Lecture Notes in Analytic Number Theory

Lectures by Dr. Sheng-Chi Liu

Throughout these notes, □ signifies end proof, and ▲ signifies end of example.

Table of Contents

Table of Contents **i**

Lecture 1 Background and Introduction **1**
1.1 Basic questions 1
1.2 Landau's problems 1
1.3 Notation 2
1.4 Counting prime numbers 3

Lecture 2 Different proofs of the infinitude of primes **3**
2.1 Prime counting 3

Lecture 3 Chebyshev's idea continued **6**
3.1 Primes in factorials 6

Lecture 4 Lower bound of Chebyshev's theorem **9**
4.1 Chebyshev finalised 9
4.2 Averages of arithmetic functions 11

Lecture 5 Dirichlet convolution **12**
5.1 Approximation of average functions by integrals 12
5.2 Dirichlet convolution 14

Lecture 6 Möbius function **15**
6.1 More convoluting 15

Lecture 7 Möbius inversion formula **16**
7.1 Möbius inversion 16
7.2 Multiplicative functions 18

Lecture 8 Dirichlet series **19**
8.1 Multiplicativity of Möbius function 19
8.2 Dirichlet series 20

Notes by Jakob Streipel. Last updated July 29, 2019.

Lecture 9 L-functions of convolutions **22**
9.1 L-functions associated with Dirichlet convolutions 22
9.2 Dirichlet series and multiplicative functions 24

Lecture 10 Euler products **25**
10.1 L-series continued 25

Lecture 11 Primes in arithmetic progressions **28**
11.1 Arithmetic progressions 28

Lecture 12 Characters **29**
12.1 Analogue of Merten's theorem 29
12.2 Characters of finite abelian groups 29

Lecture 13 Fourier analysis on finite abelian groups **31**
13.1 Orthogonality of characters 31
13.2 Fourier analysis on finite abelian groups 32
13.3 Characters on cyclic groups 33
13.4 Dirichlet characters 33

Lecture 14 Dirichlet characters **33**
14.1 L-functions attached to Dirichlet characters 33

Lecture 15 Mertens' theorem for arithmetic progressions **36**
15.1 Proof finished 36
15.2 Dirichlet L-functions at 1 37

Lecture 16 Landau's lemma **38**
16.1 Landau's lemma 38

Lecture 17 Riemann's memoir **40**
17.1 Riemann's memoir 40
17.2 Review of Fourier analysis 41

Lecture 18 Poisson summation **42**
18.1 Fourier analysis 42

Lecture 19 The functional equation for $\zeta(s)$ **45**
19.1 Mellin transformation 45
19.2 Gamma function 46
19.3 The functional equation for $\zeta(s)$ 47

Lecture 20 The functional equation for L-functions **48**
20.1 Theta series 48
20.2 Trivial zeros of $\zeta(s)$ 49
20.3 Functional equations of L-functions 49
20.4 Gauss sums 50

Lecture 21 The functional equation for L-functions, continued **51**
21.1 Gauss sums 51

Lecture 22 Functions of finite order **54**
22.1 Proof concluded 54
22.2 The Hadamard factorisation theorem 55

Lecture 23 Jensen's formula **56**
23.1 Jensen's formula 56
23.2 Application of Jacobi's formula 58

Lecture 24 Hadamard factorisation theorem **59**
24.1 Hadamard factorisation 59

Lecture 25 The infinite product for $\zeta(s)$ **60**
25.1 Hadamard factorisation finished 60
25.2 The infinite product for $\zeta(s)$ and the explicit formula 61
25.3 Infinite product for $L(s,\chi)$ 62
25.4 Application to counting zeros of $\zeta(s)$ 62

Lecture 26 Counting zeros **63**
26.1 Application to counting zeros of $\zeta(s)$ 63
26.2 Applications to countinjg zeros of $L(s,\chi)$ 64

Lecture 27 Weil's explicit formula **66**
27.1 Application to counting zeros of $L(s,\chi)$ 66
27.2 Weil's explicit formula 67

Lecture 28 Weil's explicit formula **68**
28.1 Proof continued 68

Lecture 29 The theorem of Hadamard and de la Vallée-Poussin **70**
29.1 Zero free region 70

Lecture 30 Exceptional zeros **73**
30.1 Zero free region for $L(s,\chi)$ 73

Lecture 31 Landau's theorem **75**
31.1 Exceptional zeros 75
31.2 Siegel's theorem 77

Lecture 32 Siegel's theorem **78**
32.1 Proof 78

Lecture 33 The Prime number theorem in Arithmetic progressions **80**
33.1 Prime number theorem 80

Lecture 34 Bombieri-Vinogradov **82**
34.1 Prime number theorem in arithmetic progressions 82
34.2 The Bombieri-Vinogradov theorem 83

Lecture 35 Bombieri-Vinogradov, continued **85**
35.1 The trivial case 85
35.2 The nontrivial part 86

Lecture 36 The Large Sieve **87**
36.1 The Large siece inequality 87

Lecture 37 Vaughan's Identity **90**
37.1 Basic Mean Value Theorem, again 90

Lecture 1 Background and Introduction

Number theory is the study of numbers, a natural starting point of which is the study of the integers $\mathbb{Z}$. The integers are equipped with addition and multiplication—the opposite of addition, i.e. subtraction, doesn't move us out of the integers, but the opposite of multiplication, being division, does. Hence another type of numbers of great interest is the rational numbers $\mathbb{Q}$.

On the other hand, to understand the integers one can, seemingly, settle for understanding the ***prime numbers*** $\wp$, since with those we can build the integers.

We want to study these prime numbers which, despite being the simplest building blocks, turns out to be the hardest part of these sorts of questions.

1.1 Basic questions

It is true, and has been known for a *very* long time, that there are infinitely many primes (more on this soon).

With that in mind, there are a few basic questions we will ask—and answer—in this course.

1. How many primes are there up to some number x? In other words, how does
$$\pi(x) = \#\{\, p \in \wp \mid p \leq x \,\}$$
behave as a function of x?

   To answer this question precisely is very hard; there is essentially no option apart from simply counting one by one. On the other hand, answering this question approximately, in a very precise sense, is entirely doable! In particular, the asymptotic behavious of this quantity is known as the Prime number theorem, which we will endeavour to prove in this course.

2. How many primes are there in a given arithmetic progression? That is to say, given $a, n > 0$ with $(a, n) = 1$, how does
$$\pi(x; a, n) = \#\{\, \wp \ni p \leq x \mid p \equiv a \pmod{n} \,\}$$
behave? This is a much tougher question. That $\pi(x; a, n)$ is infinite is Dirichlet's theorem. This, as well as understanding how this grows asymptotically in x, is the second goal of this course.

1.2 Landau's problems

At the 1912 International Congress of Mathematicians, Edmund Landau listed four basic problems about prime numbers. All four of these remain unsolved to this day. Listing them demonstrates how easy some of the fundamental problems in number theory are to understand, and yet how inconceivably hard they are to solve.

1. Goldbach's conjecture: Can every even integer greater than 2 be written as the sum of two primes?

Date: January 7th, 2019.

2. Twin prime conjecture: Are thjere infinitely many primes p such that $p+2$ is prime?

3. Legendre's conjecture: Does there always exist at least one prime between consecutive perfect squares?

4. Are there infinitely many primes p such that $p-1$ is a perfect square? In other words, are there infinitely many primes of the form n^2+1?

We'll give some brief information about the current state and progress on these. The biggest step toward the Goldbach conjecture is due to Chen, who proves that for n sufficiently large, we can write $2n = p + q$ where q is either prime or the product of two primes.

There is also a weaker version of the Goldbach conjecture, naturally known as the Weak Goldbach conjecture. This states that every odd number greater than 5 can be written as the sum of three primes. This was proved by Vinogradov and Helfgott.

The Twin prime conjecture is on similar grounds as Goldbach's conjecture: the best known is by Chen, proving that there are infinitely many primes p such that $p+2$ is either a prime or a product of two primes.

A related sort of problem, in a different direction, is asking about gaps between primes. In particular, are there infinitely many prime pairs with a bounded gap M, i.e. is

$$\$\{\,(p,q) \in \wp \times \wp \mid 0 < |p-q| \leq M\,\} = \infty?$$

There has recently been tremendous progress in this problem. Some foundational results are due to Goldston–Pintz–Y1ld1r1m. Recently it was proven for $M = 70$ million by Yitang Zhang, and shortly thereafter a very similar result was proven by Maynard using a completely different method. The gap has since been reduced to $M = 246$ by the Polymath Project, led by Tao. Under the assumption of the Elliot-Halberstam conjecture, M has been reduced to 6.

The closest known result to Legendre's conjecture is due to Ingham, proving that there is a prime between n^3 and $(n+1)^3$ for every sufficiently large n.

Finally, the best result on the road to the fourth of Landau's problems is due to Iwaniec, proving that there are infinitely many $n \in \mathbb{Z}$ such that n^2+1 is a prime or a product of two primes.

1.3 Notation

We will use following notation when discussion asymptotic behaviour over and over. Let $f(x)$ and $g(x)$ be two functions on $\mathbb{R}$, with $g(x) \neq 0$ for sufficiently large x.

We write $f \sim g$ to mean that

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

i.e. the values of the two functions are the same as x grows.

We write $f(x) = O(g(x))$, or $f(x) \ll g(x)$, to mean that $|f(x)| \leq Cg(x)$ for some constant C and all $x \in \mathbb{R}$, i.e. f is bounded by g (with some constant).

Finally we write $f(x) = o(g(x))$ meaning that for any $\varepsilon > 0$ there exists a constant $N > 0$ such that $|f(x)| \leq \varepsilon |g(x)|$ for all $x \geq N$, or in other words $g(x)$ is *much* bigger than $f(x)$. We might also put it as

$$\lim_{x \to \infty} \frac{|f(x)|}{|g(x)|} = 0.$$

1.4 Counting prime numbers

As claimed earlier, it is a fact that

Theorem 1.4.1. *There are infinitely many prime numbers.*

There are are *many* known proofs of this. The oldest among them is due to Euclid:

Proof. Suppose there aren't infinitely many primes, meaning that there are finitely many of them, say $p_1, p_2, \ldots, p_n$. Now consider the number $m = p_1 p_2 \cdots p_n + 1$.

This number is not divisible by p_i for any i, since its remainder is always 1. Hence $m = p_1 p_2 \cdots p_n + 1$ does not have a prime factor p_i, which is a contradiction. □

This is a very elegant proof. Indeed, it is *too* elegant, because it doesn't tell us anything more!

Lecture 2 Different proofs of the infinitude of primes

2.1 Prime counting

Define the ***prime counting function***

$$\pi(x) = \#\{\, p \in \wp \mid p \leq x \,\} = \sum_{p \leq x} 1,$$

where when indexing a sum over p we mean that it sums only over prime numbers.

The above theorem therefore says that $\pi(x) \to \infty$ as $x \to \infty$. A natural question is then at what rate this goes to infinity.

Gauss (about 1792, around age 15) and Legendre (1798) gave a conjectural asymptotic formula for $\pi(x)$. It was proved by Hadamard and de la Vallée-Poissin independently in 1896, known as

Theorem 2.1.1 (Prime number theorem)**.** *As $x \to \infty$, we have*

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

Date: January 9th, 2019.

Remark 2.1.2. In the 1830's, Dirichlet reformulated the (then) Prime number conjecture as

$$\pi(x) \sim \mathrm{Li}(x) \coloneqq \int_2^x \frac{dt}{\log(t)}.$$

Note that using integration by parts,

$$\begin{aligned}\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} = \frac{t}{\log(t)}\bigg|_2^x - \int_2^x -\frac{t}{t\log(t)^2}\,dt = \frac{x}{\log(x)} + \int_2^x \frac{1}{\log(t)^2}\,dt + O(1)\\ = \frac{x}{\log(x)} + \frac{x}{\log(x)^2} + \int_2^x \frac{1}{\log(t)^2}\,dt + O(1) = \frac{x}{\log(x)} + \frac{x}{\log(x)^2} + O\left(\frac{x}{\log(x)^3}\right)\end{aligned}$$

and so forth, whence $\mathrm{Li}(x) \sim x/\log(x)$.

Remark 2.1.3. The proof of the Prime number theorem actually gives

$$\pi(x) = \mathrm{Li}(x) + O(x\exp(-C\sqrt{\log(x)}))$$

for some constant $C > 0$.

Additionally, assuming the Riemann hypothesis we get substantial power savings, namely

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2}\log(x)^2).$$

Let us now prove the infinitude of the primes again, but this time with a very different method, courtesy of Euler.

Define the (Riemann) zeta function

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

As a historical anectode, this is named after Riemann despite Euler considering it before Riemann was around because Euler did it only for $s \in \mathbb{R}$, $s > 1$, whereas Riemann considered it for all of $\mathbb{C}$, continued it analytically and found a functional equation for it.

Consider similarly for each prime p the sum

$$\zeta_p(s) = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots = \sum_{\alpha \geq 0} \frac{1}{p^{\alpha s}} = (1 - p^{-s})^{-1}$$

since it's a geometric series, again assuming $s > 1$.

Now by the unique factorisation of integers into primes,

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

called the ***Euler product*** of $\zeta(s)$.

Now by considering the sum for $\zeta(s)$ above as a Riemann sum for the integral of $1/x^2$, we have

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

whereby as $s \to 1^+$, $\zeta(s) \to \infty$.

Now if we suppose there are only finitely many primes, then

$$\lim_{s\to 1^+}\zeta(s)=\lim_{s\to 1^+}\prod_p(1-p^{-s})^{-1}=\prod_p(1-p^{-1})^{-1},$$

is finite, which is a contradiction. Hence there are infinitely many primes.

Now suppose we want to play this same game, but instead of counting the primes all with weight 1, count them with weight $1/p$.

Theorem 2.1.4 (Euler)**.** *The sum* $\sum_p \frac{1}{p}$ *diverges.*

Proof. For $s>1$,

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

Recalling the Taylor expansion of

$$\log(1-x)=-\big(x+\frac{x^2}{2}+\frac{x^3}{3}+\dots\big)$$

(which is easy to see as the integral of $1/(1-x)=1+x+x^2+\dots$), we have

$$\log\zeta(s)=\sum_p\Big(\frac{1}{p^s}+O\Big(\frac{1}{p^{2s}}\Big)\Big).$$

On the other hand

$$\log\zeta(s)\geq\log\frac{1}{s-1}=-\log(s-1),$$

whence

$$\sum_p(p^{-s}+O(p^{-2s}))\geq-\log(s-1)$$

which goes to ∞ as $s\to 1^+$, so

$$\sum_p\frac{1}{p}+O(1)=\infty.$$ □

A more interesting question, which we will answer later, is what the asymptotic behaviour of

$$\sum_{p\leq x}\frac{1}{p}.$$

Another approach is due to Chebyshev (1850),

Theorem 2.1.5. *There exist constants* $0<c_1<c_2$ *such that for* $x\geq 2$

$$c_1\frac{x}{\log(x)}\leq\pi(x)\leq c_2\frac{x}{\log(x)}.$$

To prove this we need a bit of groundwork.

Definition 2.1.6 (p-adic valuation)**.** Let p be a prime. For $n \in \mathbb{Z} \setminus \{0\}$ define the ***p-adic valuation*** $\nu_p(n)$ to be the largest integer $\alpha \geq 0$ such that $p^\alpha \mid n$ (i.e. $p^{\alpha+1} \nmid n$).

Moreover we define $\nu_p(0) = +\infty$.

Hence by factoring into prime factors, for any n we have

$$n = \prod_p p^{\nu_p(n)}.$$

Note also that $\nu_p(mn) = \nu_p(m) + \nu_p(n)$ for all $m, n \in \mathbb{Z}$.

Chebyshev's idea is based on the property that $n!$ is divisible by all the primes less than or equal to n, and not by any other primes. We then have

$$n! = \prod_{p \leq n} p^{\nu_p(n!)},$$

which when taking logarithms becomes

$$\log(n!) = \sum_{p \leq n} \nu_p(n!) \log p,$$

but on the other hand

$$\log(n!) = \sum_{k=1}^{n} \log k = n \log n - n + O(\log n).$$

Lecture 3 Chebyshev's idea continued

3.1 Primes in factorials

Continuing the calculations above, we need to get a sense of how $\nu_p(n!)$ behaves. To this end, note that by definition

$$\nu_p(k) = \max\{\, \alpha \mid p^\alpha \mid k \,\} = \sum_{\substack{\alpha \geq 1 \\ p^\alpha \mid k}} 1,$$

which means that

$$\nu_p(n!) = \sum_{k=1}^{n} \nu_p(k) = \sum_{k=1}^{n} \sum_{\substack{\alpha \geq 1 \\ p^\alpha \mid k}} 1.$$

By switching the order of summation we get

$$\nu_p(n!) = \sum_{\alpha \geq 1} \sum_{\substack{1 \leq k \leq n \\ p^\alpha \mid k}} 1 = \sum_{\alpha \geq 1} \left\lfloor \frac{n}{p^\alpha} \right\rfloor.$$

By $\lfloor x \rfloor$ we mean the largest integer less than or equal to x, or alternatively $\lfloor x \rfloor = x - \{x\}$ where $\{x\}$ is the fractional part of x. Crucial for our purposes is that $\lfloor x \rfloor \leq x$, so

$$\nu_p(n!) \leq \sum_{\alpha \geq 1} \frac{n}{p^\alpha} = \frac{n}{p(1 - p^{-1})} = \frac{n}{p} + O\left(\frac{n}{p^2}\right)$$

Date: January 11th, 2019.

since $1/(1-p^{-1}) = 1 + 1/p + O(1/p^2)$.

Hence

$$\sum_{p\le n} \nu_p(n!)\log p \le \sum_{n\le p} \log p \left(\frac{n}{p} + O\left(\frac{n}{p^2}\right)\right) = n\sum_{p\le n}\frac{\log p}{p} + O\left(n\sum_{p\le n}\frac{\log p}{p^2}\right).$$

Note that the sum in the error term is bounded by the same sum over all $k \le n$ instead of $p \le n$, which is the Riemann sum of a convergent integral, so the error term is $O(n)$.

Combining our estimates we therefore have

$$n\log n - n + O(\log n) \le n\sum_{p\le n}\frac{\log p}{p} + O(n),$$

and dividing by n gives us

$$\sum_{p\le n}\frac{\log p}{p} \ge \log n - 1 + O(1),$$

the right-hand side of which goes to ∞ as $n \to \infty$. Hence there are infinitely many primes.

We're now ready to start proving Chebyshev's theorem:

Proof. We start with the upper bound. First let us split $\pi(x)$ into two sums:

$$\pi(x) = \sum_{p\le x} 1 = \sum_{p\le x^{1/2}} 1 + \sum_{x^{1/2}<p\le x} 1.$$

The first of these sums is trivially bounded by $x^{1/2}$. For the second one, note that

$$\sum_{x^{1/2}<p\le x} 1 \le \frac{1}{\log(x^{1/2})}\sum_{x^{1/2}<p\le x}\log p$$

since this way each term in the summand is at least 1. We will denote by $\vartheta(x)$

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

so that

$$\frac{1}{\log(x^{1/2})}\sum_{x^{1/2}<p\le x}\log p = \frac{1}{\log(x^{1/2})}\left(\vartheta(x) - \vartheta(x^{1/2})\right).$$

The very clever idea of Chebyshev's is to consider the binomial coefficient

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

Taking logarithms we have

$$\begin{aligned}\log\binom{2n}{n} &= \log((2n)!) - 2\log(n!) = \sum_{k=1}^{2n}\log k - 2\sum_{k=1}^{n}\log k\\ &= (2n)\log(2n) - 2n + O(\log(2n)) - 2(n\log n - n + O(\log n))\\ &= (\log 2)2n + O(\log(2n)).\end{aligned}$$

On the other hand, by the Binomial theorem,

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

so that $\binom{2n}{n} < 2^{2n}$, meaning that $\log \binom{2n}{n} < (\log 2)2n$.

It is also true that, by the same sort of argument as we used above, $\binom{2n}{n}$ is divisible by primes in $(n, 2n]$. Hence

$$\log \binom{2n}{n} = \sum_{p \le 2n} \nu_p \left(\binom{2n}{n} \right) \log p \ge \sum_{n < p \le 2n} \log p = \vartheta(2n) - \vartheta(n) < (\log 2)2n,$$

whereby $\vartheta(2n) - \vartheta(n) < (\log 2)2n$.

Next, $\vartheta(x) - \vartheta(x/2) \le (\log 2)x$ for $x \ge 2$ being real. To see this, for a given $x \ge 2$ take n to be the integer such that $0 \le x - 2n < 2$, i.e. the biggest even integer less than x. Then $0 \le \vartheta(x) - \vartheta(2n) \le \log x$, and

$$0 \le \vartheta(x) - \vartheta(x/2) - (\vartheta(2n) - \vartheta(n)) \le \log x,$$

wherein we bound the parenthesis by $(\log 2)2n < (\log 2)x$, so

$$\vartheta(x) - \vartheta(x/2) \le (\log 2)x + O(\log x).$$

With this in mind, let us write $\vartheta(x)$ as a telescoping sum:

$$\begin{aligned}
\vartheta(x) &= \sum_{0 \le k \le \left\lfloor \frac{\log x}{\log 2} \right\rfloor} \vartheta\left(\frac{x}{2^k}\right) - \vartheta\left(\frac{x}{2^{k+1}}\right) \\
&\le \sum_{0 \le k \le \left\lfloor \frac{\log x}{\log 2} \right\rfloor} \left((\log 2)\frac{x}{2^k} + O(\log(x/2^k)) \right) \\
&= 2x \log 2 + O((\log x)^2),
\end{aligned}$$

since the last sum is geometric.

Returning to $\pi(x)$, with this in hand we get

$$\begin{aligned}
\pi(x) &= \sum_{p \le x^{1/2}} 1 + \sum_{x^{1/2} < p \le x} 1 \le x^{1/2} + \frac{1}{\log(x^{1/2})} \sum_{x^{1/2} < p \le x} \log p \\
&\le x^{1/2} + \frac{2}{\log x}(\vartheta(x) - \vartheta(x^{1/2})) \\
&\le x^{1/2} + \frac{2}{\log 2}\left(2(\log 2)x + O((\log x)^2) + O(x^{1/2}) \right) \\
&= 4 \log 2 \frac{x}{\log x} + O(x^{1/2}).
\end{aligned}$$

Hence we can take c_2 large enough that $\pi(x) \le c_2 x / \log x$. It also establishes that $\vartheta(x) \le cx$ for some c.

It is important and interesting to note that this does not tighten to $c_2 = 1$, meaning that Chebyshev's argument is not sufficient to prove the Prime number theorem. □

Lecture 4 Lower bound of Chebyshev's theorem

4.1 Chebyshev finalised

To get a lower bound for Chebyshev's theorem we need a more precise estimate for $\nu_p(\binom{2n}{n})$. Recall how

$$\begin{aligned}\nu_p\left(\binom{2n}{n}\right) &= \nu_p((2n)!) - 2\nu_p(n!) = \sum_{k=1}^{2n}\nu_p(k) - 2\sum_{k=1}^{n}\nu_p(k)\\ &= \sum_{\alpha\geq 1}\left\lfloor\frac{2n}{p^\alpha}\right\rfloor - 2\sum_{\alpha\geq 1}\left\lfloor\frac{n}{p^\alpha}\right\rfloor = \sum_{\alpha\geq 1}\left(\left\lfloor\frac{2n}{p^\alpha}\right\rfloor - 2\left\lfloor\frac{n}{p^\alpha}\right\rfloor\right)\\ &= \sum_{1\leq\alpha\leq\frac{\log 2n}{\log p}}\beta\left(\frac{n}{p^\alpha}\right).\end{aligned}$$

Here we mean

$$\beta(x) = \lfloor 2x\rfloor - 2\lfloor x\rfloor = \begin{cases}1, & \text{if } \{x\}\in[1/2,1)\\ 0, & \text{if } \{x\}\in[0,1/2)\end{cases}$$

and the range of summation can be cut off at $\log(2n)/\log(p)$ since overwise the integer parts above are 0 anyway.

The trivial upper bound here is $\log(2n)/\log p$, naturally, since $\beta(x)\leq 1$.

Now recall

$$\log\binom{2n}{n} = \sum_{p\leq 2n}\nu_p\left(\binom{2n}{n}\right)\log p \leq \sum_{p\leq 2n}\log p\frac{\log 2n}{\log p} = (\log 2n)\pi(2n).$$

On the other hand,

$$\begin{aligned}\log\binom{2n}{n} &= \log((2n)!) - 2\log(n!) = \sum_{k=1}^{2n}\log k - 2\sum_{k=1}^{n}\log k\\ &= 2n\log(2n) - 2n + O(\log 2n) - 2(n\log n - n + O(\log n)),\end{aligned}$$

hence

$$\pi(2n)\geq(\log 2)\frac{2n}{\log n} + O(1),$$

and so for $x\geq 2$,

$$\pi(x)\geq(\log 2)\frac{x}{\log x}\left(1 + O\left(\frac{\log x}{x}\right)\right).$$

Ergo there exists some sufficiently large c_1 so that $\pi(x)\geq c_1 x/\log x$.

Date: January 14th, 2019.

We can also extract from this a lower bound for $\vartheta(x)$:

$$\begin{aligned}\vartheta(x) = \sum_{p\le x} \log p &= \sum_{p\le x^{1/2}} \log p + \sum_{x^{1/2}<p\le x} \log p \\ &\ge \log 2 + \pi(x^{1/2}) + \log(x^{1/2})\left(\pi(x) - \pi(x^{1/2})\right) \\ &\ge \log 2 + c\frac{x^{1/2}}{\log x^{1/2}} + c\log(x^{1/2})\left(\frac{x}{\log x} - \frac{x^{1/2}}{\log x^{1/2}}\right) \\ &\ge cx + O(x^{1/2}).\end{aligned}$$

Hence there exists some sufficiently large c' such that $\vartheta(x) \ge c'x$.

Theorem 4.1.1 (Mertens)**.** $\displaystyle\sum_{p\le x} \frac{\log p}{p} = \log x + o(1)$.

This result is, maybe surprisingly much easier than the Prime number theorem, even though it would seem that counting the primes with the strange weight $\log p/p$ would be harder than weight 1.

Proof. We have

$$\log n! = \sum_{k=1}^{n} \log k = n\log n - n + O(\log n),$$

but on the other hand

$$\log n! = \sum_{p\le n} \log p \sum_{\substack{\alpha\ge 1 \\ p^\alpha \le n}} \left\lfloor \frac{n}{p^\alpha} \right\rfloor.$$

The main term here comes from $\alpha = 1$, since for $\alpha \ge 2$ we have

$$\sum_{p\le n} \log p \sum_{\substack{\alpha\ge 2 \\ p^\alpha \le n}} \left\lfloor \frac{n}{p^\alpha} \right\rfloor \le \sum_{p\le n} \log p \sum_{\substack{\alpha\ge 2 \\ p^\alpha \le n}} \frac{n}{p^\alpha} \le n\sum_{p} \frac{\log p}{p^2} = O(n)$$

where for the last inequality we notice that the inner sum is $n/(p^2(1-1/p))$ since it's geometric.

Moreover $\frac{x}{=} x + \{x\}$, so

$$\begin{aligned}\sum_{p\le n} \log p \left\lfloor \frac{n}{p} \right\rfloor + O(n) &= \sum_{p\le n} \log p \left(\frac{n}{p} + O(1)\right) + O(n) \\ &= n\sum_{p\le n} \frac{\log p}{p} + O\Big(\sum_{p\le n} \log p\Big) + O(n).\end{aligned}$$

But the error term is $\vartheta(n)$, which is order n, so this is

$$n\sum_{p\le n} \frac{\log p}{p} + O(N),$$

and dividing through by n gives us what we want. □

4.2 Averages of arithmetic functions

Definition 4.2.1. An ***arithmetic function*** is a real or complex valued function on $\mathbb{N}$, i.e. $f\colon \mathbb{N} \to \mathbb{R}$ or $\mathbb{C}$.

Example 4.2.2. The constant function $1(n) = 1$ for all $n \in \mathbb{N}$ is an arithmetic function. The ***delta function*** (at 1),

$$\delta(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n \neq 1 \end{cases}$$

is another one we'll use.

Of particular interest is the characteristic function of the primes,

$$1_{\wp}(n) = \begin{cases} 1, & \text{if } n \in \wp \\ 0, & \text{if } n \notin \wp. \end{cases}$$

A final one we'll have occasion to play with is the ***von Mangoldt function***

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^{\alpha}, \alpha \geq 1 \\ 0, & \text{if } n \neq p^{\alpha}. \end{cases}$$ ▲

Definition 4.2.3. Let f be an arithmetic function. The ***average function*** $M_f(X)$ of f is the function defined on $\mathbb{R}_{\geq 0}$ by

$$M_f(X) = \sum_{1 \leq n \leq X} f(n).$$

Note that this is not quite the usual arithmetic average; for that we'd divide by X. However if we know the behaviour of one, we automatically get the behaviour of the other, so there is no need to complicate things further by that extra division.

The main question we ask ourselves about such things is what, given an arithmetic function f, the behaviour of $M_f(X)$ is as $X \to \infty$.

Example 4.2.4. Some of the functions we're used to are averages of arithmetic functions. For instance, $\pi(x) = M_{1_{\wp}}(x)$. Similarly $\vartheta(x) = M_f(x)$ where $f(n) = \log(n) 1_{\wp}(n)$.

Another function we will have reason to care about is

$$\psi(x) = M_{\Lambda}(x) = \sum_{p^{\alpha} \leq x} \log p.$$ ▲

All of these three are closely related in the problem of counting primes. Indeed we would, and should, suspect that ϑ and ψ are close to one another, since one is counting primes with weight $\log p$ and the other is counting prime powers with the same weight. Indeed

Proposition 4.2.5. *We have* $\psi(x) = \vartheta(x) + O(x^{1/2} \log x)$.

Hence by Chebyshev's theorem, $\psi(x) \asymp \vartheta(x) \asymp x$, by which we mean that they are the same order.

