mn} f(d)g\left(\frac{mn}{d}\right) \\
&= \sum_{a\mid m, b\mid n} f(ab)g\left(\frac{mn}{ab}\right) \\
&= \sum_{a\mid m, b\mid n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\
&= \sum_{a\mid m} f(a)g\left(\frac{m}{a}\right)\sum_{b\mid n} f(b)g\left(\frac{n}{b}\right) \\
&= (f \star g)(m)(f \star g)(n).
\end{aligned}$$

Now that since f is multiplicative we have $f(1) = 1 \neq 0$ and so f definitely has a Dirichlet inverse.

By the above lemma f and $f^{-1} \star f = I$ are multiplicative, thus f^{-1} must be too. □

Exercise - Do the completely multiplicative functions with $f(1) \neq 0$ form a subgroup?

2.2 Dirichlet series

A common theme throughout the undergrad course is that one can study properties of (nice) real or complex functions by looking at specific infinite sums attached to them, e.g. Taylor/Maclaurin series, power series, Fourier series, Laurent series.

Such tools serve as a kind of "approximation" as well as a measure of limiting behaviour (amongst other things).

Naturally a question we should now ask is, "How might we study properties of arithmetic functions in a similar fashion?".

Unfortunately we do not have access to **any** of the tools mentioned above. A vague reason for this is that $\mathbb{R}$ is somehow big enough for analysis to make enough sense, whereas $\mathbb{N}$ really isn't (you can make this precise by thinking topologically).

However, in analogue to the above we can associate a new analytical device to each arithmetic function.

Definition 2.17. Let $f : \mathbb{N} \to \mathbb{C}$ be an arithmetic function. The **formal Dirichlet series** attached to f is:

$$D(s, f) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

Why the need for "formal"? Well at the moment we aren't thinking of $D(s, f)$ as a function but rather an abstract object that we want to manipulate. We aren't yet assigning an actual value to s but instead treating it as an abstract variable (in exactly the same way that you are happy to write down and manipulate polynomials without ever plugging in values).

Soon we **will** be interested in plugging in values for s and once we get to that stage we will have to consider convergence issues (the term **Dirichlet series** will be reserved for this). For now we will not worry.

Example 2.18. Perhaps the most famous Dirichlet series is the Riemann zeta function:

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

This was the first Dirichlet series to be studied, dating back to the work of Euler. We will devote the entire of Chapter 3 to studying interesting properties of this function.

There are a number of operations we can do with formal Dirichlet series. Firstly we define addition and scalar multiplication in the usual way:

$$D(s, f) + D(s, g) = D(s, f + g),$$

$$\alpha D(s,f) = D(s,\alpha f).$$

We may also multiply formal Dirichlet series but not in the way you would expect.

Lemma 2.19. *Let f, g be two arithmetic functions. Then:*

$$D(s,f)D(s,g) = D(s, f \star g).$$

Proof. By definition:

$$D(s,f)D(s,g) = \left(\frac{f(1)}{1^s} + \frac{f(2)}{2^s} + \frac{f(3)}{3^s} + ...\right)\left(\frac{g(1)}{1^s} + \frac{g(2)}{2^s} + \frac{g(3)}{3^s} + ...\right).$$

It is clear that once we formally multiply out the brackets we will only get terms of the form $\frac{f(a)g(b)}{(ab)^s}$. Thus the product is another formal Dirichlet series $D(s,h)$ for some arithmetic function h.

Let $n \in \mathbb{N}$. We wish to find an expression for $h(n)$ in terms of f and g. By what we have just said it is clear that the coefficient of $\frac{1}{n^s}$ in this product will be:

$$h(n) = \sum_{ab=n} f(a)g(b) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = (f \star g)(n).$$

Thus $h = f \star g$. □

Technically the above should be the **definition** of multiplication for formal Dirichlet series. However we already have an intuition for how we would like to "multiply out brackets" and under this intuition the above result is forced.

Notice now the importance of Dirichlet convolution! The above lemma can be viewed as a discrete analogue of:

$$\mathcal{F}(f)\mathcal{F}(g) = \mathcal{F}(f \star g)$$

where f, g are real functions, $\mathcal{F}$ is the Fourier transform and $(f \star g)(t) = \int_a^b f(u)g(t-u)\, \mathrm{d}u$ is the usual convolution.

Due to the algebraic structure of arithmetic functions observed in the last subsection we can see the following:

Theorem 2.20. *The set of formal Dirichlet series forms a commutative $\mathbb{C}$-algebra under the above operations. The units of this algebra consist of those $D(s,f)$ where $f(1) \neq 0$.*

Proof. It is clear that we have a vector space structure under the above addition and scalar multiplication (if it is not clear then do it!). The zero vector here is given by $D(s,\mathbf{0})$, where $\mathbf{0}(n) = 0$ for all n.

As for the ring structure, again most of the axioms are simple to check by using properties of arithmetic functions. Commutativity follows since $f \star g = g \star f$ for all f, g.

Notice that:

$$D(s,f)D(s,I) = D(s, f \star I) = D(s,f)$$

and so $D(s,I)$ behaves as a multiplicative identity.

The claim about units follows since if

$$D(s,f)D(s,g) = D(s,I)$$

then $D(s, f \star g) = D(s,I)$ and this clearly implies that $f \star g = I$. Thus f has a Dirichlet inverse, so that $f(1) \neq 0$.

Conversely if f has a Dirichlet inverse then $D(s,f)D(s,f^{-1}) = D(s, f \star f^{-1}) = D(s,I)$ so that $D(s,f)^{-1}$ exists (and is $D(s,f^{-1})$).

□

The most important part of the above is that we now know when we can **divide** formal Dirichlet series and get other such series.

It is common to use what we know about Dirichlet convolution and Möbius Inversion to form identities between formal Dirichlet series. Such identities come in handy when considering analytic properties (for example convergence, poles, zeros etc).

For example we observed earlier that $u \star \mu = I$ and so $\mu = u^{-1}$ telling us that:

$$D(s,\mu) = \frac{1}{\zeta(s)},$$

i.e.

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

See Exercise sheet 2 for more examples.

2.2.1 Euler products

Some formal Dirichlet series have a surprising link with prime numbers. For example, consider the Riemann zeta function:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + ...$$

Notice that

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + ...$$

so that

$$\left(1-\frac{1}{2^s}\right)\zeta(s)=1+\frac{1}{3^s}+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{9^s}+...$$

We have managed to eliminate all denominators that are even.

In a similar fashion we may eliminate multiples of 3 from the denominators:

$$\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\zeta(s)=1+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{11^s}+...$$

Continuing, one can now observe that since every $n\geq 2$ has a unique prime factorisation, the corresponding $\frac{1}{n^s}$ term in $\zeta(s)$ will be eliminated exactly **once** during this process. Thus we see that:

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

Of course this is a formal manipulation, convergence will come later (there are infinitely many primes so this is an infinite product!).

Now continuing to manipulate formally we see that:

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

The above identity was discovered by Euler and so is referred to as the **Euler product expansion** of $\zeta(s)$. It gives remarkable links between properties of $\zeta(s)$ and properties of prime numbers. We will see details of this later.

For now we ask whether other Dirichlet series can have similar expansions. It will turn out that in some sense we were lucky with $\zeta(s)$ to get such a nice identity.

Definition 2.21. Given a formal Dirichlet series $D(s,f)$, an **Euler product expansion** for $D(s,f)$ is an identity of the form:

$$D(s,f)=\prod_{p \text{ prime}} D_p(s,f_p),$$

where the f_p form a sequence of arithmetic functions and each $D_p(s,f_p)$ is a formal Dirichlet series of the form:

$$D_p(s,f_p)=\sum_{k=0}^{\infty}\frac{f_p(p^k)}{p^{ks}}.$$

This is quite a hefty definition but all we are trying to capture is that $D(f,s)$ is expressible as **some** infinite product of formal Dirichlet series, indexed by primes, and such that each $D_p(s,f_p)$ only has denominators that are powers of p.

In some sense the existence of an Euler product for $D(s,f)$ tells you exactly how to work out $f(n)$ given knowledge of $f(p^k)$ for all primes p and integers k. This explains the main importance of knowing an Euler product. In practice f could be something non-trivial that you have no general formula for.

Exercise - What would the $D_p(s,f_p)$ be for $D(s,f)=\zeta(s)$? (Hint: the answer is **not** $\left(1-\frac{1}{p^s}\right)$...observe the inverses in the expansion).

Based on the answer to the above exercise we are now ready for the general theorem.

Theorem 2.22. *Let f be a* ***multiplicative*** *arithmetic function. Then $D(s,f)$ admits an Euler product expansion with $f_p=f$ for all p. In other words:*

$$D(s,f)=\prod_{p\ prime}\left(\sum_{k=0}^{\infty}\frac{f(p^k)}{p^{ks}}\right)=\prod_{p\ prime}\left(1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\frac{f(p^3)}{p^{3s}}+...\right)$$

Conversely the existence of such an expansion implies that f is multiplicative.

Proof. Suppose f is multiplicative. We aim to show that the Euler product expansion holds.

Consider formally multiplying out the product on the RHS. The product of all the 1 terms should give 1. Otherwise, using the multiplicative property of f we see that we get terms of the form:

$$\frac{f(p_1^{k_1})f(p_2^{k_2})...f(p_m^{k_m})}{p_1^{k_1s}p_2^{k_2s}...p_m^{k_ms}}=\frac{f(p_1^{k_1}p_2^{k_2}...p_m^{k_m})}{(p_1^{k_1}p_2^{k_2}...p_m^{k_m})^s}.$$

Now by unique factorisation we see that for $n\geq 2$, the term $\frac{f(n)}{n^s}$ on the LHS is represented **exactly once** by a term of the above form.

Thus the two sides represent the same sum.

Conversely given the Euler product expansion holds we see that $f(1)=1$ immediately. For $n\geq 2$ with prime factorisation $n=p_1^{k_1}p_2^{k_2}...p_m^{k_m}$ we observe by comparison of both sides that we must have

$$f(n)=f(p_1^{k_1})f(p_2^{k_2})...f(p_m^{k_m})$$

thus f is multiplicative. □

What is even better is that for completely multiplicative functions we get a much nicer identity.

Corollary 2.23. *Let f be* ***completely multiplicative****. Then $D(f,s)$ admits an Euler product expansion of the form:*

$$D(s,f) = \prod_{p\ prime} \left(1 - \frac{f(p)}{p^s}\right)^{-1}.$$

Conversely the existence of such an expansion implies that f is completely multiplicative.

Proof. Suppose f is completely multiplicative. Then f is multiplicative and so has an Euler product expansion of the form given in Theorem 2.22.

However since f is completely multiplicative $f(1) = 1$ and $f(p^k) = f(p)^k$ for all primes p and $k \geq 1$. Thus:

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

by the geometric sum formula.

Conversely, given such an expansion we see that (by reversing the geometric sum formula):

$$D(s,f) = \prod_{p \text{ prime}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p)^2}{p^{2s}} + ...\right)$$

Given $n \in \mathbb{N}$ we know by definition that the coefficient of $\frac{1}{n^s}$ in $D(s,f)$ is $f(n)$. Clearly $f(1) = 1$ is observed so we may assume that $n \geq 2$.

By unique factorisation $f(n) = f(p_1^{k_1} p_2^{k_2} ... p_m^{k_m})$. However, given the above expansion the coefficient of $\frac{1}{n^s}$ on the RHS is $f(p_1)^{k_1} f(p_2)^{k_2} ... f(p_m)^{k_m}$.

Thus f is completely multiplicative. □

2.2.2 Convergence of Dirichlet series

We now begin to observe the analytic properties of Dirichlet series.

In previous modules you have tackled infinite sums and their convergence. Recall the following definition:

Definition 2.24. Let $a_n \in \mathbb{C}$ be a sequence of complex numbers. Then we say that

$$S = \sum_{n=1}^{\infty} a_n = L$$

if as $N \to \infty$ the sequence of partial sums

$$S_N = \sum_{n=1}^{N} a_n \longrightarrow L.$$

Further we say that S **converges absolutely** if the following sum exists:

$$S' = \sum_{n=1}^{\infty} \mid a_n \mid .$$

It is known that absolute convergence implies convergence (you might have seen this proved before but it isn't too bad to do yourself).

A detail which is perhaps not focused on much in previous courses is the importance of absolute convergence.

In defining the value of an infinite sum we rely on the partial sums S_N. However calculating these values depends on the ordering of the terms a_n. Could it be that different orderings of the a_n's provide us with different limits for the S_N sequences, i.e. different values for the infinite sum?

Riemann considered this question in depth and found some incredible results. He exhibited infinite sums that converge but give **different values** upon changing the order of the terms. This is paradoxical, we definitely do not expect this behaviour based on how finite sums work (where **any** order of terms gives the same sum).

