DIRICHLET

AND

ANALYTIC NUMBER THEORY _ I

V. S. Varadarajan

W 2013

1

From: Renning Bruns <r.bruns@ucla.edu>
Subject: **Re: Distribution of primes up to 10^7 in Z/11Z**
Date: January 14, 2013 6:14:10 PM PST
To: "V. S. Varadarajan" <vsv@math.ucla.edu>

[0] was just used for counting purposes. It was all primes less than 10^7.

Here is a table for primes less than 10^10 (which took a couple
minutes on my computer):

|[1]| = 45504543
|[2]| = 45506100
|[3]| = 45503956
|[4]| = 45505446
|[5]| = 45505736
|[6]| = 45504686
|[7]| = 45505997
|[8]| = 45506529
|[9]| = 45503578
|[10]| = 45505939

-Renning

On Mon, Jan 14, 2013 at 5:28 PM, V. S. Varadarajan <vsv@math.ucla.edu> wrote:

> Dear Renning:
>
> Thanks. I do not understand [0] since we need non-zero classes. What was the limit on the primes? Like say primes less than a million, or something like that.
>
> Best
> V
>
> On Jan 14, 2013, at 4:24 PM, Renning Bruns wrote:
>
> > |[0]| = 1
> > |[1]| = 66386
> > |[2]| = 66541
> > |[3]| = 66480
> > |[4]| = 66452
> > |[5]| = 66376
> > |[6]| = 66448
> > |[7]| = 66490
> > |[8]| = 66507
> > |[9]| = 66425

12

|[10]| = 66473

They're all very close; I was not expecting that. I computed these using pari/gp.

-Renning

Dirichlet and Analytic Number Theory

W 2013 Math 191.

1. Primes:

$2, 3, 5, \ldots\ldots$

$\pm p$ is a prime if 1 and p are the only divisors of p.

(Euclid) $\exists$ infinitely many primes.

Consider ~~$p_1 p_2$~~ $2.3\ldots p+1$.

By variants of this argument we can prove:

— $\exists$ ∞ly many primes $\equiv 3\ (4)$, $\equiv 5\ (6)$.

Consider $2^2 3\ldots p - 1$. | Consider $2.3..p-1$. If $p>3$, $p \equiv 1$ or $5\ (6)$ and $p, p' \equiv 1\ (6) \Rightarrow pp' \equiv 1\ (6)$.

[Since products of numbers $\equiv 1\ (4)$ are again such, a number $\equiv 3\ (4)$ must either be prime or have a prime factor $\equiv 3\ (4)$.].

— $\exists$ ∞ly many primes $\equiv 1\ (4)$, $\equiv 5\ (8)$.

This is true but the argument is more difficult.

[$q = 3^2 5^2 \ldots p^2 + 2^2 = a^2 + b^2$, $(a,b) = 1$. LHS $= (\text{odd})^2 + 4 \equiv 5\ (8)$. Fermat $\Rightarrow$ any odd prime $| a^2+b^2$ is $\equiv 1\ (4)$.]

Two general questions frame themselves.

I. What is the asymptotic behaviour of primes?

Gauss found the result, by a combination of deep insight and enormous calculations, and formulated the conjecture:

(4

(PNT) Let $\pi(n)$ be the number of primes $\leq n$. Then

$$\pi(n) \sim \frac{n}{\log n} \quad \text{i.e.,} \quad \frac{\pi(n)}{n/\log n} \longrightarrow 1 \text{ as } n \to \infty$$

$\Updownarrow$

Let p_n be the n^{th} prime. Then

$$p_n \sim n \log n.$$

Define $\pi(x) := \#\{p \leq x\}$.
$\pi(x) \sim x/\log x$.
$y = x/\log x \Rightarrow \log y = \log x - \log\log x$
$\Rightarrow \log y \sim \log x$
$x = y \log x \sim y \log y$.

Hadamard and de la Vallee Poussin proved this in 1896 independently. ~~this result~~. Decades later Wiener deduced it as a consequence of his Tauberian theorem. In 1947-48 Selberg and Erdos discovered "elementary proofs" (= not involving complex analysis).

II: Around 1837 Dirichlet asked the following question:

Fix an integer $N > 1$ and an integer a prime to N.
Are there ∞^{ly} many primes $\equiv a \ (N)$?
He proved this by introducing new tools and concepts which allowed Analysis to be applied to N.T. This question was already in Legendre as his proof of quadratic reciprocity depended on this.

Legendre conjectured there are ∞^{ly} many primes in residue classes to prove quadratic reciprocity.

In view of PNT, it is natural to conjecture the following:

Let $\varphi(N)$ be the Euler f^n. Show that the primes are equi-distributed among the $\varphi(N)$ residue classes mod N that are prime to N: if $\pi_a(n) = \#$ primes $p \leq n$ and $\equiv a \ (N)$,

$$\pi_a(n) \sim \frac{1}{\varphi(N)} \frac{n}{\log n} \qquad n \to \infty.$$

2. Euler's introduction of the zeta f^n and his proof that $\exists \infty^{ly}$ many primes.

Euler discovered, around 17.., the following remarkable identity:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} \qquad (s > 1)$$

where we can treat the sum and product either formally or analytically, as the convergence of each side for $s>1$ is easy to show. ~~If the number of primes were finite~~ The identity is an immediate consequence of the FTA. If the number of primes were finite, the RHS $\longrightarrow$ a finite limit as $s \to 1+0$ while the LHS $\longrightarrow \infty$. So Euler concluded that $\exists \infty^{ly}$ many primes. This may be the first application of analysis to N.T.