Proof. We write

$$\psi(x) = \vartheta(x) + \sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} \log p$$

So

$$\sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} \log p = \sum_{p \le x^{1/2}} \log p \left(\sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} 1 \right)$$

where the inside is bounded by $\log x / \log p$, so

$$\le \sum_{p \le x^{1/2}} \log p \frac{\log x}{\log p} = O(\log(x) x^{1/2}),$$

where we've used the weaker bound; Chebyshev could give us something tighter. □

Lecture 5 Dirichlet convolution

5.1 Approximation of average functions by integrals

In the special case where $f \colon \mathbb{R} \to \mathbb{R}$, the average $M_f(X)$ is just a restriction to $\mathbb{N}$, so we want to compare

$$\sum_{n \le x} f(n) \sim \int_1^x f(t)\, dt.$$

Proposition 5.1.1 (Monotone comparison)**.** *Let $f \colon \mathbb{R}_{\ge 0} \to \mathbb{R}$ be continuous. Suppose f is monotone. Then we have*

$$M_f(X) = \int_1^X f(t)\, dt + O(|f(1)| + |f(X)|).$$

Proof. Suppose f is monotonically increasing. For $n \ge 2$, we have

$$\int_{n-1}^n f(t)\, dt \le f(n) \le \int_n^{n+1} f(t)\, dt.$$

Summing this over $2 \le n \le \lfloor X \rfloor$, we are done.

If f is monotonically decreasing we do precisely the same, except the inequalities above are reversed. □

Example 5.1.2. Take $f(x) = \log x$, and this immediately gives us

$$\sum_{n \le x} \log n = \int_1^X \log t\, dt + O(|\log 1| + |\log X|) = X \log X - X + O(\log X)$$

with a little bit of integration by parts thrown in. ▲

Date: January 16th, 2019.

Theorem 5.1.3 (Integration by parts)**.** *Let g be an arithmetic function and let f be a continuously differentiable function on $[1, X]$. Then*

$$M_{fg}(X) = \sum_{n\leq x} f(n)g(n) = f(X)M_g(X) - \int_1^X M_g(t)f'(t)\,dt.$$

Proof. By using integration by parts with Riemann-Stieltjes integrals,

$$\begin{aligned}\sum_{n\leq x} f(n)g(n) &= \int_{1^-}^X f(t)\,dM_g(t) = f(t)M_g(t)\Big|_{1^-}^X - \int_{1^-}^X f'(t)M_g(t)\,dt \\ &= f(X)M_g(X) - \int_{1^-}^X M_g(t)f'(t)\,dt.\end{aligned}$$

□

Proposition 5.1.4. *(i)* $\vartheta(x) = (\log x)\pi(x) + O\left(\dfrac{x}{\log x}\right)$.

(ii) $\pi(x) \sim \dfrac{x}{\log x}$ *if and only if* $\vartheta(x) \sim x$ *if and only if* $\psi(x) \sim x$.

Proof. *(i)* Writing

$$\vartheta(x) = \sum_{p\leq x} \log p = \sum_{n\leq x} \log n 1_{\wp}(n)$$

and then using the above, we get

$$\vartheta(x) = (\log x)\pi(x) - \int_1^x \pi(t)(t)\,dt,$$

and by Chebyshev's theorem

$$\int_1^x \frac{\pi(t)}{t}\,dt \leq C\int_1^x \frac{1}{t}\frac{t}{\log t}\,dt = O\left(\frac{x}{\log x}\right).$$

(ii) The first equivalence follows directly from the above, and the second equivalence we have proved before, namely Proposition 4.2.5. □

Remark 5.1.5. Both Hadamard's and de la Vallée-Poussin's theorems of the Prime number theorem actually proved $\psi(x) \sim x$.

Corollary 5.1.6 (Euler-Maclaurin formula)**.** *Let f be a C^1 function on $(0, \infty)$. Let $B_1(x) = x - \lfloor x\rfloor - 1/2 = \{x\} - 1/2$. For $x > 1$, we have*

$$M_f(X) = \sum_{n\leq X} f(n) = \int_1^X f(t)\,dt + \int_1^X B_1(t)f'(t)\,dt - B_1(1)f(1) - B_1(X)f(X).$$

In particular

$$\left|M_f(X) - \int_1^X f(t)\,dt\right| \leq \int_1^X |f'(t)|\,dt + |f(1)| + |f(X)|.$$

Proof. Use summation by parts with $g(n) = 1$ and $M_g(t) = \lfloor t\rfloor$. □

Remark 5.1.7. This formula does not require f to be monotone.

Remark 5.1.8. The function $B_1(x)$ is called the ***first Bernoulli function*** and $B_1 \coloneqq B_1(0)$ is the ***first Bernoulli number***.

5.2 Dirichlet convolution

Definition 5.2.1 (Dirichlet convolution)**.** Let f and g be arithmetic functions. Define the ***Dirichlet convolution*** $f \star g$ by

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

Proposition 5.2.2. *Dirichlet convlution*

(*i*) *is commutative,* $f \star g = g \star f$*;*

(*ii*) *is associative,* $(f \star g) \star h = f \star (g \star h)$*;*

(*iii*) *has an identity, namely the function* $\delta(n)$ *which is* 1 *if* $n = 1$ *and* 0 *otherwise;*

(*iv*) *sometimes has inverses. Specifically* f *is invertible under* $\star$*, i.e. there exists some* g *such that* $f \star g = \delta$*, if and only if* $f(1) \neq 0$*, in which case its* $\star$*-inverse* g *is determined by the recurrence relation* $g(1) = 1/f(1)$*,*

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

Proof. (*i*) This follows directly by definition. If we switch f and g, the order of summation is reversed, but the summands are the same.

(*ii*) We compute

$$(f \star g) \star h(n) = \sum_{ab=n} (f \star g)(a) h(b) = \sum_{ab=n} \sum_{cd=a} f(c)g(d)h(b) = \sum_{bcd=n} f(c)g(d)h(b).$$

Doing precisely the same thing to $f \star (g \star h)(n)$ we get the same sum, whence the two are equal for all n and so equal as functions.

(*iii*) Note that $f \star \delta(n)$ is the sum of $f(d)\delta(n/d)$, but $\delta(n/d) = 1$ onlt if $n/d = 1$, i.e. $d = n$, so $f \star \delta(n) = f(n)$ for all n.

(*iv*) For the forward direction, suppose f is $\star$-invertible. Then $f \star g = \delta$ for some g, and evaluating this at $n = 1$ we get $f \star g(1) = \delta(1) = 1$. Moreover

$$f \star g(1) = \sum_{d|1} f(d) g\left(\frac{1}{d}\right) = f(1)g(1),$$

so we have $f(1)g(1) = 1$, which has a solution $g(1)$ if and only if $f(1) \neq 0$.

For the converse direction, suppose $f(1) \neq 0$. Let us solve the equation $f \star g = \delta$ for g. First $f(1)g(1) = 1$, by the above, so $g(1) = 1/f(1)$. For $n > 1$,

$$0 = \delta(n) = f \star g(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = f(1)g(n) + \sum_{\substack{d|n \\ d>1}} f(d) g\left(\frac{n}{d}\right).$$

Solving this for $g(n)$ gives us the recurrence we want. □

Remark 5.2.3. Since $n/d < n$ for $d > 1$, $g(n)$ is completely determined by $f(1), f(2), \dots, f(n)$ and $g(1), \dots, g(\lfloor n/2 \rfloor)$.

Example 5.2.4. We define

$$d(n) \coloneqq 1 \star 1(n) = \sum_{d|n} 1,$$

which counts the number of (positive) divisors of n. Similarly

$$d_3(n) \coloneqq 1 \star 1 \star 1(n) = \sum_{abc=n} 1$$

is the number of representations of n as a product of 3 positive integers. In general,

$$d_k(n) \coloneqq \underbrace{1 \star 1 \star \cdots \star 1}_{k \text{ times}}(n) = \sum_{a_1 a_2 \cdots a_k = n} 1$$

is the number of representations of n as a product of k positive integers. ▲

Lecture 6 Möbius function

6.1 More convoluting

Proposition 6.1.1. *We have* $\log n = \Lambda \star 1(n)$*, i.e.*

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

Since $\Lambda(n)$ is multiplicative, which we will explore more later, this very neatly translates log into a multiplicative function.

Proof. Write n as its prime factorisation

$$n = \prod_p p^{\alpha_p},$$

and take logarithms, giving

$$\log n = \sum_p \alpha_p \log p = \sum_p \log p \Big(\sum_{p^\alpha | n}^{\alpha} 1 \Big) = \sum_{p^\alpha | n} \log p = \sum_{d|n} \Lambda(d). \qquad \square$$

Definition 6.1.2 (Möbius function)**.** The ***Möbius function*** μ is defined as the $\star$-inverse of 1, i.e. $\mu(1) = 1$ and

$$\mu(n) = -\sum_{\substack{d|n \\ d>1}} \mu\left(\frac{n}{d}\right).$$

We will show later that this does in fact coincide with the definition of μ commonly found in elementary number theory texts, namely

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square free} \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \ p_i \text{ all distinct primes} \\ 1 & \text{if } n = 1. \end{cases}$$

Date: January 18th, 2019.

Lecture 7 Möbius inversion formula

7.1 Möbius inversion

Recall that μ is the $\star$ inverse of 1, i.e. $\mu \star 1 = \delta$.

Theorem 7.1.1 (Möbius inversion formula)**.** *Let f and g be arithmetic functions. Then the following identities are equivalent*

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

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

Proof. Note that the first property says that $f = g \star 1$, and the second says $g = f \star \mu$. With this in mind the proof is obvious: $f = g \star 1$ if and only if $f \star \mu = g \star 1 \star \mu$ if and only if $f \star \mu = g \star \delta = g$. □

Example 7.1.2. In Proposition 6.1.1 we showed that

$$\log n = \sum_{d|n} \Lambda(d),$$

i.e. $\log n = \Lambda \star 1(n)$. This is equivalent to

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

We can use this to count primes:

Theorem 7.1.3 (Mertens)**.** (i) $\sum_{n\le x} \frac{\Lambda(n)}{n} = \log x + O(1)$.

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

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

Proof. We write

$$\sum_{n\le x} \frac{\Lambda(n)}{n} = \sum_{p\le x} \frac{\log p}{p} \sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} \frac{\log p}{p^\alpha}.$$

Now

$$\sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} \frac{\log p}{p^\alpha} = \sum_{p\le x^{1/2}} \log p \sum_{2\le \alpha \le \frac{\log x}{\log p}} \frac{1}{p^\alpha},$$

Date: January 23rd, 2019.

where the innermost sum is bounded by $1/(p^2(1-p^{-1}))$, where the geometric term is bounded, whence this is

$$\sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} \frac{\log p}{p^\alpha} \ll \sum_{p \le x^{1/2}} \frac{\log p}{p^2} = O(1).$$

Hence the first two assertions are equivalent, and we have proved the second in Theorem 4.1.1.

We'll give a direct proof of the first statement as well. Let us compute

$$\sum_{n \le x} \log n$$

in two different ways. First, we know from before that it is $x \log x + O(x)$. On the other hand,

$$\begin{aligned}\sum_{n \le x} \log n &= \sum_{n \le x} \sum_{d \mid n} \Lambda(d) = \sum_{d \le x} \Lambda(d) \sum_{n \le \lfloor x/d \rfloor} 1 \\ &= \sum_{d \le x} \Lambda(d) \frac{x}{d} + O\left(\sum_{d \le x} \Lambda(d) \cdot 1 \right) = x \sum_{d \le x} \frac{\Lambda(d)}{d} + O(x),\end{aligned}$$

since $0 \le x/d - \lfloor x/d \rfloor < 1$ and the remainder is by Chebyshev.

Combining these we see that

$$x \sum_{d \le x} \frac{\Lambda(x)}{d} + O(x) = x \log x + O(x),$$

which when dividing by x gives us

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

Finally, for the last statement, let $f(t) = 1/\log t$ and

$$g(n) = \begin{cases} \frac{\log p}{p} & \text{if } n = p \text{ prime} \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\begin{aligned}\sum_{p \le x} \frac{1}{p} = \sum_{n \le x} f(n)g(n) &= \int_{2^-}^{x} f(t)\, dM_g(t) = f(t)M_g(t)\Big|_{2^-}^{x} - \int_{2^-}^{x} f'(t)M_g(t)\, dt \\ &= \frac{1}{\log x}(\log x + O(1)) + O(1) + \int_{2^-}^{x} \frac{1}{t(\log t)^2}(\log t + O(1))\, dt \\ &= O(1) + \int_{2^-}^{x} \frac{1}{t \log t}\, dt + O\left(\int_{2^-}^{x} \frac{1}{t(\log t)^2}\, dt \right) \\ &= \log\log x + O(1),\end{aligned}$$

since the second integral is bounded. □

7.2 Multiplicative functions

Definition 7.2.1. A nonzero arithmetic function f is called ***multiplicative*** if, for $(m, n) = 1$, we have

$$f(mn) = f(m)f(n).$$

Moreover f is called ***completely multiplicative*** if $f(mn) = f(m)f(n)$ for all m and n.

Hence if we write $n = \prod p^{\alpha_p}$, for a multiplicative function f,

$$f(n) = \prod_p f(p^{\alpha_p}),$$

so f is completely determined by its value on prime powers. Similarly, for a completely multiplicative function f,

$$f(n) = \prod_p f(p)^{\alpha_p},$$

meaning that f is completely determined by its value on primes.

Note also that

$$f(1) = f(1 \cdot 1) = f(1)f(1),$$

whence $f(1) = 1$ for all multiplicative functions. Hence they always have $\star$-inverses.

In the sequel we will use the notation $p^\alpha \parallel n$ to mean that $p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$, i.e. p^α divides n precisely.

Proposition 7.2.2. *Suppose f and g are multiplicative functions. Then $f \star g$ and the $\star$-inverse of f are both multiplicative.*

Proof. Let $(m, n) = 1$. There is a bijection

$$\{\, d \mid d \mid mn \,\} \longleftrightarrow \{\, (d_1, d_2) \mid d_1 \mid m, d_2 \mid n \,\}$$

by $d \mapsto (\gcd(d, m), \gcd(d, n))$ and $d_1 d_2 \hookleftarrow (d_1, d_2)$. Under this bijection, we compute

$$\begin{aligned}
(f \star g)(mn) &= \sum_{d \mid mn} f(d) g\left(\frac{mn}{d}\right) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) g\left(\frac{m}{d_1}\frac{n}{d_2}\right) \\
&= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right) \\
&= \left(\sum_{d_1 \mid m} f(d_1) g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2 \mid n} f(d_2) g\left(\frac{n}{d_d}\right)\right) \\
&= (f \star g)(m)(f \star g)(n).
\end{aligned}$$

Now let h be the $\star$-inverse of f. First $h(1) = 1/f(1) = 1$, and further

$$h(n) = -\sum_{\substack{d \mid n \\ d > 1}} f(d) h\left(\frac{n}{d}\right).$$

Let $(m,n)=1$. We want to show that $h(mn)=h(m)h(n)$, which we will prove by induction. Suppose for all $(m',n')=1$ with $m'n'<mn$ we have $h(m'n')=h(m')h(n')$. Then

$$\begin{aligned}
h(mn) &= -\sum_{\substack{d\mid mn\\ d>1}} f(d)h\left(\frac{mn}{d}\right) = -\sum_{\substack{d_1\mid m\\ d_2\mid n\\ d_1d_2>1}} f(d_1d_2)h\left(\frac{m}{d_1}\frac{n}{d_2}\right)\\
&= \sum_{\substack{d_1\mid m\\ d_2\mid n\\ d_1d_2>1}} f(d_1)f(d_2)h\left(\frac{m}{d_1}\right)h\left(\frac{n}{d_2}\right)\\
&= -\left(\sum_{d_1\mid n} f(d_1)h\left(\frac{n}{d_1}\right)\right)\left(\sum_{d_2\mid m} f(d_2)h\left(\frac{m}{d_2}\right)\right) + f(1)f(1)h(m)h(n)\\
&= -(f\star h)(m)(f\star h)(n)+h(m)h(n) = h(m)h(n)
\end{aligned}$$

since the first two factors at the end are $\delta(m)$ and $\delta(n)$ respectively. □

Lecture 8 Dirichlet series

8.1 Multiplicativity of Möbius function

Remark 8.1.1. The previous proposition is not true if we replace multiplicativity with complete multiplicativity. In other words, for f and g completely multiplicative, neither $f\star g$ nor the $\star$-inverse of f need be completely multiplicative (though of course by the proposition they must be multiplicative).

Example 8.1.2. The constant function 1 is completely multiplicative. Thus $d(n)=1\star 1(n)$ is multiplicative (but in fact not completely multiplicative). Similarly $d_k(n)$ is multiplicative.

In particular $d(p^\alpha)=\alpha+1$ since the divisors of p^α are $p^0,p_1,\dots,p^\alpha$.

Hence if $n=\prod p^{\alpha_p}$, then

$$d(n)=\prod_p d(p^{\alpha_p})=\prod_p(\alpha_p+1).$$ ▲

Example 8.1.3. Since μ is the $\star$-inverse of 1 it is multiplicative. In particular, to compute $\mu(p^\alpha)$, let us consider $\mu\star 1(p^\alpha)=\delta(p^\alpha)$, which is 0 if $\alpha\geq 1$ and 1 if $\alpha=0$. On the other hand

$$\mu\star 1(p^\alpha)=\sum_{d\mid p^\alpha}\mu(d)=\sum_{0\leq\beta\leq\alpha}\mu(p^\beta).$$

For $\alpha=0$, $\mu(1)=1$. For $\alpha=1$, $\mu(1)+\mu(p)=0$, so $\mu(p)=-1$. Furthermore for $\alpha=2$, $\mu(1)+\mu(p)+\mu(p^2)=0$, but the first two terms add to 0, so $\mu(p^2)=0$, and in general $\mu(p^\alpha)=0$ for all $\alpha\geq 2$.

Date: January 25th, 2019.

Hence if $n = \prod p^{\alpha_p}$,

$$\mu(n) = \prod_p \mu(p^{\alpha_p}) = \begin{cases} 0 & \text{if } \alpha_p \geq 2 \text{ for some } p, \text{ i.e. } n \text{ is not square free} \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k,\ p_i \text{ distinct} \\ 1 & \text{if } n = 1. \end{cases}$$

▲

8.2 Dirichlet series

Let f be an arithmetic function. The ***Dirichlet series*** associated with f is

$$L(s, f) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \qquad s \in \mathbb{C}.$$

Remark 8.2.1. This series might not converse. We need some control of the size of f.

Definition 8.2.2. An arithmetic function f is of ***polynomial growth*** if it satisfies one of the following equivalent conditions:

(*i*) There exists a constant $A \in \mathbb{R}$, depending on f, such that $|f(n)| = O(n^A)$.

(*ii*) There exists $\sigma \in \mathbb{R}$ such that the series $L(\sigma, f)$ is absolutely convergent.

In this case we let

$$\sigma_f \coloneqq \inf\{\, \sigma \in \mathbb{R} \mid L(\sigma, f) \text{ converges absolutely} \,\} \in \mathbb{R} \cup \{\, -\infty \,\}.$$

We call σ_f the ***abscissa of convergence*** of $L(\sigma, f)$.

That (*i*) and (*ii*) are equivalent is pretty clear; in the forward direction our series looks like $\sum \frac{n^A}{n^s}$, so it converges absolutely for $\operatorname{Re} s > 1 + A$, and we can make a similar argument backwards. Hence $|f(n)| = O(n^{\sigma_f - 1})$.

Proposition 8.2.3. *Let f be an arithmetic function with polynomial growth. Let σ_f be its abscissa of convergence. Then for all $\sigma > \sigma_f$, the series $L(s, f)$ converges absolutely and uniformly in the halfplane $\{\, s \in \mathbb{C} \mid \operatorname{Re}(s) > \sigma \,\}$.*

In this domain,

$$L'(s, f) = \sum_{n \geq 1} \frac{-\log(n) f(n)}{n^s} = L(s, -\log \cdot f),$$

which also has abscissa of convergence σ_f.

Proof. Let $\sigma > \sigma_f$, and consider $\operatorname{Re}(s) \geq \sigma$. Then $|f(n)/n^s| \leq |f(n)|/n^\sigma$. Summing this over $n \geq 1$,

$$\sum_{n \geq 1} \left| \frac{f(n)}{n^s} \right| \leq \sum_{n \geq 1} \frac{|f(n)|}{n^\sigma} < \infty$$

since $L(\sigma, f)$ converges absolutely by definition since $\sigma > \sigma_f$. This bound is uniform for any $\operatorname{Re}(s) \geq \sigma$.

Finally by the absolute convergence we can switch the limit process in the series and the derivative, and hence differentiate termwise. □

An arithmetic function f determines its Dirichlet series uniquely, and a converse result is true as well.

Lemma 8.2.4. *Let f and g be two arithmetic functions of polynomial growth. Suppose $L(s,f) = L(s,g)$ for all s in*

$$\{\, s \in \mathbb{C} \mid \mathrm{Re}(s) > \max\{\, \sigma_f, \sigma_g \,\} \,\}.$$

Then $f = g$.

Hence the function is uniquely determined by its Dirichlet series.

Proof. Without loss of generality we can assume $g = 0$ (by replacing f by $f - g$, i.e. move $L(s,g)$ to the other side). So we have $L(s,f) = L(s,g) = 0$ for all $s \in \{\, s \in \mathbb{C} \mid \mathrm{Re}(s) > \sigma_f \,\}$ (since $\sigma_g = -\infty$). Let $h(n) = f(n)/n^{\sigma_f - 1}$. Then

$$L(s,f) = \sum_{n \geq 1} \frac{f(n)}{n^s} = \sum_{n \geq 1} \frac{f(n)/n^{\sigma_f - 1}}{n^{s - \sigma_f + 1}} = L(s - \sigma_f + 1, h).$$

Hence $L(s,h) = L(s + \sigma_f - 1, f)$.

For $\mathrm{Re}(s) > 1$, $\mathrm{Re}(s + \sigma_f - 1) > \sigma_f$, whence $\sigma_h \leq 1$, so $h(n) = O(n^{1-1}) = O(1)$.

Now suppose $h(n) \neq 0$ for some n, and consequently let n_0 be the smallest such n. For $\mathrm{Re}(s) > 2$,

$$0 = \sum_{n \geq n_0} \frac{h(n)}{n^s} = \frac{h(n_0)}{n_0^s} \left(1 + \frac{n_0^s}{h(n_0)} \sum_{n \geq n_0 + 1} \frac{h(n)}{n^s} \right).$$

Note that both of the $h(n_0)$ terms are nonzero by choice of n_0, so

$$1 + \frac{n_0^s}{h(n_0)} \sum_{n \geq n_0 + 1} \frac{h(n)}{n^s} = 0.$$

But

$$\sum_{n \geq n_0 + 1} \frac{h(n)}{n^s} \ll \sum_{n \geq n_0 + 1} \frac{1}{n^{\mathrm{Re}(s)}} \ll \int_{n_0 + 1}^{\infty} \frac{1}{t^{\mathrm{Re}(s)}}\, dt = \frac{1}{(\mathrm{Re}(s) - 1)(n_0 + 1)^{\mathrm{Re}(s) - 1}}.$$

Hence

$$1 + \frac{n_0^s}{h(n_0)} \sum_{n \geq n_0 + 1} \frac{h(n)}{n^s} = 1 + O\left(\frac{n_0^{\mathrm{Re}(s)}}{h(n_0)} \frac{1}{(\mathrm{Re}(s) - 1)(n_0 + 1)^{\mathrm{Re}(s) - 1}} \right) = 0$$

so

$$1 + O\left(\frac{1}{\mathrm{Re}(s) - 1} \right) = 0$$

which is a contradiction as $\mathrm{Re}(s) \to \infty$ since the remainder term vanishes. □

Lecture 9 L-functions of convolutions

9.1 L-functions associated with Dirichlet convolutions

Theorem 9.1.1. *Let f and g be arithmetic functions of polynomial growth with abscissae of convergence σ_f and σ_g respectively. Then $\sigma_{f\star g} \leq \max\{\sigma_f, \sigma_g\}$. Moreover for $\mathrm{Re}(s) = \sigma > \max\{\sigma_f, \sigma_g\}$ we have*

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

Proof. For $\mathrm{Re}(s) > \max\{\sigma_f, \sigma_g\}$,

$$\sum_{n\geq 1}\left|\frac{f\star g(n)}{n^s}\right| = \sum_{n=1}^{\infty}\frac{|\sum_{ab=n} f(a)g(b)|}{n^{\mathrm{Re}(s)}} \leq \sum_{n=1}^{\infty}\sum_{ab=n}\frac{|f(a)||g(b)|}{|ab|^{\mathrm{Re}(s)}}$$
$$= \sum_{1=1}^{\infty}\sum_{ab=n}\frac{|f(a)||g(b)|}{|a|^{\mathrm{Re}(s)}|b|^{\mathrm{Re}(s)}} = \left(\sum_{a=1}^{\infty}\frac{|f(a)|}{|a|^{\mathrm{Re}(s)}}\right)\left(\sum_{b=1}^{\infty}\frac{|g(b)|}{|b|^{\mathrm{Re}(s)}}\right) < \infty$$

so $\sigma_{f\star g} \leq \max\{\sigma_f, \sigma_g\}$.

For $\mathrm{Re}(s) > \max\{\sigma_f, \sigma_g\}$ we have absolute convergence, so we can rearrange terms in the series as desired, so

$$L(s,f)L(s,g) = \sum_{m=1}^{\infty}\frac{f(m)}{m^s}\sum_{k=1}^{\infty}\frac{g(k)}{k^s} = \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{mk=n} f(m)g(k)$$
$$= \sum_{n=1}^{\infty}\frac{f\star g(n)}{n^s} = L(s, f\star g). \qquad \square$$

Corollary 9.1.2. *Suppose f is $\star$-invertible. Let g be the $\star$-inverse of f. Assume $\sigma_f, \sigma_g < \infty$. Then for $\mathrm{Re}(s) > \max\{\sigma_f, \sigma_g\}$, we have $L(s,f)L(s,g) = 1$.*

Proof. By the last theorem, since $f\star g = \delta$, which is supported only on $n = 1$. $\square$

In particular $L(s,f)$ does not vanis on

$$\{\, s \in \mathbb{C} \mid \mathrm{Re}(s) > \max\{\sigma_f, \sigma_g\}\,\}.$$

Example 9.1.3. For $f = 1$, we have

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

converging on $\mathrm{Re}(s) > 1$, so $\sigma_1 = 1$. The Möbius function μ is the $\star$-inverse of 1, so

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

We have $|\mu(n)| \leq 1 = O(n^0)$, so $\sigma_\mu \leq 1$.

Date: January 28th, 2019.

In fact it is equal to 1; let $s = 1$, so

$$\sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} \geq \sum_p \frac{1}{p} = \infty$$

so $\sigma_\mu = 1$.

Hence $L(s,1)L(s,\mu) = 1$ for $\mathrm{Re}(s) > 1$, and $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$. Also

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

for $\mathrm{Re}(s) > 1$. ▲

Example 9.1.4. Let $d(n) = 1 \star 1(n)$. Then

$$L(s,d) = L(s, 1\star 1) = L(s,1)L(s,1) = \zeta(s)^2$$

for $\mathrm{Re}(s) > 1$. In general

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

for $\mathrm{Re}(s) > 1$. ▲

Example 9.1.5. Euler's φ-function is defined by

$$\varphi(n) = \#\{\, 1 \leq m \leq n \mid (m,n) = 1 \,\}.$$

This is multiplicative (which follows immediately from the Chinese remainder theorem), and $\varphi(n) = \mu \star \mathrm{Id}(n)$, where $\mathrm{Id}(n) = n$. It's easy to check this on prime powers.

Now

$$L(s, \mathrm{Id}) = \sum_{n=1}^{\infty} \frac{n}{n^s} = \zeta(s-1),$$

so $\sigma_{\mathrm{Id}} = 2$, and

$$L(s,\varphi) = L(s,\mu)L(s,\mathrm{Id}) = \frac{\zeta(s-1)}{\zeta(s)}$$

for $\mathrm{Re}(s) > \max\{\, \sigma_\mu, \sigma_{\mathrm{Id}} \,\} = \max\{\, 1, 2 \,\} = 2$.

Hence

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

for $\mathrm{Re}(s) > 2$. ▲

Example 9.1.6. The von Mangoldt function $\Lambda(n) = \log \star \mu(n)$, so

$$L(s,\Lambda) = L(s,\log)L(s,\mu).$$

Now

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

and so long as $\mathrm{Re}(s) > 1$, so that we have absolute convergence, we can differentiate termwise, whence

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

meaning that $L(s, \log) = -\zeta'(s)$. Then

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

for $\mathrm{Re}(s) > 1$. Note also that the fraction is a fraction of holomorphic functions, the bottom nonvanishing, so it is holomorphic and has an antiderivative, so

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

for $\mathrm{Re}(s) > 1$. ▲

9.2 Dirichlet series and multiplicative functions

Theorem 9.2.1. *Let f be a multiplicative function of polynomial growth. Then for $\mathrm{Re}(s) = \sigma > \sigma_f$, we have*

(*i*) *For all primes p,*

$$L_p(s, f) \coloneqq \sum_{\alpha \geq 0} \frac{f(p^\alpha)}{p^{\alpha s}}$$

converges absolutely and uniformly in $\mathrm{Re}(s) \geq \sigma$.

This $L_p(s, f)$ is called the **local factor** *of f at p.*

(*ii*) *We have*

$$L(s, f) = \prod_p L_p(s, f),$$

which is an infinite product, so technically we mean

$$\lim_{P \to \infty} \prod_{p \leq P} L_p(s, f),$$

which converges uniformly in $\mathrm{Re}(s) \geq \sigma$.

(*iii*) *Conversely, let f be an arithmetic funciton f such that $\sigma_f < \infty$ and $f(1) = 1$. Suppose*

$$L(s, f) = \prod_p L_p(s, f)$$

for $\mathrm{Re}(s)$ sufficiently large. Then f is multiplicative.

Proof. (*i*) This is trivial: the local factors are subseries of an absolutely and uniformly convergent series.

(*ii*) The intuition is that we can factor n into primes, and collecting them as appropriate, the two sides are equal. More precisely, for the convergence, let $P \geq 2$ and write $p_1 < p_2 < \ldots < p_k \leq P$, the set of primes less than or equal to P. Then

$$\begin{aligned}\prod_{p\leq P} L_p(s,f) &= \sum_{\alpha_1,\ldots,\alpha_k\geq 0} \frac{f(p_1^{\alpha_1})\cdots f(p_k^{\alpha_k})}{(p_1^{\alpha_1}\cdots p_k^{\alpha_k})^s} \\ &= \sum_{\alpha_1,\ldots,\alpha_k\geq 0} \frac{f(p_1^{\alpha_1}\cdots p_k^{\alpha_k})}{(p_1^{\alpha_1}\cdots p_k^{\alpha_k})^s} = \sum_{\substack{n\geq 1\\ p\mid n\Rightarrow p\leq P}} \frac{f(n)}{n^s}\end{aligned}$$

Hence

$$\left|L(s,f) - \prod_{p\leq P} L_p(s,f)\right| \leq \sum_{n>P} \frac{|f(n)|}{n^s} \to 0$$

as $P \to \infty$ since the left-hand side becomes the sum over n with all prime factors exceeding P, which is a smaller set than $n > P$, and the right-hand side is the tail of a convergent sum.