We briefly explain the main result that Riemann was able to prove.

Definition 2.25. Let a_n be a sequence of complex numbers. Then S (as defined above) **converges conditionally** if S converges but not absolutely.

The following remarkable result is mind blowing.

Theorem 2.26. *(Riemann rearrangement theorem) Given any conditionally convergent sum we may find a rearrangement of its terms to arrange for* ***any*** *of the following to occur:*

- *Convergence to* ***any*** *fixed finite limit M,*
- *Divergence to $\pm\infty$,*
- *Failure to diverge to* ***any*** *limit, finite or infinite.*

However absolutely convergent sums agree on all rearrangements of terms.

See Example sheet 2 for an example of this theorem.

The moral of the story is the following: some sums are just so inherently bad that you can make them achieve any kind of behaviour. However absolutely convergent sums behave the nicest.

Think about how many times in the past you blindly rearranged the terms of an infinite sum. You were assuming absolute convergence!

Given the above we should be careful when considering the convergence of Dirichlet series (the operations we defined on formal Dirichlet series involve reordering terms).

First let's consider what kind of region of convergence we get.

Recall that for power series $S(z) = \sum_{n=0}^{\infty} a_n z^n$ the region of convergence is a disc centered on the origin with a so called **radius of convergence** $R \in \mathbb{R}_{\geq 0} \cup \{\infty\}$ (so that $S(z)$ converges for $|z| < R$ and diverges for $|z| > R$).

We write $R = \infty$ when $S(z)$ always converges and $R = 0$ when $S(z)$ never converges.

Also for power series we have equivalence of convergence and absolute convergence, both will happen for the same values of z.

For Dirichlet series $D(s, f)$ we observe similarities but the situation is in general different. Recall from MAS207 that an infinite sum of **positive** terms converges if and only if the sequence of partial sums is bounded.

Lemma 2.27. *If $D(s_0, f)$ converges for some $s_0 \in \mathbb{C}$ then $D(s, f)$ converges for Re$(s) >$ Re(s_0).*

If $D(s_0, f)$ converges absolutely for some $s_0 \in \mathbb{C}$ then $D(s, f)$ converges absolutely for Re$(s) >$ Re(s_0).

Proof. Let $\text{Re}(s_0) = \sigma_0$. We only prove the second claim. The first is surprisingly difficult and is omitted.

Suppose $s \in \mathbb{C}$ satisfies $\text{Re}(s) > \sigma_0$. Then for all n:

$$\left|\frac{f(n)}{n^s}\right| = \frac{|f(n)|}{n^{\text{Re}(s)}} \leq \frac{|f(n)|}{n^{\sigma_0}} = \left|\frac{f(n)}{n^{s_0}}\right|.$$

By comparison we observe for $N \geq 1$:

$$0 \leq \sum_{n=1}^{N} \left|\frac{f(n)}{n^s}\right| \leq \sum_{n=1}^{N} \left|\frac{f(n)}{n^{s_0}}\right|$$

Now since $\sum_{n=1}^{\infty} \left|\frac{f(n)}{n^{s_0}}\right|$ converges (by assumption) and consists of positive terms its partial sums are bounded. Thus $\sum_{n=1}^{\infty} \left|\frac{f(n)}{n^{s}}\right|$ converges since its partial sums will also be bounded (by the above inequality) and again consists of positive terms. □

Theorem 2.28. *There exists $\alpha \in \mathbb{R} \cup \{\pm\infty\}$ such that $D(s, f)$ converges for Re$(s) > \alpha$ and diverges if Re$(s) < \alpha$.*

Similarly there exists $\beta \in \mathbb{R} \cup \{\pm\infty\}$ such that $D(s, f)$ converges absolutely for Re$(s) > \beta$.

Proof. Both claims are proved using the same argument so I will only show the argument for α.

It is clear that convergence everywhere is captured by $\alpha = -\infty$ and divergence everywhere is given by $\alpha = \infty$.

Now suppose $D(s, f)$ diverges at $s_1 \in \mathbb{C}$ **and** converges for at least one $s \in \mathbb{C}$. Then consider the set $S = \{\mathrm{Re}(s) \,|\, D(s, f) \text{ converges}\} \subseteq \mathbb{R}$.

We know S is non-empty and is bounded below (by $\mathrm{Re}(s_1)$, since $\mathrm{Re}(s_1) \notin S$ and by the above lemma neither is any $\sigma < \mathrm{Re}(s_1)$). Thus S has an infimum α. It is then clear that $D(s, f)$ converges for $\mathrm{Re}(s) > \alpha$ and diverges for $\mathrm{Re}(s) < \alpha$. □

Clearly $\beta \geq \alpha$ since absolute convergence implies convergence (in fact it is not too difficult to show that $\beta - \alpha \leq 1$ so that they may not be too far apart).

The above result tells us that once you know convergence at some $s \in \mathbb{C}$ the sum will also converge "to the right" of s (as opposed to "nearer the origin" for power series).

Definition 2.29. We call α the **abscissa of convergence** of $D(s, f)$ and refer to the region $\mathrm{Re}(s) > \alpha$ as the **half plane of convergence**.

We call β the **abscissa of absolute convergence** of $D(s, f)$ and refer to the region $\mathrm{Re}(s) > \beta$ as the **half plane of absolute convergence**.

In general it is not straight forward to find the abscissae of convergence but there is a nice criterion for telling when it is 0 (a result that we will need later).

Theorem 2.30. *Let $D(s, f)$ be a Dirichlet series. Suppose that the sequence $|f(1)|, |f(1)+f(2)|, |f(1)+f(2)+f(3)|, \ldots$ is bounded. Then $D(s, f)$ has abscissa of convergence 0.*

Proof. Let $S(m) = \sum_{n=1}^{m} f(n)$. By assumption $0 \leq |S(m)| \leq K$ for some $K > 0$.

We show that for $\mathrm{Re}(s) > 0$ the partial sums:

$$F_N(s) = \sum_{n=1}^{N} \frac{f(n)}{n^s}$$

form a **Cauchy sequence** and then by completeness of $\mathbb{C}$ the partial sums must converge, hence the infinite sum converges.

Take $m > m'$. Then:

$$\begin{aligned}
|F_m(s) - F_{m'}(s)| &= \left| \sum_{n=m'+1}^{m} \frac{f(n)}{n^s} \right| \\
&= \left| \sum_{n=m'+1}^{m} \frac{S(n) - S(n-1)}{n^s} \right| \\
&= \left| \frac{S(m)}{m^s} + \sum_{n=m'+1}^{m-1} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right| \\
&\leq \frac{|S(m)|}{m^{\mathrm{Re}(s)}} + \sum_{n=m'+1}^{m-1} |S(n)| \left(\frac{1}{n^{\mathrm{Re}(s)}} - \frac{1}{(n+1)^{\mathrm{Re}(s)}} \right) \\
&= K \left(\frac{1}{m^{\mathrm{Re}(s)}} + \sum_{n=m'+1}^{m-1} \left(\frac{1}{n^{\mathrm{Re}(s)}} - \frac{1}{(n+1)^{\mathrm{Re}(s)}} \right) \right) \\
&= \frac{K}{(m+1)^{\mathrm{Re}(s)}}
\end{aligned}$$

Let $\epsilon > 0$ and suppose $\mathrm{Re}(s) > 0$. Then for $m > m' > \left(\frac{K}{\epsilon}\right)^{\frac{1}{\mathrm{Re}(s)}}$ we have:

$$|F_m(s) - F_{m'}(s)| \leq \frac{K}{(m+1)^{\mathrm{Re}(s)}} < \frac{K}{\left(\left(\frac{K}{\epsilon}\right)^{\frac{1}{\mathrm{Re}(s)}}\right)^{\mathrm{Re}(s)}} = \epsilon.$$

Thus the sequence of partial sums is a Cauchy sequence, hence the infinite sum is convergent for $\mathrm{Re}(s) > 0$. □

We now consider not only the convergence of Dirichlet series but the stronger property of being analytic.

Let $U \subseteq \mathbb{C}$ be open. Recall that a complex function $f : U \to \mathbb{C}$ is **complex differentiable** at $z_0 \in U$ if the limit:

$$\lim_{z \to z_0} \frac{f(z_0 + z) - f(z_0)}{z}$$

exists.

Then f is **analytic** if for each $z_0 \in U$ there exists a **neighbourhood** U' of z_0 (i.e. an open set $U' \subseteq U$ containing z_0) such that f is differentiable at each point of U'.

Analytic functions are the nicest of all complex functions. Not only are they differentiable at each point, but **around** each point too. Analytic functions have power series expansions around each point and so generally we can study the behaviour of such functions easily. In fact such functions are infinitely differentiable at each point in the domain (as proved in MAS332).

Since we are going to want to perform lots of different operations with Dirichlet series we ought to check that they are analytic in their domain.

Theorem 2.31. *A Dirichlet series is analytic on its half plane of convergence.*

Theorem 2.32. *Suppose f is multiplicative and that $D(s, f)$ converges for $Re(s) > a$. Then the Euler product expansion of $D(s, f)$ converges and is analytic for $Re(s) > a$.*

We will not prove these two theorems. In fact the second of these theorems is proved in the same way that we proved existence of an Euler product, just by considering the expansion of **partial products** and observing their convergence.

3 The Riemann zeta function

As observed in the previous section the simplest non-trivial Dirichlet series is the Riemann zeta function:

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

In this section we study this function in more detail.

First we should investigate the convergence of this infinite sum.

Lemma 3.1. *$\zeta(s)$ converges and is analytic for Re$(s) > 1$ and diverges for Re$(s) < 1$, i.e. the abscissa of convergence/absolute convergence is* 1.

Proof. By Theorem 2.28 it is enough to study the convergence/divergence of $\zeta(s)$ for **real** values of s.

Firstly note that:

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

This is the Harmonic series and is well known to diverge. As a reminder here is the classical proof.

Suppose the Harmonic series converges. Then by comparison:

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{1}{n} &= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + ... \\ &> 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + ... \\ &= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + ...\end{aligned}$$

which clearly diverges, giving a contradiction.

Now it remains to prove that $\zeta(\sigma)$ converges for $\sigma > 1$ (we do not need to worry about absolute convergence since the terms in the sum are real and positive anyway).

We group the terms differently:

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{1}{n^\sigma} &= 1+\left(\frac{1}{2^\sigma}+\frac{1}{3^\sigma}\right)+\left(\frac{1}{4^\sigma}+\frac{1}{5^\sigma}+\frac{1}{6^\sigma}+\frac{1}{7^\sigma}\right)+...\\ &< 1+\left(\frac{1}{2^\sigma}+\frac{1}{2^\sigma}\right)+\left(\frac{1}{4^\sigma}+\frac{1}{4^\sigma}+\frac{1}{4^\sigma}+\frac{1}{4^\sigma}\right)+...\\ &= 1+\frac{1}{2^{\sigma-1}}+\frac{1}{4^{\sigma-1}}+\frac{1}{8^{\sigma-1}}...\\ &= \frac{1}{1-2^{-(\sigma-1)}}\\ &= \frac{2^{\sigma-1}}{2^{\sigma-1}-1}\end{aligned}$$

Finishing the proof. (Note that the use of the geometric sum formula was valid since $\frac{1}{2^{\sigma-1}}<1$ if $\sigma>1$.) □

In Exercise sheet 3 we will see that:

$$\frac{1}{\sigma-1}<\zeta(\sigma)<\frac{1}{\sigma-1}+1$$

giving the rate that $\zeta(\sigma)\to\infty$ as $\sigma\to 1$.

Recall that $\zeta(s)$ has an Euler product of the form:

$$\zeta(s)=\prod_p\frac{1}{1-p^{-s}},$$

valid also for $\mathrm{Re}(s)>1$. This will prove useful in many ways. Here are some quick properties of the zeta function, making use of the Euler product.

Lemma 3.2. *As a real function on* $(1,\infty)$, $\zeta(\sigma)$ *is strictly decreasing towards* 1 *as* $\sigma\to\infty$.

Proof. The fact that $\zeta(\sigma_1)>\zeta(\sigma_2)$ for $\sigma_1>\sigma_2>1$ is trivial to see by a comparison of terms.

To see that $\zeta(\sigma)\to 1$ as $\sigma\to\infty$ use the Euler product. Since $\left(1-\frac{1}{p^\sigma}\right)^{-1}\to 1$ as $\sigma\to\infty$ we see that:

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

□

Lemma 3.3. $\zeta(s)\neq 0$ *for Re*$(s)>1$.