To see $\zeta(s) \to \infty$ as $s \to 1+0$,

$$\zeta(s) \geq 1 + 2^{-s} + \dots + N^{-s} \quad \text{for any integer } N \geq 1$$

$$\Rightarrow \quad \varliminf_{s \to 1+0} \zeta(s) \geq 1 + \frac{1}{2} + \dots + \frac{1}{N}. \quad \text{Now let } N \to +\infty.$$

With a little more effort we can prove a little more.

Prove rigorously: cgce $s>1$ i.e. $s \geq 1+\delta > 1$.

Thm $\sum_p 1/p = \infty$. ~~(compatible with PNT)~~.

Since we are dealing with quantities > 0,

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

For $p \geq 2$, $s > 1$, $p^{-s} \leq 1/2$ and ~~$-\log(1-$~~

$$-\log(1-x) = x + \theta(x), \qquad |\theta(x)| \leq 2x^2, \quad 0 \leq x \leq 1/2$$

$\left[|\theta(x)| \leq x^2(1+x+x^2+\dots) \leq \frac{x^2}{1-x} \leq 2x^2 \text{ for } 0 \leq x \leq \frac{1}{2} \right]$.

So
$$-\log(1-p^{-s}) = p^{-s} + \theta_p(s) \qquad |\theta_p(s)| \leq 2p^{-2s} \quad (s>1)$$

$$\Rightarrow \sum -\log(1-p^{-s}) = \sum_p p^{-s} + \theta(s), \quad |\theta(s)| \leq 2\sum_p p^{-2s} \quad (s>1).$$

Since $\sum_p p^{-2s} \leq \sum_n n^{-2s} \leq \sum n^{-2}$ for $s \geq 1$, $|\theta(s)| = O(1)$

as $s \to 1+0$. So

$$\left| \log \zeta(s) - \sum_p p^{-s} \right| = O(1) \quad s \to 1+0.$$

$$\Rightarrow \sum_p p^{-s} \longrightarrow +\infty \quad \text{as } s \longrightarrow 1+0.$$

If $\sum 1/p < \infty$, $\sum_p p^{-s} \leq \sum 1/p$ for $s > 1$ uniformly,

so $\sum_p p^{-s}$ (which increases as $s \searrow 1$) will be $O(1)$ for $s \to 1+0$,

a contradiction.

Rmk The result is consistent with PNT: $p_n \sim n \log n$.

3. An example. Dirichlet extended the scope of Euler's ideas enormously ~~by~~ by introducing completely new ~~ideas~~ concepts. We begin with the case $p \equiv 1\,(4)$. This case was treated by Euler.

Let χ be the function $\mathbb{Z} \to \{\pm 1\}$ defined by

$$\chi(m) = \begin{cases} 0 & m \text{ even} \\ 1 & m \equiv 1\,(4) \\ -1 & m \equiv 3\,(4) \end{cases}$$

It is then easy to verify that

$$\chi(mn) = \chi(m)\chi(n)$$

Anticipating later terminolog we say χ is a ~~Dirichlet~~ character mod 4. ~~Σ~~ We introduce the ~~Dirichlet~~ series $\sum_{n \geq 1} \chi(n) n^{-s}$ which has the following properties:

(i) $L(s:\chi) = \sum_{n \geq 1} \chi(n) n^{-s}$ is absolutely cgt for $s>1$, uniformly for $s \geq 1+\delta > 1$ for any $\delta > 0$. It is also cgt for $s>0$, uniformly for $s \geq \delta > 0$. L is thus continuous for $s>0$.

current terminology

(ii) $L(s:\chi)$ has an Euler product representation

$$L(s:\chi) = \prod_p (1-\chi(p)p^{-s})^{-1} \qquad (s>1)$$

the product being absolutely convergent.

(iii) $L(1:\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \cdots = \frac{\pi}{4} > 0.$

The absolute cgce of the series for $s > 1$ which is uniform for $s \geq 1+\delta$ is obvious since $|\chi(n) n^{-s}| \leq n^{-(1+\delta)}$. For the range $0 < s \leq 1$ it is more delicate. We use Dirichlet's test for convergence and uniform cgce, devised by him to handle Fourier Series which are usually not absolutely cgt:

Exercise

<u>Dirichlet test</u> Consider a series $\sum_{n \geq 1} a_n b_n$. Sufficient conditions for cgce are:

(1) $A_n := a_1 + \cdots + a_n = O(1)$ as $n \to \infty$

(2) $\sum_n |b_n - b_{n+1}| < \infty$, $b_n \to 0$ / or (2′) b_n real, $\downarrow 0$.

If a_n, b_n depend on a parameter and (1) & (2) (or (2′)) hold uniformly, then the cgce is uniform.

We use Abel's partial summation, the discrete version of integration by parts:

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

Clearly under (1) and (2), the LHS $\to \sum_{n=1}^{\infty} A_n (b_n - b_{n+1})$

proving convergence. With (2') in place of (2), note that $|b_n - b_{n+1}| = b_n - b_{n+1}$ and so $\sum |b_n - b_{n+1}| < \infty$, thus reducing to the earlier situation. For uniform cge note, with $|A_N| \le C$,

$$\Big|\sum_1^N a_n b_n - \sum_1^\infty A_n (b_n - b_{n+1})\Big| \le C \sum_N^\infty |b_n - b_{n+1}| + C|b_N| \longrightarrow 0$$

uniformly.