Lecture 10 Euler products

10.1 L-series continued

Proof continued. (*iii*) Let $\tilde{f}$ be the multiplicative function defined by

$$\hat{f}(n) = \prod_{p^\alpha \| n} f(p^\alpha).$$

For $\sigma > \sigma_f$, $|f(n)|/n^\sigma = o(1)$, so for n large enough, say $n > N$, we have $|f(n)|/n^\sigma < 1$.

Hence

$$\frac{|\tilde{f}(n)|}{n^\sigma} = \prod_{p^\alpha\|n} \frac{|f(p^\alpha)|}{p^{\alpha\sigma}} = \prod_{\substack{p^\alpha\|n\\ p^\alpha\leq N}} \frac{|f(p^\alpha)|}{p^{\alpha\sigma}} \prod_{\substack{p^\alpha\|n\\ p^\alpha> N}} \frac{|f(p^\alpha)|}{p^{\alpha\sigma}} = O(1)$$

with the implied constant depending on f, since the first product is a finite product, hence a constant, and the second product is $o(1)$ by choice of N. Therefore $L(s,\tilde{f})$ converges absolutely for $\mathrm{Re}(s) > \sigma + 1$.

For such s,

$$L(s,\tilde{f}) = \prod_p L_p(s,\tilde{f}) = \prod_p \sum_{\alpha\geq 0} \frac{p^\alpha}{p^{\alpha s}} = \prod_p L_p(s,f) = L(s,f)$$

so for $\mathrm{Re}(s)$ sufficiently large, the L-functions are equal, whence by Lemma 8.2.4 $\tilde{f} = f$, and so f is multiplicative since $\tilde{f}$ is multiplicative by construction. □

Date: January 30th, 2019.

Corollary 10.1.1. *If f is completely multiplicative with $\sigma_f < \infty$, then for* $\mathrm{Re}(s) > \sigma_f$,

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

Proof. This follows immediately from $f(p^\alpha) = f(p)^\alpha$ when f is completely multiplicative, so

$$L_p(s,f) = \sum_{\alpha \geq 0} \frac{f(p^\alpha)}{p^{\alpha s}} = \sum_{\alpha \geq 0} \frac{f(p)^\alpha}{p^{s\alpha}} = \left(1 - \frac{f(p)}{p^s}\right)^{-1},$$

the last sum being geometric. □

We call such a product representation an ***Euler product***.

Proposition 10.1.2. *Let f be multiplicative with $\sigma_f < \infty$. Let $\sigma > \sigma_f$. Then there exists $P > 0$ such that*

$$\prod_{p > P} L_p(s,f) = \frac{L(s,f)}{\prod\limits_{p \leq P} L_p(s,f)}$$

does not vanish in $\mathrm{Re}(s) \geq \sigma$.

Thus the zeros of $L(s,f)$ in $\mathrm{Re}(s) \geq \sigma$ *are exactly the zeros of the local factors $L_p(s,f)$, $p \leq P$.*

Proof. Let $\sigma > \sigma_f$. By the previous Theorem 9.2.1,

$$L(s,f) = \prod_p L_p(s,f)$$

for $\mathrm{Re}(s) \geq \sigma$. The right-hand side is interpreted as a convergent limit, so there exists some $P > 0$ such that for $p > P$,

$$|L_p(s,f) - 1| < \frac{1}{2}$$

for $\mathrm{Re}(s) \geq \sigma$. Hence $L_p(s,f) \neq 0$ for $p > P$, $\mathrm{Re}(s) \geq \sigma$, since it is bounded away from zero. □

Example 10.1.3. For $\mathrm{Re}(s) > 1$,

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

which is never 0, so $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$. Correspondingly

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

is also nonvanishing in $\mathrm{Re}(s) > 1$. ▲

Example 10.1.4. For $\mathrm{Re}(s) > 1$,

$$L(s,d) = \sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta(s)^2 = \prod_p \left(1 - \frac{1}{p^s}\right)^{-2}.$$

Let f be the $\star$-inverse of d. Then

$$L(s,f) = \frac{1}{\zeta(s)^2} = \prod_p \left(1 - \frac{1}{p^s}\right)^2 = \prod_p \left(1 - \frac{2}{p^s} + \frac{1}{p^{2s}}\right). \qquad \blacktriangle$$

Example 10.1.5. Let φ be the Euler φ-function. We have

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

for $\mathrm{Re}(s) > 2$. $\blacktriangle$

Let us now explore a slightly more esoteric example, but that serves a point in finding zeros between σ_f and σ_g, where f and g are each other's $\star$-inverses.

Example 10.1.6. Let μ_s be the multiplicative function f defined by

$$\mu_2(p^\alpha) = \begin{cases} 1, & \text{if } \alpha = 0 \\ 0, & \text{if } \alpha \geq 2 \\ -1, & \text{if } \alpha = 1,\ p \neq 2 \\ -4, & \text{if } \alpha = 1,\ p = 2. \end{cases}$$

In other words, it is the usual Möbius function, except we've modified it specifically on $n = 2$. Note that $|\mu_2(n)| \leq 4$, so $L(s,\mu_2)$ converges absolutely for $\mathrm{Re}(s) > 1$; $\sigma_{\mu_2} \leq 1$. Moreover at $s = 1$,

$$|L(1,\mu_2)| = \sum_{n=1}^{\infty} \frac{|\mu_2(n)|}{n^s} \geq \sum_{p \neq 2} \frac{1}{p} = \infty,$$

so in fact $\sigma_{\mu_2} = 1$.

Now a natural question to ask is what the zeros of $L(s,\mu_2)$ are for $\mathrm{Re}(s) > 1$. We compute the local factors

$$L_2(s,\mu_2) = \sum_{\alpha \geq 0} \frac{\mu_2(2^\alpha)}{2^{\alpha s}} = 1 - \frac{4}{2^s},$$

and for $p \neq 2$,

$$L_p(s,\mu_2) = \sum_{\alpha \geq 0} \frac{\mu_2(p^\alpha)}{p^{\alpha s}} = 1 - \frac{1}{p^s},$$

meaning that

$$L(s,\mu_2) = \left(1 - \frac{4}{2^s}\right) \prod_{p \neq 2} \left(1 - \frac{1}{p^s}\right),$$

where the first factor is 0 if $s = 2$, and the remaining factors are never zero for $\mathrm{Re}(s) > 1$. Hence the only zero of $L(s,\mu_2)$ on $\mathrm{Re}(s) > 1$ is $s = 2$.

Now let $\mu_2^{(-1)}$ be the $\star$-inverse of μ_2. It is multiplicative, since μ_2 is, and

$$\mu_2^{(-1)}(p^\alpha) = \begin{cases} 1, & \text{if } p \neq 2 \\ 4^\alpha, & \text{if } p = 2. \end{cases}$$

Let $\sigma > 2$. For $\mathrm{Re}(s) > \sigma$,

$$|L(s, \mu_2^{(-1)})| \leq \sum_{n\geq 1} \frac{|\mu_2^{(-1)}(n)|}{n^\sigma} = \left(1 - \frac{4}{2^s}\right)^{-1} \prod_{p\neq 2} \left(1 - \frac{1}{p^s}\right)^{-1} = \frac{1 - 1/2^\sigma}{1 - 4/2^\sigma}\zeta(\sigma).$$

We chose $\sigma > 2$ because

$$L_2(s, \mu_2^{(-1)}) = \sum_{\alpha\geq 0} \frac{\mu_2^{(-1)}(2^\alpha)}{2^{\alpha s}} = \sum_{\alpha\geq 0} \frac{4^\alpha}{2^{s\alpha}} = \sum_{\alpha\geq 0} \left(\frac{4}{2^s}\right)^\alpha,$$

which is geometric and converges for $\mathrm{Re}(s) < 2$, so $\sigma_{\mu_2^{(-1)}} \leq 2$, and moreover

$$\sum_{n\geq 1} \frac{|\mu_2^{(-1)}(n)|}{n^2} \geq \sum_{\alpha\geq 0} \left(\frac{4}{2^2}\right)^\alpha = \infty,$$

so $\sigma_{\mu_2^{(-1)}} = 2$.

Hence $L(s, \mu_2)L(s, \mu_2^{(-1)}) = 1$ for $\mathrm{Re}(s) > 2$, and between $\sigma_{\mu_2} = 1$ and $\sigma_{\mu_2^{(-1)}} = 2$ we find the one zero at $s = 2$. ▲

Lecture 11 Primes in arithmetic progressions

11.1 Arithmetic progressions

Definition 11.1.1. An ***arithmetic progression*** is an infinite subset of $\mathbb{Z}$ satisfying the property that there exists an integer $q > 0$ such that the distance between any two consecutive integers of this subset is q.

This integer q is called the ***modulus*** of the arithmetic progression. Hence an arithmetic progression of modulus q is of the form

$$L_{q,a} = a + q\mathbb{Z},$$

with $a \in \mathbb{Z}$.

Note that if $a \equiv b \pmod q$, then $L_{q,a} = L_{q,b}$. Therefore the arithmetic progressions of modulus q are indexed by the residue classes modulo q, i.e. $\mathbb{Z}/q\mathbb{Z}$.

Theorem 11.1.2 (Dirichlet)**.** *Let $a, q \in \mathbb{Z}$, $q > 0$, with $(a, q) = 1$. Then the set $\wp_{q,a} = \wp \cap L_{q,a}$ is infinite, i.e. there exist infinitely many primes p such that $p \equiv a \pmod q$.*

Remark 11.1.3. The condition $(a, q) = 1$ is necessary. Indeed if $(a, q) > 1$, then there exists at most one prime $p \equiv a \pmod q$, and such a prime $p = (a, q)$. This is easy to see: everywhing in the arithmetic progression is of the form $a + kq$, but out of all of them we can factor (a, q) by definition.

Hence the residue classes containing infinitely many primes are $(\mathbb{Z}/q\mathbb{Z})^\times$.

Date: February 1st, 2019.

As with the infinitude of the primes leading to us wondering about the Prime number theorem, a natural question to ask here is this: what is the density of the set $\wp_{q,a}$? In the same vein, let

$$\pi(x;q,a) = \#(\wp_{q,a} \cap [1,x]) = \#\{\, p \le x \mid p \equiv a \pmod q \,\}.$$

Theorem 11.1.4 (Landau)**.** *Let $a, q > 0$ with $(a,q) = 1$. Then*

$$\pi(x;q,a) = \frac{1}{\varphi(q)}\pi(x)(1+o(1)) \sim \frac{\pi(x)}{\varphi(q)} \sum \frac{x}{\varphi(q)\log x}$$

as $x \to \infty$, the last being the Prime number theorem.

Now in particular, by definition, $|(\mathbb{Z}/q\mathbb{Z})^\times| = \varphi(q)$, so the primes are equidistributed amongst the residue classes modulo q.

Lecture 12 Characters

12.1 Analogue of Merten's theorem

Theorem 12.1.1. *Let $a, q > 0$, $(a,q) = 1$. Then we have*

$$(i) \quad \sum_{\substack{n \le x \\ n \equiv a \pmod q}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)} \log x + O(1).$$

$$(ii) \quad \sum_{\substack{p \le x \\ p \equiv a \pmod q}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O(1).$$

$$(iii) \quad \sum_{\substack{p \le x \\ p \equiv a \pmod q}} \frac{1}{p} = \frac{1}{\varphi(q)} \log\log x + O(1).$$

We will prove (i) later. Moreover (i) implies (ii) implies (iii) in exactly the same way as in Merten's theorem.

Remark 12.1.2. Note that this theorem implies Dirichlet's theorem, since for weighted sums over the primes in arithmetic progressions to diverge, there must be infinitely many primes in them.

12.2 Characters of finite abelian groups

Let G be a finite abelian group with identity denoted by 1.

Definition 12.2.1. A ***character*** χ of G is a group homomorphism $\chi\colon G \to \mathbb{C}^*$.

Remark 12.2.2. Such a character χ has the following properties:

(i) $\chi(ab) = \chi(a)\chi(b)$ for every $a, b \in G$ since it is a homomorphism.

(ii) $\chi(1) = 1$.

Date: February 4th, 2019.

(*iii*) $\chi(a)^m = \chi(a^m)$, which in turn is $\chi(1) = 1$ if $m = |G|$. Hence every $\chi(a)$ is an mth root of unity, and $|\chi(a)| = 1$. Thus $\chi\colon G \to S^1 \subset \mathbb{C}$, the unit circle.

This also means that $\overline{\chi(a)} = \chi(a^{-1})$.

Let $\hat{G}$ denote the set of all characters of G. Then $\hat{G}$ is a group with multiplcation defined by $\chi_1 \cdot \chi_2(a) = \chi_1(a)\chi_2(a)$. We call $\hat{G}$ the ***dual group*** of G, and its identity element is the ***trivial character*** $\chi_0(a) = 1$ for all $a \in G$.

Proposition 12.2.3. *Let H be a subgroup of the finite abelian group G. Then every character of H extends to a character of G.*

Proof. We prove it by induction on the index $[G : H] = |G/H|$. If $[G : H] = 1$, then $G = H$ and we are done.

Assume that it is true for every subgroup H' of G with $[G : H'] < [G : H]$.

Take $g \in G \setminus H$, and let n be the smallest positive integer such that $g^n \in H$ (which exists since $g^n = 1$ in G/H for some n). Then we have our character $\chi\colon H \to \mathbb{C}$, but what should we define $\chi(g)$ to be? That's hard to say, but certainly $\chi(g^n) = t \in \mathbb{C}$ is well-defined, since $g^n \in H$. Let $H' = \langle H, g\rangle$. Now $w^n = t$ for some w (actually n options), so pick one of them and define $\chi'\colon H' \to \mathbb{C}^*$ by $\chi'(h) = \chi(h)$ for $h \in H$, and $\chi'(g) = w$.

For each $h' \in H'$, we have $h' = hg^k$ for some $h \in H$ and $k \in \mathbb{Z}$, so $\chi'(h') = \chi(h)w^k$. This is well-defined, and clearly it is a character on H' and restricts to χ on H.

Now $H < H' < G$, with the first subgroup strict, so $[G : H'] < [G : H]$, so by our inductive hypothesis, χ' extends to G. □

Remark 12.2.4. The restriction $\rho\colon \hat{G} \to \hat{H}$ defined by $\chi \mapsto \chi|_H$ is a homomorphism. The proposition implies that ρ is surjective.

It's kernel is, by definition,

$$\ker \rho = \{\, \chi \in \hat{G} \mid \chi|_H = \chi_0 \,\},$$

which is the same as $\widehat{G/H}$, so we have the short exact sequence

$$\{\,1\,\} \longrightarrow \widehat{G/H} \longrightarrow \hat{G} \xrightarrow{\ \rho\ } \hat{H} \longrightarrow \{\,1\,\}.$$

Proposition 12.2.5. *Let G be a finite abelian group. Then $|\hat{G}| = |G|$.*

Proof. If $G = \langle g\rangle$ is cyclic, then $\chi \in \hat{G}$ is determined by $\chi(g)$. Since $\chi(g)$ is a $|G|$th root of unity, and each $|G|$th root of unity determines a character χ, $|\hat{G}| = |G|$.

Suppose G is not cyclic. Then there exists a nontrivial cyclic subgroup H of G, and as above we have the short exact sequence

$$\{\,1\,\} \longrightarrow \widehat{G/H} \longrightarrow \hat{G} \xrightarrow{\ \rho\ } \hat{H} \longrightarrow \{\,1\,\}.$$

Hence $|\hat{G}| = |\widehat{G/H}| \cdot |\hat{H}|$.

Now suppose the proposition is true for all finite abelian groups of order less than $n = |G|$. Then

$$|\hat{G}| = |\widehat{G/H}| \cdot |\hat{H}| = |G/H| \cdot |H| = |G|,$$

where in the penultimate step we use the inductive hypothesis for G/H and our argument about H being cyclic for the second term. □

Remark 12.2.6. One can show that there is an isomorphism between G and $\hat{G}$, however it is not canonical—it depends on the choice of generators.

That said, if G is isomorphic to its dual $\hat{G}$, then similarly $\hat{G}$ must be isomorphic to *its* dual $\hat{\hat{G}}$, and it turns out there is a canonical isomorphism between that and G.

Lecture 13 Fourier analysis on finite abelian groups

13.1 Orthogonality of characters

Let G be a finite abelian group. Let $g \in G$. Then g defines a character of $\hat{G}$ by

$$\hat{g}\colon \hat{G} \to \mathbb{C}^*$$

by $\hat{g}(\chi) = \chi(g)$. So we have a homomorphism $\varepsilon\colon G \to \hat{\hat{G}}$ defined by $g \mapsto \hat{g}$.

Proposition 13.1.1. *The homomorphism $\varepsilon\colon G \to \hat{\hat{G}}$ is an isomorphism.*

Proof. We have $|G| = |\hat{G}| = |\hat{\hat{G}}|$. Hence it suffices to show that ε is injective, i.e. if $g \neq 1$, then $\hat{g} \neq 1$, so $\hat{g}$ is not the trivial character on $\hat{G}$. In other words, there exists some $\chi \in \hat{G}$ such that $\hat{g}(\chi) \neq 1$, i.e. $\chi(g) \neq 1$.

Now let $H = \langle g \rangle \subset G$. Define $\chi\colon H \to \mathbb{C}^*$ by $\chi(g) = \xi \neq 1$, with ξ an $|H|$th root of unity. Now extending χ to G finishes the proof. □

Theorem 13.1.2. *Let G be a finite abelian group of order n. Then*

$$(i)\ \sum_{g\in G} \chi(g) = \begin{cases} n & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0 \end{cases},$$

$$(ii)\ \sum_{\chi\in \hat{G}} \chi(g) = \begin{cases} n & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases}.$$

Proof. For the first one, if $\chi = \chi_0$, then

$$\sum_{g\in G} \chi_0(g) = \sum_{g\in G} 1 = n.$$

If $\chi \neq \chi_0$, then there exists some $a \in G$ with $\chi(a) \neq 1$. Multiplying the sum by $\chi(a)$ we have

$$\chi(a) \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(a)\chi(g) = \sum_{g\in G} \chi(ag) = \sum_{g\in G} \chi(g)$$

since χ is a homomorphism, and moreover ag, as g runs over G, is just permuting the arguments. Hence

$$(\chi(a) - 1) \sum_{g\in G} \chi(g) = 0,$$

Date: February 6th, 2019.

but by choice of a the parenthesis is nonzero, so the sum is 0.

For the second orthogonality relation, note that

$$\sum_{\chi\in\hat{G}} \chi(g) = \sum_{\chi\in\hat{G}} \hat{\hat{g}}(\chi),$$

so it reduces to the first case. □

13.2 Fourier analysis on finite abelian groups

Let G be a finite abelian group. Let $\mathcal{C}(G) = \{ f\colon G \to \mathbb{C} \}$, which is a vector space over $\mathbb{C}$.

A basis for $\mathcal{C}(G)$ is given by $\mathcal{B} = \{ \delta_g \mid g \in G \}$ where

$$\delta_g(a) = \begin{cases} 1 & \text{if } a = g, \\ 0 & \text{if } a \neq g. \end{cases}$$

Hence $\dim_{\mathbb{C}} \mathcal{C}(G) = |G|$, and we can write any $f \in \mathcal{C}(G)$ as

$$f(a) = \sum_{g\in G} f(g)\delta_g(a).$$

We can also define the Hermitian inner product $\langle \cdot, \cdot \rangle$ on $\mathcal{C}(G)$ by

$$\langle f, h \rangle = \frac{1}{|G|} \sum_{g\in G} f(g)\overline{h(g)}.$$

Then $\mathcal{B}$ is an orthogonal basis since

$$\langle \delta_g, \delta_a \rangle = \frac{1}{|G|} \sum_{h\in G} \delta_g(h)\overline{\delta_a(h)} = \begin{cases} \frac{1}{|G|} & \text{if } g = a \\ 0 & \text{if } g \neq a. \end{cases}$$

Remark 13.2.1. All of these properties hold for any finite set G. In other words, we have not used the group structure of G.

In order to instead take advantage of the group structure of G, let $\chi_1, \chi_2 \in \hat{G}$. Then

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g\in G} \chi_1(g)\overline{\chi_2(g)} = \begin{cases} 1 & \text{if } \chi_1 = \chi_2 \\ 0 & \text{if } \chi_1 \neq \chi_2 \end{cases}$$

by the orthogonality relation, since $\chi_1(g)\overline{\chi_2(g)} = (\chi_1\overline{\chi_2})(g)$ is another character, which is trivial if and only if they're the same.

Now $|\hat{G}| = |G| = \dim_{\mathbb{C}} \mathcal{C}(G)$ so $\hat{G}$ is an orthonormal set spanning $\mathcal{C}(G)$, and hence an orthonormal basis.

This means that we also have a ***Fourier transform***: for $f \in \mathcal{C}(G)$, $\hat{f}\colon \hat{G} \to \mathbb{C}^*$ by

$$\hat{f}(\chi) = \langle f, \chi \rangle = \frac{1}{|G|} \sum_{g\in G} f(g)\overline{\chi(g)}.$$

By orthogonality we then have the ***Fourier expansion***

$$f(g) = \sum_{\chi\in\hat{G}} \hat{f}(\chi)\chi(g).$$

Moreover we have the ***Parseval-Plancherel formula***

$$\|f\|^2 = \frac{1}{|G|}\|\hat{f}\|^2.$$

13.3 Characters on cyclic groups

Let $G = \langle g \rangle$ be a finite cyclic group of order n. Note that a character $\chi \in \hat{G}$ is completely determined by $\chi(g)$; i.e., $\chi(g) = \xi$ is an nth root of unity and each nth root of unity determined a character.

Proposition 13.3.1. *Let $G = \langle g \rangle$ be a finite cyclic group of order n. Let μ_n be the set of all nth roots of unity. Then $\varphi\colon \mu_n \to \hat{G}$ defined by $\xi \mapsto \chi_\xi$, where $\chi_\xi(g)$, is an isomorphism.*

Example 13.3.2. A finite cyclic group G of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$, seen as an additive group. The characters of G are ψ_m where

$$\psi_m(1) = e^{2\pi i m/n},$$

for $m = 0, 1, 2, \ldots, n-1$, noting that μ_n is a cyclic group of order n generated by $\xi = e^{2\pi i/n}$. ▲

13.4 Dirichlet characters

Definition 13.4.1. Let $q \geq 1$ be an integer. The characters of the abelian group $(\mathbb{Z}/q\mathbb{Z})^\times$ are called ***Dirichlet characters*** of modulus q. The trivial character is denoted by ξ_0. This defines $\chi\colon (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^*$; we extend it to $\mathbb{Z}/q\mathbb{Z}$ and then to $\mathbb{Z}$ by taking $\chi(a) = 0$ if $(a, q) \neq 1$. In other words

$$\chi\colon \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}^*$$

by

$$\chi(n) = \begin{cases} \chi(n \mod q) & \text{if } (n,q) = 1 \\ 0 & \text{if } (n,q) \neq 1. \end{cases}$$

Note two things: there are precisely $\varphi(q)$ Dirichlet characters to the modulus q, and for the record $(\mathbb{Z}/q\mathbb{Z})^\times$ is not usually cyclic: it is cyclic only when q is 2, 4, p^k for $p \neq 2$, or $2p^k$ (this is when there exist primitive roots modulo q).

Lecture 14 Dirichlet characters

14.1 L-functions attached to Dirichlet characters

Remark 14.1.1. Dirichlet characters χ are completely multiplicative, i.e., $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \in \mathbb{Z}$. Hence the Dirichlet series associated with χ has an Euler product

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

for $\mathrm{Re}(s) > 1$ since $|\chi(n)| \leq 1$.

Date: February 8th, 2019.

Proposition 14.1.2. *Let $\chi \pmod q$ be a Dirichlet character.*

(*i*) *If $\chi = \chi_0$, we have for $\operatorname{Re}(s) > 1$,*

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

which has an analytic continuation to $\operatorname{Re}(s) > 0$ with a simple pole at $s = 1$.

(*ii*) *If $\chi \neq \chi_0$, then $L(s, \chi)$ converges uniformly on compact subsets in $\operatorname{Re}(s) > 0$ and thus it is a holomorphic function in $\operatorname{Re}(s) > 0$.*

Moreover we have for $\operatorname{Re}(s) = \sigma > 0$ and $X \geq 2$,

$$L(s, \chi) = \sum_{n \leq X} \frac{\chi(n)}{n^s} + O\left(\frac{q|s|}{\sigma} x^{-\sigma}\right),$$

with the convergence here being conditional.

Proof. (*i*) If $\chi = \chi_0$, then

$$L(s, \chi_0) = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1},$$

where $\chi_0(p)$ is 1 on primes $(p, q) = 1$ and otherwise 0, so

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

where the last factor is $\zeta(s)$. The first product is finite and defined for all $s \in \mathbb{C}$. Hence the analytic continuation and the simple pole follows from same of $\zeta(s)$.

(*ii*) If $\chi \neq \chi_0$, by orthogonality

$$\sum_{a \leq n < a+q} \chi(n) = 0,$$

so if we let

$$M_\chi(t) = \sum_{1 \leq n \leq t} \chi(n),$$

then $|M_\chi(t)| \leq q$ uniformly, since each interval of length q is 0, and only the tail end can contribute at most q nonzero terms. (Indeed we can do sligthly better, in terms of $\varphi(q)$, but it's not necessary for our purposes.)

Hence

$$\sum_{1 \leq n \leq X} \frac{\chi(n)}{n^s} = \int_{1^-}^X \frac{1}{t^s}\, dM_\chi(t) = \frac{M_\chi(t)}{t^s}\bigg|_{1^-}^X + s \int_{1^-}^X M_\chi(t) t^{-s-1}\, dt.$$

For $\operatorname{Re}(s) = \sigma > 0$, the first term is

$$\left|\frac{M_\chi(X)}{X^s}\right| \leq \frac{q}{X^\sigma} \to 0$$

as $X \to \infty$. For the integral, consider the tail

$$\Big|\int_X^\infty M_\chi(t)t^{-s-1}\,dt\Big| \le \frac{|s|q}{\sigma X^\sigma} \to 0$$

as $X \to \infty$. Hence $L(s,\chi)$ converges uniformly on compact subsets in $\mathrm{Re}(s) > 0$. □

Remark 14.1.3. Note that this is essentially the proof of Dirichlet's test for convergence; if

$$\Big|\sum_{n\le N} a_n\Big| < M$$

uniformly, and b_n decreases monotonically to 0, then

$$\sum_{n\ge 0} a_n b_n$$

converges.

With this we are finally equipped to prove Merten's theorem for arithmetic progressions.

Proof. We want to prove

$$\sum_{\substack{n\le X\\ n\equiv a \pmod q}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)}\log X + O(1).$$

Now to filter the terms $n \equiv a \pmod q$ out of the sum over all n, we average the sum over all characters $\chi \pmod q$, since

$$\sum_{\chi \pmod q} \chi(b) = \begin{cases} 0 & \text{if } b \not\equiv 1 \pmod q \\ \varphi(q) & \text{if } b \equiv 1 \pmod q. \end{cases}$$

Hence

$$\sum_{\substack{n\le X\\ n\equiv a \pmod q}} \frac{\Lambda(n)}{n} = \sum_{n\le X} \frac{\Lambda(n)}{n}\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi(a)}\chi(n),$$

since the latter sum is $\varphi(q)$ if $a \equiv n \pmod q$, and 0 otherwise. We rewrite this sum as

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi(a)} \sum_{n\le X} \frac{\Lambda(n)\chi(n)}{n} = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi(a)} S_\chi(X).$$

We split this into two sums, one for χ_0 and one for $\chi \ne \chi_0$. If $\chi = \chi_0$,

$$S_{\chi_0}(X) = \sum_{n\le X} \frac{\Lambda(n)\chi_0(n)}{n} = \sum_{\substack{n\le X\\ (n,q)=1}} \frac{\Lambda(n)}{n} = \sum_{n\le X} \frac{\Lambda(n)}{n} - \sum_{p\mid q} \log p \sum_{\substack{\alpha\ge 1\\ p^\alpha \le X}} \frac{1}{p^\alpha}.$$

Looking carefully at the last sum, the innermost sum is geometric and bounded by $1/(p(1-1/p)) \le 1$, and with that bound in mind the sum over $p \mid q$ becomes bounded by $\log q$ by bringing the sum inside the logarithm as a product. Hence

$$S_{\chi_0}(X) = \log X + O(1) + O(\log q) = \log X + O_q(1)$$

by Merten's regular theorem.

Now it remains to show that for $\chi \neq \chi_0$,

$$S_\chi(X) = \sum_{n \leq X} \frac{\Lambda(n)\chi(n)}{n} = O_q(1).$$

□

Lecture 15 Mertens' theorem for arithmetic progressions

15.1 Proof finished

Proof continued. Carrying on from last time, we wish to show that for $\chi \neq \chi_0$, $S_\chi(X) = O_q(1)$. To this end, consider

$$T_\chi(X) = \sum_{n \leq X} (\log n) \frac{\chi(n)}{n}.$$

By Dirichlet's test for convergence, this is $O_q(1)$.

Recall that

$$\log n = \sum_{d|n} \Lambda(d) = \sum_{ab=n} \Lambda(a).$$

This means

$$T_\chi(X) = \sum_{n \leq X} \Big(\sum_{ab=n} \Lambda(n) \Big) \frac{\chi(n)}{n} = \sum_{a \leq X} \frac{\Lambda(a)\chi(a)}{a} \sum_{b \leq X/a} \frac{\chi(b)}{b}.$$

Looking at these carefully, we recognise the first sum as $S_\chi(X)$ and the inner sum is $L(1,\chi) + O(qa/X)$ by Proposition 14.1.2. Hence the above is

$$T_\chi(X) = S_\chi(X)L(1,\chi) + O\left(\sum_{a \leq x} \frac{\Lambda(a)\chi(a)}{a} \frac{qa}{X} \right),$$

and the error term is

$$\ll \frac{q}{X} \sum_{a \leq X} \Lambda(a) \ll \frac{q}{X} X = q$$

where the second step is Chebyshev's theorem.

Hence

$$T_\chi(X) = S_\chi(X)L(1,\chi) + O_q(1),$$

where the left-hand side is $O_q(1)$ too, so if $L(1,\chi) \neq 0$, then $S_\chi(X) = O_q(1)$. □

Date: February 13th, 2019.