Proof. Let $\mathrm{Re}(s) = \sigma > 1$. Then consider an arbitrary factor in the Euler product:

$$\begin{aligned}\left|\left(1 - \frac{1}{p^s}\right)^{-1}\right| &= \left|1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + ...\right| \\ &\geq \left|1 - \frac{1}{p^\sigma} - \frac{1}{p^{2\sigma}} - \frac{1}{p^{3\sigma}} - ...\right|\end{aligned}$$

But

$$\begin{aligned}1 - \frac{1}{p^\sigma} - \frac{1}{p^{2\sigma}} - \frac{1}{p^{3\sigma}} - ... &= 1 - \frac{1}{p^\sigma - 1} \\ &\geq 1 - \frac{1}{2^\sigma - 1} > 0\end{aligned}$$

Then:

$$|\zeta(s)| = \left|\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}\right| = \prod_p \left|\left(1 - \frac{1}{p^s}\right)^{-1}\right| \geq \prod_p \left(1 - \frac{1}{2^\sigma - 1}\right) \neq 0.$$

Thus $|\zeta(s)| \neq 0$ for $\mathrm{Re}(s) > 1$, hence $\zeta(s) \neq 0$ in this range.

□

The existence of the Euler product presents a 4th proof of the infinitude of primes.

Proof 4

Suppose there are finitely many primes. Then the Euler product would converge when $s = 1$ (since it is a finite product). However we know that $\zeta(s)$ diverges as $s \to 1$. □

This proof highlights a useful strategy in analytic number theory. Here we have a complex-valued function that seems to have been plucked out of thin air. However encoded in the analytic properties of this function are many things of number theoretic interest.

For example the Euler product reflects unique factorisation in $\mathbb{Z}$, the divergence at $s = 1$ proves there are infinitely many primes. The prime number theorem may even be proved using the fact that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) \geq 1$.

Later we will briefly see the celebrated Riemann Hypothesis, one of the most important unsolved problems in analytic number theory (so important that it is worth **a million dollars**). Again this will link analytic behaviour of $\zeta(s)$ to the distribution of prime numbers.

We can actually salvage another proof of the fact that $\sum_{i=1}^{\infty} \frac{1}{p_i}$ diverges by using the Euler product.

Alternate proof

Since $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$ we may take logs in the Euler expansion:

$$\ln(\zeta(s)) = -\sum_p \ln(1 - p^{-s}).$$

Recall the Taylor series expansion

$$\ln(1-z) = -\sum_{n=1}^{\infty} \frac{z^n}{n}$$

which converges (absolutely) for $|z| < 1$.

Since $|p^{-s}| = p^{\mathrm{Re}(s)} < \frac{1}{p} < 1$ whenever $\mathrm{Re}(s) > 1$ we may use the Taylor expansion and find that:

$$\begin{aligned} \ln(\zeta(s)) = \sum_p \sum_{n=1}^{\infty} \frac{p^{-ns}}{n} &= \sum_p \frac{1}{p^s} + \sum_p \sum_{n \geq 2} \frac{1}{np^{ns}} \\ &= \sum_p \frac{1}{p^s} + A(s). \end{aligned}$$

Claim: $A(s)$ is bounded in absolute value in a small enough neighbourhood of $s = 1$, hence converges to a finite limit as $s \to 1$.

To see this note that if $\mathrm{Re}(s) = \sigma$ then:

$$\left| \sum_p \sum_{n \geq 2} \frac{1}{np^{ns}} \right| \leq \sum_p \sum_{n \geq 2} \left| \frac{1}{np^{ns}} \right| = \sum_p \sum_{n \geq 2} \frac{1}{np^{n\sigma}}$$

and via a string of inequalities:

$$\begin{aligned} \sum_p \sum_{n \geq 2} \frac{1}{np^{n\sigma}} &< \frac{1}{2} \sum_p \sum_{n \geq 2} \frac{1}{p^{n\sigma}} \\ &= \frac{1}{2} \sum_p \frac{p^{-2\sigma}}{1 - p^{-\sigma}} \\ &< \frac{1}{2(1 - \frac{1}{2})} \sum_p p^{-2\sigma} \\ &= \sum_p p^{-2\sigma}, \end{aligned}$$

where the middle equality uses the geometric sum formula (which we can guarantee to converge if we take $\sigma > 0$, so that $0 < p^{-\sigma} < 1$).

Then the claim follows since

$$\sum_p p^{-2\sigma} < \sum_{n=1}^{\infty} n^{-2\sigma} = \zeta(2\sigma),$$

and this converges for any $\sigma > \frac{1}{2}$ by the above. Thus choosing some σ_0 such that $\frac{1}{2} < \sigma_0 < 1$ we see that for $\text{Re}(s) > \sigma_0$:

$$|A(s)| < \zeta(2\ \text{Re}(s)) < \zeta(2\sigma_0).$$

Hence we have the required boundedness in a neighbourhood of $s = 1$ □

Returning to our main proof we are now done since as $s \to 1$ we know that $\ln(\zeta(s)) \to \infty$ (since $\zeta(\sigma) \to \infty$ as $\sigma \to 1^+$), whereas by the above this limit is equal to:

$$\sum_p \frac{1}{p} + C$$

for some constant C with $|C| < \zeta(2)$. Thus it must be that $\sum_p \frac{1}{p}$ diverges. □

Even though the above proof is much more disturbing than our original one it will come in handy. When proving Dirichlet's theorem in Chapter 4 we will essentially use the same strategy but with different Dirichlet series in place of $\zeta(s)$.

Hopefully after reading the above you will understand why existence of an Euler product is extremely useful!

3.1 Special values of ζ

Hidden inside ζ are many beautiful identities, for example:

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

It is tough **not** to find such results intriguing and mysterious. On the LHS we have a number theortic sum whereas on the RHS we have something geometrical/transcendental, relating to areas of circles!

Originally Euler is credited with discovery and "proof" of this result (known as the Basel problem).

Euler's "proof"

Consider formally the Taylor expansion of $f(z) = \frac{\sin(z)}{z}$ around $z = 0$:

$$\frac{\sin(x)}{z} = 1 - \frac{z^2}{6} + \frac{z^4}{120} - ...$$

Euler's big assumption is that we may treat such expansions like polynomials so that once we know the zeros of $f(z)$ we may factorise into an infinite product.

Now $f(z) = 0$ if and only if $z = n\pi$ for $n = \pm 1, \pm 2, ...$

Under Euler's assumption (which in fact works but needs rigorous proof) we see that:

$$\begin{aligned} f(z) &= \left(1 - \frac{z}{\pi}\right)\left(1 + \frac{z}{\pi}\right)\left(1 - \frac{z}{2\pi}\right)\left(1 + \frac{z}{2\pi}\right)\left(1 - \frac{z}{3\pi}\right)\left(1 + \frac{z}{3\pi}\right)... \\ &= \left(1 - \frac{z^2}{\pi^2}\right)\left(1 - \frac{z^2}{4\pi^2}\right)\left(1 - \frac{z^2}{9\pi^2}\right)... \\ &= 1 - \frac{1}{\pi^2}\left(\sum_{n=1}^{\infty}\frac{1}{n^2}\right)z^2 + ... \end{aligned}$$

Thus by uniqueness of Taylor expansions we can compare the z^2 cofficients and get:

$$-\frac{1}{\pi^2}\left(\sum_{n=1}^{\infty}\frac{1}{n^2}\right) = -\frac{1}{6}$$

so that:

$$\left(\sum_{n=1}^{\infty}\frac{1}{n^2}\right) = \frac{\pi^2}{6}.$$

□

Euler used similar arguments to find more values of ζ, such as:

$$\begin{aligned} \zeta(4) &= \frac{\pi^4}{90} \\ \zeta(6) &= \frac{\pi^6}{945}. \end{aligned}$$

We will consider the question of finding a general formula for $\zeta(2k)$ for any integer $k \geq 1$ and will observe that $\zeta(2k) = \alpha_{2k}\pi^{2k}$ for some $\alpha_{2k} \in \mathbb{Q}$. In fact we will go further and give formulae for α_{2k} in terms of so called **Bernoulli numbers**.

The interest in finding ζ values goes further than just finding elegant formulae. There are many applications of zeta values, a very small selection of uses are listed below.

Interesting fact - ζ and probability.

What is the probability of picking two coprime integers at random?

Here is a heuristic argument.

Suppose a, b are the two integers. The probability of **both** a and b sharing a prime factor p is $\frac{1}{p^2}$ so the probability that they **don't** share the prime factor p is $1 - \frac{1}{p^2}$.

Thus, the probability that a, b share **no** prime factor should be:

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

(Implicitly assuming independence of events)

Exercise - Simulate this yourself and check it works.

In fact in general, the probability of choosing $n \geq 2$ coprime integers at random is given by $\frac{1}{\zeta(n)}$.

Since $\zeta(n)$ decreases strictly towards 1 as $n \to \infty$, this means you are **more likely** to choose a big lists of coprime integers!

(Which makes sense, if I asked you to choose $5,000$ numbers at random would you expect it more likely that they **all** share a common factor than if you just picked two numbers?)

Interesting fact - ζ and modular forms.

For z in the complex upper half plane define $q = e^{2\pi i z}$.

Consider the **discriminant** function:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

This looks like a weird function but is related to discriminants of elliptic curves. It was a function of particular interest to Ramanujan.

Now expand $\Delta(z)$ as a power series:

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n$$

Ramanujan paid particular interest to the arithmetic function τ. He observed many interesting things about it such as multiplicativity.

In particular he observed the mysterious congruence $\tau(n) \equiv \sigma_{11}(n) \bmod 691$.

What is the significance of the 691? It comes from the Riemann zeta function!

Consider the **Eisenstein series** of weight $2k \geq 4$:

$$G_k(z) = \sum_{(m,n)\in\mathbb{Z}^2 (m,n)\neq(0,0)} \frac{1}{(mz+n)^{2k}}.$$

These series are absolutely convergent for the values of k given.

Now since $G_{2k}(z+1) = G_{2k}(z)$ we see that G_{2k} is periodic and so we have a complex Fourier series. It turns out to be:

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n.$$

Notice the appearance of ζ and σ_{2k-1}.

By the formula we will generate later we will see that $\zeta(12) = \frac{691\pi^{12}}{638512875}$, and so the congruence can be explained by "reducing mod 691" and getting the same Fourier series (although some of this is not obvious).

The functions we considered above are examples of **modular forms** and it is common to find such arithmetic information in the Fourier coefficients of such forms. This is just the beginning!

For example it is possible to use modular forms to prove extremely non-obvious identities such as:

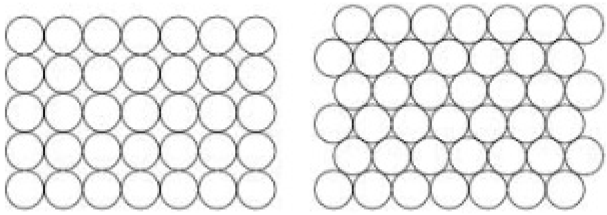
$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

Exercise - Test this identity and check that it works!

Interesting fact - ζ and sphere packing.

A natural question arising in geometry asks for the "best" way of packing equal sized spheres into n-dimensional space $\mathbb{R}^n$. This is a tough question so we settle for looking at regular packings (where the spheres are packed symmetrically i.e. in a "lattice").

For example when $n = 2$ there are at least two different ways to pack spheres regularly, "square packing" and "hexagonal packing".



In some sense the hexagonal packing is "better" than the square one but in what way?

We can assign a number to each packing called its **density**. Intuitively this is the proportion of volume covered by spheres (of course this isn't a rigorous definition since volumes are infinite here!).

The square packing turns out to have density $\frac{\pi}{4}$ whereas the hexagonal packing has density $\frac{\pi}{2\sqrt{3}}$. Notice that the hexagonal packing has the higher density so is classed as a better packing.

In fact it is possible to prove that the hexagonal packing is the best packing, i.e. has the highest density. The same problem has been solved for dimensions up to 8 (and other special cases).

However in general we happen to know a lower bound for the best regular packing in $\mathbb{R}^n$.

Theorem 3.4. *(Minkowski-Hlawka) Any regular packing in $\mathbb{R}^n$ of highest density δ_n satisfies:*

$$\delta_n \geq \frac{\zeta(n)}{2^{n-1}}.$$

Thus, for example the best packing in 2-dimensions must have density satisfying $\delta_2 \geq \frac{\zeta(2)}{2} = \frac{\pi^2}{12}$. Notice that this eliminates the square packing and supports the fact that hexagonal is the best (although it doesn't prove this).

Given a formula for $\zeta(n)$ we could effortlessly find these lower bounds for higher dimensions (without having to find the zeta values numerically).

3.1.1 Bernoulli numbers/polynomials

We begin with a strange definition.