We apply this to $\sum \chi(n) n^{-s}$. Clearly $\chi(1) + \dots + \chi(N) = \pm 1$ for all N while $|n^{-s} - (n+1)^{-s}| = s \cdot (n+\theta)^{-(s+1)}$ for some $\theta \in (0,1)$ (Mean value theorem) and for $s \geqslant \delta > 0$,

$$|n^{-s} - (n+1)^{-s}| \le (n-1)^{-(1+\delta)}.$$

For the product representation, note first that the product converges absolutely for $s > 1$. In fact

$$(1 - \chi(p) p^{-s})^{-1} = 1 + \chi(p) p^{-s} + \chi(p)^2 p^{-2s} + \dots$$
$$= 1 + \theta_p(s) p^{-s}$$

where $|\theta_p(s)| \le 1 + p^{-s} + p^{-2s} + \dots = \dfrac{1}{1-p^{-s}} \le \dfrac{1}{1-2^{-s}}$, while for $s \geqslant 1 + \delta > 0$, $|\theta_p(s)| p^{-s} \le (1-2^{-\delta})^{-1} p^{-(1+\delta)}$, giving uniform

If $p_1, \dots, p_N$ are the first N primes,

$$\cancel{\Big|\sum_{n \geqslant 1} \chi(n) n^{-s} - \prod_{1 \le j \le N} (1 - \chi(p_j) p_j^{-s})}$$

$$\prod_1^N (1-\chi(p_j)p_j^{-s})^{-1} = \prod_1^N (1+\chi(p_j)p_j^{-s}+\chi(p_j^2)p_j^{-2s}+\cdots)$$

$$= \sum_n{}' \chi(n) n^{-s}$$

where Σ' refers to summation over all n whose prime factors are among $p_1, \ldots, p_N$. In particular every integer from 1 to N has this property so that

$$\Big| \sum_{n\geq 1} \chi(n) n^{-s} - \prod_{p\leq p_N} (1-\chi(p)p^{-s})^{-1} \Big| \leq \sum_{n\geq N+1} n^{-s} \longrightarrow 0$$

as $N \to \infty$, uniformly for $s \geq 1+\delta > 0$. Thus

$$L(s:\chi) = \sum_{n\geq 1} \chi(n) n^{-s} = \prod_p (1-\chi(p)p^{-s})^{-1} \quad (s>1).$$

Since $L(s:\chi)$ and $(1-\chi(p)p^{-s})^{-1}$ are >0 we can take logs:

$$\log L(s:\chi) = \sum_p -\log(1-\chi(p)p^{-s})^{-1}$$

$$= \sum_p \chi(p)p^{-s} + \sum_p \theta_p(s) p^{-2s} \qquad |\theta_p(s)| \leq 2$$

For $s\geq 1$ we have $\sum_p |\theta_p(s)| p^{-2s} \leq 2\sum_p p^{-2}$ and so

$$\log L(s:\chi) = \sum_p \chi(p)p^{-s} + F(s), \qquad F(s) = O(1) \text{ for } s\to 1$$

If A and B are two functions defined for $s>1$, we write $A \approx B$ if $A-B$ is $O(1)$ when $s \to 1+0$. Hence

$$\log L(s:\chi) \approx \sum_p \chi(p)p^{-s} = \sum_{p\equiv 1(4)} p^{-s} - \sum_{p\equiv 3(4)} p^{-s}$$

On the other hand, we have seen

$$\log \zeta(s) \approx \sum_p p^{-s} = \sum_{p\equiv 1(4)} p^{-s} + \sum_{p\equiv 3(4)} p^{-s}$$

Hence, for $s \to 1+0$

$$\sum_{p\equiv 1(4)} p^{-s} \approx \frac{1}{2}\left[\log L(s:\chi) + \log \zeta(s)\right]$$

$$\sum_{p\equiv 3(4)} p^{-s} \approx \frac{1}{2}\left[-\log L(s:\chi) + \log \zeta(s)\right].$$

But $\log \zeta(s) \longrightarrow +\infty$ as $s \to 1+0$ while $L(s:\chi)$ is continuous for $s \geq 1$ and $L(1:\chi) > 0$. Hence $\log L(s:\chi)$ tends to a <u>finite</u> limit as $s \to 1+0$. We thus obtain

$$\sum_{p\equiv 1(4)} p^{-s} \longrightarrow +\infty, \quad \sum_{p\equiv 3(4)} p^{-s} \longrightarrow +\infty$$

as $s \to 1+0$. As before we get

$$\sum_{p\equiv 1(4)} p^{-1} = \infty, \quad \sum_{p\equiv 3(4)} p^{-1} = \infty .$$

In particular, there are infinitely many primes $\equiv 1\ (4)$ and infinitely many $\equiv 3\ (4)$.

<u>4. Dirichlet's method.</u> ~~Dirichlet~~ The above example is the key to understanding Dirichlet's idea: Fix a modulus $N > 1$. Then the residue classes mod N form a ring $\mathbb{Z}_N$ ($= \mathbb{Z}/N\mathbb{Z}$) and the units ($=$ invertible elements) of $\mathbb{Z}_N$ form a group G_N under multiplication. We know that

$$|G_N| = \varphi(N) = \# \text{ of integers} \geq 1, < N \text{ and prime to } N.$$

The group $\widehat{G_N}$ dual to G_N is the group of <u>characters</u> of G_N: homomorphisms $\chi : G_N \to \mathbb{C}^\times$. Clearly each $\chi \in \widehat{G_N}$ takes values in the group Φ_N of $\varphi(N)^{th}$ roots of unity. The χ are called <u>Dirichlet characters mod N</u>. ~~Each χ may be regarded as a function $\mathbb{Z} \to \Phi_N \subset \mathbb{C}^\times$, also denoted by χ,~~

To each χ we associate the function $\chi' : \mathbb{Z} \to \mathbb{C}$ such that

$$\chi'(m) = \begin{cases} 0 & (m, N) > 1 \\ \chi([m]) & \text{if } (m, N) = 1 \end{cases}$$

where $[m]$ is the residue class of m mod N. Alternatively χ' is the lift to $\mathbb{Z}$ via $\mathbb{Z} \to \mathbb{Z}_N$ of the function which is χ on G_N and 0 on $\mathbb{Z}_N \setminus G_N$. ~~Instead~~ We shall identify χ' with χ; this will create no confusion.