15.2 Dirichlet L-functions at 1

This is one of Dirichlet's results:

Theorem 15.2.1 (Dirichlet)**.** *Let $\chi \pmod q$ be a nontrivial Dirichlet character. Then $L(1,\chi) \neq 0$.*

There are essentially two proofs of this, one using real analysis and one using complex analysis. We will discuss the second here.

Proof. Consider

$$L_q(s) = \prod_{\chi \,(\mathrm{mod}\ q)} L(s,\chi) = L(s,\chi_0) \prod_{\chi \neq \chi_0} L(s,\chi).$$

Note that this is a finite product since there are finitely many Dirichlet characters. If we enumerate those Dirichlet characters as $\chi_0, \chi_1, \ldots, \chi_{\varphi(q)-1}$, we have in other words

$$L_q(s) = L(s, \chi_0 \star \chi_1 \star \cdots \star \chi_{\varphi(q)-1}),$$

so

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

with $a_q(n) = \chi_0 \star \chi_1 \star \cdots \star \chi_{\varphi(q)-1}(n)$, with abscissa of convergence $\sigma_q \leq 1$ since it is bounded by the maximum of σ_χ for all χ, all of which are 1.

We will show two properties later, which we will use here:

1. $a_q(n) \geq 0$ for all $n \geq 1$, and
2. $a_q(n^{\varphi(q)}) \geq 1$ for all $(n,q) = 1$.

Evaluating our $L_q(s)$ at $\sigma = 1/\varphi(q)$, we get

$$\sum_{n=1}^{\infty} \frac{a_q(n)}{n^\sigma} \geq \sum_{(n,q)=1} \frac{a_q(n^{\varphi(q)})}{n} \geq \sum_{(n,q)=1} \frac{1}{n} = \infty,$$

so $\sigma_q \geq 1/\varphi(q)$. Hence

$$\frac{1}{\varphi(q)} \leq \sigma_q \leq 1.$$

This contradicts the following lemma of Landau. □

Lemma 15.2.2 (Landau)**.** *Let*

$$L(s) = \sum_{n \geq 1} \frac{f(n)}{n}$$

be a Dirichlet series with $\sigma_f < \infty$ and $f(n) \geq 0$ for all $n \in \mathbb{N}$. Then $L(s)$ does not admit a holomorphic continuation in a neighbourhood of $s = \sigma_f$.

The contradiction is as follows: By Landau's theorem, $L_q(s)$ does not admit a holomorphic continuation in some neighbourhood of $s = \sigma_f$. But by Proposition 14.1.2, $L_q(s)$ admits a meromorphic continuation to $\mathrm{Re}(s) > 0$ with the only possible simple pole at $s = 1$ (from χ_0).

However if we suppose $L(1,\chi) = 0$ for some $\chi \neq \chi_0$, then we no longer have a pole at $s = 1$, so $L_q(s)$ is holomorphic on $\mathrm{Re}(s) > 0$, which contradicts with Landau's lemma.

Lecture 16 Landau's lemma

We'll finish up the proof of Dirichlet's theorem by proving the three outstanding details: Landau's lemma, and our two conditions on the coefficients $a_q(n)$.

16.1 Landau's lemma

Lemma 16.1.1 (Landau)**.** *Let*

$$L(s) = \sum_{n\geq 1} \frac{f(n)}{n^s}$$

be a Dirichlet series with $\sigma_f < \infty$, and $f(n) \geq 0$ for all $n \in \mathbb{N}$. Then $L(s)$ does not admit a holomorphic continuation in a neighbourhood of $s = \sigma_f$.

Proof. Without loss of generality, assume $\sigma_f = 0$ (else replace $L(s)$ by $L(s-\sigma_f)$). Suppose that $L(s)$ has a holomorphic continuation in an open disk D centred at $\sigma_f = 0$. Thus $L(s)$ and all of its derivatives are holomorphic in $D \cup \{\, s \,|\, \mathrm{Re}(s) > 0 \,\}$. We will show that $L(\sigma)$ converges for some $\sigma \in D$ with $\sigma < 0$, which contradicts $\sigma_f = 0$, since $f(n) \geq 0$ means that this convergence is absolute at σ.

First, we claim that

$$\sum_{n\geq 1} f(n) = L(0).$$

In other words, what we naively would like the $L(0)$ to be is, in fact, correct.

Since $f(n) \geq 0$,

$$L(\sigma) = \sum_{n\geq 1} \frac{f(n)}{n^\sigma}$$

is increasing as $\sigma \to 0^+$, and it is also bounded above by $L(0)$. So by the monotone convergence theorem, $L(\sigma) \to L(0)$ as $\sigma \to 0^+$. Now consider

$$\sum_{n\leq n} f(n) = \lim_{\sigma\to 0^+} \sum_{n\leq N} \frac{f(n)}{n^\sigma} \leq \lim_{\sigma\to 0^+} \sum_{n=1}^{\infty} \frac{f(n)}{n^\sigma} = L(0).$$

On the other hand, for $\sigma > 0$,

$$L(\sigma) = \sum_{n\geq 1} \frac{f(n)}{n^\sigma} \leq \sum_{n\geq 1} f(n),$$

and as $\sigma \to 0^+$, the left-hand side goes to $L(0)$, so putting this together

$$L(0) \leq \sum_{n\geq 1} f(n) \leq L(0),$$

so they're equal.

Secondly, we claim that $L(\sigma)$ converges for some $\sigma < 0$, $\sigma \in D$.

Date: February 20th, 2019.

First, by assumption, L is holomorphic here. For $\mathrm{Re}(s) > 0$,

$$L^{(k)}(s) = (-1)^k \sum_{n \geq 1} \frac{f(n)(\log n)^k}{n^s}.$$

Now importantly $f(n)(\log n)^k \geq 0$, so the above argument again means that

$$L^{(k)}(0) = (-1)^k \sum_{n \geq 1} f(n)(\log n)^k.$$

For $\sigma \in D$ with $\sigma < 0$, we have the Taylor expansion

$$L(\sigma) = \sum_{k=0}^{\infty} \frac{L^{(k)}(0)}{k!}\sigma^k = \sum_{k=0}^{\infty} \frac{(-1)^k \sum f(n)(\log n)^k}{k!}\sigma_k.$$

Switching the order of summation, which we can do since $-\sigma \geq 0$, so we have absolute convergence and can rearrange the sum, we get

$$L(\sigma) = \sum_{n \geq 1} f(n) \sum_{k \geq 0} \frac{(-\sigma \log n)^k}{k!} = \sum_{n \geq 1} f(n) \exp(-\sigma \log n) = \sum_{n \geq 1} \frac{f(n)}{n^\sigma} < \infty.$$

□

With this done, we need to establish two things about the coefficients $a_q(n)$ of

$$L_q(s) = \prod_{\chi \pmod q} L(s, \chi) = \sum_{n=1}^{\infty} \frac{a_q(n)}{n^s}.$$

The two items it remains to show is that first, $a_q(n) \geq 0$ for all n, and second, $a_q(n^{\varphi(q)}) \geq 1$ for $(n, q) = 1$.

Since $a_q(n)$ is multiplicative (being the convolution of many (completely) multiplicative characters χ), it suffices to show $a_q(p^k) \geq 0$ for all primes p, $k \geq 0$.

We have

$$(L_q)_p(s) = \prod_{\chi \pmod q} L_p(s, \chi) = \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{k \geq 0} \frac{a_q(p^k)}{p^{ks}}.$$

Now if $p \mid q$¡ then $(L_q)_p(s) = 1$, so

$$a_q(p^k) = \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{if } k \neq 0, \end{cases}$$

which is definitely nonnegative.

If $(p, q) = 1$, then for notational convenience let $z = p^{-s}$. We have $|z| < 1/p$ for $\mathrm{Re}(s) > 1$. Let

$$E(z) = \prod_{\chi} (1 - \chi(p)z)^{-1} = \sum_{k \geq 0} a_q(p^k) z^k.$$

Taking logarithms,

$$\log E(z) = \sum_{\chi} -\log(1 - \chi(p)z) = \sum_{\chi} \sum_{k \geq 1} \frac{\chi(p)^k z^k}{k}$$

where we've Taylor expanded the logarithm, since $|z| < 1/p < 1$. Switching the order of summation, this is

$$\log E(z) = \sum_{k \geq 1} \frac{z^k}{k} \sum_{\chi} \chi(p^k) = \varphi(q) \sum_{\substack{k \geq 1 \\ p^k \equiv 1 \pmod{q}}} \frac{z^k}{k}.$$

Note that this is a power series with nonnegative coefficients, so taking exponentials to retrieve $E(z)$, we get

$$E(z) = \exp(\log E(z)) = 1 + \log E(z) + \frac{(\log E(z))^2}{2!} + \dots,$$

whence the coefficients of $E(z)$ are also nonnegative, so $a_q(p^k) \geq 0$.

For the second property, consider $n = p^m$. We want $a_q(p^{m\varphi(q)}) \geq 1$, with $(p, q) = 1$. Let e_p be the order of p in $(\mathbb{Z}/q\mathbb{Z})^\times$, i.e. $p^{\varphi(q)} \equiv 1 \pmod{q}$. Then $p^k \equiv 1 \pmod{q}$ if and only if $e_p \mid k$, by Lagrange's theorem. Hence $e_p \mid \varphi(q)$.

In the above computation, then,

$$\log E(z) = \frac{\varphi(q)}{e_p} \sum_{k} \frac{z^{e_p k}}{k} = \frac{\varphi(q)}{e_p} \left(-\log(1 - z^{e_p})\right) = \log\left((1 - z^{e_p})^{-\varphi(q)/e_p}\right),$$

so

$$E(z) = (1 - z^{e_p})^{-\varphi(q)/e_p} = \left(\frac{1}{1 - z^{e_p}}\right)^{\varphi(q)/e_p} = \left(1 + z^{e_p} + z^{2e_p} + \dots\right)^{\varphi(q)/e_p}.$$

The exponent is an integer, and $e_p \mid m\varphi(q)$, so if $h = m\varphi(q)$, $a_q(p^k)$ is the kth coefficient, and hence $a_q(p^k) \geq 1$.

Lecture 17 Riemann's memoir

17.1 Riemann's memoir

In 1860 Riemann published his one and only paper on number theory. In it he proved two results:

1. The Riemann zeta function $\zeta(s)$ has a meromorphic continuation to all of $\mathbb{C}$. It is holomorphic except for $s = 1$, which is a simple pole with residue 1.

2. $\zeta(s)$ satisfies the functional equation

$$\pi^{-\frac{1}{2}s}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{\frac{1}{2}(1-s)}\Gamma\left(\frac{1}{2}(1-s)\right)\zeta(1-s),$$

which is invariant under the transformation $s \mapsto 1 - s$.

Riemann further made several remarkable conjectures:

Date: February 22nd, 2019.

1. $\zeta(s)$ has infinitely many zeros in the critical strip $0 < \mathrm{Re}(s) < 1$.

   Note that the distribution of zeros is symmetric with respect to the real axis and $\mathrm{Re}(s) = 1/2$.

2. The number $N(T)$ of zeros of $\zeta(s)$ in the critical strip with $0 < \mathrm{Im}(s) < T$ satisfies
$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T),$$
   proved by von Mangoldt in 1895. We will show $N(T) \sim T \log T$.

3. The integral function
$$\zeta_0(s) = s(s-1)\pi^{-\frac{1}{2}s}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$
   has the product representation
$$\zeta_0(s) = e^{A+Bs}\prod_{\rho}\left(1 - \frac{s}{\rho}\right)e^{s/\rho},$$
   where A and B are constants and ρ runs through the zeros of $\zeta(s)$ in the critical strip. This was proved by Hadamard in 1893, and is a special case of the Hadamard factorisation theorem. (Note that $s-1$ comes from the pole, and s comes from the wish to make it invariant under $s \mapsto 1-s$.)

4. There exists an explicit formula for $\pi(x) - \mathrm{Li}(x)$ with $x > 1$, involving a sum over the zeroes of $\zeta(s)$. This was proved by von Mangoldt in 1895.

5. Finally, and most importantly, the ***Riemann hypothesis***: the zeros of $\zeta(s)$ in the critical strip all lie on the critical line $\mathrm{Re}(s) = 1/2$.

   This, of course, remains unproven. There has been some progress, the most important of which is: Hardy, in 1914, showed that there are infinitely many zeros on $\mathrm{Re}(s) = 1/2$. (His argument also generalises to $L(s,\chi)$, and moreover to GL_2 L-functions, but for higher dimensions it remains unknown.)

   Then, in 1942, Selberg showed that there is a positive proportion of zeros of $\zeta(s)$ in the critical strip lying on the critical line. This is where the (very powerful) mollifier method comes from.

17.2 Review of Fourier analysis

Definition 17.2.1. Let $(G,+)$ be an abelian topological group, i.e. $(G,+)$ is an abelian group, G is a topological space, and moreover
$$\begin{aligned} G \times G &\to G \\ (a,b) &\mapsto a+b \end{aligned}$$
and
$$\begin{aligned} G &\to G \\ a &\mapsto -a \end{aligned}$$

are continuous.

A ***character*** ψ of G is a continuous group homomorphism $\psi\colon G \to \mathbb{C}^\times$. Let $\mathrm{Hom}(G, \mathbb{C}^\times)$ denote the set of all such characters. It is an abelian group under the multiplication of functions.

Definition 17.2.2. A character ψ is called ***unitary*** if $\psi\colon G \to S^1 = \{\, z \in \mathbb{C}^\times \mid |z| = 1 \,\}$. Let $\hat{G}$ denote the subgroup of $\mathrm{Hom}(G, \mathbb{C}^\times)$ consisting of unitary characters.

Remark 17.2.3. If G is compact, then every character is unitary.

Proof. Let $\psi\colon G \to \mathbb{C}^\times$ be a character. Then its image $\psi(G)$ is compact since G is compact and ψ, by definition, is continuous. Hence $\psi(G)$ is closed and bounded, since this characterises compact sets in $\mathbb{C}$.

Now suppose there exists some $\psi(g) = z$ with $|z| \neq 1$. Then $\psi(g^n) = \psi(g)^n = z^n \in \psi(G)$. Since $|z| \neq 1$, we have two options: if it exceeds 1, then as n increases, z^n diverges to infinity, which contradicts $\psi(G)$ being bounded. If $|z| < 1$, then z^n converges to 0, and this contradicts $\psi(G)$ being closed. □

In the sequel we will write $\mathrm{e}(x) \coloneqq \exp(2\pi i x)$.

Theorem 17.2.4. *The map $\varphi\colon (\mathbb{C}, +) \to \mathrm{Hom}(\mathbb{R}, \mathbb{C}^\times)$ defined by $y \mapsto \varphi_y$, with $\varphi_y(x) \coloneqq \mathrm{e}(yx)$ is an isomorphism of groups. The restriction of φ to $\mathbb{R}$ gives an isomoprhism of groups $(\mathbb{R}, +) \cong \hat{\mathbb{R}}$.*

Lecture 18 Poisson summation

18.1 Fourier analysis

Proof. That this is a homomorphism is clear by definition.

To see that it is injective, let $y \in \ker \varphi$. Then $\varphi_y(x) = \mathrm{e}(xy) = 1$ for every $x \in \mathbb{R}$, which naturally requires $y = 0$.

For surjectivity, given $\psi \in \mathrm{Hom}(\mathbb{R}, \mathbb{C}^\times)$ we need to show that $\psi(x) = \mathrm{e}(xy)$ for some $y \in \mathbb{C}$. To this end, let

$$\Psi(x) = \int_0^x \psi(t)\, dt.$$

Then

$$\Psi(x+y) = \int_0^{x+y} \psi(t)\, dt = \int_0^x \psi(t)\, dt + \int_x^{x+y} \psi(t)\, dt.$$

In the latter integral, shift $t \mapsto t + x$, so

$$\int_x^{x+y} \psi(t)\, dt = \int_0^y \psi(t+x)\, dt = \int_0^y \psi(t)\psi(x)\, dt$$

since ψ is a homomorphism. Hence the above becomes

$$\Psi(x+y) = \int_0^x \psi(t)\, dt + \psi(x) \int_0^y \psi(t)\, dt.$$

Date: February 25th, 2019.

In other words,

$$\Psi(x+y) = \Psi(x) + \psi(x)\Psi(y).$$

We now fix y such that $\Psi(y) \neq 0$. This is possible since $\Psi'(t) = \psi(t)$ isn't identically zero.

Taking derivatives with respect to x, this results in

$$\psi(x+y) = \psi(x) + \psi'(x)\Psi(y),$$

where again we use the fact that ψ is a homomorphism to rewrite this as

$$\psi(x)\psi(y) = \psi(x) + \psi'(x)\Psi(y).$$

Rearranging this becomes

$$\Psi(y)\psi'(x) + (1-\psi(y))\psi(x) = 0,$$

which is a first order ordinary differential equation, and

$$\psi(x) = C\exp(ux)$$

for some constants $C, u \in \mathbb{C}$. Now $\psi(0) = 1$ so $C = 1$, i.e. $\psi(x) = \exp(ux)$, so we have surjectivity! □

Note that $\varphi_y(x)$ is unitary if and only if $y \in \mathbb{R}$, since $\mathrm{e}(xy) = \exp(2\pi ixy)$, and $x \in \mathbb{R}$.

Corollary 18.1.1. *The map*

$$(\mathbb{Z}, +) \to \mathrm{Hom}(\mathbb{R}/\mathbb{Z}, \mathbb{C}^\times) = \widehat{\mathbb{R}/\mathbb{Z}}$$

defined by $n \mapsto \varphi_n$, $\varphi_n(x) = \mathrm{e}(nx)$, is an isomorphism of groups.

Proof. First, note that $\mathrm{Hom}(\mathbb{R}/\mathbb{Z}, \mathbb{C}^\times) = \widehat{\mathbb{R}/\mathbb{Z}}$ since $\mathbb{R}/\mathbb{Z}$ is compact.

The injectivity part is identical to what we did for the previous theorem.

For the onto part, consider $\psi\colon \mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times$. Extend it to $\psi\colon \mathbb{R} \to \mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times$ periodically, i.e. $\psi\big|_{\mathbb{Z}} \equiv 1$. Using the previous theorem., $\psi = \varphi_y$ with $y \in \mathbb{R}$ by unitarity. Moreover $\psi(1) = \varphi_y(1) = \mathrm{e}(y) = 1$ since $1 \in \mathbb{Z}$, so $y \in \mathbb{Z}$. □

Definition 18.1.2. A function $f\colon \mathbb{R} \to \mathbb{C}$ is said to be in the ***Schwartz class*** $\mathcal{S}(\mathbb{R})$ if f and all of its derivatives are rapidly decaying, meaning that for all $A \geq 0$ and $j \geq 0$,

$$f^{(j)}(x) \ll (1+|x|)^{-A}.$$

In other words, f and its derivatives go to 0 very quickly.

Definition 18.1.3. Let $f \in \mathcal{S}(\mathbb{R})$. The ***Fourier transform*** of f is the function

$$\hat{f}(y) = \int_{\mathbb{R}} f(x)\,\mathrm{e}(-yx)\,dx,$$

for $y \in \mathbb{R}$.

Remark 18.1.4. Because of the rapid decay, $\hat{f}(y)$ converves absolutely and uniformly for all $y \in \mathbb{R}$. Hence $\hat{f}$ is infinitely differentiable with

$$\hat{f}^{(j)}(y) = \int_{\mathbb{R}} (-2\pi i x)^j f(x) e(-yx)\, dx.$$

Integrating this by parts, for $y \neq 0$, we have

$$\hat{f}^{(j)}(y) = \frac{1}{2\pi i y} \int_{\mathbb{R}} f'(x) e(-yx)\, dx = \frac{1}{2\pi i y} \widehat{f'}(y) = \left(\frac{1}{2\pi i y}\right)^j \widehat{f^{(j)}}(y).$$

So for $|y| \geq 1$,

$$\hat{f}(y) \ll |y|^{-j} \int_{\mathbb{R}} |f^{(j)}(x)|\, dx \ll |y|^{-j}$$

for every $j \geq 0$. Hence

Proposition 18.1.5. *The Fourier transform is a linear map from $\mathcal{S}(\mathbb{R})$ to $\mathcal{S}(\mathbb{R})$.*

Let us note a few basic properties of the Fourier transformation. Let $f \in \mathcal{S}(\mathbb{R})$.

1. Let $h \in \mathbb{R}$, and $g(x) = f(x+h)$. Then $\hat{g}(y) = \mathrm{e}(-hy)\hat{f}(y)$.
2. $\widehat{f^{(j)}}(y) = (2\pi i y)^j \hat{f}(y)$.
3. Let $\lambda \in \mathbb{R}$, $\lambda \neq 0$, and $g(x) = f(\lambda x)$. Then $\hat{g}(y) = \frac{1}{|\lambda|}\hat{f}(y/\lambda)$.
4. The Fourier inversion formula says $\hat{\hat{f}}(x) = f(-x)$.
5. The Fourier transform of the Gaussian: if $f(x) = e^{-\pi x^2}$, then $\hat{f}(y) = f(y)$.

One particular and very important property is

Theorem 18.1.6 (Poisson summation formula)**.** *Let $f \in \mathcal{S}(\mathbb{R})$. Then for $x \in \mathbb{R}$,*

$$\sum_{n \in \mathbb{Z}} f(x+n) = \sum_{n \in \mathbb{Z}} \hat{f}(n)\, \mathrm{e}(nx).$$

Proof. Let

$$g(x) = \sum_{n \in \mathbb{Z}} f(x+n).$$

Since $f \in \mathcal{S}(\mathbb{R})$, $g(x)$ converges absolutely and uniformly for all $x \in \mathbb{R}$. Hence we can rearrange terms, differentiate or integrate under the summation, and so on, and $g \in C^\infty(\mathbb{R})$, and it is periodic with period 1 by construction. Hence $g(x)$ has a Fourier expansion,

$$g(x) = \sum_{n \in \mathbb{Z}} a(n)\, \mathrm{e}(nx),$$

with

$$\begin{aligned} a(n) &= \int_0^1 g(x)\,\mathrm{e}(-nx)\,dx = \int_0^1 \sum_{m\in\mathbb{Z}} f(x+m)\,\mathrm{e}(-nx)\,dx \\ &= \sum_{m\in\mathbb{Z}} \int_0^1 f(x+m)\,\mathrm{e}(-n(x+m))\,dx = \sum_{m\in\mathbb{Z}} \int_m^{m+1} f(t)\,\mathrm{e}(-nt)\,dt \\ &= \int_{\mathbb{R}} f(t)\,\mathrm{e}(-nt)\,dt = \hat{f}(n). \end{aligned}$$

Hence

$$g(x) = \sum_{n\in\mathbb{Z}} \hat{f}(n)\,\mathrm{e}(nx).$$

□

Corollary 18.1.7. *For $f \in \mathcal{S}(\mathbb{R})$,*

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

Proof. Take $x = 0$ in the previous theorem. □

This result is true in general for averaging over any lattice.

Lecture 19 The functional equation for $\zeta(s)$

19.1 Mellin transformation

An important corollary to the Poisson summation formula is the following, doing the same kind of averge but over an arithmetic sequence,

Corollary 19.1.1. *Let $q, a \in \mathbb{Z}$ with $q \geq 1$. For $f \in \mathcal{S}(\mathbb{R})$,*

$$\sum_{n\equiv a \pmod q} f(n) = \frac{1}{q} \sum_{n\in\mathbb{Z}} \hat{f}\left(\frac{n}{q}\right) \mathrm{e}\left(\frac{qn}{q}\right).$$

Proof. First note that

$$\sum_{n\equiv q \pmod q} f(n) = \sum_{n\in\mathbb{Z}} f(qk+q).$$

Let $g(x) = f(qx+a)$, an affine shift. By the properties of the Fourier transformation,

$$\hat{g}(y) = \frac{1}{q} \hat{f}\left(\frac{y}{q}\right) \mathrm{e}\left(\frac{ay}{q}\right),$$

so

$$\sum_{n\in\mathbb{Z}} f(qk+q) = \sum_{n\in\mathbb{Z}} g(n) = \sum_{n\in\mathbb{Z}} \hat{g}(n) = \frac{1}{q} \sum_{n\in\mathbb{Z}} \hat{f}\left(\frac{n}{q}\right) \mathrm{e}\left(\frac{an}{q}\right).$$ □

Date: February 27th, 2019.

Definition 19.1.2. Let $f(x) \in C^\infty(\mathbb{R}_{\geq 0})$ with rapid decay as $x \to \infty$. The ***Mellin transform*** of f is

$$\tilde{f}(s) = \int_0^\infty f(x) x^s \frac{dx}{x},$$

for $s \in \mathbb{C}$, $\mathrm{Re}(s) > 0$.

The integral converges uniformly on compact subsets of $\{ s \in \mathbb{C} \,|\, \mathrm{Re}(s) > 0 \}$ since f decays rapidly, and hence $\tilde{f}(s)$ is a holomorphic function in $\mathrm{Re}(s) > 0$.

Moreover, note that if $f(x) = O(x^N)$ as $x \to 0$, then $\tilde{f}(s)$ defines a holomorphic function in the domain $\mathrm{Re}(s) > -N$, by just studying the power of x in the integrand.

Like the Fourier transform, the Mellin transform has an inversion formula: Suppose $f \in \mathcal{S}(\mathbb{R})$. For any $y > 0$,

$$f(y) = \frac{1}{2\pi i} \int_{(\sigma)} \tilde{f}(s) y^{-s} \, ds$$

for any $\sigma > 0$, where (σ) means the line $\sigma + it$ for $-\infty < t < \infty$.

Remark 19.1.3. The Mellin inversion formula and the Fourier inversion formula are equivalent.

19.2 Gamma function

The Gamma function is defined as the Mellin transform of e^{-x}, i.e.

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

for $\mathrm{Re}(s) > 0$.

This function, which turns out to be remarkably important, has many fascinating properties. For instance,

1. $\Gamma(s)$ admits a meromorphic continuation to $\mathbb{C}$, which has simple poles at $s = -n$, $n = 0, 1, 2, \ldots$ with residues $(-1)^n/n!$, and no other poles;
2. $\Gamma(s+1) = s\Gamma(s)$;
3. $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$;
4. $\Gamma(s)\Gamma(s+\frac{1}{2}) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s)$;
5. $\Gamma(\frac{1}{2}) = \sqrt{\pi}$, and $\Gamma(k+1) = k!$ for $k = 0, 1, 2, \ldots$ (which is a consequence of property 2);
6. $\Gamma(s)$ has no zeros, i.e. $\Gamma(s) \neq 0$ for all $s \in \mathbb{C}$; and finally (and incredibly usefully),
7. Sterling's formula: For any $s > 0$, $-\pi + \delta < \arg s < \pi - \delta$,

$$\log \Gamma(s) = \left(s - \frac{1}{2}\right) \log s - s + \frac{1}{2} \log(2\pi) + O\left(\frac{1}{|s|}\right)$$

as $|s| \to \infty$.

19.3 The functional equation for $\zeta(s)$

Theorem 19.3.1. *Let*

$$\xi(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

for $\mathrm{Re}(s) > 1$. *Then* $\xi(s)$ *has a meromorphic continuation to* $\mathbb{C}$, *holomorphic on* $\mathbb{C} \setminus \{0, 1\}$, *and has simple poles as* $s = 0$ *ans* $s = 1$ *with residues* -1 *and* 1 *respectively.*

Moreover it satisfies the functional equation

$$\xi(s) = \xi(1 - s).$$

Proof. By the definition of Γ,

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty e^{-t}t^{\frac{1}{2}t}\frac{dt}{t}.$$

Let $t = n^2\pi x$. Then

$$\pi^{-\frac{1}{2}s}\Gamma\left(\frac{s}{2}\right)n^{-s} = \int_0^\infty e^{-n^2\pi x}x^{\frac{1}{2}s}\frac{dx}{x}.$$

Summing this over n, so as to develop a $\zeta(s)$ on the left-hand side, this becomes

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \sum_{n=1}^\infty \int_0^\infty e^{-n^2\pi x}x^{\frac{1}{2}s}\frac{dx}{x} = \int_0^\infty \left(\sum_{n=1}^\infty e^{-n^2\pi x}\right)x^{\frac{1}{2}x}\frac{dx}{x},$$

where switching the sum and integration is permitted since the rapid decay of the exponential gives us uniform convergence.

Let

$$w(x) = \sum_{n=1}^\infty e^{-n^2\pi x},$$

so that

$$\xi(s) = \int_0^\infty w(x)x^{\frac{1}{2}s}\frac{dx}{x} = \int_0^1 w(x)x^{\frac{1}{2}s}\frac{dx}{x} + \int_1^\infty w(x)x^{\frac{1}{2}s}\frac{dx}{x}.$$

Riemann's trick was splitting this integral into two, and now performing the change of variables $x \mapsto 1/x$ in the first one

$$\xi(s) = \int_1 w\left(\frac{1}{x}\right)x^{-\frac{1}{2}s}\frac{dx}{x} + \int_1^\infty w(x)x^{\frac{1}{2}s}\frac{dx}{x}.$$

In order to make sense of $w(x)$, we wish to extend it to a sum over all $n \in \mathbb{Z}$, rather than $n \geq 1$, so that we may use Poisson summation on it. To this end,

Definition 19.3.2. The ***theta series*** $\theta(x)$ is defined by

$$\theta(x) = \sum_{n\in\mathbb{Z}} e^{-n^2\pi x} = 1 + 2\sum_{n\geq 1} e^{-n^2\pi x} = 1 + 2w(x),$$

so

$$w(x) = \frac{1}{2}(\theta(x) - 1).$$

We'll prove the following lemma for the theta series in a moment:

Lemma 19.3.3. *$\theta\left(\frac{1}{x}\right) = x^{1/2}\theta(x)$ for $x > 0$.*

Taking the lemma for granted just now, we then get

$$w\left(\frac{1}{x}\right) = \frac{1}{2}\left(\theta\left(\frac{1}{x}\right) - 1\right) = \frac{1}{2}(x^{1/2}\theta(x) - 1) = \frac{1}{2}(x^{1/2}(1 + 2w(x)) - 1)$$
$$= -\frac{1}{2} + \frac{1}{2}x^{1/2} + x^{1/2}w(x).$$

Hence

$$\int_1^\infty w\left(\frac{1}{x}\right) x^{-\frac{1}{2}s}\frac{dx}{x} = \int_1^\infty \left(-\frac{1}{2} + \frac{1}{2}x^{1/2} + x^{1/2}w(x)\right) x^{-\frac{1}{2}s}\frac{dx}{x}$$
$$= -\frac{1}{s} + \frac{1}{s-1} + \int_1^\infty w(x)x^{\frac{1}{2}(1-s)}\frac{dx}{x}.$$

Therefore

$$\xi(s) = -\frac{1}{s} + \frac{1}{s-1} + \int_1^\infty w(x)\left(x^{\frac{1}{2}(1-s)} + x^{\frac{1}{2}s}\right)\frac{dx}{x}.$$

Staring at this carefully we see that the first term above is defined for $s \neq 0$, the second is defined for $s \neq 1$, and the integral is defined for all $s \in \mathbb{C}$ since $w(x)$ decays rapidly. Hence $\xi(s)$ has meromorphic continuation to $\mathbb{C}$ from the right-hand side, and $\xi(s) = \xi(1-s)$ since the right-hand side is symmetric under $s \mapsto 1 - s$. □

Lecture 20 The functional equation for L-functions

20.1 Theta series

It remains, form the last result, to prove

Lemma 20.1.1. *$\theta(\frac{1}{x}) = x^{1/2}\theta(x)$ for $x > 0$.*

Proof. Let $f(y) = e^{-y^2\pi x}$. Then

$$\hat{f}(u) = \frac{1}{\sqrt{x}}e^{-\pi u^2/x},$$

so

$$\theta(x) = \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n) = \frac{1}{\sqrt{x}}\sum_{n\in\mathbb{Z}} e^{-\pi n^2/x} = \frac{1}{\sqrt{x}}\theta\left(\frac{1}{x}\right),$$

by Poisson summation. □

Corollary 20.1.2. *The Riemann zeta function $\zeta(s)$ has analytic continuation to $\mathbb{C}\setminus\{1\}$, has a simple pole at $s = 1$ with residue 1, and satisfies the functional equation*

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

Date: March 1st, 2019.