Definition 3.5. The **Bernoulli numbers** are the numbers B_k defined by the following generating series:

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Advice: Do not be phased by this definition! All it is saying is that the Bernoulli numbers are (essentially) the power series coefficients of the function $f(t) = \frac{t}{e^t-1}$.

It is perhaps uncommon for you to see such a definition in the undergrad course. Often the use of a generating series to encode a sequence of numbers can tell you about underlying properties of the numbers that are otherwise hidden.

We will **not** find a closed formula for B_k but we will be able to manage fine without one!

Let's try and find a few Bernoulli numbers.

Explicitly (using the geometric sum formula):

$$\begin{aligned}\frac{t}{e^t-1} &= \frac{t}{t+\frac{t^2}{2!}+\frac{t^3}{3!}+...}\\ &= \frac{1}{1+\frac{t}{2!}+\frac{t^2}{3!}+...}\\ &= 1-\left(\frac{t}{2!}+\frac{t^2}{3!}+...\right)+\left(\frac{t}{2!}+\frac{t^2}{3!}+...\right)^2-...\\ &= 1-\frac{1}{2}t+\frac{1}{6}\frac{t^2}{2!}-\frac{1}{30}\frac{t^4}{4!}+...\end{aligned}$$

Thus we see that $B_0=1, B_1=-\frac{1}{2}, B_2=\frac{1}{6}, B_3=0, B_4=-\frac{1}{30}...$

In Exercise sheet 3 we will find simple recursions that generate the Bernoulli numbers. For now we consider certain facts about them.

From the above expansion we observe the following:

Lemma 3.6. *$B_k \in \mathbb{Q}$ for all $k \geq 0$.*

Proposition 3.7. *If $k \geq 3$ is odd then $B_k = 0$.*

Proof. It suffices to show that the function $\frac{t}{e^t-1}+\frac{t}{2}$ is even, so that the Taylor expansion contains only even powers of t.

But this is simple since:

$$\frac{t}{e^t-1}+\frac{t}{2}=\frac{2t+t(e^t-1)}{2(e^t-1)}=\frac{t}{2}\left(\frac{e^t+1}{e^t-1}\right)$$

and it is clear that this is invariant under the change of variables $t \mapsto -t$. □

Interesting fact - Sums of powers

The Bernoulli numbers appear in many guises throughout number theory. One amazing use of them is the following.

Recall the following formula:

$$\sum_{m=1}^{n} m = \frac{n(n+1)}{2}.$$

There are many ways of proving this, for example using the fact $1, 2, 3, 4..., m$ is an arithmetic progression of common difference 1 or by using induction.

There are also similar formulae for sums of squares and cubes:

$$\sum_{m=1}^{n} m^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{m=1}^{n} m^3 = \frac{n^2(n+1)^2}{4} = \left(\frac{n(n+1)}{2}\right)^2.$$

These may be familliar to you. Again there are ways to prove them (induction etc).

It is natural to ask for a general formula for:

$$S_k(n) = \sum_{m=1}^{n} m^k,$$

where $k \geq 1$ is an integer. One can easily provide recursions that produce a formula based on formulae for previous powers but the Bernoulli numbers provide a closed formula:

$$S_k(n) = \frac{1}{k+1}\sum_{r=0}^{k}\binom{k+1}{r}B_r \cdot (n+1)^{k+1-r}.$$

A proof of this will be found on Exercise sheet 3.

The Bernoulli numbers will appear in the general formula for $\zeta(2k)$, however in order to get this we will use Fourier series on a set of functions connected to Bernoulli numbers.

Definition 3.8. The **Bernoulli polynomials** are the polynomials $B_k(x)$ given by the generating series:

$$\frac{te^{xt}}{e^t - 1} = \sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!}.$$

As with Bernoulli numbers we can explicitly work out such polynomials for small k by computing the expansion. We find:

$$\begin{aligned}
B_0(x) &= 1\\
B_1(x) &= x - \frac{1}{2}\\
B_2(x) &= x^2 - x + \frac{1}{6}\\
B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x\\
B_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30}\\
B_5(x) &= x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x.
\end{aligned}$$

One observes the following from the expansion.

Lemma 3.9. *$B_k(x)$ is a polynomial of degree k with rational coefficients.*

We note some other good properties of the Bernoulli polynomials.

Proposition 3.10. *The Bernoulli polynomials satisfy the following:*

1. *For $k \geq 0$: $B_k(0) = B_k$,*
2. *For $k \geq 0$: $\frac{d}{dx}(B_{k+1}(x)) = (k+1)B_k(x)$,*
3. *For $k \geq 1$: $\int_0^1 B_k(x)dx = 0$,*
4. *For $k \geq 2$: $B_k(0) = B_k(1)$.*

Proof. 1. If $x = 0$ then:

$$\frac{te^{xt}}{e^t - 1} = \frac{t}{e^t - 1}$$

and so in terms of generating series:

$$\sum_{k=0}^{\infty} B_k(0)\frac{t^k}{k!} = \sum_{k=0}^{\infty} B_k\frac{t^k}{k!}.$$

By uniqueness of Taylor expansion we must have $B_k = B_k(0)$ for all $k \geq 0$.

2. Note that:

$$\frac{d}{dx}\left(\frac{te^{xt}}{e^t - 1}\right) = \frac{t^2e^{xt}}{e^t - 1}$$

By interchangability of sum and differential the LHS has Taylor expansion:

$$\frac{d}{dx}\left(\sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!}\right) = \sum_{k=0}^{\infty} \frac{d}{dx}(B_k(x))\frac{t^k}{k!}.$$

The RHS has Taylor expansion:

$$t\sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!} = \sum_{k=0}^{\infty} B_k(x)\frac{t^{k+1}}{k!} = \sum_{k=0}^{\infty}(k+1)B_k(x)\frac{t^{k+1}}{(k+1)!}.$$

By uniqueness of Taylor expansions we now observe that $\frac{d}{dx}(B_{k+1}(x)) = (k+1)B_k(x)$ for all $k \geq 0$.

3. Note that:

$$\int_0^1 \frac{te^{xt}}{e^t - 1}\mathrm{d}x = \left(\frac{e^t}{e^t - 1}\right) - \left(\frac{1}{e^t - 1}\right) = 1.$$

By interchangability of sum and integral we also have:

$$\int_0^1 \frac{te^{xt}}{e^t - 1}\mathrm{d}x = \sum_{k=0}^{\infty}\left(\int_0^1 B_k(x)\ \mathrm{d}x\right)\frac{t^k}{k!}.$$

By uniqueness of Taylor series all coeffs for $k \geq 1$ must be 0, as required.

4. For $k \geq 1$ we must have $B_{k+1}(1) = B_{k+1}(0)$ since by parts 2 and 3:

$$\int_0^1 B_k(x) \, \mathrm{d}x = \left[\frac{B_{k+1}(x)}{k+1} \right]_0^1 = \frac{B_{k+1}(1) - B_{k+1}(0)}{k+1} = 0.$$

   Thus $B_k(1) = B_k(0)$ for all $k \geq 2$.

□

Actually the above theorem gives us a recursion to find the Bernoulli polynomials given knowledge of the Bernoulli numbers.

Example 3.11. We know that $B_0(x) = 1$ and so by point 2:

$$B_1(x) = x + C_1$$

for some constant C_1.

But by point 1

$$C_1 = B_1(0) = B_1 = -\frac{1}{2}.$$

Thus we find that $B_1(x) = x - \frac{1}{2}$, as expected.

Example 3.12. Let's do another step in this recursion.

We know that $B_1(x) = x - \frac{1}{2}$ and so by point 2:

$$B_2(x) = 2\left(\frac{x^2}{2} - \frac{1}{2}x\right) + C_2 = x^2 - x + C_2$$

for some constant C_2.

Again by point 1 we know that:

$$C_2 = B_2(0) = B_2 = \frac{1}{6},$$

and so we see that $B_2(x) = x^2 - x + \frac{1}{6}$, as expected.

Exercise - Continue the recursion to check all previously described Bernoulli polynomials.

There are better ways to generate the Bernoulli polynomials. Some are outlined in Exercise sheet 3.

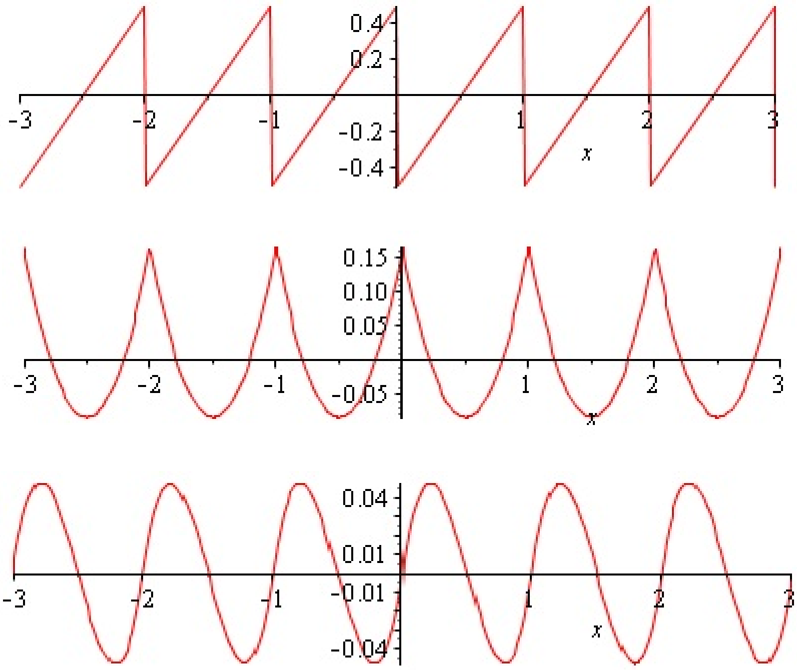
3.1.2 $\zeta(2k)$

We are now ready to generate formulae for $\zeta(2k)$. As mentioned earlier we will be using Fourier series. However to do this properly we will need some periodic functions.

Definition 3.13. The **periodic Bernoulli polynomials** are the functions $P_k(x) : \mathbb{R} \to \mathbb{R}$ given by $P_k(x) = B_k(x - \lfloor x \rfloor)$.

One can see at once that $x - \lfloor x \rfloor$ is periodic of period 1 (since adding/subtracting 1 doesn't change the fractional part). Hence the periodic Bernoulli polynomials are also periodic of period 1.

Below are graphs of $P_1(x), P_2(x)$ and $P_3(x)$.



Proposition 3.14. *The periodic Bernoulli polynomials have the following properties.*

1. $P_k(x) = B_k(x)$ *for* $x \in [0, 1)$,
2. *For* $n \geq 2$: $P_n(x)$ *is continuous everywhere,*
3. *For* $n \geq 1$: $\frac{d}{dx}(P_n(x)) = nP_{n-1}(x)$,
4. *For* $n \geq 0$: $\int_{x_0}^{x_0+1} P_n(x)dx = 0$.

Proof. 1. This is clear by definition.

2. For $x \notin \mathbb{Z}$ we know that $P_n(x)$ is defined by a polynomial and so is continuous. Also for $k \geq 2$ we know that $B_k(0) = B_k(1)$ and so by periodicity $P_k(n) = P_k(0)$ for all $n \in \mathbb{Z}$. Thus $P_k(x)$ is continuous at integer inputs too (the "endpoints" match up).

3. This is clear for $x \in [0,1)$ by point 1 and the corresponding property for $B_k(x)$. Thus by periodicity of $P_k(x)$ it is true for all x.

4. Same argument as point 3.

□

Recall that a real periodic function $f(x)$ of period L has a Fourier series of the form:

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos\left(\frac{2\pi n x}{L}\right) + b_n \sin\left(\frac{2\pi n x}{L}\right) \right)$$

and converges wherever f is continuous. The formulae for the coefficients are given by:

$$a_0 = \frac{1}{L} \int_{x_0}^{x_0+L} f(x)\ \mathrm{d}x$$

$$a_n = \frac{2}{L} \int_{x_0}^{x_0+L} f(x) \cos\left(\frac{2\pi n x}{L}\right) \mathrm{d}x$$

$$b_n = \frac{2}{L} \int_{x_0}^{x_0+L} f(x) \sin\left(\frac{2\pi n x}{L}\right) \mathrm{d}x$$

for any choice of $x_0 \in \mathbb{R}$ (all give the same answer by periodicity).

Let's work out the Fourier series of $P_k(x)$.

Theorem 3.15. *For $k \geq 1$ we have the following Fourier expansions, valid for all $x \in \mathbb{R}$:*

$$P_{2k}(x) = (-1)^{k+1}(2k)! \sum_{n=1}^{\infty} \frac{2}{(2n\pi)^{2k}} \cos(2n\pi x),$$

$$P_{2k+1}(x) = (-1)^{k+1}(2k+1)! \sum_{n=1}^{\infty} \frac{2}{(2n\pi)^{2k+1}} \sin(2n\pi x).$$

Proof. We will use induction.