One must remember that the theory of finite groups and the characters did not exist at that time and so Dirichlet had to determine the characters by hand, explicitly. We shall c[...] to this point later.

<u>Character theory of finite abelian groups.</u> All grps considered are abelian. For any finite group G we define a <u>character</u> of G as a homomorphism $\chi : G \to$ [...] If $|G|$ is the order of G, the values of χ are in the gr[oup] $\Phi_{|G|}$ of $|G|^{th}$ roots of unity, hence $|\chi(x)| = 1 \ \forall x$. The character (trivial) $x \mapsto 1$ is denoted by χ_0. U[...]

pointwise multiplication the characters of G form a group $\hat{G}$, the group <u>dual</u> to G. The <u>duality theorem</u> asserts that $G \approx \hat{\hat{G}}$ naturally; each $x \in G$ may be viewed as a character of $\hat{G}$ by $\chi \longmapsto \chi(x)$, and the map $G \longrightarrow \hat{\hat{G}}$ thus obtained is a group isomorphism. If $G_1, \dots, G_r$ are finite groups and $G = G_1 \times \dots \times G_r$, there is a natural isomorphism $\hat{G} \approx \hat{G}_1 \times \dots \times \hat{G}_r$.
If G is a cyclic group of order m with generator g, the map $g^r \longrightarrow [r]_m$ gives an isomorphism $G \simeq \mathbb{Z}_m$. If ω is a primitive m^{th} root of unity, then $\chi_\omega : g^r \longmapsto \omega^r$ defines a character of G; ~~the general~~ $\{1, \chi_\omega, \dots \chi_\omega^{m-1}\}$ are all the characters of G and $\hat{G} \approx \mathbb{Z}_m$ also. Thus $G \simeq \hat{G}$, but the isomorphism is non canonical. In particular $|G| = |\hat{G}|$ for cyclic G, hence all G, as any G is a direct sum of cyclic groups. If H is a subgroup of G, the restriction from G to H defines a map $\hat{G} \longrightarrow \hat{H}$. The kernel of this map is $\widehat{G/H}$ and it follows from $|\widehat{G/H}| = |G/H| = |G|/|H| = |\hat{G}|/|\hat{H}|$ that $\hat{G} \to \hat{H}$ is surjective: any character of H has at least one extension to G.

<u>Fourier series on G</u> Let $\mathcal{F} = \mathcal{F}(G)$ be the space of complex functions on G. For $f, g \in \mathcal{F}$ we define

$$(f, g) = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}$$

With $(\cdot,\cdot)$, $\mathcal{F}$ becomes a Hilbert space of dimension $|G|$.

<u>orthogonality relations</u> assert that the characters form an ON basis of $\mathcal{F}$: if $\chi, \chi' \in \hat{G}$,

$$\frac{1}{|G|} \sum_{x \in G} \chi(x) \overline{\chi'(x)} = \begin{cases} 0 & \chi \neq \chi' \\ 1 & \chi = \chi' \end{cases}$$

Indeed, let $\sum_x \omega(x) = a$ where $\omega \in \hat{G} \setminus (1)$. For any $y \in G$,

$\sum_x \omega(xy) = a = \omega(y) \sum \omega(x)$. So $a(1-\omega(y)) = 0$. As $\omega \neq 1$, we choose y s.t. $\omega(y) \neq 1$, concluding $a = 0$:

$$\sum_{x \in G} \omega(x) = 0 \quad (\omega \in \hat{G} \setminus (1))$$

If $\omega = \chi\overline{\chi'}$, then $\omega = 1 \iff \chi = \chi'$ and so we get the ortho-gonality relations. In particular

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

which is the <u>Fourier series</u> of f in analogy with the circle grp. let

$$\delta_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}$$

Then $(\delta_a, \chi) = |G|^{-1} \overline{\chi(a)}$ and hence

$$|G|.\, \delta_a(x) = \sum_{\chi \in \hat{G}} \overline{\chi(a)}\, \chi(x). \quad f(x) = \sum \hat{f}(\chi)\chi(x)$$

By analogy with <u>circle grp</u>, this is the <u>Fourier inversion formula</u>.

<u>Dirichlet series.</u> Any infinite series of the form

$$\sum_{n\geq 1} a_n n^{-s} \qquad (a_n \in \mathbb{C}) \qquad (1)$$

is called a <u>Dirichlet series</u>. The coefficients a_n can lie in any Banach or topological vector space, but we always remain in the case when all the a_n are complex numbers. We may view the series formally (like formal power series) or analytically. For Dirichlet s was always real, but for Riemann it was essential to view s as a cplex variable. If s is complex and the series cges for some s_0, $s_0 = \sigma_0 + i\tau_0$, then $|a_n| n^{-\sigma_0} \to 0$ as $n \to \infty$, in particular $O(1)$, and for $s = \sigma + i\tau$ with $\sigma > \sigma_0$, $|a_n n^{-s}| = |a_n n^{-\sigma_0}| \cdot n^{-(\sigma-\sigma_0)} < \text{const.}\, n^{-(\sigma-\sigma_0)}$ and so the series converges absolutely for $\mathrm{Re}(s) > \mathrm{Re}(s_0)+1$, uniformly for $\mathrm{Re}(s) \geq \mathrm{Re}(s_0)+1+\delta$ for every $\delta > 0$. Hence (1) represents a function holomorphic on some half-plane $\mathrm{Re}(s) > A$.