Proof. Recall how

$$\xi(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

is holomorphic except at $s = 0$ and $s = 1$.

At $s = 0$, it has a simple pole. Moreover, $\Gamma(\frac{s}{2})$ has a simple pole at $s = 0$, so $\zeta(s)$ must not have a pole there, since otherwise we have a double pole. For the same reason, $\zeta(0) \neq 0$.

At $s = 1$, $\xi(s)$ has a simple pole with residue 1, but $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ does not, so $\zeta(s)$ must have a simple pole at $s = 1$. Moreover

$$1 = \operatorname*{Res}_{s=1}\xi(s) = \pi^{-\frac{1}{2}}\pi^{\frac{1}{2}}\operatorname*{Res}_{s=1}\zeta(s),$$

so the residue of $\zeta(s)$ at $s = 1$ is 1.

Finally $\xi(s) = \xi(1 - s)$ implies that

$$\zeta(1-s) = \pi^{\frac{1}{2}-s}\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}\zeta(s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s)$$

by manipulating the Gamma factors. □

20.2 Trivial zeros of $\zeta(s)$

Since

$$\xi(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

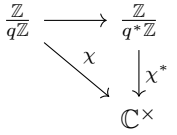
is holomorphic in $\mathrm{Re}(s) < 0$, and since $\Gamma(\frac{s}{2})$ has simple poles as $s = -2, -4, -6, \ldots$, it means that $\zeta(s) = 0$ for $s = -2, -4, -6, \ldots$. We call those the ***trivial zeros*** of $\zeta(s)$.

20.3 Functional equations of L-functions

Definition 20.3.1. Let χ be a Dirichlet character modulo q. Then there exists a minimal $q^* \mid q$ such that $\chi = \chi_0 \cdot \chi^*$, with χ^* a Dirichlet character modulo q^* and χ_0 the trivial character modulo q.

This character χ^* is uniquely determined by χ, and q^* is called the ***conductor*** of χ. If $q^* = q$, then χ is called a ***primitive character***.

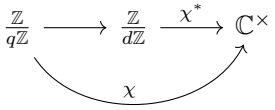
We think of it in terms of the following commutative diagram:



Proposition 20.3.2. *The number of primitive characters modulo q is*

$$\varphi^*(q) = \varphi \star \mu(q) = \sum_{d\mid q}\mu(d)\varphi\left(\frac{q}{d}\right) = q\prod_{p\parallel q}\left(1-\frac{2}{p}\right)\prod_{p^2\parallel q}\left(1-\frac{1}{p}\right)^2.$$

Proof. The number of Dirichlet characters modulo q is $\varphi(q)$. Now for $d \mid q$, consider the diagram



Hence for every $d \mid q$, if we find the primitive characters modulo d and extend them (as we know we can) to characters modulo q. In other words,

$$\varphi(q) = \sum_{d|q} \varphi^*(d),$$

i.e. $\varphi = \varphi^* \star 1$. By Möbius inversion, convolving with μ, we get $\varphi^* = \varphi \star \mu$. □

Remark 20.3.3. Note that because of the first factor above, $\varphi^*(q) = 0$ if and only if $2 \mid q$ and $2^2 \nmid q$, i.e. $q \equiv 2 \pmod 4$. Hence primitive characters χ modulo q exist only when $q \not\equiv 2 \pmod 4$.

Proposition 20.3.4. *For $(n, q) = 1$, we have*

$$\sum_{\chi \,(\mathrm{mod}\ q)}^{*} \chi(n) = \sum_{d|(n-1,q)} \varphi(d)\mu\left(\frac{q}{d}\right),$$

where by $\sum^*$ we mean that we sum only over primitive characters.

Example 20.3.5. For $q = 4$, $\varphi^*(4) = 1$, so there is only one primitive Dirichlet character modulo 4, namely $\chi_4(n) = (-1)^{\frac{n-1}{2}}$ if $2 \nmid n$, else 0. Specifically $\chi_4(1) = -1$, $\chi_4(3) = 1$, and otherwise it is 0. ▲

Example 20.3.6. For $q = 8$, $\varphi^*(8) = 2$, so there are two primitive characters. The first one is $\chi_8(n) = (-1)^{\frac{(n-1)(n+1)}{8}}$ if $2 \nmid n$, and the second one is $\chi_4 \cdot \chi_8(n) = (-1)^{\frac{(n-1)(n+5)}{8}}$ if $2 \nmid n$. ▲

20.4 Gauss sums

Definition 20.4.1. Let $\chi \pmod q$ be a Dirichlet character. Then

$$\tau(\chi) = \sum_{b \,(\mathrm{mod}\ q)} \chi(b)\,\mathrm{e}\left(\frac{b}{q}\right)$$

is called the ***Gauss sum*** of χ.

Note that this sum only sums over $b \in (\mathbb{Z}/q\mathbb{Z})^\times$ since otherwise $\chi(b) = 0$. By orthogonality, for $(a, q) = 1$,

$$\mathrm{e}\left(\frac{a}{q}\right) = \frac{1}{\varphi(q)} \sum_{\chi \,(\mathrm{mod}\ q)} \overline{\chi}(a)\tau(\chi).$$

This formula is very useful since it transforms from an additive character to a multiplicative character. Note also that it is the Fourier expansion of the additive character on $(\mathbb{Z}/q\mathbb{Z})^\times$.

Proposition 20.4.2. *Let χ be a primitive character modulo q. Then*

$$\sum_{b \,(\mathrm{mod}\ q)} \chi(b)\,\mathrm{e}\left(\frac{ab}{q}\right) = \overline{\chi}(a)\tau(\chi).$$

Lecture 21 The functional equation for L-functions, continued

21.1 Gauss sums

Proposition 21.1.1. *Let χ be a primitice character modulo q. Then*

$$\sum_{b \pmod q} \chi(b)\,\mathrm{e}\left(\frac{ab}{q}\right) = \overline{\chi(a)}\tau(\chi).$$

Proof. We have two cases to consider: when $(a,q)=1$, and when they're not coprime. Let us start with when they are.

Then

$$\begin{aligned}\sum_{b \pmod q} \chi(b)\,\mathrm{e}\left(\frac{ab}{q}\right) &= \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi(b)\,\mathrm{e}\left(\frac{ab}{q}\right) = \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi(ba^{-1})\,\mathrm{e}\left(\frac{aba^{-1}}{q}\right)\\ &= \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi(b)\chi(a^{-1})\,\mathrm{e}\left(\frac{b}{q}\right) = \overline{\chi(a)}\tau(\chi),\end{aligned}$$

where we sum only over units since otherwise the charcater is 0 anyway, and we perform the change of variable $b \mapsto ba^{-1}$ since that just permutes the terms we're summing over.

If $(a,q)\neq 1$, then $\overline{\chi(a)}=0$, so we need to show that

$$\sum_{b \pmod q} \chi(b)\,\mathrm{e}\left(\frac{ab}{q}\right) = 0.$$

Letting $d=(a,q)$ and writing $a=da_1$, $q=dq_1$, with (a_1,q_1), so that

$$\begin{aligned}\sum_{b \pmod q} \chi(b)\,\mathrm{e}\left(\frac{ab}{q}\right) &= \sum_{b \pmod q} \chi(b)\,\mathrm{e}\left(\frac{a_1 b}{q_1}\right)\\ &= \sum_{r \pmod{q_1}} \left(\sum_{\substack{b \pmod q\\ b\equiv r \pmod{q_1}}} \chi(b)\right) \mathrm{e}\left(\frac{a_1 r}{q_1}\right).\end{aligned}$$

We claim, and will prove momentarily, that there exists some $c \equiv q \pmod{q_1}$ with (c,q) such that $\chi(c)\neq 1$.

In that case,

$$\sum_{\substack{b \pmod q\\ b\equiv r \pmod{q_1}}} \chi(b) = \sum_{\substack{b \pmod q\\ b\equiv r \pmod{q_1}}} \chi(bc) = \chi(c) \sum_{\substack{b \pmod q\\ b\equiv r \pmod{q_1}}} \chi(b)$$

by changing $b \mapsto bc$, since c is a unit modulo q. Then

$$(1-\chi(c)) \sum_{\substack{b \pmod q\\ b\equiv r \pmod{q_1}}} \chi(b) = 0,$$

Date: March 4th, 2019.

so the sub over the characters must be zero, since $\chi(c) \neq 1$.

Now let us prove the claim. Suppose there is no such c, i.e., $\chi(c) = 1$ for all $c \equiv 1 \pmod{q_1}$ with $(c, q) = 1$. Then for any $m, n \in (\mathbb{Z}/q\mathbb{Z})^\times$ with $n \equiv m \pmod{q_1}$, we have $n\bar{m} \equiv 1 \pmod{q_1}$, where by $\bar{m}$ we mean the multiplicative inverse modulo q_1. Thus $\chi(n\bar{m}) = 1$, implying that $\chi(n) = \chi(m)$, meaning that χ factors modulo q_1, so it is not primitive. □

Proposition 21.1.2. *Let χ be a primitive character modulo q. Then $|\tau(\chi)| = \sqrt{q}$.*

Proof. We write

$$\left|\overline{\chi(a)}\tau(\chi)\right|^2 = \left|\sum_{b \pmod q} \chi(b)\,\mathrm{e}\left(\frac{ab}{q}\right)\right|^2 = \sum_{\substack{b_1 \pmod q \\ b_2 \pmod q}} \chi(b_1)\overline{\chi(b_2)}\,\mathrm{e}\left(\frac{a(b_1-b_2)}{q}\right).$$

Now summing this over $a \pmod q$, we note that the right-hand side is nonzero only for $b_1 - b_2 = 0$ since by orthogonality

$$\sum_{a \pmod q} \mathrm{e}\left(\frac{am}{q}\right) = \begin{cases} 0 & \text{if } q \nmid m, \\ q & \text{if } q \mid m. \end{cases}$$

Hence

$$|\tau(\chi)|^2 \sum_{a \pmod q} |\chi(a)|^2 = q \sum_{b \pmod q} |\chi(b)|^2,$$

where the sums are nonzero, so dividing through we get $|\tau(\chi)|^2 = q$. □

The proof of the functional equation for $L(s, \chi)$ is now very similar to that of the Riemann zeta function.

Theorem 21.1.3. *Let χ be a primitive character modulo q. Let*

$$\Lambda(s, \chi) = L_\infty(s, \chi)L(s, \chi)$$

be the completed L-function, where

$$L_\infty(s, \chi) = \left(\frac{q}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\kappa}{2}\right)$$

is called the **archimedean factor** *of the* **(local) factor at infinity**, *and*

$$\kappa = \frac{1}{2}(1 - \chi(-1)) = \begin{cases} 0 & \text{if } \chi \text{ is even,} \\ 1 & \text{if } \chi \text{ is odd.} \end{cases}$$

A character χ being even means $\chi(-1) = 1$, so that $\chi(-n) = \chi(n)$, and odd correspondingly means $\chi(-1) = -1$, so $\chi(-n) = -\chi(n)$.

Then $\Lambda(s, \chi)$ has a holomorphic continuation to all $s \in \mathbb{C}$ and satisfies the functional equation

$$\Lambda(s, \chi) = \varepsilon(\chi)\Lambda(1 - s, \overline{\chi}),$$

where

$$\varepsilon(\chi) = i^\kappa \frac{\tau(\chi)}{\sqrt{q}}$$

is called the **root number** *of χ.*

Note that by the previous proposition, $|\varepsilon(\chi)| = 1$.

Proof. We separate the case where χ is even and where it's odd. If it is even, we use the definition of $\Gamma(s)$, from which we have

$$\pi^{-\frac{1}{2}s} q^{\frac{1}{2}s} \Gamma\left(\frac{1}{2}s\right) n^{-s} = \int_0^\infty e^{-\frac{n^2\pi t}{q}} t^{\frac{1}{2}s} \frac{dt}{t}$$

for $\mathrm{Re}(s) > 0$. (Cf. $\zeta(s)$ with $q = 1$.) Twisting by $\chi(n)$ and summing over n, we get

$$\pi^{-\frac{1}{2}s} q^{\frac{1}{2}s} \Gamma\left(\frac{1}{2}s\right) L(s,\chi) = \int_0^\infty \left(\sum_{n\geq 1} \chi(n) e^{-\frac{n^2\pi t}{q}}\right) t^{\frac{1}{2}s} \frac{dt}{t}.$$

We switch the order of integration and summation since the exponential decay guarantees us absolute and uniform convergence for $\mathrm{Re}(s) > 1$.

Now let

$$\theta_\chi(t) = \sum_{n=-\infty}^{\infty} \chi(n) e^{-\frac{n^2\pi t}{q}},$$

so that

$$\begin{aligned}\Lambda(s,\chi) &= \frac{1}{2}\int_0^\infty \theta_\chi(t) t^{\frac{1}{2}t} \frac{dt}{t} = \frac{1}{2}\int_0^1 \theta_\chi(t) t^{\frac{1}{2}t} \frac{dt}{t} + \frac{1}{2}\int_1^\infty \theta_\chi(t) t^{\frac{1}{2}t} \frac{dt}{t} \\ &= \frac{1}{2}\int_1^\infty \theta_\chi\left(\frac{1}{t}\right) t^{-\frac{1}{2}t} \frac{dt}{t} + \frac{1}{2}\int_1^\infty \theta_\chi(t) t^{\frac{1}{2}t} \frac{dt}{t}\end{aligned}$$

We claim, and will prove momentarily, that

$$\theta_\chi\left(\frac{1}{t}\right) = \left(\frac{t}{q}\right)^{1/2} \tau(\chi)\theta_{\overline{\chi}}(t).$$

With that as writ,

$$\Lambda(s,\chi) = \frac{1}{2}\frac{\tau(\chi)}{\sqrt{q}}\int_1^\infty \theta_\chi(t) t^{-\frac{1}{2}(1-s)} \frac{dt}{t} + \frac{1}{2}\int_1^\infty \theta_\chi(t) t^{\frac{1}{2}s} \frac{dt}{t},$$

and

$$\Lambda(1-s,\overline{\chi}) = \frac{1}{2}\frac{\tau(\overline{\chi})}{\sqrt{q}}\int_1^\infty \theta_\chi(t) t^{-\frac{1}{2}s} \frac{dt}{t} + \frac{1}{2}\int_1^\infty \theta_{\overline{\chi}}(t) t^{\frac{1}{2}(1-s)} \frac{dt}{t},$$

and comparing these we see that

$$\Lambda(s,\chi) = \varepsilon(\chi)\Lambda(1-s,\overline{\chi}),$$

where in this case, for even χ, $\varepsilon(\chi) = \tau(\chi)/\sqrt{q}$. Note that as part of the computation,

$$\tau(\chi)\tau(\overline{\chi}) = \tau(\chi)\overline{\tau(\chi)} = |\tau(\chi)|^2 = q.$$

□

Lecture 22 Functions of finite order

22.1 Proof concluded

We left the proof with two outstanding issues: we had only considered χ beign even, and we had a claim we hadn't yet proved.

Claim. *With* $\theta_\chi(t) = \sum_{n\in\mathbb{Z}} \chi(n)\theta_{\overline{\chi}} e^{-\frac{n^2\pi t}{q}}$, *we have*

$$\theta_\chi\left(\frac{1}{t}\right) = \left(\frac{t}{q}\right)^{1/2} \tau(\chi)\theta_{\overline{\chi}}(t).$$

Proof. By definition,

$$\tau(\chi)\theta_{\overline{\chi}}(t) = \sum_{b \,(\mathrm{mod}\ q)} \chi(b)\,\mathrm{e}\left(\frac{b}{q}\right) \sum_{n\in\mathbb{Z}} \overline{\chi}(n) e^{-\frac{n^2\pi t}{q}}.$$

Combining the exponentials and using Poisson summation, this becomes

$$\sum_{b \,(\mathrm{mod}\ q)} \chi(b) \sum_{n\in\mathbb{Z}} e^{-\frac{n^2\pi t}{q} + \frac{2\pi i b n}{1}} = \sum_{b \,(\mathrm{mod}\ q)} \chi(b) \sum_{n\in\mathbb{Z}} \left(\frac{q}{t}\right)^{1/2} e^{-\frac{(n+\frac{b}{q})^2\pi q}{t}}.$$

Multiplying and dividing the exponent by q, we get $-(qn+b)^2\pi/(qt)$, where the parenthesis then ranges over all integers n, so this becomes

$$\left(\frac{q}{t}\right)^{1/2} \sum_{n\in\mathbb{Z}} \chi(n) e^{-\frac{n^2\pi}{qt}} = \left(\frac{q}{t}\right)^{1/2} \theta_\chi\left(\frac{1}{t}\right). \qquad \square$$

Hence, for χ even, we are done.

Now let us tackle the case where χ is odd, i.e. $\chi(-1) = -1$.

Proof. Note that the method used above no longer works, since by χ being odd, $\theta_\chi(t)$ is identically 0 for all t. Instead what we'll do is replace s by $s+1$ in the expression we play with for Γ, so

$$\pi^{-\frac{1}{2}(s+1)} q^{\frac{1}{2}(s+1)} \Gamma\left(\frac{1}{2}(s+1)\right) n^{-s} = \int_0^\infty n e^{-\frac{n^2\pi t}{q}} t^{\frac{1}{2}(s+1)} \frac{dt}{t},$$

where we've moved one of the n from $n^{-(s+1)}$ over to the other side, so as to make the exponential, together with n, an odd function in n. We then proceed as usual: we twist by $\chi(n)$ and sum over $n \geq 1$, getting

$$\pi^{-\frac{1}{2}(s+1)} q^{\frac{1}{2}(s+1)} \Gamma\left(\frac{1}{2}(s+1)\right) L(s,\chi) = \int_0^\infty \left(\sum_{n\geq 1} \chi(n) n e^{-\frac{n^2\pi t}{t}}\right) t^{\frac{1}{2}(s+1)} \frac{dt}{t},$$

where the summand is now an even function in n. Defining

$$\theta'_\chi(t) = \sum_{n\in\mathbb{Z}} \chi(n) n e^{-\frac{n^2\pi t}{q}},$$

Date: March 6th, 2019.

the sum is $\frac{1}{2}\theta'_\chi(t)$, and as before we write this as the integral from 0 to 1 plus the integral from 1 to ∞, then make a change of variables $t \mapsto 1/t$ in the former,

$$\begin{aligned}\Lambda(s,\chi) &= \frac{1}{2}\int_0^\infty \theta'_\chi(t)t^{\frac{1}{2}(s+1)}\frac{dt}{t} = \frac{1}{2}\int_0^1 \theta'_\chi(t)t^{\frac{1}{2}(s+1)}\frac{dt}{t} + \frac{1}{2}\int_1^\infty \theta'_\chi(t)t^{\frac{1}{2}(s+1)}\frac{dt}{t} \\ &= \frac{1}{2}\int_0^1 \theta'_\chi\left(\frac{1}{t}\right)t^{-\frac{1}{2}(s+1)}\frac{dt}{t} + \frac{1}{2}\int_1^\infty \theta'_\chi(t)t^{\frac{1}{2}(s+1)}\frac{dt}{t}.\end{aligned}$$

By the same kind of computation as before, with Poisson summation and all,

$$\theta'_\chi\left(\frac{1}{t}\right) = -iq^{-1/2}t^{3/2}\tau(\chi)\theta'_{\overline{\chi}}(t),$$

by which

$$\Lambda(s,\chi) = \frac{\pi^{1/2}}{2}\left(\frac{-i\tau(\chi)}{q}\int_1^\infty \theta'_{\overline{\chi}}(t)t^{-\frac{1}{2}(s+1)}\frac{dt}{t} + \frac{1}{q^{1/2}}\int_1^\infty \theta'_\chi(t)t^{\frac{1}{2}(s+1)}\frac{dt}{t}\right)$$

which is the same as

$$\varepsilon(\chi)\Lambda(1-s,\overline{\chi}). \qquad \square$$

22.2 The Hadamard factorisation theorem

The goal of the coming discussion is to express a holomorphic function on $\mathbb{C}$ as an infinite product indexed by its zeros. To start this, we need some preliminaries.

Definition 22.2.1. A holomorphic function $f\colon \mathbb{C} \to \mathbb{C}$ is of ***finite order*** if there exists a constant $\alpha > 0$ such that for any $\varepsilon > 0$, we have

$$|f(s)| \ll \exp\left(|s|^{\alpha+\varepsilon}\right)$$

for all $s \in \mathbb{C}$, with the implied constant depending on ε and f.

In this case we say that f is of order $\leq \alpha$. We say that f is of ***order*** α if it is of order $\leq \alpha$ but not of order $\leq \beta$ for any $\beta < \alpha$.

Example 22.2.2. Let $P_n(s) = a_n s^n + a_{n-1}s^{n-1} + \ldots + a_0$, $a_i \in \mathbb{C}$ and $a_n \neq 0$. This is of order 0. ▲

Example 22.2.3. The function $f(s) = \exp(s)$ is of order 1. ▲

Example 22.2.4. The function $f_n(s) = \exp(P_n(s))$ is of order $n = \deg P_n$. ▲

Note also that $f_n(s)$, as defined above, is a function of order n which does not vanish in $\mathbb{C}$. This is not a coincidence:

Proposition 22.2.5. *A function f of order $\leq \alpha$ which does not vanish on $\mathbb{C}$ is of the form $f(s) = \exp(p(s))$ for some polynomial $p(s)$ of degree $\leq \alpha$. Hence f is of integral order* $\deg p$.

Proof. Since $f(x)$ does not vanish on $\mathbb{C}$, we can take its logarithm, i.e., $g(s) \coloneqq \log f(s)$ can be defined and is holomorphic on $\mathbb{C}$. Hence it has a Taylor expansion at $s = 0$, i.e.

$$g(s) = \sum_{n=0}^{\infty} c_n s^n,$$

with $c_n \in \mathbb{C}$. We claim that $c_n = 0$ for $n > \alpha$, from which the result follows.

To prove the claim, note that since f is of order $\leq \alpha$,

$$\operatorname{Re} g(s) = \log|f(s)| \leq C_{\varepsilon,f}|s|^{\alpha+\varepsilon} = C_{\varepsilon,f}R^{\alpha+\varepsilon},$$

calling $|s| = R$. Writing $c_n = a_n + ib_n$, with $a_n, b_n \in \mathbb{R}$, and letting $s = Re^{2\pi ix}$, we have

$$\operatorname{Re} g\left(Re^{2\pi ix}\right) = \sum_{n\geq 0} a_n R^n \cos(2\pi nx) - i\sum_{n\geq 1} b_n R6n \sin(2\pi nx).$$

Hence

$$a_n R^n = \begin{cases} \int_0^1 \operatorname{Re}(g(Re^{2\pi ix}))\,dx & \text{if } n = 0, \\ 2\int_0^1 \operatorname{Re}(g(Re^{2\pi ix}))\cos(2\pi nx)\,dx & \text{if } n \geq 1 \end{cases}$$

and

$$b_n R^n = 2\int_0^1 \operatorname{Re}(g(Re^{2\pi ix}))\sin(2\pi inx)\,dx,$$

whence

$$|a_n|R^n \leq 2\int_0^1 |\operatorname{Re}(g(Re^{2\pi ix}))|\cdot 1\,dx \leq 2C_{\varepsilon,f}R^{\alpha+\varepsilon}$$

by bounding cos by 1. Hence for $n > \alpha$,

$$|a_n| \leq 2C_{\varepsilon,f}R^{\alpha-n+\varepsilon} \to 0$$

as $R \to \infty$, so $a_n = 0$.

By the same argument, b_n is 0 for $n > \alpha$ too. □

Lecture 23 Jensen's formula

23.1 Jensen's formula

Remark 23.1.1. Note that in the proof of Proposition 22.2.5, it suffices to study a sequence of positive real numbers $\{ R_n \}_{n=1}^{\infty}$ with $R_n \to \infty$ such that for all $n \geq 0$, $\varepsilon > 0$, and $|s| = R_n$,

$$f(s) \ll_{f,\varepsilon} \exp(|s|^{\alpha+\varepsilon}).$$

This is because of the maximal principle, having control on the boundary of a circle implies having control inside the circle.

In order to state Jensen's theorem we need a bit of set up. Let $f\colon \mathbb{C} \to \mathbb{C}$. For $R > 0$, we define

$$Z(f, R) \coloneqq \{ \rho \in \mathbb{C} \mid f(\rho) = 0, |\rho| \leq R \}$$

and

$$Z(f) \coloneqq \{ \rho \in \mathbb{C} \mid f(\rho) = 0 \}.$$

We will also take sums and products over these sets—in this case we add or multiply with multiplicity.

Date: March 18th, 2019.

Theorem 23.1.2 (Jensen's formula)**.** *Let $R > 0$. Let f be a holomorphic function in a neighbourhood of $D_R = \{ s \in \mathbb{C} \mid |s| < R \}$. Suppose f does not vanish at $s = 0$ nor on $C_R = \{ s \in \mathbb{C} \mid |s| = R \}$. Then*

$$\int_0^1 \log\left|\frac{f(Re^{2\pi it})}{f(0)}\right| dt = \log \prod_{\rho \in Z(f,R)} \frac{R}{|\rho|} = \sum_{\rho \in Z(f,r)} \log \frac{R}{|\rho|}.$$

Note that like usual residue calculus with Cauchy's redisue theorem on f'/f, this also counts zeros, but not with weight 1.

Proof. Write

$$f(s) = F(s) \prod_{\rho \in Z(f,R)} (s - \rho)$$

where $F(s)$ is a holomorphic function that doesn't vanish in D_R. Hence

$$\log\left|\frac{f(s)}{f(0)}\right| = \log\left|\frac{F(s)}{F(0)}\right| + \sum_{\rho \in Z(f,R)} \log\left|\frac{s-\rho}{\rho}\right|.$$

Looking at the first term,

$$\log\left|\frac{F(s)}{F(0)}\right| = \operatorname{Re} \log \frac{F(s)}{F(0)}.$$

The inside of this real part is a holomorphic function in a neighbourhood of D_R, and vanishes at $s = 0$, so taking $Re^{2\pi it} = z$,

$$\int_0^1 \log \frac{F(Re^{2\pi it})}{F(0)}\, dt = \frac{1}{2\pi i} \int_{C_R} \log \frac{F(z)}{F(0)} \frac{dz}{z} = 0$$

since the integrand is a holomorphic function, so we can contract the integration to a point.

For the second term, note that

$$\left|\frac{Re^{2\pi it} - \rho}{\rho}\right| = \frac{R}{|\rho|}\left|e^{2\pi it} - \frac{\rho}{R}\right| = \frac{R}{|\rho|}\left|1 - \frac{\overline{\rho}}{R} e^{2\pi it}\right|$$

meaning that

$$\log\left|\frac{Re^{2\pi it} - \rho}{\rho}\right| = \log \frac{R}{|\rho|} + \log\left|1 - \frac{\overline{\rho}}{R} e^{2\pi it}\right| = \log \frac{R}{|\rho|} + \operatorname{Re} \log\left(1 - \frac{\overline{\rho}}{R} e^{2\pi it}\right).$$

As above, the latter is a holomorphic function vanishing at $z = 0$, so

$$\int_0^1 \log\left(1 - \frac{\overline{\rho}}{R} e^{2\pi it}\right) dt = 0,$$

so when all the dust settles only the sum of $\log(R/|\rho|)$ remains. □

23.2 Application of Jacobi's formula

Theorem 23.2.1. *Let f be a holomorphic function of order $\leq \alpha$. Let*

$$N(f,R) = \sum_{\rho \in Z(f,R)} 1,$$

i.e., the number of zeros of f of modulus $\leq R$, with multiplicity.

(*i*) *For all $R > 0$, $\varepsilon > 0$, we have*

$$N(f,R) \ll_{f,\varepsilon} R^{\alpha+\varepsilon} + \begin{cases} 1, & \text{if } f(0) = 0, \\ 0, & \text{if } f(0) \neq 0. \end{cases}$$

(*ii*) *The series*

$$\sum_{\rho \in Z(f)} \frac{1}{1+|\rho|^{\alpha+\varepsilon}}$$

converges.

Proof. Suppose $f(0) \neq 0$ and $f(s) \neq 0$ on C_{2R}. For $\rho \in Z(f,R)$, $\log(2R/\rho) \geq \log 2$, so

$$\begin{aligned}(\log 2) N(f,R) &\leq \sum_{\rho \in Z(f,R)} \log \frac{2R}{|\rho|} \leq \sum_{\rho \in Z(f,2R)} \log \frac{2R}{|\rho|} = \int_0^1 \log \left| \frac{f(2Re^{2\pi i t})}{f(0)} \right| dt \\ &\ll \int_0^1 (2R)^{\alpha+\varepsilon}\, dt = (2R)^{\alpha+\varepsilon} \ll R^{\alpha+\varepsilon},\end{aligned}$$

where for the integral we use Jensen's formula, and the bound is by the order.