First we show that

$$P_2(x) = \sum_{n=1}^{\infty} \frac{1}{(n\pi)^2} \cos(2n\pi x).$$

To this end we simply use the formulae for Fourier coefficients along with Theorem 3.14.

$$\begin{aligned}
a_0 &= \int_0^1 P_2(x)\ \mathrm{d}x = 0,\\
b_n &= 0 \qquad\qquad \text{(since } P_2 \text{ is even)}.\\
a_n &= 2\int_0^1 P_2(x)\cos(2n\pi x)\ \mathrm{d}x\\
&= 2\int_0^1 \left(x^2 - x + \frac{1}{6}\right)\cos(2n\pi x)\ \mathrm{d}x\\
&= 2\left(\left[\frac{(x^2 - x + \frac{1}{6})\sin(2n\pi x)}{2n\pi}\right]_0^1 - \int_0^1 \frac{(2x-1)\sin(2n\pi x)}{2n\pi}\ \mathrm{d}x\right)\\
&= -\frac{1}{n\pi}\int_0^1 (2x-1)\sin(2n\pi x)\ \mathrm{d}x\\
&= -\frac{1}{n\pi}\left(\left[-\frac{(2x-1)\cos(2n\pi x)}{2n\pi}\right]_0^1 + 2\int_0^1 \frac{\cos(2n\pi x)}{2n\pi}\ \mathrm{d}x\right)\\
&= -\frac{1}{n\pi}\left(-\frac{1}{n\pi} + \frac{1}{n\pi}\left[\frac{\sin(2n\pi x)}{2n\pi}\right]_0^1\right)\\
&= \frac{1}{(n\pi)^2}
\end{aligned}$$

Now we show that if the Fourier series above is true for P_{2k} then it must be true for P_{2k+1}.

To do this note that by Theorem 3.14:

$$P_{2k+1}(x) = (2k+1)\int P_{2k}(x)\mathrm{d}x$$

under the condition that $\int_0^1 P_{2k+1}(x)\mathrm{d}x = 0$.

So assuming the Fourier series for $P_{2k}(x)$ we have:

$$\begin{aligned}
P_{2k+1}(x) &= (2k+1)\left[(-1)^{k+1}(2k)!\sum_{n=1}^{\infty}\frac{2}{(2n\pi)^{2k}}\int\cos(2n\pi x)\mathrm{d}x\right]\\
&= \left((-1)^{k+1}(2k+1)!\sum_{n=1}^{\infty}\frac{2}{(2n\pi)^{2k+1}}\sin(2n\pi x)\right) + C
\end{aligned}$$

for some constant C.

Integrating both sides between 0 and 1 gives $C = 0$, as required.

In order to finish the induction it must also be shown that the Fourier series for P_{2k+1} implies the one for P_{2k+2}. However this is a similar calculation. □

Exercise - Finish off the proof.

Of course $P_1(x)$ has a Fourier series too (you have probably calculated it before). However since $P_1(x)$ is discontinuous at $x \in \mathbb{Z}$ we have no need for it here.

We are now able to produce the famous formula for $\zeta(2k)$.

Corollary 3.16. *(Euler) For $k \geq 1$:*

$$\zeta(2k) = (-1)^{k+1}\frac{B_{2k}(2\pi)^{2k}}{2(2k)!}.$$

Proof. We know that $P_{2k}(x)$ is continuous at $x = 0$ for all $k \geq 1$. Hence the Fourier series for $P_{2k}(x)$ converges there.

Thus:

$$\begin{aligned} B_{2k} = P_{2k}(0) &= (-1)^{k+1}(2k)!\sum_{n=1}^{\infty}\frac{2}{(2n\pi)^{2k}} \\ &= (-1)^{k+1}(2k)!\frac{2}{(2\pi)^{2k}}\sum_{n=1}^{\infty}\frac{1}{n^{2k}} \\ &= (-1)^{k+1}(2k)!\frac{2}{(2\pi)^{2k}}\zeta(2k). \end{aligned}$$

Rearranging gives the result.

□

Exercise - Check this formula matches the values for $\zeta(2), \zeta(4), \zeta(6)$ given at the beginning of Section 3.1.

Exercise - Use Euler's formula to explain why even indexed Bernoulli numbers alternate in sign.

Euler did not find the above formula using Fourier series (the invention of this was about 20 years after he died). We will see his method in Exercise sheet 3.

Interesting fact - Odds and ends

Now that we have a closed formula for $\zeta(2k)$ it is natural to ask about $\zeta(2k+1)$ too.

This is actually an unsolved problem! There is no known closed formula for generating these values (note the Fourier expansions of P_{2k+1} tell us nothing). Of course we may approximate these values numerically but this is the best method we have so far.

In fact it isn't even known if all of these values are irrational. It wasn't until 1978 that the first value $\zeta(3)$ was proved to be irrational using complicated arguments with modular forms (after which $\zeta(3)$ became known as Apéry's constant).

However, it has been known since the year 2000 that infinitely many of these values are irrational.

One thing is for certain, it is not the case that $\zeta(2k+1) = \alpha_{2k+1}\pi^{2k+1}$ for $\alpha_{2k+1} \in \mathbb{Q}$ (a pattern which you would expect given the behaviour of the even zeta values).

3.2 Analytic continuation

The notion of analytic continuation is probably one that is totally new to you. However it is a completely natural one. Let's begin with a straight-forward example.

Consider the infinite series:

$$f(z) = \sum_{k=0}^{\infty} z^k = 1 + z + z^2 + ...$$

We know that $f(z)$ only ever makes sense when $|z| < 1$ (the radius of convergence of the sum is $R = 1$).

However most maths undergrads like to quote the geometric sum formula:

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

Question - Is it true that $f(z) = \frac{1}{1-z}$ for **all** $z \in \mathbb{C}\backslash\{1\}$?

The answer is **no**...and this cannot be stressed enough.

Whilst we have a "formula" saying these two things are equal it is easy to forget that the formula only holds **when both sides converge**.

Even though f agrees with $\frac{1}{1-z}$ for $|z| < 1$, only the function $\frac{1}{1-z}$ makes sense for **all** $z \neq 1$.

Exercise - It is a common undergrad error to use identities blindly without caring about convergence. If you still do this then get a friend to slap you silly...right now! (Oh and then remember in future not to make this error).

Definition 3.17. Let $f : U \to \mathbb{C}$ be a function on some subset $U \subset \mathbb{C}$. Suppose $W \subseteq \mathbb{C}$ contains U. Then a **continuation** of f to W is a function $g : W \to \mathbb{C}$ such that $g(z) = f(z)$ for all $z \in U$.

Of course continuations are quite boring. There are infinitely many ways to continue a function from V to W, most of them being completely arbitrary. What is more interesting is if I wish to keep analytical properties too!

Definition 3.18. Let f be analytic on an open subset $U \subset \mathbb{C}$. Let $W \subseteq \mathbb{C}$ be an open set containing U. An **analytic continuation** of f to W is an analytic function g on W that is also a continuation of f to W.

Example 3.19. The function $g(z) = \frac{1}{1-z}$ is an analytic continuation of $f(z) = 1 + z + z^2 + ...$ to $\mathbb{C} \backslash \{1\}$.

Example 3.20. In MAS342 you met the **Gamma function**. The purpose of this function was to create a continuation of the factorial function to $\mathbb{R}_{>0}$ by defining the integral:

$$\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} \mathrm{d}t.$$

In fact doing so in this fashion created a smooth function out of the factorial function. This is another classical example of analytic continuation.

It is in fact possible to analytically continue Γ to $\mathbb{C} \backslash \{-1, -2, -3, ...\}$.

It might be intuitive to think that there are infinitely many analytic continuations of a function in general. This would certainly be the case for real functions (if I give you a bit of a curve how many ways can you extend it keeping it smooth?).

However, for nice enough domains there is a remarkable fact for analytic continuations of complex functions:

Theorem 3.21. *Let $U \subset W \subseteq \mathbb{C}$ be open sets with W connected. Suppose f is analytic on U. If an analytic continuation of f to W exists then it is unique.*

We will not prove this theorem, it belongs to complex analysis and is beyond the scope of the course. However note the strange outcome, if there exists a way to analytically continue f to W then there is only **one** way to do it!

Of course an analytic continuation doesn't always exist. For example it would be silly to expect an analytic continuation of $\frac{1}{1-z}$ to exist on the whole of $\mathbb{C}$. How ever much we try to fill in a value at $z = 1$ we will always break the analytic nature of the function.

3.2.1 Continuation of $\zeta(s)$ to $\mathbf{Re}(s) > 0$

We seek a way to analytically continue the Riemann zeta function. Fortunately there is simple way to do it for the domain $\mathrm{Re}(s) > 0$ (well upto a simple pole at $s = 1$).

Definition 3.22. Define the **Dirichlet eta function**:

$$\eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}.$$

This is a harmless looking function, it is just the Riemann zeta function but with alternating signs between terms.

Lemma 3.23. *The Dirichlet eta function converges and is analytic for Re*$(s) > 0$. *Absolute convergence takes place for Re*$(s) > 1$.

Proof. Absolute convergence for $\mathrm{Re}(s) > 1$ follows since:

$$\sum_{n=1}^{\infty} \left| \frac{(-1)^{n+1}}{n^s} \right| = \sum_{n=1}^{\infty} \frac{1}{n^{\mathrm{Re}(s)}} = \zeta(\mathrm{Re}(s)).$$

The fact that η is convergent and analytic on $\mathrm{Re}(s) > 0$ follows by Theorem 2.30 since the sequence $|1|, |1+(-1)|, |1+(-1)+1|, |1+(-1)+1+(-1)|, ...$ is clearly bounded above by 1. □

We now exploit a connection between η and ζ.

Theorem 3.24. *For Re*$(s) > 1$.

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

Proof. Note that by absolute convergence of both series on $\mathrm{Re}(s) > 1$:

$$\zeta(s) - \eta(s) = \sum_{m=1}^{\infty} \frac{2}{(2m)^s} = \frac{1}{2^{s-1}} \sum_{m=1}^{\infty} \frac{1}{m^s} = \frac{1}{2^{s-1}}\zeta(s).$$

Thus:

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

□

Corollary 3.25. *The function:*

$$F(s) = \frac{\eta(s)}{\left(1 - \frac{1}{2^{s-1}}\right)}$$

is an analytic continuation of $\zeta(s)$ *to Re*$(s) > 0$ *except for a simple pole at* $s = 1$.

Proof. For $\mathrm{Re}(s) > 1$ we know that $F(s) = \zeta(s)$ by the above Theorem.

Now $\eta(s)$ is analytic and convergent for $\mathrm{Re}(s) > 0$.

The function $f(s) = \left(1 - \frac{1}{2^{s-1}}\right)$ is analytic and convergent on $\mathbb{C}$, except for simple poles at $s = 1 + \frac{2k\pi i}{\ln(2)}$ (for $k \in \mathbb{Z}$). This is a simple exercise in complex analysis.

However, it turns out that $\eta(1+\frac{2k\pi i}{\ln(2)})=0$ for all $k\neq 0$ so all but one of these simple poles cancel out with a zero of η. We will not prove this claim about η.

Note that $\eta(1)=1-\frac{1}{2}+\frac{1}{3}-...=\ln(2)\neq 0$ so the simple pole at $s=1$ remains.

Thus $F(s)$ is analytic on $\text{Re}(s)>0$ except for a simple pole at $s=1$. □

Interesting fact - Going further

It is in fact possible to analytically continue $\zeta(s)$ to $\mathbb{C}$, still with the exception of a simple pole at $s=1$. This is a much tougher thing to do but is one of Riemann's biggest achievements, for reasons we discuss in a moment.

The way Riemann did it was via a **functional equation**. A functional equation defines a function at certain points via values at other points.

For example I might define a function f on $[0,\infty)$ and then demand the property $f(x)=f(-x)$ in order to define a function on $\mathbb{R}$. Then I can find say $f(-59)$ by just knowing $f(59)$.

The functional equation defining $\zeta(s)$ for $s\neq 1$ relates $\zeta(s)$ with $\zeta(1-s)$. But we already have a definition of $\zeta(s)$ for $\text{Re}(s)>0$ and so this is fine! Using this new definition of ζ I can work out say $\zeta(-34)$ by knowing $\zeta(35)$ or $\zeta(-\pi+56i)$ by knowing $\zeta((1+\pi)-56i)$.

The functional equation itself is quite messy:

$$\zeta(s)=2^s\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s)$$

but every term of this is well defined.