The series (1) is an <u>Euler product</u> if $\exists$ constants c_p (p prime) such that

$$\sum_n a_n n^{-s} = \prod_p (1 - c_p p^{-s})^{-1}$$

at least formally. It is easy to see that this is the case iff

$$a_{mn} = a_m a_n, \qquad a_p = c_p. \qquad (2)$$

Sequences (a_n) s.t. $a_{mn} = a_m a_n$ are called <u>unrestrictedly</u> (= fully) multiplicative, and Dirichlet series with Euler products are generating functions of such sequences.

~~Initiating~~ Given an integer $N > 1$ (modulus), Dirichlet introduced a Dirichlet series with Euler product for each $\chi \in \hat{C}_N$, a Dirichlet character mod N. As mentioned earlier, we identify χ with the function $\chi' : \mathbb{Z} \to \mathbb{C}$: ~~whose values~~

$$\chi'(m) = \begin{cases} 0 & (m,N) > 1 \\ \chi([m]) & (m,N) = 1 \end{cases}$$

Then Dirichlet's L-function is

$$L(s:\chi) = \sum_{n \geq 1} \chi'(n) n^{-s} .$$

Since $\chi'(mn) = \chi'(m)\chi'(n)$ we have

$$L(s:\chi) = \prod_p \left(1 - \chi(p) p^{-s}\right)^{-1}$$

The series for L converges in $Re(s) > 1$, uniformly for $Re(s) \geq 1+\delta >$ and defines L as a holomorphic function on $Re(s) > 1$. If we are (as was Dirichlet) only concerned with ~~Rat~~ real s, then L is certainly continuous on $s > 1$. The series obtained by differentiating ~~=~~ (w.r.t. s) is

$$(-1)^k \sum \chi'(n) (\log n)^k n^{-s}$$

which is absolutely cgt in $s>1$, uniformly in $s \geq 1+\delta > 1$. Thus L is a smooth function on $s>1$. If χ is non-trivial, we can say more. The function χ' is periodic of period N and as $\sum_{x\in G_N}\chi(x)=0$, we have $\sum_{1\le n<N}\chi'(n)=0$ and so $\sum_{1\le n\le m}\chi'(n)=O(1)$ for $m\to\infty$. Moreover, by the Mean Value Theorem,

$$|n^{-s}-(n+1)^{-s}| = |-s\cdot(n+\theta)^{-(s+1)}| \qquad 0<\theta<1$$
$$\leq 2(n-1)^{-(s+1)} \qquad \text{for } 0<s\leq 2$$

and so the series converges by the Dirichlet test, uniformly for $0<\delta\leq s\leq 2$. The differentiated series is $\sum \chi'(n)(\log n)^r n^{-s}$ and $|(\log n)^r n^{-s} - (\log(n+1))^r (n+1)^{-s}| \leq \text{Const.}(\log n)^r (n-1)^{-(s+1)}$, showing that $L(s:\chi)$ is defined and smooth for $s>0$. The first estimate proves that L is holomorphic for $Re(s)>0$. The Euler product for L is proved exactly as in the earlier cases.

Now, for $s>1$, using the branch of $\log(1-u)$ for $|u|<1$ defined by the power series

$$(1-\chi(p)p^{-s})^{-1} = \exp\left\{-\log(1-\chi(p)p^{-s})\right\}$$
$$= \exp\left\{\chi(p)p^{-s} + \theta(p,s)p^{-2s}\right\} \qquad |\theta(p,s)|\leq 2$$

Hence

$$\prod_p (1-\chi(p)p^{-s})^{-1} = \exp\left\{\sum_p \chi(p)p^{-s} + \sum_p \theta(p,s)p^{-2s}\right\}$$

Thus

$$L(s:\chi) = \exp\left\{ \sum_p \chi(p) p^{-s} + \sum_p \theta_p(s) p^{-2s} \right\}.$$

This shows that we can define $\log L(s:\chi)$ as a continuous function for $s>1$ (holomorphic for $\mathrm{Re}(s)>1$):

$$\log L(s:\chi) \approx \sum_p \chi(p) p^{-s} \qquad (s>1).$$

When $\chi = \chi_0$, the trivial character, this shows

$$\log L(s:\chi_0) \approx \sum_p p^{-s} \approx \log \zeta(s)$$

so that

$$\log L(s:\chi_0) \longrightarrow \infty \quad \text{as } s \to 1+0.$$

By the Fourier inversion on G_N, for fixed $a \in G_N$,

$$\frac{1}{|G_N|} \sum_{\chi \in \widehat{G_N}} \overline{\chi(a)} \log L(s:\chi) \approx \sum_p \frac{1}{|G_N|} \sum_{\chi \in \widehat{G_N}} \overline{\chi(a)} \chi(p) p^{-s}$$