Note that if $f(s) = 0$ for some $s \in C_{2R}$, then we consider $R < R' < R + \delta$ for some $\delta > 0$, such that $f(s) \neq 0$ for all $s \in C_{2R'}$. This is possible since f is a holomorphic function, meaning that if it has an accumulation point of zeros, then it is identically zero. Thus

$$N(f,R) \leq N(f,R') \ll (R')^{\alpha+\varepsilon} \ll R^{\alpha+\varepsilon}.$$

Now suppose $f(0) = 0$, with the zero of order m. Then

$$N(f,R) = N\left(\frac{f(s)}{s^m}, R\right) + m \ll_f R^{\alpha+\varepsilon} + 1.$$

For the series,

$$\begin{aligned}\sum_{\rho \in Z(f,R)} \frac{1}{1+|\rho|^{\alpha+\varepsilon}} &= \int_0^R \frac{1}{1+r^{\alpha+\varepsilon}}\, dN(f,r) \\ &= \frac{N(f,r)}{1+r^{\alpha+\varepsilon}}\bigg|_0^R - \int_0^R N(f,r) \frac{r^{\alpha-1+\varepsilon}}{(1+r^{\alpha+\varepsilon})^2}\, dr \\ &= \frac{N(f,R)}{1+R^{\alpha+\varepsilon}} - \int_0^R N(f,r) \frac{r^{\alpha-1+\varepsilon}}{(1+r^{\alpha+\varepsilon})^2}\, dr.\end{aligned}$$

By the first part, this is $O(1)$, and letting $R \to \infty$ we are done. □

Lecture 24 Hadamard factorisation theorem

24.1 Hadamard factorisation

Theorem 24.1.1. *Let f be a holomorphic function of order at most 1 such that $f(0) \neq 0$. Then we have*

$$f(s) = A \exp(bs) \prod_{\rho \in Z(f)} \left(1 - \frac{s}{\rho}\right) e^{s/\rho}$$

where $A = f(0)$, $b = f'(0)/f(0)$, and the product converges uniformly on compact subsets of $\mathbb{C}$.

Proof. Let $K \subset \mathbb{C}$ be a compact subset. Then $K \cap Z(f)$ is a finite set (since otherwise $f = 0$, since a holomorphic function with an accumulation point of zeros must be zero everywhere). For $s \in K$ and $\rho \in Z(f) \setminus K$, we have

$$\left(1 - \frac{s}{\rho}\right) e^{s/\rho} = 1 + O_K\left(\frac{1}{|\rho|^2}\right)$$

by expanding the exponential as a Taylor series.

Note that an infintie product $\prod(1 + a_n)$, with $a_n \geq 0$, converges if and only if $\sum a_n$ converges, and since

$$\sum_{\rho \in Z(f)} \frac{1}{|\rho|^2}$$

converges by Jensen's formula,

$$\prod_{\rho \in Z(f)} \left(1 - \frac{s}{\rho}\right) e^{s/\rho}$$

converges uniformly on K (since our estimate above is independent of s).

Set

$$h(s) = \prod_{\rho \in Z(f)} \left(1 - \frac{s}{\rho}\right) e^{s/\rho}.$$

This is holomorphic and has exactly the same zeros as $f(s)$. Hence $f(s)/h(s)$ is holomorphic and does not vanish on $\mathbb{C}$.

We claim that $f(s)/h(s)$ has order ≤ 1.

Then, by Proposition 22.2.5,

$$\frac{f(s)}{h(s)} = \exp(a + bs)$$

for some $a, b \in \mathbb{C}$.

Now for all $\rho \in Z(f)$,

$$\left(1 - \frac{s}{\rho}\right) e^{s/\rho}\Big|_{s=0} = 1,$$

so $h(0) = 1$, whence $f(0) = \exp(a) = A$.

Date: March 20th, 2019.

Similarly,

$$\frac{d}{ds}\left(1-\frac{s}{\rho}\right)e^{s/\rho}\Big|_{s=0}=0$$

so $h'(0)=0$, so $b=f'(0)/f(0)$. □

It remains to prove the claim, meaning we need to show

$$\log\left|\frac{f(s)}{h(s)}\right|=O(|s|^{1+\varepsilon}).$$

Proof. Writing the logarithm as

$$\log|f(s)|-\log|h(s)|,$$

we note first that $f(s)$ is order at most 1 by assumption, so

$$\log|f(s)|\ll R^{1+\varepsilon}$$

on $|s|=R$ for all $R>0$.

It remains to show that $-\log|h(s)|\ll R^{1+\varepsilon}$ on a sequence of $R\to\infty$, $|s|=R$. The intelligent idea is this: Since

$$\sum_{\rho\in Z(f)}\frac{1}{|\rho|^2}<\infty,$$

the total length of all intervals □

Lecture 25 The infinite product for $\zeta(s)$

25.1 Hadamard factorisation finished

The missing piece from our proof of Hadamard factorisation is to show that for

$$h_3(s)=\prod_{|\rho|>2R}\left(1-\frac{s}{\rho}\right)e^{s/\rho},$$

we have

$$-\log|h_3(s)|\ll R^{1+\varepsilon}$$

for $R=|s|$.

Write this as

$$-\log|h_3(s)|=\sum_{|\rho|>2R}-\log\left|\left(1-\frac{s}{\rho}\right)e^{s/\rho}\right|=\sum_{|\rho|>2R}-\log\left(1+O(|s/\rho|^2)\right)$$

since

$$\left(1-\frac{s}{\rho}\right)e^{s/\rho}=\left(1-\frac{s}{\rho}\right)\left(1+\frac{s}{\rho}+O\left(\left|\frac{s}{\rho}\right|^2\right)\right)=1+O(|s/\rho|^2),$$

Date: March 25th, 2019.

by expanding the exponential as a Taylor series.

Now expanding this logarithm as a Taylor series in turn, we have

$$-\log|h_3(s)| \ll \sum_{|\rho|>2R} \left|\frac{s}{\rho}\right|^2 = \sum_{|\rho|>2R} \frac{1}{|\rho|^{1+\varepsilon}} \frac{R^{1-\varepsilon}}{|\rho|^{1-\varepsilon}} R^{1+\varepsilon} \ll R^{1+\varepsilon}$$

since the first term in the latter sum converges since the order is ≤ 1, and the second term is bounded by $(1/2)^{1+\varepsilon}$ since $|\rho| > 2R$.

Corollary 25.1.1. *Let f be a holomorphic function of order at most 1 such that $f(0) \neq 0$. For $s \in \mathbb{C} \setminus Z(f)$, we have*

$$\frac{d}{ds}(\log f(s)) = \frac{f'(s)}{f(s)} = b + \sum_{\rho \in Z(f)} \left(\frac{1}{\rho} - \frac{1}{\rho - s}\right),$$

with $b = f'(0)/f(0)$. Moreover

$$\sum_{\rho \in Z(f)} \left(\frac{1}{\rho} - \frac{1}{\rho - s}\right)$$

converges uniformly on compact subsets $K \subset \mathbb{C} \setminus Z(f)$.

Proof. The first part is Hadamard factorisation on $f'(s)/f(s)$. For the second part, note that if $s \in K$,

$$\frac{1}{\rho} - \frac{1}{\rho - s} = \frac{-s}{\rho(\rho - s)} = O_K\left(\frac{1}{|\rho|^2}\right)$$

since s is in a bounded set. □

25.2 The infinite product for $\zeta(s)$ and the explicit formula

Let

$$\xi_0(s) = s(1-s)\zeta(s) = s(1-s)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

Proposition 25.2.1. *$\xi_0(s)$ has order at most 1.*

Proof. Since $\xi(s) = \xi(1-s)$, we also have $\xi_0(s) = \xi_0(1-s)$, so by symmetry we may assume $\mathrm{Re}(s) \geq 1/2$.

Bounding each factor above one at a time, we have

$$|\pi^{-\frac{s}{2}}| = e^{-\frac{s}{2}\log\pi} \ll \exp\left(|s|^{1+\varepsilon}\right).$$

Next,

$$\left|\Gamma\left(\frac{s}{2}\right)\right| \ll \exp\left(|s|^{1+\varepsilon}\right)$$

by Stirling's formula.

Finally,

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

for $\mathrm{Re}(s) > 0$. The first term is bounded, with the pole at $s = 1$ cancelled by the factor $(1-s)$ from $\xi_0(s)$. The integral is convergent since $\mathrm{Re}(s) > 0$.

Hence $s(1-s)\zeta(s) \ll \exp(|s|^\varepsilon)$, hence $\xi_0(s)$ has order at most 1. □

Corollary 25.2.2. (*i*) $\xi_0(s) = A\exp(bs)\prod_{\rho\in Z(\xi_0)}\left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}}$,

(*ii*) $\sum_{\rho\in Z(\xi_0)}\frac{1}{|\rho|^{1+\varepsilon}} < \infty$.

Remark 25.2.3. The zeros of $\xi_0(s)$ are precisely the nontrivial zeros of $\zeta(s)$, since $s\Gamma(\frac{s}{2})$ has no zeros and the zero of $(1-s)$ is cancelled by the pole of $\zeta(s)$ at $s=1$.

25.3 Infinite product for $L(s,\chi)$

Let $\chi \pmod q$ be a primitive character, and

$$\Lambda(s,\chi) = \left(\frac{q}{\pi}\right)^{\frac{1}{2}(s+\kappa)}\Gamma\left(\frac{s+\kappa}{2}\right)L(s,\chi),$$

satisfying

$$\Lambda(s,\chi) = \varepsilon(\chi)\Lambda(1-s,\overline{\chi})$$

with

$$\kappa = \begin{cases} 0, & \text{if } \chi \text{ is even,} \\ 1, & \text{if } \chi \text{ is odd,} \end{cases}$$

and $|\varepsilon(\chi)| = 1$.

Proposition 25.3.1. *$\Lambda(s,\chi)$ has order at most 1.*

Proof. By essentially the same proof as for $\zeta(s)$, except here we have

$$L(s,\chi) = s\int_1^\infty \frac{S(t)}{t^{2+1}}\,dt$$

for $\mathrm{Re}(s) > 0$, with

$$S(t) = \sum_{n\le t}\chi(n),$$

and $|S(t)| \le q$. This integral is convergent, so $\ll \exp(|s|^\varepsilon)$. □

25.4 Application to counting zeros of $\zeta(s)$

By Corollary 25.1.1,

$$\frac{\xi_0'}{\xi_0}(s) = \frac{1}{s} + \frac{1}{s-1}\frac{\zeta_\infty'}{\zeta_\infty}(s) + \frac{\zeta'}{\zeta}(s) = b + \sum_{\rho\in Z(\xi_0)}\left(\frac{1}{\rho}-\frac{1}{\rho-s}\right)$$

converges uniformly on compact subsets of $\mathbb{C}\setminus Z(f)$.

Note that $\xi_0(s)$ takes real values on the real line, and it is holomorphic, so by Schwartz reflection principle $\xi_0(s) = \overline{\xi_0(\overline{s})}$.

Hence $Z(\xi_0)$ is invariant under complex conjugation, so

$$\sum_{\rho\in Z(\xi_0)}\left(\frac{1}{\rho}-\frac{1}{\rho-s}\right) = \frac{1}{2}\sum_{\rho\in Z(\xi_0)}\left(\frac{1}{\rho}+\frac{1}{\overline{\rho}}-\frac{1}{\rho-s}-\frac{1}{\overline{\rho}-s}\right).$$

Writing $\rho = \beta + i\gamma$, $0 \le \beta \le 1$, $\gamma \in \mathbb{R}$, and

$$\frac{1}{\rho} + \frac{1}{\overline{\rho}} = \frac{2\beta}{|\rho|^2},$$

we have

$$\sum_{\rho \in Z(\xi_0)} \left(\frac{1}{\rho} + \frac{1}{\overline{\rho}} \right) < \infty,$$

whereby

$$\frac{1}{2} \sum_{\rho \in Z(\xi_0)} \left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}} \right).$$

converges uniformly on compact subsets of $\mathbb{C} \setminus Z(f)$.

Proposition 25.4.1. *For every $s \in Z(\xi_0)$,*

$$\frac{\xi_0'}{\xi_0}(s) = \frac{1}{2} \sum_{\rho \in Z(\xi_0)} \left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}} \right) + O(1)$$

and

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s} + \frac{1}{s-1} - \frac{1}{2} \sum_{\rho \in Z(\xi_0)} \left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}} \right) + \frac{\zeta_\infty'}{\zeta_\infty}(s) + O(1).$$

Lecture 26 Counting zeros

26.1 Application to counting zeros of $\zeta(s)$

Corollary 26.1.1. *Let $N(T) \coloneqq \#\{\, \rho = \beta + i\gamma \in Z(\xi_0) \mid |\gamma| \le T \,\}$. For $T \ge 1$, we have*

(a) $N(T+1) - N(T) \ll \log(2+T)$,

(b) $N(T) \ll T \log(2+T)$.

Proof. We have

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s} + \frac{1}{s-1} + \frac{\zeta_\infty'}{\zeta_\infty}(s) - \frac{1}{2} \sum_{\rho \in Z(\xi_0)} \left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}} \right) + O(1).$$

Letting $s = 2 + iT$, we have the series representation

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

since we are in the region of absolute convergence. Also,

$$\frac{\zeta_\infty'}{\zeta_\infty}(s) \ll \log(2+T)$$

Date: March 27th, 2019.

by Stirling's formula.

Hence

$$\frac{1}{2}\sum_{\rho\in Z(\xi_0)}\left(\frac{1}{s-\rho}+\frac{1}{s-\overline{\rho}}\right)\ll\log(2+T).$$

Now writing $\rho=\beta+i\gamma$, with $0\le\beta\le 1$, we have

$$\operatorname{Re}\left(\frac{1}{s-\rho}\right)=\frac{2-\beta}{|s-\rho|^2}\ge\frac{1}{(2-\beta)^2+|\gamma-T|^2}\ge\frac{1}{4+|\gamma-T|^2}\ge\frac{1}{5}\delta_{|\gamma-T|\le 1}.$$

Therefore

$$\frac{1}{5}\sum_{|\gamma\pm T|\le 1}1\le\sum_{\rho\in Z(\xi_0)}\operatorname{Re}\left(\frac{1}{s-\rho}+\frac{1}{s-\overline{\rho}}\right)\ll\log(2+T),$$

where the left-hand side sum, of course, is $N(T+1)-N(T-1)$, which in turn is an upper bound for $N(T+1)-N(T)$, so

$$N(T+1)-N(T)\ll\log(2+T).$$

For the second part, simply write $N(T)$ as a telescoping sum,

$$N(T)=\sum_{n=1}^{T}(N(n)-N(n-1))\ll T\log(2+T).\qquad\square$$

Remark 26.1.2. From the proof we note, in particular, that

$$\sum_{\rho\in Z(\xi_0)}\frac{1}{4+|\gamma\pm T|^2}\ll\log(2+T),$$

where $\rho=\beta+i\gamma$.

Secondly, moving things over,

$$\frac{\xi_0'}{\xi_0}(s)=\frac{1}{2}\sum_{|\gamma\pm T|\le 1}\left(\frac{1}{s-\rho}+\frac{1}{s-\overline{\rho}}\right)+O(\log(2+|T|)),$$

where $s=\sigma+iT\notin Z(\xi_0)$, $-1\le\sigma\le 2$.

26.2 Applications to countinjg zeros of $L(s,\chi)$

We wish to perform the same sort of estimates for $L(s,\chi)$.

Let χ be a primitive character modulo $q\ge 1$. Let $\kappa=\frac{1}{2}(1-\chi(-1))$, and

$$L_\infty(s,\chi)\coloneqq\left(\frac{\pi}{q}\right)^{-\frac{s}{2}}\Gamma\left(\frac{s+\kappa}{2}\right).$$

Then $\Lambda(s,\chi)=L_\infty(s,\chi)L(s,\chi)=\varepsilon(\chi)\Lambda(1-s,\overline{\chi})$. Note that

$$Z(\Lambda(s,\chi))\subset\{\,s\in\mathbb{C}\mid 0\le\operatorname{Re}(s)\le 1\,\}$$

is exactly the set of nontrivial zeros of $L(s,\chi)$.

By Hadamard factorisation,

$$\frac{\Lambda'}{\Lambda}(s,\chi) = \frac{L'_\infty}{L_\infty}(s,\chi) + \frac{L'}{L}(s,\chi) = b(\chi) + \sum_{\rho \in Z(\Lambda(s,\chi))} \left(\frac{1}{\rho} - \frac{1}{\rho - s}\right),$$

where

$$b(\chi) = \frac{\Lambda'}{\Lambda}(0,\chi).$$

This causes trouble, since unlike for ζ it depends on a sum over zeros.

Note that

$$\Lambda(s,\chi) = \varepsilon(\chi)\Lambda(1-s,\overline{\chi}) = \varepsilon\chi\overline{\Lambda(1-\overline{s},\chi)},$$

so if $\rho \in Z(\Lambda(s,\chi))$, then $1-\overline{\rho} \in Z(\Lambda(s,\chi))$. Thus

$$b(\chi) = \frac{\Lambda'}{\Lambda}(0,\chi) = -\frac{\Lambda'}{\Lambda}(1,\overline{\chi}) = -b(\overline{\chi}) - \sum_{\rho' \in Z(\Lambda(s,\overline{\chi}))} \left(\frac{1}{\rho'} - \frac{1}{\rho' - 1}\right).$$

Writing $\rho = 1 - \rho' \in Z(\Lambda(s,\chi))$, this becomes

$$-b(\overline{\chi}) - \sum_{\rho \in Z(\Lambda(s,\chi))} \left(\frac{1}{1-\rho} + \frac{1}{\rho}\right).$$

Combining this we have

$$\operatorname{Re} b(\chi) = -\frac{1}{2} \sum_{\rho \in Z(\Lambda(s,\chi))} \left(\frac{1}{1-\rho} + \frac{1}{\rho}\right)$$

since $b(\overline{\chi}) + b(\chi) = 2\operatorname{Re} b(\chi)$, so

$$\operatorname{Re} b(\chi) = -\frac{1}{2} \sum_{\rho \in Z(\Lambda(s,\chi))} \operatorname{Re}\left(\frac{1}{\overline{\rho}} + \frac{1}{\rho}\right) = -\sum_{\rho \in Z(\Lambda(s,\chi))} \operatorname{Re}\frac{1}{\rho}.$$

Thus

$$\operatorname{Re}\frac{\Lambda'}{\Lambda}(s,\chi) = \sum_{\rho \in Z(\Lambda(s,\chi))} \operatorname{Re}\frac{1}{s-\rho}.$$

Summarising,

Proposition 26.2.1. *For $s \notin Z(\Lambda(s,\chi))$,*

(a) $\operatorname{Re}\dfrac{\Lambda'}{\Lambda}(s,\chi) = \displaystyle\sum_{\rho \in Z(\Lambda(s,\chi))} \frac{1}{s-\rho}$, *and*

(b) $\operatorname{Re}\dfrac{L'}{L}(s,\chi) = \displaystyle\sum_{\rho \in Z(\Lambda(s,\chi))} \operatorname{Re}\frac{1}{s-\rho} - \operatorname{Re}\frac{L'_\infty}{L_\infty}(s,\chi).$

Lecture 27 Weil's explicit formula

27.1 Application to counting zeros of $L(s,\chi)$

Corollary 27.1.1. *Let* $N(T,\chi) \coloneqq \#\{\,\rho = \beta + i\gamma \in Z(\Lambda(s,\chi)) \mid |\gamma| \le T\,\}$. *For* $T \ge 1$, *we have*

(a) $N(T+1,\chi) - N(T,\chi) \ll \log(q(2+T))$, *and*

(b) $N(T,\chi) \ll T\log(q(2+T))$.

Proof. For $s = 2+iT$, we have the (absolutely) convergent series representation

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

and

$$\frac{L'_\infty}{L_\infty}(s,\chi) \ll \log(q(2+T))$$

by Stirling's formula. By Proposition 26.2.1, we hence have

$$\sum_{\rho \in Z(\Lambda(s,\chi))} \operatorname{Re}\frac{1}{s-\rho} \ll \log(q(2+T)).$$

Note that

$$\operatorname{Re}\frac{1}{s-\rho} = \frac{\sigma-\beta}{|s-\rho|^2} \ge \frac{1}{4+|T-\gamma|^2} \ge \frac{1}{5}\delta_{|T-\gamma|\le 1},$$

writing $\rho = \beta + i\gamma$. For $s = 2-iT$ we get the same result, but $|T-\gamma|$ is replaced by $|T+\gamma|$. Hence

$$\frac{1}{5}\sum_{|T\pm\gamma|\le 1} 1 \le \sum_{\rho} \operatorname{Re}\frac{1}{s-\rho} \ll \log(q(2+T)),$$

so

$$N(T+1,\chi) - N(T,\chi) \le N(T+1,\chi) - N(T-1,\chi) \ll \log(q(2+T)).$$

The second part, as before, is just a telescoping sum. □

Remark 27.1.2. We have

$$\sum_{\rho \in Z(\Lambda(s,\chi))} \frac{1}{4+|\gamma \pm T|^2} \ll \log(q(2+T)).$$

Moreover,

$$\frac{\Lambda'}{\Lambda}(s,\chi) = \sum_{|\gamma\pm T|\le 1} \frac{1}{s-\rho} + O(\log(q(2+T)))$$

for $s = \sigma + iT \notin Z(\Lambda(s,\chi))$, $-1 \le \sigma \le 2$.

Date: March 29th, 2019.

Proof. The second part is a little bit more delicate in this case than for $\zeta(s)$. For $s = 2 + iT$,

$$\frac{\Lambda'}{\Lambda}(s,\chi) = b(\chi) + \sum_\rho \left(\frac{1}{\rho} + \frac{1}{2+iT-\rho}\right),$$

where the left-hand side is $\ll \log(q(2+T))$. Thus

$$\begin{aligned}\frac{\Lambda'}{\Lambda}(s,\chi) &= \sum_\rho \left(\frac{1}{s-\rho} - \frac{1}{(2+iT)-\rho}\right) + O(\log(q(2+T))) \\ &= \sum_{|\gamma\pm T|\le 1} \frac{1}{s-\rho} - \sum_{|\gamma\pm T|\le 1} \frac{1}{2+iT-\rho} + \sum_{|\gamma\pm T|>1} \left(\frac{1}{s-\rho} - \frac{1}{2+iT-\rho}\right) + O(\log(q(2+T))).\end{aligned}$$

Now estimating the sums,

$$\sum_{|\gamma\pm T|\le 1} \frac{1}{2+iT-\rho} \ll \sum_{|\gamma\pm T|\le 1} 1 \ll \log(q(2+T)),$$

and since

$$\frac{1}{s-\rho} - \frac{1}{2+iT-\rho} = \frac{s-\sigma}{(s-\rho)(2+iT-\rho)} \ll \frac{1}{|T\pm\gamma|^2}.$$

Summing both sides, we get $\ll \log(q(2+T))$, meaning that all of the sums we don't care about get baked into the same error term. □

27.2 Weil's explicit formula

Theorem 27.2.1. *Let $f \in C_c^\infty((0,\infty))$, (i.e., infinitely differentiable with compact support) and let*

$$\tilde{f}(s) = \int_0^\infty f(x) x^s \frac{dx}{x}$$

be its Mellin transform. Let

$$\check{f}(x) = \frac{1}{x} f\left(\frac{1}{x}\right).$$

We have

$$\sum_{n\ge 1} (f(n)+\check{f}(n))\Lambda(n) = \tilde{f}(1)+\tilde{f}(0)+\frac{1}{2\pi i}\int_{(\frac{1}{2})} \left(\frac{\zeta_\infty'}{\zeta_\infty}(s) + \frac{\zeta_\infty'}{\zeta_\infty}(1-s)\right)\tilde{f}(s)\,ds - \sum_{\rho\in Z(\xi_0)} \tilde{f}(\rho).$$

Proof. First we claim that

$$\frac{1}{2\pi i}\int_{(\frac{3}{2})} \tilde{f}(s)\frac{\xi_0'}{\xi_0}(s)\,ds = \frac{1}{2\pi i}\int_{(\frac{3}{2})} \left(\frac{1}{s} + \frac{1}{s-1} + \frac{\zeta_\infty'}{\zeta_\infty}(s)\right)\tilde{f}(s) - \sum_{n\ge 1}\Lambda(n)f(n).$$

Since $\xi_0(s) = s(1-s)\zeta_\infty(s)\zeta(s)$, and

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

in the region of absolute convergence,

$$\frac{1}{2\pi i}\int_{(\frac{3}{2})} \tilde{f}(s)\frac{\xi_0'}{\xi_0}(s)\,ds = \frac{1}{2\pi i}\int_{(\frac{3}{2})} \tilde{f}(s)\left(\frac{1}{s} + \frac{1}{s-1} + \frac{\zeta_\infty'}{\zeta_\infty}(s)\right)ds - \sum_{n\ge 1}\Lambda\frac{1}{2\pi i}\int_{(\frac{3}{2})}\tilde{f}(s)n^{-s}\,ds.$$

The final integral is the Mellin inversion of $f(n)$, whence we have our claim. □

Lecture 28 Weil's explicit formula

28.1 Proof continued

We have

$$\sum_{\rho\in Z(\xi_0)} \tilde{f}(\rho) = \frac{1}{2\pi i}\int_{(\frac{3}{2})} \tilde{f}(s)\frac{\xi_0'}{\xi_0}(s)\,ds - \frac{1}{2\pi i}\int_{(-\frac{1}{2})} \tilde{f}(s)\frac{\xi_0'}{\xi_0}(s)\,s.$$

By making the change of variables $s \mapsto 1-s$ in the second integral, we switch from $\tilde{f}(s) \mapsto \tilde{f}(1-s)$, $\frac{\xi_0'}{\xi_0}(s) \mapsto \frac{\xi_0'}{\xi_0}(1-s) = -\frac{\xi_0'}{\xi_0}(s)$, and finally the line of integration moves to $\frac{3}{2}$. Hence by the claim this becomes

$$\frac{1}{2\pi i}\int_{(\frac{3}{2})} \left(\frac{1}{s} + \frac{1}{s-1} + \frac{\zeta_\infty'}{\zeta_\infty}(s)\right)\tilde{f}(s)\,ds - \sum_{n\geq 1}\Lambda(n)f(n) +$$
$$\frac{1}{2\pi i}\int_{(\frac{3}{2})} \left(\frac{1}{s} + \frac{1}{s-1} + \frac{\zeta_\infty'}{\zeta_\infty}(s)\right)\tilde{f}(1-s)\,ds - \sum_{n\geq 1}\Lambda(n)\check{f}(n),$$

where we've used

$$\tilde{\check{f}}(s) = \frac{1}{2\pi i}\int_0^\infty \tilde{f}(x)x^s\frac{dx}{x} = \frac{1}{2\pi i}\int_0^\infty \frac{1}{x}f\left(\frac{1}{x}\right)x^s\frac{dx}{x},$$

which if we switch $\frac{1}{x} \mapsto t$ becomes

$$\int_0^\infty tf(t)t^{-s}\frac{dt}{t} = \tilde{f}(1-s).$$

Moving the line of integration from $(\frac{3}{2})$ to $(\frac{1}{2})$ we pick up a pole at $s=1$, with residues $\tilde{f}(1)$ in the first integral and $\tilde{f}(0)$ in the second, so our expression becomes

$$\frac{1}{2\pi i}\int_{(\frac{3}{2})} \left(\frac{1}{s} + \frac{1}{s-1}\right)(\tilde{f}(s) + \tilde{f}(1-s))\,ds =$$
$$\tilde{f}(1) + \tilde{f}(0) + \frac{1}{2\pi i}\int_{(\frac{1}{2})} \left(\frac{1}{s} + \frac{1}{s-1}\right)(\tilde{f}(s) + \tilde{f}(1-s))\,ds.$$

This last integral is 0, since if we switch $s \mapsto 1-s$, we get negative the same integral, so it is equal to negative itself.

Theorem 28.1.1. *Let χ be a Dirichlet character modulo q. Then, with $\check{f}$ as above,*

$$\sum_{n\geq 1}(\chi(n)f(n) + \overline{\chi}(n)\check{f}(n))\Lambda(n) =$$
$$\frac{1}{2\pi i}\int_{(\frac{1}{2})} \left(\frac{L_\infty'}{L_\infty}(s,\chi) + \frac{L_\infty'}{L_\infty}(1-s,\overline{\chi})\right)\tilde{f}(s)\,ds - \sum_{\rho\in Z(\Lambda(s,\chi))}\tilde{f}(\rho).$$

Proof. The proof is the same as above, except with L_∞ in place of ζ_∞. □

Date: April 1st, 2019.

Theorem 28.1.2 (Hadamard, de la Vallée-Poussin)**.** *There exist an absolute constant $c > 0$ such that $\zeta(s) \neq 0$, $s = \sigma + it$, in the region*

$$\sigma \geq 1 - \frac{c}{\log(2 + |t|)}.$$

We will prove this later on. For now, remark that the value of c is actually computable. For instance, Habiba and Kadin computed

$$c = \frac{1}{5.69693}$$

in 2005. People are often improving this ever so slightly.

Corollary 28.1.3. *There exists a constant $c > 0$ such that for $f \in C_c^\infty((0, \infty))$, $X \geq 2$ large,*

$$\sum_{n \geq 1} \Lambda(n) f\left(\frac{n}{X}\right) = X \int_0^\infty f(t)\, dt + O_f\left(X \exp(-c\sqrt{\log X})\right).$$

We call this a *smooth sum* since f is smooth. One can 'unsmooth' the sum, obtaining

$$\sum_{n \leq X} \Lambda(n) = X + O(X \exp(-c'\sqrt{\log X}))$$

for some $c' > 0$, whence $\sum \Lambda(n) \sim X$, which is equivalent to the Prime number theorem.

Remark 28.1.4. If $\operatorname{supp} f = [1, 2]$, we get $1 \leq \frac{n}{X} \leq 2$, i.e., $X \leq n \leq 2X$.

Proof of Corollary 28.1.3. Let $g(t) = f(\frac{t}{X})$. Then $\tilde{g}(s) = \tilde{f}(s)X^s$, so

$$\check{g}(t) = \frac{1}{t} g\left(\frac{1}{t}\right) = \frac{1}{t} f\left(\frac{1}{tX}\right),$$

which is zero for $t \geq 1$ and X large since f has compact support, and $\frac{1}{tX} \approx 0$.