There is a cleaner version, if one defines the **completed Riemann zeta function**:

$$\xi(s)=\frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

then the functional equation becomes:

$$\xi(s)=\xi(1-s).$$

This functional equation tells us something about the zeros of $\zeta(s)$. Studying it closely we see that the only zeros of $\zeta(s)$ are the **trivial zeros** at $s=-2,-4,-6,...$ and the **non-trivial zeros** that lie in the **critical strip** $0<\text{Re}(s)<1$.

Note also that by the analytic continuation and our formula for $\zeta(2k)$ ($k\geq 1$) we see that $\zeta(-k)=-\frac{B_{k+1}}{k+1}$, supporting the fact that ζ is zero at the negative even integers (since odd Bernoulli numbers are 0). Also it tells us a non-obvious thing, that zeta of a negative odd integer is actually a rational number!

3.2.2 The Riemann Hypothesis

Riemann's most famous paper, published in 1859, was entitled "On the number of primes less than a given magnitude". This is still considered a revolutionary paper in analytic number theory and provided great insights into the behaviour of $\pi(x)$.

In a nutshell Riemann managed to find a concrete link, via analytic continuation and use of the Euler product, between $\pi(x)$ and the non-trivial zeros of the Riemann zeta function. Then using this link he was able to predict a series of stronger approimations to $\pi(x)$, generalising the PNT (as well as showing how strong the original PNT is).

His clever idea was the study the function:

$$F(x) = \sum_{n=1}^{\infty} \frac{\pi(\sqrt[n]{x})}{n} = \pi(x) + \frac{\pi(\sqrt{x})}{2} + \frac{\pi(\sqrt[3]{x})}{3} + ...$$

(Note that this is **not** an infinite sum, eventually $\sqrt[n]{x} < 2$ so that eventually $\pi(\sqrt[n]{x}) = 0$).

Via a generalisation of Möbius inversion Riemann was able to extract a formula for $\pi(x)$ in terms of $F(x)$:

$$\pi(x) = \sum_{n=1}^{\infty} \mu(n) \frac{F(\sqrt[n]{x})}{n} = F(x) - \frac{F(\sqrt{x})}{2} - \frac{F(\sqrt[3]{x})}{3} ...$$

(again a finite sum).

Then using a lot of complex analysis he was able to find the following **explicit formula** for $F(x)$:

$$F(x) = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}(x^{\rho}) - \ln(2) + \int_{x}^{\infty} \frac{dt}{t(t^2-1)\ln(t)}$$

where ρ ranges through all **non-trivial** zeros of $\zeta(s)$ (the ones in the critical strip $0 < \mathrm{Re}(s) < 1$).

The final two terms in this formula are not so important. Indeed $\ln(2) = 0.693147...$ and the integral turns out to be at most $0.140010...$ for $x \geq 2$ (we don't really care about $F(x)$ for $x < 2$ since we already know that $\pi(x) = 0$ for $x < 2$).

All that remains is to study the second term of the formula, the sum.

A few questions come to mind. How many zeros does $\zeta(s)$ have in the critical strip? Can we explicitly find them all?

It turns out that there are in fact infinitely many zeros of $\zeta(s)$ in the critical strip (so we are dealing with an infinite sum). What is actually quite startling is that all **known** zeros have real part $\frac{1}{2}$.

Conjecture 3.26. *(Riemann Hypothesis)*

***All** non-trivial zeros of $\zeta(s)$ lie on the line $Re(s) = \frac{1}{2}$.*

This conjecture is incredibly easy to understand, after all it is only about a certain function being zero. However the proof of this result has eluded mathematicians since Riemann's paper was published in 1859.

In fact this conjecture is now one of the seven famous Millennium Problems offered by the Clay Mathematics Institute, each worth \$1,000,000 to anyone with a full solution.

Taking a step back, what would the Riemann Hypothesis tell us if it were true? Well in that case the sum in the explicit formula would be incredibly well behaved.

We already know that:

$$\mathrm{Li}(x) - F(x) \approx \sum_{\rho} \mathrm{Li}(x^{\rho}).$$

So that if **all** such ρ had real part $\frac{1}{2}$ we see that $F(x)$ is **well** approximated by $\mathrm{Li}(x)$.

But then a good approximation for $\pi(x)$ is given by:

$$\pi(x) \approx \sum_{n=1}^{\infty} \mu(n) \frac{\mathrm{Li}(\sqrt[n]{x})}{n} = \mathrm{Li}(x) - \frac{\mathrm{Li}(\sqrt{x})}{2} - \frac{\mathrm{Li}(\sqrt[3]{x})}{3} - ...$$

This gives a series of good approximations for $\pi(x)$ (truncating the sum) and one can study them in more detail to find out just how good they are by using the zeros of the zeta function.

In particular one finds, assuming the Riemann Hypothesis is true, that for x sufficiently large:

$$|\pi(x) - \mathrm{Li}(x)| \leq C\sqrt{x}\,\ln(x)$$

making precise how good $\mathrm{Li}(x)$ is at approximating $\pi(x)$. In particular this proves the PNT!

Interesting Fact - The general Riemann hypothesis

As we know, the Riemann zeta function is one of the original Dirichlet series. However there are many others coming from natural number theoretic sources (we will see a huge class of examples in the next chapter). Other sources include modular forms, elliptic curves, number fields (finite extensions of $\mathbb{Q}$, such as $\mathbb{Q}$ itself).

All of these objects have natural analytic continuations (possibly with the exception of a simple pole somewhere). The general Riemann hypothesis claims that the (non-trivial) zeros of these functions all have real part $\frac{1}{2}$ too.

Why do we care? Well just as the Riemann hypothesis provides huge insight to $\pi(x)$, the other functions give other estimates about number theoretic behaviour (such as estimates for $\pi_{m,a}(x)$, numbers of primes in number fields of bounded norm, information about point counts mod p on elliptic curves, etc).

This is the beginning of a fascinating area of number theory!

4 Dirichlet's theorem

In this section of the notes we will study the proof of Dirichlet's theorem on primes in arithmetic progressions. As a reminder, here is the theorem we wish to prove.

Conjecture 4.1. *Let $a, m \in \mathbb{N}$ be coprime. Then there are infinitely many primes of the form $mk + a$ (i.e. congruent to $a \bmod m$).*

The full proof will be difficult but before we start let's motivate the underlying argument via an example.

Example 4.2. Let's prove the infinitude of primes of the form $4k+1$ and $4k+3$ in one. We use two Dirichlet series together:

$$L(s, \chi_0) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + ...$$
$$L(s, \chi_1) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} + ...$$

Here

$$\chi_0(n) = \begin{cases} 0 & \text{if } 2 \mid n \\ 1 & \text{if } n \equiv 1 \bmod 4 \\ 1 & \text{if } n \equiv 3 \bmod 4 \end{cases}$$
$$\chi_1(n) = \begin{cases} 0 & \text{if } 2 \mid n \\ 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4 \end{cases}$$

Now both χ_0, χ_1 are completely multiplicative and so we have Euler products:

$$L(s, \chi_0) = \prod_{p \neq 2} \left(1 - \frac{1}{p^s}\right)^{-1}$$
$$L(s, \chi_1) = \prod_{p \neq 2} \left(1 - \frac{\chi_1(p)}{p^s}\right)^{-1}$$

We wish to study the convergence of these at $s = 1$.

Note that since $L(s, \chi_0) = \left(1 - \frac{1}{2^s}\right) \zeta(s)$ we have divergence as $s \to 1$. However notice that $L(s, \chi_1)$ converges at $s = 1$, since the series converges for $\mathrm{Re}(s) > 0$ (by Theorem 2.30).

In fact $L(1, \chi_1) = 1 - \frac{1}{3} + \frac{1}{5} - ... = \frac{\pi}{4} \neq 0$.

Both series converge absolutely for $\mathrm{Re}(s) > 1$ and are analytic in their half planes of convergence.

Now taking logs of both Dirichlet series for $\mathrm{Re}(s) > 1$ (which is valid) we see that:

$$\begin{aligned}
\ln(L(s,\chi_0)) &= \sum_{p\neq 2} \frac{1}{p^s} + \sum_{p\neq 2}\sum_{n\geq 2} \frac{1}{np^{ns}} \\
&= \sum_{p\neq 2} \frac{1}{p^s} + A(s,\chi_0) \\
\ln(L(s,\chi_1)) &= \sum_{p\neq 2} \frac{\chi_1(p)}{p^s} + \sum_{p\neq 2}\sum_{n\geq 2} \frac{\chi_1(p)^n}{np^{ns}} \\
&= \sum_{p\neq 2} \frac{\chi_1(p)}{p^s} + A(s,\chi_1)
\end{aligned}$$

This looks similar to what we did for the Riemann zeta function. Indeed the same outcome holds, the functions $A(s,\chi_0)$ and $A(s,\chi_1)$ are bounded in absolute value so converge to a finite limit as $s \to 1$.

Clever trick alert: Let's take suitable linear combinations of these two series.

$$\begin{aligned}
\ln(L(s,\chi_0)) + \ln(L(s,\chi_1)) &= 2 \sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} + A(s,\chi_0) + A(s,\chi_1) \\
\ln(L(s,\chi_0)) - \ln(L(s,\chi_1)) &= 2 \sum_{p\equiv 3 \bmod 4} \frac{1}{p^s} + A(s,\chi_0) - A(s,\chi_1)
\end{aligned}$$

Notice how we have managed to somehow focus on **only** those primes in a given class mod 4. This is a piece of black magic at the moment but is tied up in the construction of χ_0, χ_1.

Now we are done since as $s \to 1$ the LHS's diverge so that the RHS's must. However as $s \to 1$:

$$\begin{aligned}
2 \sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} + A(s,\chi_0) + A(s,\chi_1) &\longrightarrow 2 \sum_{p\equiv 1 \bmod 4} \frac{1}{p} + C \\
2 \sum_{p\equiv 3 \bmod 4} \frac{1}{p^s} + A(s,\chi_0) - A(s,\chi_1) &\longrightarrow 2 \sum_{p\equiv 3 \bmod 4} \frac{1}{p} + D
\end{aligned}$$

for two constants C, D.

Thus the two series $\sum_{p\equiv 1 \bmod 4} \frac{1}{p}$ and $\sum_{p\equiv 3 \bmod 4} \frac{1}{p}$ must diverge, proving that there are infinitely many primes of either form.

4.1 General setup

In order to generalize the above strategy we will have to invent some new tools. What do we need?

1. Analogues "mod m" of the "mod 4" arithmetic frunctions χ_0 and χ_1. We may need more than two of these in general.
2. All of the χ's except χ_0 to be such that $L(s, \chi)$ is analytic and non-zero in a neighbourhood of $s = 1$ (so that we may take logs).
3. For χ_0 to be such that $L(s, \chi_0)$ is analytic and non-zero in a neighbourhood of $s = 1$, except for a pole at $s = 1$ (so we may still take logs **and** have divergence as $s \to 1$).
4. For nice enough Euler products to exist. Thus we should try and make all χ's completely multiplicative.
5. The functions $A(s, \chi)$ to be bounded in absolute value (so that they converge as $s \to 1$).
6. To find the correct linear combination of logs in order to give a sum of the form $\sum_{p \equiv a \bmod m} \frac{1}{p^s}$.

In this subsection we address these questions.

4.1.1 Characters of $(\mathbb{Z}/m\mathbb{Z})^\times$

We are ready to construct analogues of χ_0, χ_1 now. First we introduce a more general concept for an arbitrary group.

Definition 4.3. A **character** of a (finite) group G is a group homomorphism

$$\chi : G \to \mathbb{C}^\times.$$

Essentially characters let you translate group elements (which might be weird objects) into complex numbers in a coherent way. Since we wish to use analysis this is not a strange thing to want to do.

There are notions of character for infinite groups but for simplicity G will represent a finite group from now on.

For this course we will concern ourselves with the case $G = (\mathbb{Z}/m\mathbb{Z})^\times$ but nearly everything can be done generally.

We should first focus on generating some examples.

Example 4.4.

1. There is a character χ_0 for any group G given by $\chi_0(g) = 1$ for all $g \in G$. This is called the trivial character.
2. Let p be prime. A well known non-trivial character of $(\mathbb{Z}/p\mathbb{Z})^\times$ is given by the Legendre symbol. The homomorphism property is encoded in the fact that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all a, b coprime to p.

Most characters don't come neatly packaged with an intuition/interpretation but we will see soon that it is easy to find all characters of a (finite) group explicitly.

First let's see some general properties of characters.

Proposition 4.5. *Let χ be a character of G. Then:*

1. $\chi(e) = 1$
2. $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$ *for all* $g \in G$
3. *For each* $g \in G$ *we have that* $\chi(g)$ *is a* $|G|$*th root of unity.*
   More specifically, if g *has order* $l \mid |G|$ *then* $\chi(g)$ *is an* l*th root of unity.*

Proof. It is clear that $\chi(e) = 1$ and $\chi(g^{-1}) = \chi(g)^{-1}$ by general properties of homomorphisms (if you are unsure then do it from scratch).