$$\approx \sum_{p \equiv a (N)} p^{-s}.$$

<u>If we can show that</u> for $\chi \neq \chi_0$,

$$\log L(s:\chi) \approx 0 \qquad (s \to 1+0) \qquad (*)$$

then we get

$$\sum_{p \equiv a(N)} p^{-s} \longrightarrow \infty \qquad s \to 1+0$$

This leads as usual to

$$\sum p^{-1} = \infty.$$

~~Dirichlet~~ ~~Su~~: For $\chi \neq \chi_0$ we know that $L(s:\chi)$ is defined and continuous for $0 < s$ (holomorphic on $\mathrm{Re}(s) > 0$). If

$$L(1:\chi) \neq 0 \qquad (\chi \neq \chi_0) \qquad (**)$$

then there is a continuous branch of $\log L(s:\chi)$ for $|s-1| < \varepsilon$, which will differ from $\log L(s:\chi)$ defined earlier for $1 < s < 1+\varepsilon$. So we would have ~~too~~

$$\log L(s:\chi) \approx 0 \qquad s \longrightarrow 1+0.$$

So Dirichlet reduced the proof of his theorem to $(**)$.

<u>5. Proof that $L(1:\chi) \neq 0$ for $\chi \neq \chi_0$.</u> In his 1837 paper Dirichet proved $L(1:\chi) \neq 0$ for $\chi \neq \chi_0$, only when the modulus $N = q$, an odd prime. In this case $G_q = \mathbb{F}_p^{\times}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, so G_q is cyclic (Euler) and has a generator, say θ. The choice of θ leads to $G_q \approx \mathbb{Z}_{p-1} \approx \widehat{\mathbb{Z}}_{p-1} \approx \widehat{G}_q$ and so everything is explicit. Later he worked out the case for an arbitrary modulus N. We give first, for arbitrary N, an analytical proof.

The analytic proof uses the holomorphic aspects. We need two facts.

<u>Fact A</u> $L(s:\chi_0)$ extends meromorphically to ~~≥~~ $Re(s)>0$ with exactly one singularity at $s=1$ which is a simple pole of residue $A>0$.

<u>Fact B</u> Let $D(s) = \prod_{\chi} L(s:\chi)$. Then $|D(s)| \geq 1$ for s real and >1.

<u>Proof of A</u>. First we consider $\zeta(s)$. For $n>1$, (by partial summation)

$$\sum_{k=1}^{n} n^{-s} = \sum_{1}^{n-1} k\left(k^{-s} - (k+1)^{-s}\right) + n^{1-s}$$

$$= \sum_{1}^{n-1} \int_{k}^{k+1} [x]\, s x^{-(1+s)}\, dx + n^{1-s}$$

Since $x = [x] + (x)$ where $0 \leq (x) \leq 1$, this becomes

$$= \sum_{1}^{n-1} \int_{k}^{k+1} x \cdot s x^{-(1+s)}\, dx - \sum_{1}^{n-1} \int_{k}^{k+1} (x)\, s x^{-(1+s)}\, dx + n^{1-s}$$

$$= s\int_{1}^{n} x^{-s}\, dx - s\int_{1}^{n} (x) x^{-(1+s)}\, dx + n^{1-s}.$$

With $Re(s)>1$, let $n \to \infty$. Then

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

The integral on the right converges for $Re(s)>0$, uniformly for $Re(s)\geqslant\delta>0$. So it defines a holomorphic function for $Re(s)>0$. So

$$\zeta(s)=\frac{1}{s-1}+Z(s) \qquad Z \text{ holomorphic in } Re(s)>0.$$

Now

$$L(s:\chi_0)=\zeta(s)\prod_{p\mid N}(1-p^{-s})$$

showing $L(s:\chi_0)$ extends meromorphically to $Re(s)>0$, with exactly one singularity at $s=1$ which is a simple pole of residue $\prod_p(1-p^{-1})=A>0$.

<u>Proof of B</u> $D(s)=\prod_p\prod_\chi(1-\chi(p)p^{-s})^{-1}$. Let ν_p be the order of $[p]$ in G_N and $d_p=\varphi(N)/\nu_p$. If C_p is the cyclic group generated in G_N by $[p]$, then $\nu_p=|C_p|$ and $d_p=|G_N/C_p|$. So every character of C_p extends to a character of G_N, while characters of C_p are determined uniquely by $\omega=\chi(p)$ which is a ν_p^{th}-root of unity. For each ω, the number of characters χ of G_N with $\chi(p)=\omega$ is d_p. Hence

$$\prod_{\chi} (1-\chi(p)p^{-s})^{-1} = \Big(\prod_{\omega} (1-\omega p^{-s})^{-1} \Big)^{d_p}.$$

But as $\prod_{\omega} (T-\omega) = T^{\cancel{d_p}\,\nu_p} - 1$, $\prod_{\omega} (1-\omega T^{-1}) = 1 - T^{-\cancel{d_p}\,\nu_p}$

and so

$$\cancel{D(s)} = \prod_{\chi} (1-\chi(p)p^{-s})^{-1} = \left(1 - p^{\cancel{d_p}\,-s\nu_p}\right)^{-d_p}$$

Hence

$$D(s) = \prod_{p} \left(1 - p^{-s\nu_p}\right)^{-d_p}$$

For s real and >1, it is obvious that $D(s) \geq 1$.

<u>Completion of the proof that $L(1:\chi) \neq 0$ for $\chi \neq \chi_0$.</u>

Let $D^*(s) = \prod_{\chi \neq \chi_0} L(s:\chi)$ so that $D(s) = L(s:\chi_0)\,D^*(s)$

Suppose $L(1:\chi) = 0$ for some χ.

<u>Case 1</u> χ is complex, i.e., $\chi \neq \bar{\chi}$. Since $L(1:\bar{\chi}) = L(1:\chi) = 0$, $D^*(s)$ has a double zero at $s=1$ while $L(s:\chi_0)$ has only a simple pole at $s=1$. So $D(1) = 0$ contradicting Fact B.