Thus by Weil's explicit formula

$$\sum_{n \geq 1} \Lambda(n) g(n) = \tilde{g}(1) + \tilde{g}(0) + \frac{1}{2\pi i} \int_{(\frac{1}{2})} \left(\frac{\zeta_\infty'}{\zeta_\infty}(s) - \frac{\zeta_\infty'}{\zeta_\infty}(1 - s)\right) \tilde{g}(s)\, ds - \sum_{\rho \in Z(\xi_0)} \tilde{g}(\rho),$$

whence

$$\sum_{n \geq 1} \Lambda(n) f\left(\frac{n}{X}\right) =$$

$$\tilde{f}(1)X + \tilde{f}(0) + \frac{1}{2\pi i} \int_{(\frac{1}{2})} \left(\frac{\zeta_\infty'}{\zeta_\infty}(s) - \frac{\zeta_\infty'}{\zeta_\infty}(1 - s)\right) \tilde{f}(s) X^s\, ds - \sum_{\rho \in Z(\xi_0)} \tilde{f}(\rho) X^\rho.$$

The first term is the integral we want, with the second term being $O_f(1)$. For the sum over zeros,

$$\sum_\rho \tilde{f}(\rho) X^\rho \leq \sum_{\rho = \beta + i\gamma} |\tilde{f}(\rho)| X^\beta \leq X \sum_\rho |\tilde{f}(\rho)| X^{-\frac{c}{\log(2 + |\gamma|)}}$$

by the zero free region, where the exponential in the end is

$$\exp\left(-\frac{x\log X}{\log(2+|\gamma|)}\right).$$

We attack this final sum by splitting the sum over zeros with $\log(2+|\gamma|) \leq \sqrt{\log X}$ and those with $\log(2+|\gamma|) > \sqrt{\log X}$. The former becomes

$$\exp(-c\sqrt{\log X})\sum_{\rho}|\tilde{f}(\rho)|$$

wherein the sum converges by exponential decay of the Mellin transform. The latter is bounded by

$$\ll \sum_{\rho}|\tilde{f}(\rho)|$$

and the summand is $\ll 1/|\gamma|^s$ by rapid decay—we can take any exponent. Such a sum converges since the L-function is of order ≤ 1. □

Lecture 29 The theorem of Hadamard and de la Vallée-Poussin

29.1 Zero free region

Surprisingly and remarkably, most of the following discussion is a consequence of the following elementary trigonometric inequality: for all $\theta \in \mathbb{R}$,

$$3 + 4\cos(\theta) + \cos(2\theta) \geq 0.$$

To see that this is true, note simply that the left-hand side is equal to $2(1+\cos(\theta))^2$, which is of course nonnegative.

To recover the proper zero free region, we need to first establish that there are no zeros on the line (1).

Theorem 29.1.1. *$\zeta(1+it) \neq 0$ for all $t \in \mathbb{R}$.*

Proof. For $s = \sigma + it$, $t \neq 0$, $\sigma > 1$, we have

$$\log\zeta(s) = \sum_{p}\sum_{n=1}^{\infty}\frac{1}{np^{n\sigma}}e^{-itn\log p}.$$

Taking real parts,

$$\operatorname{Re}\log\zeta(s) = \sum_{p}\sum_{n=1}^{\infty}\frac{1}{np^{n\sigma}}\cos(tn\log p).$$

Calling $tn\log p = \theta$, we apply the inequality, getting

$$3\operatorname{Re}\log\zeta(\sigma) + 4\operatorname{Re}\log\zeta(\sigma+it) + \operatorname{Re}\log\zeta(\sigma+2it) \geq 0.$$

Date: April 3rd, 2019.

More to the point,

$$3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+it)| + \log|\zeta(\sigma+2it)| \geq 0.$$

Taking exponentials,

$$|\zeta(\sigma)|^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)| \geq 1.$$

Now $\zeta(\sigma) = \frac{1}{\sigma-1} + O(1)$ as $\sigma \to 1^+$. Suppose $\zeta(\sigma+it) = 0$ for some $t \neq 0$. This implies $|\zeta(\sigma+it)|^4 = O_t((\sigma-1)^4)$ as $\sigma \to 1^+$, and also that $|\zeta(\sigma+2it)| = O_t(1)$ as $\sigma \to 1^+$. Hence

$$|\zeta(\sigma)|^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)| \to 0$$

as $\sigma \to 1^+$, which is a contradiction to it being bounded below by 1. Hence there can't be any zeros on $\mathrm{Re}(s) = 1$. □

Theorem 29.1.2. *There exists a constant $c > 0$ such that*

$$Z(\xi_0) \subset \left\{ s \in \mathbb{C} \;\middle|\; \mathrm{Re}(s) \leq 1 - \frac{c}{\log(2+|\mathrm{Im}(s)|)} \right\},$$

i.e., $\zeta(s) \neq 0$ for

$$\mathrm{Re}(s) > 1 - \frac{c}{\log(2+|\mathrm{Im}(s)|)}.$$

Proof. For $\sigma > 1$, we have the series representation

$$-\frac{\zeta'}{\zeta}(\sigma+it) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma+it}},$$

where as above we write the imaginary exponent $n^{-it} = e^{-it\log n}$.

Hence taking real parts, we have

$$\mathrm{Re}\left(-\frac{\zeta'}{\zeta}(\sigma+it)\right) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma}} \cos(t\log n).$$

Hence, in our trigonometric inequality,

$$3\left(-\frac{\zeta'}{\zeta}(\sigma)\right) + 4\,\mathrm{Re}\left(-\frac{\zeta'}{\zeta}(\sigma+it)\right) + \mathrm{Re}\left(-\frac{\zeta'}{\zeta}(\sigma+2it)\right) \geq 0.$$

Recall that by Hadamard factorisation, for $s = \sigma + it \in Z(\xi_0)$,

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s} + \frac{1}{s-1} + b - \sum_{\rho \in Z(\xi_0)} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) + \frac{\zeta_\infty'}{\zeta_\infty}(s).$$

For $\sigma > 1$,

$$-\frac{\zeta'}{\zeta}(\sigma) \leq \frac{1}{\sigma-1} + C_1$$

because of the pole.

For $s = \sigma + it$, $\sigma > 1$, $t \neq 0$, we have

$$-\operatorname{Re}\left(\frac{\zeta'}{\zeta}(\sigma+it)\right) \leq C_2 \log(2+|t|) - \sum_{\rho} \operatorname{Re}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right),$$

where the logarithm is from the arhimedian factor, bounded with Stirling's formula. In particular,

$$\operatorname{Re}\frac{1}{s-\rho} = \frac{\sigma-\beta}{|s-\rho|^2} \leq \frac{1}{|s-\rho|^2},$$

so the sum is bounded.

Applying this for $\sigma + it$, we get

$$-\operatorname{Re}\left(\frac{\zeta'}{\zeta}(\sigma+it)\right) \leq C_2 \log(2+|t|),$$

and for $\sigma + 2it$,

$$-\operatorname{Re}\left(\frac{\zeta'}{\zeta}(\sigma+2it)\right) \leq C_3 \log(2+|t|)$$

as well. However we don't want the first of those two estimates above quite as-is, as it gets rid of the information from the zeros. Instead let us detect zeros one at a time, by fixing $\rho_0 = \beta_0 + i\gamma_0 \in Z(\xi_0)$, and taking $s = \sigma + it$ with $t = \gamma_0$. Then

$$\operatorname{Re}\frac{1}{s-\rho} = \operatorname{Re}\frac{1}{\sigma+i\gamma_0-(\beta_0+i\gamma_0)} = \frac{1}{\sigma-\beta_0},$$

so if we get rid of the sum over zeros, except keeping only this one term from ρ_0, we have

$$-\operatorname{Re}\left(\frac{\zeta'}{\zeta}(\sigma+it)\right) \leq C_2 \log(2+|t|) - \frac{1}{\sigma-\beta_0}.$$

Thus our basic inequality becomes

$$3\left(\frac{1}{\sigma-1}+C_1\right) + 4\left(C_2\log(2+|t|) - \frac{1}{\sigma-\beta_0}\right) + C_3\log(2+|t|) \geq 0$$

for $t = \gamma_0$ and all $\sigma > 0$. Thus

$$\frac{4}{\sigma-\beta_0} - \frac{3}{\sigma-1} \leq C_4 \log(2+|t|)$$

for all $\sigma > 1$. Taking in particular $\sigma = 1 + \frac{\delta}{\log(2+|t|)}$, for some $\delta > 0$, we get

$$\beta_0 \leq 1 + \frac{\delta}{\log(2+|t|)} - \frac{4\delta}{(\delta C_4+3)\log(2+|t|)} \leq 1 - \frac{c}{\log(2+|t|)}$$

for some $c > 0$ by taking δ small enough. □

Lecture 30 Exceptional zeros

30.1 Zero free region for $L(s,\chi)$

Theorem 30.1.1. *There exista a constant $c>0$ such that if χ is a Dirichlet character modulo q, then $L(s,\chi)$ has no zeros in a region defined by*

$$\sigma > 1 - \frac{c}{\log(q(2+|t|))},$$

writing $s=\sigma+it$, unless χ is a real quadratic character in which case $L(s,\chi)$ has at most *one (necessarily real) zero $\beta<1$ in this region. Such a zero is called an* **exceptional zero** *or a* **Siegel zero**.

Proof. The strategy is essentially the same, we just need to take a little bit of extra care sometimes. Letting $s=\sigma+it$ with $\sigma>1$ we again have the series representation

$$-\frac{L'}{L}(s,\chi) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma}\chi(n)e^{-it\log n}.$$

Note that $|\chi(n)e^{-it\log n}|=1$ for $(n,q)=1$ (else 0), so let us write $\chi(n)e^{-it\log n} = e^{i\theta}$, so that $\cos(\theta)=\operatorname{Re}(\chi(n)e^{-it\log n})$, and correspondingly $e^{2i\theta}=\chi^2(n)e^{-i2t\log n}$, and so $\cos(2\theta)=\operatorname{Re}(\chi^2(n)e^{-2it\log n})$.

We also need to be a little bit careful with the constant 3 in our basic triginometric inequality: we'll write $1=\chi_0(n)$ for $(n,q)=1$ (and we don't care about other n, since they contribute nothing). Hence, multiplying by the appropriate factors and summing, the inequality becomes

$$-3\frac{L'}{L}(\sigma,\chi_0) + 4\operatorname{Re}\left(-\frac{L'}{L}(\sigma+it,\chi)\right) + \operatorname{Re}\left(-\frac{L'}{L}(\sigma+2it,\chi^2)\right) \geq 0.$$

As before we want an upper bount for this. Note first of all that if $\chi=\chi_0$, then

$$L(s,\chi) = \zeta(s)\prod_{p|q}(1-p^{-s}),$$

so the result follows from Theorem 29.1.2 for $\zeta(s)$.

Now consider the case where χ is complex, in which case χ^2 is nontrivial, so for $\sigma>1$,

$$-\frac{L'}{L}(\sigma,\chi_0) = \sum_{n=1}^{\infty}\frac{\chi_0(n)\Lambda(n)}{n^\sigma} \leq -\frac{\zeta'}{\zeta}(\sigma) \leq \frac{1}{\sigma-1} + C_1.$$

Secondly, by Hadamard factorisation,

$$-\frac{L'}{L}(s,\chi) = \frac{1}{2}\log\frac{q}{\pi} + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+\kappa}{2}\right) - b(\chi) - \sum_{0\leq\operatorname{Re}(\rho)\leq 1}\left(\frac{1}{s-\rho}-\frac{1}{\rho}\right).$$

We showed before that

$$\operatorname{Re} b(\chi) = -\sum_{\rho}\frac{1}{\rho},$$

Date: April 5th, 2019.

so taking real parts we have

$$\operatorname{Re}\left(-\frac{L'}{L}(s,\chi)\right) = \frac{1}{2}\log\frac{q}{\pi} + \frac{1}{2}\operatorname{Re}\frac{\Gamma'}{\Gamma}\left(\frac{s+\kappa}{2}\right) - \sum_{\rho}\operatorname{Re}\frac{1}{s-\rho}.$$

By Stirling's formula for the Gamma factors and by nonnegativity of the last sum, we have

$$\operatorname{Re}\left(-\frac{L'}{L}(\sigma+2it,\chi^2)\right) \leq C_2\log(q(2+|t|))$$

for $\chi^2 \neq \chi_0$.

For the middle term, as before, we isolate a zero: given $\rho_0 = \beta_0 + i\gamma_0$, take $s = \sigma + it$ with $\sigma > 0$ and $t = \gamma_0$. Then keeping precisely that term from the above sum,

$$\operatorname{Re}\left(-\frac{L'}{L}(\sigma+it,\chi)\right) \leq C_2\log(q(2+|t|)) - \frac{1}{\sigma-\beta_0}.$$

Inserting these and going through the motions,

$$\beta_0 \leq 1 - \frac{c}{\log(q(2+|t|))},$$

for some $c > 0$ and $t = \gamma_0$.

Secondly, and more intricately, we need to consider the case where χ is real. The above bound works only for $\chi^2 \neq \chi_0$, but now we in fact have precisely $\chi^2 = \chi_0$, so we need to do something else.

There are three cases to consider now. First, we are dealing with zeros at great height, say $|\gamma_0| \geq 6(1-\beta_0)$. Take $s = \sigma + it$ with $t = \gamma_0$ again, and estimate

$$\operatorname{Re}\left(-\frac{L'}{L}(\sigma+2it,\chi^2)\right) \leq C_3\log(q(2+|t|)) + \operatorname{Re}\frac{1}{(\sigma+2it)-1} \leq C_3\log(q(2+|t|)) + \frac{\sigma-1}{(\sigma-1)^2+144(1-\beta_0)^2}$$

where the last term comes from the term $\frac{1}{s-1}$, and the estimate stems from

$$\operatorname{Re}\frac{1}{(\sigma+2it)-1} = \frac{\sigma-1}{(\sigma-1)^2+4\gamma_0^2} \leq \frac{\sigma-1}{(\sigma-1)^2+144(1-\beta_0)^2}.$$

Therefore

$$3\left(\frac{1}{\sigma-1}+C_1\right)+4\left(C_2\log(q(2+|t|)) - \frac{1}{\sigma-\beta_0}\right)+\left(\frac{\sigma-1}{(\sigma-1)^2+144(1-\beta_0)^2} + C_3\log(q(2+|t|))\right) \geq 0.$$

Taking $\sigma = 1 + 6(1-\beta_0)$, it eventually follows that

$$\beta_0 \leq 1 - \frac{c}{\log(q(2+|t|))}.$$

Secondly, suppose we are concerned with a low-lying zero, say $0 < |\gamma_0| < 6(1-\beta_0)$. Since χ is rael, $\rho_0 = \beta_0 + i\gamma_0$ being a zero implies $\overline{\rho_0} = \beta_0 - i\gamma_0$ is one too. Taking $s = \sigma$ since the height t is quite small now, we have

$$-\frac{L'}{L}(\sigma,\chi) \leq -\operatorname{Re}\left(\frac{1}{\sigma-\rho_0}\right) - \operatorname{Re}\left(\frac{1}{\sigma-\overline{\rho_0}}\right) + C_5\log q = \frac{-2(\sigma-\beta_0)}{(\sigma-\beta_0)^2+\gamma_0^2} + C_5\log q.$$

Since $t = 0$ and χ real, $\chi^2 = \chi_0$, our inequality becomes simply

$$-\frac{L'}{L}(\sigma, \chi_0) - \frac{L'}{L}(\sigma, \chi) \geq 0.$$

For the first term the old bound works just fine, and for the second term we use the above. Taking $\sigma = 1 + \delta(1 - \beta_0)$, and then later $\delta = 13$ (for example), we get the result we want.

Finally, suppose $\gamma_0 = 0$, so $\rho_0 = \beta_0 \in \mathbb{R}$. This is where we might get an exceptional zero.

Suppose there are two real zeros, say, $0 \leq \beta_0 \leq \beta_1 < 1$. Then

$$-\frac{L'}{L}(\sigma, \chi) \leq -\frac{1}{\sigma - \beta_0} - \frac{1}{\sigma - \beta_1} + C_5 \log q \leq -\frac{2}{\sigma - \beta_0} + C_5 \log q,$$

so

$$\frac{1}{\sigma - 1} + C_1 - \frac{2}{\sigma - \beta_0} + C_5 \log q \geq 0.$$

Taking $\sigma = 1 + \delta(1 - \beta_0)$,

$$\frac{1}{1 - \beta_0}\left(\frac{1}{\delta} + \frac{2}{\delta + 1}\right) + C_6 \log q \geq 0,$$

which if we take $\delta = 2$ gives us

$$\beta_0 \leq 1 - \frac{c}{\log q},$$

for some $c > 0$.

Now this gives the same sort of zero free region, except for the notable hitch that it bounds β_0—we might still have the hypothetical β_1 to the right of it.

Note that there can only ever be one exceptional zero, since otherwise we can repeat this argument with β_1 in place of β_0. □

A question one now asks is this: For which $q \in \mathbb{N}$ is there a real quadratic character $\chi \pmod q$ such that $L(s, \chi)$ has an exceptional zero?

There are no known examples. Moreover, if we assume the Riemann hypothesis for $L(s, \chi)$, then such q cannot exist.

Indeed, Landau shows that such a q is very, very rare if it exists.

Lecture 31 Landau's theorem

31.1 Exceptional zeros

Theorem 31.1.1 (Landau)**.** *There exists a constant $c > 0$ such that if $\chi_1 \pmod{q_1}$ and $\chi_2 \pmod{q_2}$ are real quadratic characters such that $\chi_1\chi_2$ is non-trivial, then $L(s, \chi_1)L(s, \chi_2)$ has at most one real zero β such that*

$$1 - \frac{c}{\log q_1 q_2} < \beta < 1.$$

Date: April 8th, 2019.

Proof. We have

$$1 + \chi_1(n) + \chi_2(n) + \chi_1\chi_2(n) = (1 + \chi_1(n))(1 + \chi_2(n)) \geq 0,$$

so for $\sigma > 1$, multiply by $\Lambda(n)/n^\sigma$ and sum over n, getting

$$-\frac{\zeta'}{\zeta}(\sigma) - \frac{L'}{L}(\sigma, \chi_1) - \frac{L'}{L}(\sigma, \chi_2) - \frac{L'}{L}(\sigma, \chi_1\chi_2) \geq 0.$$

Now assume $L(s, \chi_i)$ has an exceptional zero β_i, and assume $\beta_1 \leq \beta_2$. We want an upper bound for the left-hand side above, and we have some from our previous discussion:

$$-\frac{\zeta'}{\zeta}(\sigma) \leq \frac{1}{\sigma - 1} + c_1,$$

as well as

$$-\frac{L'}{L}(\sigma, \chi_i) \leq -\frac{1}{\sigma - \beta_i} + c_2 \log q_i,$$

and finally

$$-\frac{L'}{L}(\sigma, \chi_1\chi_2) \leq c_3 \log q_1 q_2$$

since by assumption $\chi_1\chi_2 \neq \chi_0$. Hence

$$\frac{1}{\sigma - 1} - \frac{1}{\sigma - \beta_1} - \frac{1}{\sigma - \beta_2} + c_4 \log q_1 q_2 \geq 0.$$

Since $\beta_1 \leq \beta_2$, we have moreover

$$\frac{1}{\sigma - 1} - \frac{2}{\sigma - \beta_1} + c_4 \log q_1 q_2 \geq 0.$$

Taking $\sigma = 1 + 2(1 - \beta_1)$, we get

$$\beta_1 \leq 1 - \frac{c}{\log q_1 q_2},$$

for some $c > 0$. □

Note that this means that if $\beta_1 = \beta_2$, then neither zero is in this special region.

Corollary 31.1.2. *There exists a constant $c > 0$ such that*

$$\prod_{\chi \pmod q} L(s, \chi)$$

has at most one zero in the region

$$\sigma > 1 - \frac{c}{\log q(2 + |t|)},$$

for $s = \sigma + it$. If such a zero exists, then it is real and the associated character χ is quadratic.

Corollary 31.1.3 (Page)**.** *There exista a constant $c > 0$ such that for every $Q \geq 1$,*

$$\prod_{q \leq Q\chi} \prod_{(\mathrm{mod}\ q)}^{*} L(s, \chi),$$

where by the asterisk we mean a product over primitive characters, has at most one zero in the region

$$\sigma < 1 - \frac{c}{\log Q(2 + |t|)},$$

for $s = \sigma + it$. If such a zero exists, then it's real and the associated character is quadratic.

31.2 Siegel's theorem

Siegel's theorem is about bounding the zero-free region away from 1, and essentially the idea is to leverage upper bounds of the L-function at 1.

Theorem 31.2.1. *Let $\chi \neq \chi_0$ be a quadratic character modulo q. Then $L(1, \chi) \gg q^{-1/2}$.*

Proof. Define $\tau(n) \coloneqq 1 \star \chi(n)$. We have showed before (in past homework) that $\tau(n) \geq 0$ for all n and $\tau(n) \geq 1$ if n is a perfect square.

Consider

$$\sum_{n \geq 1} \tau(n) e^{-\frac{n}{x}}.$$

We can easily get a lower bound for this:

$$\sum_{n \geq 1} \tau(n) e^{-\frac{n}{x}} \geq \sum_{m \geq 1} \tau(m^2) e^{-\frac{m^2}{x}} \geq \sum_{m \geq 1} e^{-\frac{m^2}{x}} \gg x^{1/2}$$

by comparing with the integral.

To get asymptotics for it, note that by Mellin inversion

$$e^{-x} = \frac{1}{2\pi i} \int_{(2)} \Gamma(s) X^{-s}\, ds,$$

so

$$\sum_{n \geq 1} \tau(n) e^{-\frac{n}{x}} = \frac{1}{2\pi i} \int_{(2)} \left(\sum_{n \geq 1} \frac{\tau(n)}{n^s} \right) \Gamma(s) X^s\, ds,$$

where the inner sum is $\zeta(s)L(s, \chi)$ by the definition of $\tau(n)$. Shifting the line of integration from (2) to $(-\frac{1}{2})$ picks up residues from $\zeta(s)$ at $s = 1$, namely $XL(1, \chi)$, and from $\Gamma(s)$ at $s = 0$, namely $\zeta(0)L(0, \chi)$.

Hence the sum is

$$L(1, \chi)X + \zeta(0)L(0, \chi) + \frac{1}{2\pi i} \int_{(-\frac{1}{2})} \zeta(s)L(s, \chi)\Gamma(s)X^s\, ds.$$

We have $\zeta(0) = -\frac{1}{2}$, and $L(0, \chi) \geq 0$ since it's positive at 1, and we translate by the functional equation. By studying the completed L-function for $L(s, \chi)$ at 3/2, using Stirling, and then using the functional equation we translate to

$-1/2$ and get that $L(s,\chi) \ll q|t|$ on this line. Hence by exponential decay, the entire integral is $\ll qX^{-1/2}$.

Thus

$$X^{1/2} \ll L(1,\chi)X + O(qX^{-1/2}).$$

Taking $X = q$, we deduce $L(1,\chi) \gg q^{-1/2}$. □

Corollary 31.2.2. *There exists a cosntant $c > 0$ such that if $\chi \pmod q$ is a quadratic character with $L(s,\chi)$ having an exceptional zero β, then*

$$\beta \leq 1 - \frac{c}{q^{1/2}(\log q)^2}.$$

Proof. We can show $L'(\sigma,\chi) \ll (\log q)^2$ for

$$1 - \frac{1}{\log q} \leq \sigma \leq 1.$$

By the mean value theorem,

$$q^{-1/2} \ll L(1,\chi) = L(1,\chi) - L(\beta,\chi) = L'(\sigma,\chi)(1-\beta) \ll (1-\beta)(\log q)^2,$$

so

$$\beta \leq 1 - \frac{c}{q^{1/2}(\log q)^2},$$

for $c > 0$. □

Theorem 31.2.3 (Siegel's theorem)**.** *For any $\varepsilon > 0$, there exists a constant $C(\varepsilon) > 0$ such that*

$$L(1,\chi) \geq \frac{C(\varepsilon)}{q^\varepsilon}$$

for all primitive quadratic characters $\chi \pmod q$.

Remark 31.2.4. This constant is ineffective—we don't know how to compute a numerical value for $\varepsilon < 1/2$.

Lecture 32 Siegel's theorem

32.1 Proof

Proof. Let $\chi_1 \pmod{q_1}$ and $\chi_2 \pmod{q_2}$ be two primitive characters. Define

$$\tau(n) = 1 \star \chi_1 \star \chi_2 \star \chi_1\chi_2(n),$$

so that

$$L(s,\tau) = \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2).$$

We have (essentially) showed before that $\tau(n) \geq 0$ for all n.

We claim that for any $\varepsilon > 0$, there exists a primitive quadratic character $\chi_1 \pmod{q_1}$ and β with $1 - \varepsilon < \beta < 1$ such that $L(\beta,\tau) \leq 0$ for all primitive quadratic characters $\chi_2 \pmod{q_2}$, with $q_2 \neq q_1$.

Date: April 10th, 2019.

Remark 32.1.1. We do not know how to compute this q_1, which is what makes this result ineffective.

We prove this in two cases. First, suppose there are no zeros on $[1-\varepsilon, 1]$ of $L(s,\chi)$ for any quadratic character χ. Then take any $\chi_1 \pmod{q_1}$. We have $L(\beta,\chi) > 0$ since $L(1,\chi) > 0$ for quadratic characters $\chi \neq \chi_0$. Likewise $L(s,\chi_2) > 0$, and $L(s,\chi_1\chi_2) > 0$ since $\chi_1\chi_2 \neq \chi_0$ because $q_1 \neq q_2$.

Moreover $\zeta(\beta) < 0$ since it is approximately $1/(s-1)$ near 1, so $L(\beta,\tau) < 0$.

Secondly, suppose there exists $\chi \pmod{()q}$ with a real zero $\beta \in [1-\varepsilon, 1]$. Take $\chi_1 = \chi$, so that $L(\beta,\chi_1) = 0$. Then of course $L(\beta,\tau) = 0$ too.

With this in hand we are ready to prove Siegel's theorem. Take χ_1, q_1, and β as in the claim. Let

$$\lambda = \operatorname*{Res}_{s=1} L(s,\tau) = L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2).$$

Then

$$\frac{1}{e} \leq \sum_{n\geq 1} \frac{\tau(n)}{n^\beta} e^{-\frac{n}{x}} = \frac{1}{2\pi i}\int_{(2)} L(s+\beta,\tau)\Gamma(s)X^s\,ds$$

by Mellin inversion. Moving the line of integration from (2) to $(-\beta)$, we pick up poles at $s = 1-\beta$ and $s = 0$ with residues $\lambda\Gamma(1-\beta)X^{1-\beta}$ and $L(\beta,\tau)$ respectively. Thus

$$\frac{1}{e} \leq \lambda\Gamma(1-\beta)X^{1-\beta} + L(\beta,\tau) + \frac{1}{2\pi i}\int_{(-\beta)} L(s+\beta,\tau)\Gamma(s)X^s\,ds,$$

where by choice of β, $L(\beta,\tau) \leq 0$ by the claim.

We have

$$L(it,\chi) \ll ((2+|t|)q)^{1/2+\varepsilon}$$

for $\chi \pmod{q}$, and

$$\zeta(it) \ll (2+|t|)^{1/2+\varepsilon},$$

so

$$L(it,\tau) \ll (2+|t|)^{2+\varepsilon}(q_1q_2)^{1+\varepsilon}.$$

Note that $-\beta$ is close to -1, and $\Gamma(s)$ has a simple pole at $s = -1$, so $\Gamma(-\beta) = O(1/(1-\beta))$, meaning that the integral above is

$$O\left(\frac{(q_1q_2)^{1+\varepsilon}X^{-\beta}}{1-\beta}\right),$$

and therefore

$$\frac{1}{e} \leq \lambda\Gamma(1-\beta)X^{1-\beta} + O\left(\frac{(q_1q_2)^{1+\varepsilon}X^{-\beta}}{1-\beta}\right),$$

having dropped $L(\beta,\tau)$ since it's nonpositive. Now if $\lambda X^{1-\beta} \geq (q_1q_2)^{1+\varepsilon}X^{-\beta}$, so $\lambda X \geq (q_1q_2)^{1+\varepsilon}$, so since

$$\lambda = L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2) \gg (q_1q_2)^{-1},$$

we have

$$\frac{X}{q_1q_2} > (q_1q_2)^{1+\varepsilon},$$

meaning that

$$1 \ll \frac{\lambda X^{1-\beta}}{1-\beta}$$

provided $(q_1q_2)^{2+\varepsilon} \ll X$, guaranteeing that

$$\lambda\Gamma(1-\beta)X^{1-\beta} \geq O\left(\frac{(q_1q_2)^{1+\varepsilon}X^{-\beta}}{1-\beta}\right)$$

so that we have the asymptotics we want.

Now for $\chi \neq \chi_0 \pmod q$, $L(1,\chi) \ll \log q$, so

$$\lambda \ll L(1,\chi_2)(\log q_1)(\log q_1q_2).$$

Take $X = (q_1q_2)^{2+\varepsilon}$, which may be a new epsilon, and insert into the bound on λ above. Then

$$L(1,\chi_2) \gg \frac{1}{(\log q_1)(\log q_1q_2)} \cdot (q_1q_2)^{-(2+\varepsilon)(1-\beta)}(1-\beta)$$

Now q_1 and β depend on ε, so we get

$$L(1,\chi_2) \geq C(\varepsilon)q_2^{-(2+\varepsilon)(1-\beta)}(\log q_2)^{-1}.$$

Moreover, $(1-\beta) < \varepsilon$, so $(2+\varepsilon)(1-\beta) < 3\varepsilon$, and $\log q \ll q^{\varepsilon}$, so

$$L(1,\chi_2) \geq \frac{C(\varepsilon)}{q^{\varepsilon}}.$$ □

Corollary 32.1.2. *For any $\varepsilon > 0$, there exists a constant $C(\varepsilon) > 0$ such that if $\chi \pmod q$ is a quadratic character such that $L(s,\chi)$ has an exceptional zero β, then*

$$\beta \leq 1 - \frac{C(\varepsilon)}{q^{\varepsilon}}.$$

Proof. The same as Corollary 31.2.2. □

Lecture 33 The Prime number theorem in Arithmetic progressions

33.1 Prime number theorem

Recall how we proved the ordinary Prime number theorem by

$$\pi(x) \sim \frac{x}{\log x} \quad \Leftrightarrow \quad \vartheta(x) = \sum_{p \leq x} \log p \sim x \quad \Leftrightarrow \quad \psi(x) = \sum_{n \leq x} \Lambda(n) \sim x.$$

We prove this last step by smoothing the sum over all n with a smoothing function, using the explicit formula to write in terms of the Zeta function, and then use the zero-free region of $\zeta(s)$.

Date: April 12th, 2019.