The fact that $\chi(g)^{-1} = \overline{\chi(g)}$ will follow once we know that $\chi(g)$ is a root of unity, since then $|\chi(g)|^2 = 1$ implies that $\chi(g)\overline{\chi(g)} = 1$, hence $\overline{\chi(g)} = \chi(g)^{-1}$.

It remains to prove the third claim. Recall that by a corollary of Lagrange's theorem $g^{|G|} = e$ for every $g \in G$. Applying χ to both sides gives

$$\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(e) = 1$$

showing that $\chi(g)$ is a $|G|$th root of unity.

The stronger claim follows by the same argument but using the fact that $g^l = e$ by definition. □

So, how many characters of G are there? Well thanks to the proposition we can actually prove there are finitely many and get an obvious upper bound.

Corollary 4.6. *There are at most* $|G|^{|G|}$ *characters of* G.

Proof. Let $G = \{g_1, g_2, g_3, ..., g_{|G|}\}$. Then any character must send each g_i to a $|G|$th root of unity. There are $|G|$ of these.

Since there are $|G|$ possibilities for g we thus see that there are at most $|G|^{|G|}$ possibilities for the tuple $(\chi(g_1), \chi(g_2), ..., \chi(g_{|G|}))$. Thus there are at most this number of characters (not all possibilities are expected to give a homomorphism). □

It is simple to improve this bound. For a start we know that $\chi(e) = 1$, giving a smaller bound $(|G| - 1)^{|G|}$. There are much better bounds once you take orders of elements into consideration. We will not go into the finer details here since we will not need to.

Since the codomain of any character is $\mathbb{C}^\times$, a multiplicative group, it seems plausible that we can multiply characters. In fact we can and we get another group!

Theorem 4.7. *Let $\hat{G}$ be the set of characters of the finite group G. Then $\hat{G}$ is an abelian group under the operation:*

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g).$$

The identity element is the trivial character χ_0.

Proof. 1. Let $\chi_1, \chi_2 \in \hat{G}$. We wish to show that $\chi_1\chi_2 \in \hat{G}$.

It is clear that $\chi_1\chi_2$ is a map from G to $\mathbb{C}^\times$ so it remains to show that it is a homomorphism. This is not too difficult:

$$\begin{aligned}(\chi_1\chi_2)(gh) = \chi_1(gh)\chi_2(gh) &= (\chi_1(g)\chi_1(h))(\chi_2(g)\chi_2(h)) \\ &= (\chi_1(g)\chi_2(g))(\chi_1(h)\chi_2(h)) \\ &= (\chi_1\chi_2)(g)(\chi_1\chi_2)(h).\end{aligned}$$

2. Associativity in $\hat{G}$ is a simple consequence of associativity in $\mathbb{C}^\times$.

3. It is easy to see that $\chi\chi_0 = \chi_0\chi = \chi$ for all $\chi \in \hat{G}$ and so χ_0 behaves as an identity element.

4. As for inverses define $\chi^{-1}(g) = \chi(g)^{-1}$. Then it is easy to see that $\chi^{-1} \in \hat{G}$ and $\chi\chi^{-1} = \chi^{-1}\chi = \chi_0$ for all $\chi \in \hat{G}$. Thus we have inverses.

5. The abelian condition is simple to see. For all $\chi_1, \chi_2 \in \hat{G}$ and $g \in G$ we have:
$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = \chi_2(g)\chi_1(g) = (\chi_2\chi_1)(g).$$
Thus $\chi_1\chi_2 = \chi_2\chi_1$.

□

Example 4.8. It is quite easy to find the characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ when m is small.

1. $m = 4$. Here $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$.

Suppose χ is a character of $(\mathbb{Z}/4\mathbb{Z})^\times$. Then we already know that $\chi(\overline{1}) = 1$.

Since the order of $\overline{3}$ mod 4 is 2 we must have that $\chi(\overline{3})$ is a square root of unity, i.e. $\chi(\overline{3}) \in \{\pm 1\}$.

Thus there are two possibilities:

$$\begin{array}{ll} \chi_0(\overline{1}) = 1 & \chi_0(\overline{3}) = 1 \\ \chi_1(\overline{1}) = 1 & \chi_1(\overline{3}) = -1 \end{array}$$

It is easily checked that both possibilities are characters, hence the character group is $\{\chi_0, \chi_1\} \cong C_2$.

2. $m = 8$. Here $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

   Suppose χ is a character of $(\mathbb{Z}/8\mathbb{Z})^\times$. Then we already know that $\chi(\overline{1}) = 1$. Now $\overline{3}$ and $\overline{5}$ both have order 2 and so $\chi(\overline{3}), \chi(\overline{5}) \in \{\pm 1\}$. Also $\overline{7} = \overline{3} \cdot \overline{5}$ and so $\chi(\overline{7}) = \chi(\overline{3})\chi(\overline{5})$.

   Thus there are four possibilities:

$$\begin{array}{llll}
\chi_0(\overline{1}) = 1 & \chi_0(\overline{3}) = 1 & \chi_0(\overline{5}) = 1 & \chi_0(\overline{7}) = 1 \\
\chi_1(\overline{1}) = 1 & \chi_1(\overline{3}) = -1 & \chi_1(\overline{5}) = 1 & \chi_1(\overline{7}) = -1 \\
\chi_2(\overline{1}) = 1 & \chi_2(\overline{3}) = 1 & \chi_2(\overline{5}) = -1 & \chi_2(\overline{7}) = -1 \\
\chi_3(\overline{1}) = 1 & \chi_3(\overline{3}) = -1 & \chi_3(\overline{5}) = -1 & \chi_3(\overline{7}) = 1
\end{array}$$

   Again it is easy to check that all four possibilities give characters, hence the character group is $\{\chi_0, \chi_1, \chi_2, \chi_3\}$.

   Which group of order 4 did we get? Well notice that $\chi_1^2, \chi_2^2, \chi_3^2 = \chi_0$ hence the character group is isomorphic to the Klein four group $C_2 \times C_2$ (with generators χ_1 and χ_2 since $\chi_3 = \chi_1\chi_2$).

How many characters are there for a general group G? This is a tough question but there is a straight-forward answer.

Theorem 4.9. *Let G be a finite group with h conjugacy classes. Then $|\hat{G}| = h$.*

We will not prove this theorem since it beyond the scope of the course. However we note a useful consequence of it.

Corollary 4.10. *The character group of $(\mathbb{Z}/m\mathbb{Z})^\times$ has $\phi(m)$ elements.*

Proof. The group $(\mathbb{Z}/m\mathbb{Z})^\times$ is abelian and so each element lies in its own conjugacy class. Hence there are $|\,(\mathbb{Z}/m\mathbb{Z})^\times\,| = \phi(m)$ conjugacy classes. By the theorem this is how many characters there are. □

Example 4.11. It is easy to demonstrate the above when $m = p$ is prime (which was done in MAS330 in 2013/14).

We will exhibit exactly $\phi(p) = p - 1$ characters of $G = (\mathbb{Z}/p\mathbb{Z})^\times$.

Let $\chi \in \hat{G}$. It is known that G is cyclic of order $p - 1$ so we may choose a generator $\overline{a} \in G$.

Then χ is completely determined by the value $\chi(\overline{a})$ since if $\overline{b} \in G$ then $\overline{b} = \overline{a}^k$ for some $k = 1, 2, ..., p - 1$, giving:

$$\chi(\overline{b}) = \chi(\overline{a}^k) = \chi(\overline{a})^k.$$

So it remains to find the possibilities for $\chi(\overline{a})$. Now $\overline{a}$ has order $p - 1$ in G by definition and so $\chi(\overline{a})$ is a $(p - 1)$th root of unity. There are $p - 1$ of these and so we get the possibilities:

$$\chi_j(\overline{a}) = \zeta^j \qquad \text{for } j = 0, 1, 2, ..., p-2$$

where $\zeta = e^{\frac{2\pi i}{p-1}}$.

It is easy to check that all of these possibilities do in fact give characters of G, hence $\hat{G} = \{\chi_0, \chi_1, ..., \chi_{p-2}\}$ is of order $p-1$.

Further $\hat{G} \cong \mathbb{Z}/(p-1)\mathbb{Z}$ is cyclic of order $p-1$. To see this either observe that $\hat{G} = \langle \chi_1 \rangle$, or use the explicit isomorphism $\chi_j \mapsto \overline{j}$.

Example 4.12. To demonstrate the above let $p = 5$. Then $(\mathbb{Z}/5\mathbb{Z})^\times = \langle \overline{2} \rangle$.

We have $\phi(5) = 5 - 1 = 4$ and $\zeta = e^{\frac{2\pi i}{4}} = e^{\frac{\pi i}{2}} = i$ so the possibilities are:

$$\begin{aligned} \chi_0(\overline{2}) &= i^0 = 1 \\ \chi_1(\overline{2}) &= i^1 = i \\ \chi_2(\overline{2}) &= i^2 = -1 \\ \chi_3(\overline{2}) &= i^3 = -i \end{aligned}$$

There are exactly 4 characters here as expected.

Exercise - Now that we know the values $\chi_j(\overline{2})$ we should be able to find all other values $\chi_j(\overline{a})$ for $\overline{a} = \overline{1}, \overline{3}, \overline{4}$. Do this!

One last result is needed before we can continue. This result concerns summing values of characters.

Theorem 4.13. *(Orthogonality relations)*

1. *Let χ be a fixed character of $(\mathbb{Z}/m\mathbb{Z})^\times$. Then:*

$$\sum_{\overline{a}} \chi(\overline{a}) = \begin{cases} \phi(m) & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

2. *Let $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ be fixed. Then as χ runs through all characters of $(\mathbb{Z}/m\mathbb{Z})^\times$:*

$$\sum_{\chi} \chi(\overline{a}) = \begin{cases} \phi(m) & \text{if } \overline{a} = \overline{1} \\ 0 & \text{otherwise} \end{cases}$$

Proof.

1. It is clear that if $\chi = \chi_0$ then the sum is $\phi(m)$ (it is a sum of 1's, one for each element of the group).

   Now assume that χ is non-trivial. Then there exists $\overline{n}$ such that $\chi(\overline{n}) \neq 1$.

Let S be the sum in question. Then:

$$\chi(\overline{n})S = \chi(\overline{n})\sum_{\overline{a}}\chi(\overline{a}) = \sum_{\overline{a}}\chi(\overline{na}) = \sum_{\overline{b}}\chi(\overline{b}) = S.$$

Thus $(\chi(\overline{a})-1)S = 0$, however $\chi(\overline{a}) \neq 1$, hence $S = 0$.

2. It is clear that if $\overline{a} = \overline{1}$ then the sum is $\phi(m)$ (every character sends $\overline{1}$ to 1 so again you get a sum of 1's).

   Now assume $\overline{a} \neq \overline{1}$. Then there exists a character $\hat{\chi}$ such that $\hat{\chi}(\overline{a}) \neq 1$.

   Let S be the sum in question. Then:

$$\hat{\chi}(\overline{a})S = \hat{\chi}(\overline{a})\sum_{\chi}\chi(\overline{a}) = \sum_{\chi}\hat{\chi}(\overline{a})\chi(\overline{a}) = \sum_{\chi}(\hat{\chi}\chi)(\overline{a}) = \sum_{\eta}\eta(\overline{a}) = S.$$

   Thus $(\hat{\chi}(\overline{a})-1)S = 0$, however $\hat{\chi}(\overline{a}) \neq 1$, hence $S = 0$.

□

Essentially this result tells you that if you sum along the rows/columns of the character table then you'll almost always get 0 (unless you pick the first row/column, in which case you get $\phi(m)$).

We can use the orthogonality relations to isolate a given class mod m.

Corollary 4.14. *Suppose a and n are coprime to m. Then as χ runs over all characters of $(\mathbb{Z}/m\mathbb{Z})^{\times}$:*

$$\sum_{\chi}\chi(\overline{a})^{-1}\chi(\overline{n}) = \begin{cases} \phi(m) & \textit{if } \overline{n} = \overline{a} \\ 0 & \textit{otherwise} \end{cases}$$

Proof. We note that:

$$\sum_{\chi}\chi(\overline{a})^{-1}\chi(\overline{n}) = \sum_{\chi}\chi(\overline{a}^{-1}\overline{n}).$$

Now the orthogonality relations tell us that this sum is $\phi(m)$ whenever $\overline{a}^{-1}\overline{n} = \overline{1}$, i.e. $\overline{n} = \overline{a}$. It also tells us that the sum is 0 otherwise. □

We have spent a while developing the theory of characters. It is now apparent to us that we can build the arithmetic functions that we desire from characters of $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

Definition 4.15. Given a character χ of $(\mathbb{Z}/m\mathbb{Z})^{\times}$ we may associate to it the arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}^{\times}$ such that:

$$\chi(n) = \begin{cases} \chi(\overline{n}) & \text{if hcf}(m,n) = 1 \\ 0 & \text{if hcf}(m,n) \neq 1 \end{cases}$$

Such an arithmetic function is known as a mod m **Dirichlet character**.