<u>Case 2</u> $\chi = \bar{\chi}$. So χ is ± 1-valued. Consider

$$M(s) = \frac{L(s:\chi)\,L(s:\chi_0)}{L(2s:\chi_0)}$$

Then $M(s)$ is an Euler product and the factor corresponding to p is

$$(1-\chi(p)p^{-s})^{-1}(1-p^{-s})^{-1}\Big/(1-p^{-2s})^{-1}.$$

If $\chi(p)=-1$, this is 1. Thus

$$M(s) = \prod_{p:\chi(p)=1} \frac{1+p^{-s}}{1-p^{-s}} = \prod_{p:\chi(p)=1}(1+p^{-s})(1+p^{-s}+p^{-2s}+\cdots)$$

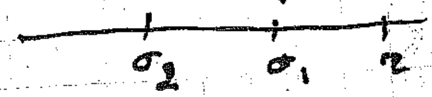
$$= \prod_{p:\chi(p)=1}(1+p^{-s})\prod_{p:\chi(p)=1}(1+p^{-s}+\cdots) = \sum a_n n^{-s} \sum b_n n^{-s}$$

where a_n, b_n are integers, $0 \le a_n, b_n \le 1$, $a_1 = b_1 = 1$.

Hence $M(s) = \sum_{n\ge 1} c_n n^{-s}$ where c_n are integers, $c_1 = 1$, and $0 \le c_n \le n$ for all n. So $M(s)$ is cgt for $Re(s) > 2$. But by definition $M(s)$ is holomorphic for $Re(s) > \frac{1}{2}$. We now need a lemma.

<u>Lemma</u> Let $f(s) = \sum_{n\ge 1} d_n n^{-s}$ where $d_1 = 1$ and $d_n \ge 0$ for all n. Suppose f converges absolutely for $Re(s) > \sigma_1$ and for some $\sigma_2 < \sigma_1$, f extends analytically to $Re(s) > \sigma_2$. Then $f(\sigma) \ge 1$ for all $\sigma > \sigma_2$.

<u>Proof of Lemma.</u> Take a real $\tau > \sigma_1$. Since f is analytic on $\mathrm{Re}(s) > \sigma_2$, we can expand f as a ~~Taylor~~ powerseries in $s-\tau$ with a radius of convergence at least $\tau - \sigma_2$:



$$f(s) = \sum \frac{f^{(m)}(\tau)}{m!}(s-\tau)^m \qquad |s-\tau| < \tau - \sigma_2.$$

Now

$$f(s) = \sum d_n n^{-s} \qquad \mathrm{Re}(s) > \sigma_1$$

and hence

$$f^{(m)}(\tau) = \sum d_n (-\log n)^m n^{-\tau} = (-1)^m k_m \qquad (m \geq 0)$$

where

$$k_m = \sum d_n (\log n)^m n^{-\tau} \geq 0, \quad k_0 = f(\tau)$$

Hence

$$f(s) = \sum_m \frac{k_m}{m!}(\tau - s)^m \qquad |\tau - s| < \tau - \sigma_2.$$

If now $s = \sigma > \sigma_2$,

$$f(\sigma) = \sum \frac{k_m}{m!}(\tau-\sigma)^m \geq k_0 = f(\tau) \geq 1.$$

We apply this lemma to $M(s)$ which is a Dirichlet series $\sum c_n n^{-s}$ with $c_n \geq 0$, $c_1 = 1$, cgt for $\mathrm{Re}(s) > 2$.

It extends analytically to $\mathrm{Re}(s) > \frac{1}{2}$. So by the Lemma, $M(\sigma)$ remains ≥ 1 for all $\sigma > 1/2$. But $M(\sigma) \to 0$ as $\sigma \to \frac{1}{2} + 0$. This contradiction proves that $L(1:\chi) \neq 0$.

This completes the proof of Dirichlet's theorem. This proof is due to Landau.

Dirichlet however went in a different direction to prove that $L(1:\chi) \neq 0$ for real $\chi \neq \chi_0$. He first treated in his 1837 paper the case when the modulus $N = q$, q an odd prime and explicitly evaluated $L(1:\chi)$ for a real χ and found it to be > 0. In subsequent work he treated the case of an arbitrary modulus N. Eventually he interpreted $L(1:\chi)$ (χ real, $\chi \neq \chi_0$) as a <u>class number</u> upto a positive constant, and hence > 0 automatically. The class number is the number of classes of quadratic forms with integer coefficients.

In the modern point of view, G_N is viewed as the Galois group of the cyclotomic extension $\mathbb{Q}(\sqrt[N]{1}) = K_N$ so that χ, interpreted as a character of $\mathrm{Gal}(K_N/\mathbb{Q})$, defines a <u>quadratic extension</u> L of $\mathbb{Q}$: $\mathbb{Q} \subset L \subset K_N$. The class number is then the class number of L. Since this depends on the ideal theory of L, not discovered till Kummer came into the scene much later, Dirichlet had to use the theory of classification of integral quadratic forms, essentially as a substitute for the ideal theory of L. The consideration of $D(s)$ also becomes natural from the modern point of view: it is essentially the Dedekind zeta function of K_N.