The strategy for arithmetic progressions is largely the same. For a and q with $(a,q)=1$,

$$\pi(x;q,a) = \sum_{\substack{p\le x\\ p\equiv a \pmod q}} 1 \sim \frac{\pi(x)}{\varphi(q)}$$

is equivalent to

$$\varphi(x;q,a) = \sum_{\substack{p\le x\\ p\equiv a \pmod q}} \log p \sim \frac{x}{\varphi(q)},$$

is equivalent to

$$\psi(x;q,a) = \sum_{\substack{n\le x\\ n\equiv a \pmod q}} \Lambda(n) \sim \frac{x}{\varphi(q)},$$

which we will prove.

Let $f \in C_c^\infty((0,\infty))$, $(a,q)=1$. Define

$$\psi_f(x;q,a) \coloneqq \sum_{\substack{n\le x\\ n\equiv a \pmod q}} \Lambda(n) f\left(\frac{n}{x}\right).$$

By the orthogonality relations,

$$\psi_f(x;q,a) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi}(a)\psi_f(x,\chi),$$

where

$$\psi_f(x,\chi) \coloneqq \sum_{n\ge 1} \Lambda(n)\chi(n) f\left(\frac{n}{x}\right).$$

For $\chi = \chi_0$ we get

$$\psi_f(x,\chi_0) = \sum_{(n,q)=1} \Lambda(n) f\left(\frac{n}{x}\right) = \sum_{n\ge 1} \Lambda(n) f\left(\frac{n}{x}\right) - \sum_{(n,q)>1} \Lambda(n) f\left(\frac{n}{x}\right).$$

Studying each sum separately,

$$\sum_{(n,q)>1} \Lambda(n) f\left(\frac{n}{x}\right) \ll \sum_{\substack{n\ll x\\ (n,q)>1}} \Lambda(n) = \sum_{p\mid q} \sum_{p^\alpha << x} \log p \ll (\log x) \sum_{p\mid q} \log p = (\log x)(\log q).$$

On the other hand,

$$\sum_{n\ge 1} \Lambda(n) f\left(\frac{n}{x}\right) = x \int_0^\infty f(t)\,dt + O_f(x\exp(-c\sqrt{\log x}))$$

for some $c>0$ by Corollary 28.1.3.

Hence

$$\psi_f(x;q,a) = \frac{x}{\varphi(q)} \int_0^\infty f(t)\,dt + \frac{1}{\varphi(q)} \sum_{\chi\ne\chi_0 \pmod q} \overline{\chi}(a)\psi_f(x,\chi) + O_f\left(\frac{1}{\varphi(q)}(x\exp(-c\sqrt{\log x}) + \log x \log q)\right).$$

Proposition 33.1.1. *Suppose* $q \ll \exp(\frac{1}{2}\sqrt{\log x})$.

(a) *If $\chi \neq \chi_0$ such that $L(s,\chi)$ has no exceptional zeros, then there exists a constant $c > 0$ such that $\psi_f(x,\chi) \ll_f x\exp(-c\sqrt{\log x})$ uniformly in χ.*

(b) *If $\chi \neq \chi_0$ such that $L(s,\chi)$ has an exceptional zero $\beta \in \mathbb{R}$, then there exists a constant $c > 0$ such that*

$$\psi_f(x,\chi) = -\tilde{f}(\beta)X^\beta + O_f(x\exp(-c\sqrt{\log x}))$$

uniformly in χ.

Proof. Choose x large enough such that $f(\frac{1}{nx}) = 0$ for all $n \geq 1$. By the explicit formula,

$$\psi_f(x,\chi) = \frac{1}{2\pi i}\int_{(\frac{1}{2})}(\frac{L'_\infty}{L_\infty}(s,\chi) - \frac{L'_\infty}{L_\infty}(1-s,\overline{\chi}))\tilde{f}(s)x^s\,ds - \sum_{\rho\in Z(\Lambda(s,\chi))}\tilde{f}(\rho)x^\rho.$$

The integral is $\ll x^{1/2}$. By Theorem 30.1.1,

$$\sum_{\rho\in Z(\Lambda(s,\chi))}{}' |\tilde{f}(\rho)| \ll \exp\left(-\frac{c\log x}{\log q(2+\gamma)}\right),$$

with $\mathrm{Im}(\rho) = \gamma$.

Then

$$\sum_{\substack{\rho\in Z(\Lambda(s,\chi))\\ \log(q(2+|\gamma|))\leq\sqrt{\log x}}}{}' |\tilde{f}(\rho)| \ll \exp(-c\sqrt{\log x}),$$

and

$$\sum_{\substack{\rho\in Z(\Lambda(s,\chi))\\ \log(q(2+|\gamma|))>\sqrt{\log x}}}{}' |\tilde{f}(\rho)| \ll \sum|\tilde{f}(\rho)| \ll \sum\frac{1}{|\gamma|^2} \ll \sum\frac{1}{|\gamma|^{3/2}}\frac{1}{|\gamma|^{1/2}}. \qquad \square$$

Corollary 33.1.2. *Suppose $q \ll \exp(\frac{1}{2}\sqrt{\log x})$. Then*

$$\psi(x;q,a) = \frac{x}{\varphi(q)}\int_0^\infty f(t)\,dt - \frac{1}{\varphi(q)}\sum_\chi \overline{\chi}(a)\tilde{f}(\beta)x^\beta + O_f(x\exp(-c\sqrt{\log x}))$$

for some $c > 0$, where the sum is over χ with exceptional zero β.

Lecture 34 Bombieri-Vinogradov

34.1 Prime number theorem in arithmetic progressions

We can now finish the prime number theorem:

Theorem 34.1.1 (Siegel-Walfisz theorem)**.** *Let $C < 0$ (effective) as in Corollary 33.1.2. Then for all $A > 0$, $q \ll (\log x)^A$, $(a,q) = 1$, and $X \geq 2$, we have*

$$\psi_f(x;q,a) = \frac{x}{\varphi(q)}\int_0^\infty f(t)\,dt + O_{f,A}(x\exp(-c\sqrt{\log x})),$$

where the implied constant depending on A and f is ineffective.

Date: April 15th, 2019.

The ineffectiveness comes from us using Siegel's theorem in the proof.

Proof. We have

$$x^\beta = x\exp(-(1-\beta)\log x) \le x\exp(-C(\varepsilon)q^{-\varepsilon}\log x)$$

by Siegel's theorem. Since $q \ll (\log x)^A$,

$$x^\beta \ll x\exp(-C(\varepsilon)(\log x)^{1-A\varepsilon}).$$

Taking $\varepsilon = 1/(3A)$, we get

$$x^\beta \ll x\exp(-C(\varepsilon)(\log x)^{2/3}). \qquad \square$$

Thus also:

Theorem 34.1.2 (Siegel-Walfisz)**.** *Suppose $A > 0$. For $q \ll (\log x)^A$, $(a,q) = 1$, $x \ge 2$, we have*

$$\psi(x;q,a) = \frac{x}{\varphi(q)} + O_A(\exp(-c\sqrt{\log x})),$$

for some $c > 0$, which is equivalent with the Prime number theorem in arithmetic progressions.

Another way of saying this:

Theorem 34.1.3 (Siegel-Walfisz, variant)**.** *Suppose $A > 0$. For $q \ll (\log x)^A$ and $\chi \pmod q$, we have*

$$\psi(x,\chi) - \delta(\chi)x \ll_A x\exp(-c\sqrt{\log x})$$

for some $c > 0$, where

$$\delta(\chi) = \begin{cases} 1, & \text{if } \chi = \chi_0, \\ 0, & \text{if } \chi \ne \chi_0. \end{cases}$$

34.2 The Bombieri-Vinogradov theorem

There are two questions we want to ask about all of this.

- In the proof we use that there is no real zeros of $L(s,\chi)$ near 1 (i.e., Siegel's theorem). What is the error term if we assume the Generalised Riemann Hypothesis (GRH), i.e., all zeros of $L(s,\chi)$ in $0 \le \mathrm{Re}(s) \le 1$ lie on $\mathrm{Re}(s) = \frac{1}{2}$.
- Can we enlarge the range of q?

Under GRH we can deduce that

$$\psi(x;q,a) = \frac{x}{\varphi(q)} + O(x^{1/2}(\log x)^2)$$

uniformly for all q.

To have this make asymptotic sense, note that $\varphi(q) \sim q$, so

$$\frac{x}{q} > x^{1/2}(\log x)^2$$

implies

$$q < \frac{x^{1/2}}{(\log x)^2},$$

meaning $q < x^{1/2}$.

A remarkable result is that we can achieve the GRH error term on average:

Theorem 34.2.1 (Bombieri-Vinogradov)**.** *For any $A > 0$, $Q \le X^{1/2}$,*

$$\sum_{q \le Q} \max_{(a,q)=1} \max_{y \le X} \left| \psi(y; q, a) - \frac{y}{\varphi(q)} \right| \ll_A X(\log X)^{-A} + X^{1/2} Q (\log X)^4.$$

Remark 34.2.2. (*i*) The implied constant is ineffective since we use Siegel's theorem in the proof. However, in 2013, Akbary and Hambrook managed to prove Bombieri-Vinogradov without relying on Siegel's theorem.

(*ii*) Taking $X^{1/2}(\log X)^{-A-4} \le Q \le X^{1/2}$, then the second term in the theorem is larger, so the sum is bounded by $X^{1/2}(\log X)^4$. The theorem says that if we average over q, this bound is as good as GRH for all $\chi \pmod q$, $q \le X^{1/2}(\log X)^{-A-4}$.

(*iii*) For $Q > X^{1/2}$, we use the trivial bound

$$\psi(X; q, a) = \sum_{\substack{n \le X \\ n \equiv a \pmod q}} \Lambda(n) \le (\log X) \left(\frac{X}{q} + 1 \right),$$

so the sum is

$$\ll \sum_{q \le Q} \left(\frac{X}{q} + 1 \right) \log X \ll X(\log X)(\log Q) + Q(\log X),$$

which is a better bound than the theorem.

Proof. By orthogonality,

$$\psi(X; q, a) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi}(a) \psi(X, \chi).$$

Hence

$$\left| \psi(y; q, a) - \frac{y}{\varphi(q)} \right| = \frac{1}{\varphi(q)} \left| \sum_{\chi \pmod q} \overline{\chi}(a) \psi(y, \chi) - \delta(\chi) y \right|.$$

Getting rid of the character, since it is of modulus 1, we may potentially lose some cancellation. We get

$$\le \frac{1}{\varphi(q)} \sum_{\chi \pmod q} |\psi(y, \chi) - \delta(\chi) y|.$$

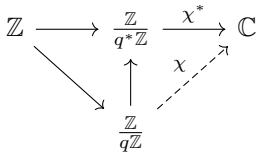
So it suffices to bound

$$\sum_{q \le Q} \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \max_{y \le X} |\psi(y, \chi) - \delta(\chi) y|.$$

We can moreover reduce this to primitive characters. If $\chi \pmod q$ is induced by a primitive character $\chi^* \pmod{q^*}$, $q^* \mid q$, then

$$\psi(y,\chi) = \psi(y,\chi^*) + O\left(\sum_{\substack{p\mid q\\ p\nmid q^*}} (\log p) \sum_{k\le \frac{\log y}{\log p}} 1\right).$$

To see this, note that



Evaluating at $n = p^k$, $p \mid q$, $p \nmid q^*$, we have $\chi(n) = 0$ but $\chi^*(n) \neq 0$, and the $\log p$ accounts for $\Lambda(p^k)$, and the inner sum counts how many of them there are. □

Lecture 35 Bombieri-Vinogradov, continued

35.1 The trivial case

The remainder at the end of the last discussion is of order $(\log y)(\log q)$, so the sum is

$$\sum_{q\le Q} \frac{1}{\varphi(q)} \sum_{q^*\mid q} \sideset{}{^*}\sum_{\chi^* \pmod{q^*}} \max_{y\le X} |\psi(y,\chi^*) - \delta(\chi^*)y| + O(Q(\log q)(\log X)).$$

Writing $q = q^*r$,

$$\sum_{q^*\le Q} \sum_{r\le Q/q^*} \frac{1}{\varphi(q^*r)} \sideset{}{^*}\sum_{\chi^* \pmod{q^*}} \max_{y\le X} |\psi(y,\chi^*) - \delta(\chi^*)y|. \tag{35.1.1}$$

Note that $\varphi(q^*r) \ge \varphi(q^*)\varphi(r)$. Moreover

$$\sum_{q\le Q} \frac{1}{\varphi(q)} \ll \log Q$$

since

$$\begin{aligned}\sum_{q\le Q} \frac{1}{\varphi(q)} &\le \prod_{p\le Q} \sum_{n=0}^{\infty} \frac{1}{\varphi(p^n)} = \prod_{p\le Q} \left(1 + \sum_{n=1}^{\infty} \frac{1}{p^n - p^{n-1}}\right)\\ &= \prod_{p\le Q} \left(1 - \frac{1}{p}\right)^{-1} \left(1 + \frac{1}{p(p-1)}\right) \ll \log Q.\end{aligned}$$

Thus for (35.1.1) we have the bound

$$\ll \sum_{q\le Q} \frac{\log Q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \max_{y\le X} |\psi(y,\chi) - \delta(\chi)y|.$$

Date: April 17th, 2019.

Let $R = (\log X)^{A+4}$. We will splot the range of q according to whether $q \le R$, for which we can use Siegel's theorem, and $R < q \le Q$, for which we need new machienery, namely the Large Sieve and Polya's inequality.

Claim. *With definitions as above,*

$$\sum_{q\le R} \frac{\log Q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \max_{y\le X} |\psi(y,\chi) - \delta(\chi)y| \ll_A R(\log X)X\exp(-c\sqrt{\log X})$$

for some $c > 0$. Note that this moreover is

$$\ll X(\log X)^{-K}$$

for any $K > 0$.

Proof. We consider two cases: $y \le \sqrt{X}$, and $\sqrt{X} < y \le X$. First, when $y \le \sqrt{X}$,

$$|\psi(y,\chi) - \delta(\chi)y| \ll y \le \sqrt{X}$$

trivially since we can bound the left-hand side by $\psi(y) \sim y$. Hence

$$\sum_{q\le R} \frac{\log Q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \sqrt{X} \ll (\log Q)\sqrt{X}R \ll (\log X)\sqrt{X}R.$$

Second, when $\sqrt{X} < y \le X$, $q \le R = (\log X)^{A+4} \ll (\log y)^{A+4}$, so by Siegel-Walfisz,

$$|\psi(y,\chi) - \delta(\chi)y| \ll_A y\exp(-c\sqrt{\log y}) \ll X\exp(-c\sqrt{\log X}).$$

Hence

$$\sum_{q\le R} \frac{\log Q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} X\exp(-c\sqrt{\log X}) \ll (\log Q)X\exp(-c\sqrt{\log X})R,$$

and $\log Q \ll \log X$. □

35.2 The nontrivial part

We now need to deal with

$$\sum_{R<q\le Q} \frac{\log Q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \max_{y\le X} |\psi(y,\chi) - \delta(\chi)y|.$$

Note that in this range of q, or in particular $q > 1$, there are no trivial primitive characters modulo q, so $\delta(\chi) = 0$, and we really only need to deal with

$$\log Q \sum_{R<q\le Q} \frac{1}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \max_{y\le X} |\psi(y,\chi)|. \tag{35.2.1}$$

Theorem 35.2.1 (Basic mean value theorem)**.** *Let*

$$T(X,Q) \coloneqq \sum_{q\le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \max_{y\le X} |\psi(y,\chi)|.$$

Then for $Q \ge 1$, $X \ge 2$, we have

$$T(X,Q) \ll (X + X^{5/6}Q + X^{1/2}Q^2)(\log XQ)^3.$$

We will prove this at some point, but for now let us assume it true.
Let

$$f(q) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q}^{*} \max_{y \le X} |\psi(y, \chi)|,$$

the inner summand above, so that (35.2.1) is

$$(\log Q) \sum_{R < q \le Q} f(q) = (\log Q) \sum_{R < q \le Q} \frac{1}{q} f(q) q.$$

Writing this as a Stieltje's integral,

$$(\log Q) \int_R^Q \frac{1}{t}\, d\Big(\sum_{q \le t} f(q) q \Big),$$

where the weight is $T(X, t)$. Integrating by parts gives us

$$(\log Q) \left(\frac{1}{t} T(X,t) \Big|_R^Q + \int_R^Q \frac{1}{t^2} T(X,t)\, dt \right)$$

Using the Mean value theorem above, this is

$$\ll (\log Q) \left(Q^{-1}(X + X^{5/6}Q + X^{1/2}Q^2)(\log XQ)^3 + \int_R^Q t^{-2}(X + X^{5/6}t + X^{1/2}t^2)(\log Xt)^3\, dt \right)$$

and by bounding $\log Q \ll \log X$ and $\log Xt \ll \log XQ$,

$$\ll Q^{-1}(X + X^{5/6}Q + X^{1/2}Q^2)(\log X)^4 + (XR^{-1} + X^{5/6} \log Q + X^{1/2}Q)(\log X)^4,$$

which we can finally bound as

$$\ll X(\log X)^{-A} + X^{1/2}Q(\log X)^4$$

since $R = (\log X)^{A+4}$.

Theorem 35.2.2 (Polya-Vinogradov inequality)**.** *Let $\chi \neq \chi_0 \pmod q$, with $q > 1$. Then*

$$\Big| \sum_{n=M+1}^{M+N} \Big| \le 2q^{1/2}(\log q).$$

Note that trivially the sum is $\le q$, but we know that if we sum over a full set of residues it is 0, so we should expect a lot of cancellation. This theorem reveals just how much!

Lecture 36 The Large Sieve

36.1 The Large siece inequality

For $N, Q > 1$, we have

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sum_{\chi \pmod q}^{*} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll (N + Q^2)^{1/2} \sum_{n=M+1}^{M+N} |a_n|^2$$

Date: April 19th, 2019.

for any $\{ a_n \} \subset \mathbb{C}$.

A consequence of this is

Theorem 36.1.1.

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \max_y \Big| \sum_{\substack{m=1 \\ mn \le y}}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) \Big|$$

$$\ll (\log 2MN)(M+Q^2)^{1/2}(N+Q^2)^{1/2} \left(\sum_{m=1}^{M} |a_m|^2 \right)^{1/2} \left(\sum_{n=1}^{N} |b_n|^2 \right)^{1/2}$$

Note that without the condition $mn \le y$, the sum splits (since $\chi(mn) = \chi(m)\chi(n)$ by complete multiplicativity), and by Cauchy's inequality

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \Big| \sum_{m=1}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) \Big|$$

$$\le \left(\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \left| \sum_{m=1}^{M} a_m \chi(m) \right|^2 \right)^{1/2} \left(\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \left| \sum_{n=1}^{N} b_n \chi(n) \right|^2 \right)^{1/2}$$

We can then use the Large sieve at each factor separately, getting

$$\ll (M+Q^2)^{1/2} \left(\sum_{m=1}^{M} |a_m|^2 \right)^2 (N+Q^2)^{1/2} \left(\sum_{n=1}^{N} |b_n|^2 \right)^2$$

So dropping the condition $mn \le y$ gives us something quite close. We need a good way to detect this condition $mn \le y$.

Lemma 36.1.2. *For any $T > 0$, $\beta > 0$, $\alpha \in \mathbb{R}$, and $\beta \neq |\alpha|$, we have*

$$\int_{-T}^{T} e^{it\alpha} \frac{\sin(t\beta)}{\pi t} \, dt = \delta_\beta(\alpha) + O\left(\frac{1}{T|\beta - |\alpha||} \right),$$

where

$$\delta_\beta(\alpha) = \begin{cases} 1, & \text{if } |\alpha| < \beta, \\ 0, & \text{if } |\alpha| > \beta. \end{cases}$$

Proof sketch. First,

$$\int_{-\infty}^{\infty} e^{it\alpha} \frac{\sin(t\beta)}{\pi t} \, dt = \delta_\beta(\alpha).$$

This is essentially a consequence of studying

$$\int_{(c)} y^s \frac{ds}{s}$$

for $c > 0$, and then letting $c \to 0$.

Secondly, by integration by parts

$$\int_{T}^{\infty} e^{it\alpha} \frac{\sin(t\beta)}{\pi t} \, dt \ll \frac{1}{T|\beta - |\alpha||},$$

and similarly for the lower tail. □

Now to use this lemma to detect $mn \le y$, we take $\beta = \log y$ and $\alpha = \log mn$, except the lemma only applies if $\beta \ne |\alpha|$. We can get around this: since $mn \in \mathbb{Z}$, without loss of generality we can take $y = k + \frac{1}{2}$, $k \in \mathbb{Z}$, so $0 \le k \le MN$. Thus

$$\begin{aligned}\delta_\beta(\log mn) &= \int_{-T}^{T} e^{it\log(mn)} \frac{\sin(t\log y)}{\pi t}\,dt + O\left(\frac{1}{T|\beta - |\alpha||}\right)\\ &= \int_{-T}^{T} (mn)^{it} \frac{\sin(t\log y)}{\pi t}\,dt + O\left(\frac{1}{T|\beta - |\alpha||}\right).\end{aligned}$$

Note that the term $(mn)^{it}$ is of modulus 1, which will come in handy soon.

Note also that

$$|\beta - |\alpha|| = |\log y - \log mn| = \left|\log \frac{mn}{y}\right|.$$

Hence

$$\sum_{\substack{m=1\\ mn\le y}}^{M}\sum_{n=1}^{N} a_m b_n \chi(mn) = \sum_{m=1}^{M}\sum_{n=1}^{N} a_m b_n \chi(mn)\delta_\beta(\log mn)$$

$$= \int_{-T}^{T} \left(\sum_{m=1}^{M} a_m m^{it}\right)\left(\sum_{n=1}^{N} b_n n^{it}\right)\frac{\sin(t\log y)}{\pi t}\,dt + O\left(T^{-1}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|\left|\log\frac{mn}{y}\right|^{-1}\right).$$

We need a few estimates. First, $|\log x| \gg \min\{\,1, |x-1|\,\}$ for all $x > 0$, and therefore

$$\left|\log\frac{mn}{y}\right| \gg \min\left\{\,1, \left|\frac{mn}{y} - 1\right|\,\right\} \gg \min\left\{\,1, \left|\frac{y+\frac{1}{2}}{y} - 1\right|\,\right\} \gg \frac{1}{y} \gg \frac{1}{MN}.$$

Also,

$$|\sin(t\log y)| \le \min\{\,1, |t\log y|\,\} \le \min\{\,1, |t|\log 2MN\,\},$$

where we've taken $2MN$ to avoid the possible issue when $M = N = 1$.

Therefore

$$\max_y \left|\sum_{\substack{m=1\\ mn\le y}}^{M}\sum_{n=1}^{N} a_m b_n \chi(mn)\right| \ll \int_{-T}^{T}\left|\sum_{m=1}^{M} a_m m^{-it}\chi(m)\right|\left|\sum_{n=1}^{N} b_n n^{-it}\chi(n)\right| \min\left\{\,\frac{1}{|t|}, \log 2MN\,\right\} dt$$

$$+O\left(T^{-1}MN\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|\right),$$

and by Cauchy the sums in the error term is

$$\ll \left(\sum_{m=1}^{M}|a_m|^2\right)^{1/2} M^{1/2}\left(\sum_{n=1}^{N}|b_n|^2\right)^{1/2} N^{1/2}.$$

Therefore the final error term is

$$O\left(T^{-1}M^{3/2}N^{3/2}\left(\sum_{m=1}^{M}|a_m|^2\right)^{1/2}\left(\sum_{n=1}^{N}|b_n|^2\right)^{1/2}\right)$$

and we'll pick an appropriate T toward the end.

Now average over

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \pmod q},$$

bring it into the integral, since only the sums with χ in them depend on q, and so by the large sieve

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \pmod q}\max_y\Big|\sum_{\substack{m=1\\ mn\le y}}^{M}\sum_{n=1}^{N}a_m b_n\chi(mn)\Big|$$

$$\ll (M+Q^2)^{1/2}(N+Q^2)^{1/2}\left(\sum_{m=1}^{M}|a_m|^2\right)^{1/2}\left(\sum_{n=1}^{N}|b_n|^2\right)^{1/2}\int_{-T}^{T}\min\left\{\frac{1}{|t|},\log 2MN\right\}dt+$$

$$+\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \pmod q}T^{-1}(MN)^{3/2}\left(\sum_{m=1}^{M}|a_m|^2\right)^{1/2}\left(\sum_{n=1}^{N}|b_n|^2\right)^{1/2}.$$

This last term is

$$\ll T^{-1}(MN)^{3/2}\left(\sum_{m=1}^{M}|a_m|^2\right)^{1/2}\left(\sum_{n=1}^{N}|b_n|^2\right)^{1/2}\sum_{q\le Q}q,$$

with the final sum being $\ll Q^2$, so taking $T=(MN)^{3/2}$ we get the error we want.

Finally the remaining integral is

$$\int_{-T}^{T}\min\left\{\frac{1}{|t|},\log 2MN\right\}dt\ll\log(2MN)$$

since $T=(MN)^{3/2}$. Note that therefore it is important we didn't take $T\to\infty$ at first to det just $\delta_\beta(\alpha)$, with no error, since then our upper bound is just infinity.

Lecture 37 Vaughan's Identity

37.1 Basic Mean Value Theorem, again

Lemma 37.1.1 (Vaughan's Identity)**.** *Suppose $u>0$, $v>0$, $y\ge 2$, and $f\colon\mathbb{N}\to\mathbb{C}$. Then*

$$\sum_{n\le y}\Lambda(n)f(n)=S_1-S_2-s_3+s_4$$

Date: April 22nd, 2019.

where

$$S_1(f) = \sum_{m \le u} \mu(m) \sum_{n \le \frac{y}{m}} f(mn) \log(n),$$

$$S_2(f) = \sum_{m \le uv} C_m \sum_{n \le \frac{y}{m}} f(mn), \qquad \text{where} \quad C_m = \sum_{\substack{k \le u \\ \ell \le v \\ k\ell = m}} \Lambda(k)\mu(\ell),$$

$$S_3(f) = \sum_{m > u} \sum_{\substack{n > v \\ mn \le y}} \left(\sum_{\substack{k \mid m \\ k > u}} \Lambda(k) \right) \mu(n) f(mn),$$

$$S_4(f) = \sum_{n \le v} \Lambda(n) f(n).$$

Remark 37.1.2. Note how $S_1(f)$ and $S_2(f)$ are bilinear forms of the type $\sum_{m,n} a_m c_{mn}$. If the length of the sum over m isn't too big, then we can handle it. So we want u and v small compared to y.

Next, $S_3(f)$ is a bilinear form of the type $\sum_{m,n} a_m b_n c_{mn}$. Here we can use the Large Sieve.

Finally, $S_4(f)$ is of the same form as the original sum, but it's shorter.

Proof. Consider the purely algebraic identity

$$-\frac{\zeta'}{\zeta}(s) = G(s)(-\zeta'(s)) - F(s)G(s)\zeta(s) - (-\zeta'(s) - F(s)\zeta(s))(G(s) - \frac{1}{\zeta(s)}) + F(s),$$

where

$$F(s) = \sum_{n \le u} \frac{\Lambda(n)}{n^s}$$

and

$$G(s) = \sum_{n \le v} \frac{\mu(n)}{n^s}.$$

Call the first terms $D_1(s)$, $D_2(s)$, $D_3(s)$, and $D_4(s)$, respectively, and write them as Dirichlet series

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

for $j = 1, 2, 3, 4$. Since the left-hand side above has coefficients $\Lambda(n)$, we get the identity

$$\Lambda(n) = a_1(n) - a_2(n) - a_3(n) + a_4(n),$$

where consequently

$$a_1(n) = \sum_{\substack{md=n \\ d\le v}} \mu(d)\log n,$$

$$a_2(n) = \sum_{\substack{mdr=n \\ m\le u \\ d\le v}} \Lambda(m)\mu(d),$$

$$a_3(n) = \sum_{\substack{mk=u \\ m>u \\ k>1}} \Lambda(m)\sum_{\substack{d\mid k \\ d\le v}} \mu(d),$$

$$a_4(n) = \begin{cases} \Lambda(n), & n \le u \\ 0, & n > u. \end{cases}$$

Adding these up and weighing by $f(n)$, we get

$$\sum \Lambda(n)f(n) = \sum a_1(n)f(n) - \sum a_2(n)f(n) - \sum a_3(n)f(n) + \sum a_4(n)f(n),$$

which is the identity sought. □

We have an outstanding result ot prove.

We want to show that

$$T(X,Q) \coloneqq \sum_{q\le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \pmod q} \max_{y\le X} |\psi(y,\chi)| \ll (X + X^{5/6}Q + X^{1/2}Q^2)(\log XQ)^3,$$

where

$$\psi(y,\chi) = \sum_{n\le y} \Lambda(n)\chi(n).$$

Proof of Basic mean value theorem. We have two cases. First, if $Q^2 > X$, then apply the Large Sieve with $M = 1$, $a_1 = 1$, $N = \lfloor X \rfloor$, and $b_n = \Lambda(n)$, getting

$$T(X,Q) \ll (\log X)Q(X+Q^2)^{1/2}\left(\sum_{n=1}^{\lfloor X\rfloor} \Lambda(n)^s\right)^{1/2}$$

The penultimate term is $\ll (Q^2)^{1/2} = Q$, and the final term we can bound by

$$\ll \left(\sum_{p^\alpha \le X} (\log q)^2\right)^{1/2} \ll \left((\log X)^2 X\right)^{1/2}.$$

So in all, this expression is bounded by

$$\ll (\log X)^2 Q^2 X^{1/2}.$$

For the second case, $Q^2 \le X$, we split into $y \le u^2$ and $u^2 < y \le X$. If we cheat a bit and let $u = v = \min\{ Q^2, X^{1/3}, XQ^{-2} \}$ (which are properly acquired

by doing the calculations with u and v and then optimising), we get, for $y \le u^2$, via the Large Sieve,

$$\begin{aligned}
&\ll Q(u^2+Q^2)^{1/2}(\log u^2)\left(\sum_{n\le u^2}\Lambda(n)^2\right)^{1/2}\\
&\ll Q(u^2+Q^2)^{1/2}(\log u^2)(\log(u^2)u)^{1/2} \ll Q(uQ)(\log u)^2 u\\
&\ll (QX^{2/3}+Q^2X^{1/3})(\log X)^2.
\end{aligned}$$

Finally for $u^2 < y \le X$, apply Vaughan's theorem with

$$f(n) = \begin{cases} \chi(n), & n \le y \\ 0, & n > y. \end{cases}$$

Then it suffices to bound

$$T_j := \sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \pmod q}\max_{u^2<y\le X}|S_j(\chi)|.$$

□