Example 4.16. Using the two characters of $(\mathbb{Z}/4\mathbb{Z})^{\times}$ found earlier we get two mod 4 Dirichlet characters:

$$\chi_0(n) = \begin{cases} 0 & \text{if } 2 \mid n \\ 1 & \text{if } n \equiv 1 \bmod 4 \\ 1 & \text{if } n \equiv 3 \bmod 4 \end{cases}$$

$$\chi_1(n) = \begin{cases} 0 & \text{if } 2 \mid n \\ 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4 \end{cases}$$

Notice that these are the same as the χ_0, χ_1 that we constructed in our sample proof of Dirichlet's theorem! In general we will use mod m Dirichlet characters to build Dirichlet series in order to study distribution of primes mod m.

Lemma 4.17. *A mod m Dirichlet character χ is completely multiplicative.*

Proof. Let $a, b \in \mathbb{N}$.

If either of a, b shares a proper factor with m then so does ab. Thus:

$$\chi(ab) = 0 = \chi(a)\chi(b).$$

If both a, b are coprime with m then by the fact that χ comes from a character of $(\mathbb{Z}/m\mathbb{Z})^{\times}$:

$$\chi(ab) = \chi(a)\chi(b).$$

Thus in either case we have $\chi(ab) = \chi(a)\chi(b)$. □

We also note the analogue of Corollary 4.14.

Corollary 4.18. *Suppose a, m and n are coprime. Then as χ runs over all mod m Dirichlet characters:*

$$\sum_{\chi} \chi(a)^{-1}\chi(n) = \begin{cases} \phi(m) & \textit{if } n \equiv a \bmod m \\ 0 & \textit{otherwise} \end{cases}$$

It might not look like it but we have now solved the question of which linear combinations of logs to take in order to isolate the primes that are $p \equiv a \bmod m$.

It now remains to study the corresponding Dirichlet series in detail.

4.1.2 Dirichlet L-series

Given a mod m Dirichlet character χ we can of course associate to it a Dirichlet series:

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

Also since χ is completely multiplicative we see that $L(s,\chi)$ has an Euler product of the form:

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

Of course we haven't yet studied the convergence of such series so we will add this to our to-do list. We will observe that for non-trivial χ we have much better behaviour than for trivial χ.

Definition 4.19. The series $L(s,\chi)$ is called the **Dirichlet L-series** attached to χ.

Example 4.20. If $\chi = \chi_0$ is the trivial character then:

$$\begin{aligned} L(s,\chi_0) &= \prod_{p\nmid m}\left(1-\frac{1}{p^s}\right)^{-1} \\ &= \prod_{p|m}\left(1-\frac{1}{p^s}\right)\zeta(s). \end{aligned}$$

By the above example we can now observe the following:

Corollary 4.21. *$L(s,\chi_0)$ is analytic on Re$(s) > 0$, except for a pole at $s = 1$. Also $L(s,\chi_0)$ is absolutely convergent for Re$(s) > 1$.*

Proof. We have already seen that an analytic continuation of $\zeta(s)$ to $\mathrm{Re}(s) > 0$ exists, except for the pole at $s = 1$. Also for each prime p the function $f(s) = \left(1-\frac{1}{p^s}\right)$ is analytic on $\mathbb{C}$.

Now by the above example:

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

and so the claim follows.

Absolute convergence for $\mathrm{Re}(s) > 1$ is obvious by the above connection with $\zeta(s)$. □

So we now know that the L-series for the trivial character is sufficiently "bad", but not too "bad" to be of any use.

We must now prove that all of the other L-series are sufficiently "good".

Lemma 4.22. *Suppose that $\chi \neq \chi_0$. Then $L(s,\chi)$ converges and is analytic for Re$(s) > 0$ (with **no** pole).*

Proof. We show that the sequence $|\chi(1)|, |\chi(1)+\chi(2)|, |\chi(1)+\chi(2)+\chi(3)|, ...$ is bounded above, then by Theorem 2.30 we have the result.

Consider the quantity:

$$S(k) = \left|\sum_{n=1}^{k} \chi(n)\right|.$$

Now χ is non-trivial so by the orthogonality relations:

$$S(m) = \left|\sum_{n=1}^{m} \chi(n)\right| = 0.$$

Thus writing $k = qm + r$ for $0 < r \leq m$ we find that $S(k) = S(r)$.

Hence the sequence $S(1), S(2), ...$ is bounded above by

$$M = \max\{S(1), S(2), ..., S(m-1)\}.$$

□

Lemma 4.23. *All Dirichlet L-series are absolutely convergent for Re$(s) > 1$.*

Proof. This follows since:

$$\sum_{n=1}^{\infty} \left|\frac{\chi(n)}{n^s}\right| = \sum_{n \nmid m} \frac{1}{n^s} = L(s, \chi_0)$$

and we already know that $L(s, \chi_0)$ is absolutely convergent for Re$(s) > 1$. □

Our final result is the following:

Theorem 4.24. *For χ non-trivial we have $L(1, \chi) \neq 0$.*

We will not prove this result in this course. In fact it is the hardest part of Dirichlet's proof. We need this fact so that $\ln(L(s, \chi))$ remains bounded as $s \to 1$ (to avoid taking log of 0).

In practice it is actually very easy to show this result for a given L-series. The key is to just group the terms in a specific way, then observe positivity. This technique will be practiced in Exercise sheet 4.

Interesting Fact - Special values of L-series

As we saw in Chapter 3, it is a non-trivial thing to evaluate the Riemann zeta function at integers. We have a formula for positive even integers but no such formula for positive odd integers. The formula we have contains lots of interesting features, in particular the Bernoulli numbers (which appear in many guises throughout number theory, way more than we have seen in this course).

We have seen in this chapter that it is handy to know the behaviour of Dirichlet L-series at $s = 1$. Naturally we ask whether there are formulae for evaluating L-series at integers, similar to those for the Riemann zeta function.

Indeed there do exist formulae for such special values of L-series.

Given a mod m Dirichlet character χ consider the **χ-Bernoulli polynomials** $B_n(\chi, x)$, defined by generating series:

$$\frac{te^{tx}}{e^{mt}-1}\sum_{r=0}^{m-1}\chi(r)e^{rt} = \sum_{n=0}^{\infty} B_n(\chi, x)\frac{t^n}{n!}$$

Also consider the **χ-Bernoulli numbers**, defined by $B_n(\chi) = B_n(\chi, 0)$.

It turns out that we can use Fourier series for these polynomials (in a similar fashion to what we did in Chapter 3) to tell us about special values of $L(s, \chi)$.

Alternatively one finds, in analogue to the formula $\zeta(-k) = -\frac{B_{k+1}}{k+1}$, the formula:

$$L(-k, \chi) = -\frac{B_{k+1}(\chi)}{k+1}.$$

Then via a functional equation for $L(s, \chi)$ relating values at s to values at $1 - s$ we may find information on values of $L(s, \chi)$ at positive integers.

In particular we can find formulae for $L(1, \chi)$ which help to prove that this value is non-zero when χ is non-trivial.

Also such formulae both explain and produce identities such as:

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - ... = \frac{\pi}{4}.$$

Going further, but not explaining how or why, a more detailed study of L-values gives startling links with solutions to Pell's equation, units of quadratic rings, class numbers of quadratic forms/number fields (Dedekind zeta function) amongst many other advanced things of number theoretic interest.

This is only the beginning!

4.2 The proof

We are ready to prove Dirichlet's theorem on primes in arithmetic progressions.

Proof

Let $a, m \in \mathbb{Z}$ be coprime. We show that the sum $\sum_{p\equiv a \bmod m} \frac{1}{p}$ diverges and hence there are infinitely many primes $p \equiv a \bmod m$.

Consider the trivial character χ_0 of $(\mathbb{Z}/m\mathbb{Z})^{\times}$. We know that the corresponding L-series $L(s,\chi_0)$ is convergent and analytic on $\mathrm{Re}(s) > 0$ except for a pole at $s = 1$.

For any other character χ of $(\mathbb{Z}/m\mathbb{Z})^{\times}$ the L-series $L(s,\chi)$ is convergent and analytic on the whole half-plane $\mathrm{Re}(s) > 0$.

All of the L-series are absolutely convergent for $\mathrm{Re}(s) > 1$.

We know that $L(s,\chi_0)$ is not 0 in a neighbourhood of $s = 1$ (by the link with $\zeta(s)$).

Also we have that $L(1,\chi) \neq 0$ for all $\chi \neq \chi_0$ and so the same can be said about $L(s,\chi)$ (by the fact that it is analytic).

It is now valid to take logs of both sides in the Euler product expansions for **each** χ (in a neighbourhood of $s = 1$, restricted to $\mathrm{Re}(s) > 1$ for absolute convergence):

$$\begin{aligned}\ln(L(s,\chi)) &= -\sum_{p\nmid m} \ln\left(1 - \frac{\chi(p)}{p^s}\right)\\ &= \sum_{p\nmid m} \frac{\chi(p)}{p^s} + A(s,\chi)\end{aligned}$$

where

$$A(s,\chi) = \sum_{p\nmid m}\sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}$$

Claim - For **each** χ we have that $A(s,\chi)$ is bounded in absolute value in a small enough neighbourhood of $s = 1$, hence converges to a finite limit as $s \to 1$.

We have already seen a similar result for the Riemann zeta function and the same proof will work here.

If $\mathrm{Re}(s) = \sigma$ then:

$$\left|\sum_{p\nmid m}\sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}\right| \leq \sum_{p\nmid m}\sum_{n\geq 2} \left|\frac{\chi(p)^n}{np^{ns}}\right| = \sum_{p\nmid m}\sum_{n\geq 2} \frac{1}{np^{n\sigma}}$$

and via a string of inequalities:

$$\begin{aligned}\sum_{p\nmid m}\sum_{n\geq 2}\frac{1}{np^{n\sigma}} &< \frac{1}{2}\sum_{p\nmid m}\sum_{n\geq 2}\frac{1}{p^{n\sigma}}\\ &= \frac{1}{2}\sum_{p\nmid m}\frac{p^{-2\sigma}}{1-p^{-\sigma}}\\ &< \frac{1}{2(1-\frac{1}{2})}\sum_{p\nmid m}p^{-2\sigma}\\ &= \sum_{p\nmid m}p^{-2\sigma},\end{aligned}$$

where the middle equality uses the geometric sum formula (which we can guarantee to converge if we take $\sigma > 0$, so that $0 < p^{-\sigma} < 1$).

Then the claim follows since:

$$\sum_{p\nmid m}p^{-2\sigma} < \sum_{n=1}^{\infty}n^{-2\sigma} = \zeta(2\sigma)$$

and this converges for any $\sigma > \frac{1}{2}$. Thus choosing some σ_0 such that $\frac{1}{2} < \sigma_0 < 1$ we see that for $\text{Re}(s) > \sigma_0$:

$$|A(s,\chi)| < \zeta(2\,\text{Re}(s)) < \zeta(2\sigma_0).$$

Hence we have the required boundedness in a neighbourhood of $s = 1$. □

Continuing with the proof we may now take the following linear combination of logs (working in a neighbourhood of $s = 1$, restricted to $\text{Re}(s) > 1$):

$$\sum_{\chi}\chi(a)^{-1}\ln(L(s,\chi)) = \sum_{\chi}\chi(a)^{-1}\left(\sum_{p\nmid m}\frac{\chi(p)}{p^s} + A(s,\chi)\right).$$

Now by Corollary 4.18 this becomes:

$$\sum_{\chi}\chi(a)^{-1}\ln(L(s,\chi)) = \phi(m)\sum_{p\equiv a \bmod m}\frac{1}{p^s} + \sum_{\chi}\chi(a)^{-1}A(s,\chi).$$

As $s \to 1$ the LHS diverges, due to the pole of $L(s,\chi_0)$ at $s = 1$ and all other L-series being convergent there (so not cancelling out the bad behaviour).

However the RHS gives:

$$\phi(m)\sum_{p\equiv a \bmod m}\frac{1}{p} + \sum_{\chi}\chi(a)^{-1}C_\chi$$

for some constants C_χ.

Hence $\sum_{p\equiv a \bmod m}\frac{1}{p}$ diverges as required. □