~~Dirichlet's explicit proof that $L(1:\chi)>0$ for χ real, $\neq \chi_0$, $N=q$, an odd prime.~~

It is to be noted that the holomorphic aspects of $L(s:\chi)$ come into play only when we consider $L(1:\chi)$ for real χ. The reduction to real χ can be carried out ~~using~~ considering $L(s:\chi)$ only as a function of real s. Since it is smooth for $s>0$, $\chi \neq \chi_0$, and the same for $(s-1)\zeta(s)$, the argument using the multiplicity of zeros at $s=1$ remains valid. Thus only the case χ real is left to be treated.

~~Dirichlet's formula for $L(1, \chi)$, χ real, $\neq \chi_0$, $N = q$ an odd~~ prime.

Fourier Series

f a bounded RI on $[0,1]$, extended by periodicity (period 1).

$$c_n = \int_0^1 f(t) e^{-2\pi i n t}\, dt$$

$$S_N(f:x) = \sum_{-N}^{N} \int_0^1 f(t) e^{2\pi i n (x-t)}\, dt$$

$$D_N(u) = \sum_{-N}^{N} e^{2\pi i n u} = D_N(-u)$$

$$S_N(f:x) = \int_0^1 f(t) D_N(x-t)\, dt$$

$$\left(f = 1 \text{ gives } \int_0^1 D_N(u)\, du = 1 \right)$$

$$\zeta = e^{2\pi i u} \qquad \zeta^{-N} + \zeta^{-N+1} + \dots + \zeta^{N} = \zeta^{-N} \frac{(1 - \zeta^{2N+1})}{1 - \zeta}$$

$$\cancel{= e^{-2\pi i N u} \frac{(1 - e^{(2N+1)2\pi i u})}{1 - e^{2\pi i u}}} = \cancel{\frac{e^{-2\pi i N u} - e^{2\pi i (N+1) u}}{1 - e^{2\pi i u}}}$$

$$=$$

$$\zeta = e^{i\theta} \qquad \zeta^{-N} + \zeta^{-N+1} + \cdots + \zeta^{N} = \frac{\zeta^{-N}(1-\zeta^{2N+1})}{1-\zeta}$$

$$= \frac{e^{-iN\theta} - e^{i(N+1)\theta}}{1-e^{i\theta}} = \frac{e^{-i\theta/2}\left(e^{-iN\theta} - e^{i(N+1)\theta}\right)}{e^{-i\theta/2} - e^{i\theta/2}}$$

$$= e^{i(N+\frac{1}{2})\theta} - e^{-i(N+\frac{1}{2}\theta)} \Big/ e^{i\theta/2} - e^{-i\theta/2}$$

$$= \frac{\sin (N+\frac{1}{2})\theta}{\sin \frac{1}{2}\theta}.$$

$$D_N(u) = \frac{\sin (N+\frac{1}{2})2\pi u}{\sin \frac{1}{2}\cdot 2\pi u}.$$

$$S_N(f:x) = \int_0^1 f(t)\, D_N(x-t)\, dt$$

$\mathcal{D}$ = Dirichlet class.

Thm (D) For $f \in \mathcal{D}$

$$S_N(f:x) \longrightarrow \frac{1}{2}\left[f(x+) + f(x-)\right].$$

$$\sigma_N(f:x) = \frac{S_0(f:x) + \cdots + \cancel{S_N f(}\cdot S_N(f:x)}{N+1}$$

$$= \int_0^1 f(t)\, F_N(x-t)\, dt$$

$$F_N(u) = \frac{D_0(u) + \cdots + D_N(u)}{N+1}.$$

$$\frac{1}{N+1}\sum_{k=0}^{N} \frac{\sin(k+\frac{1}{2})\theta}{\sin\frac{1}{2}\theta} = \frac{1}{N+1}\sum \frac{2\sin\frac{1}{2}\theta\,\sin(k+\frac{1}{2})\theta}{2\sin^2\frac{1}{2}\theta}$$

$$= \cancel{\frac{\sum \cos k\theta - \cos(k+1)\theta}{2\sin^2\frac{1}{2}\theta}} \qquad \cancel{\cos A - \cos B = 2\sin\frac{A-B}{2}\sin\frac{A+B}{2}}.$$

$$2\sin A \sin B = \cos A-B - \cos A+B$$

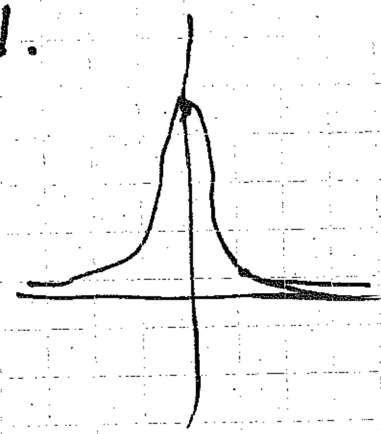
$$= \frac{1}{N+1}\sum_0^N \frac{\cos k\theta - \cos(k+1)\theta}{2\sin^2\frac{1}{2}\theta} = \frac{1}{N+1}\,\frac{1-\cos(N+1)\theta}{2\sin^2\frac{1}{2}\theta} = \frac{\sin^2\frac{N+1}{2}\theta}{(N+1)\sin^2\frac{1}{2}\theta}.$$

$$F_N(u) = \frac{\sin^2\frac{N+1}{2}\cdot 2\pi u}{(N+1)\sin^2\frac{1}{2}\cdot 2\pi u} = \frac{\sin^2(N+1)\pi u}{(N+1)\sin^2\pi u}.$$

D_N oscillates rapidly.

$F_N \geqslant 0$. $\qquad \int_0^1 F_N(t)\,dt = 1.$

$F_N(t) = F_N(-t)$



For $|u| \geqslant \delta$, $\quad F_N \leqslant \dfrac{C\delta}{N+1}$.

(Fejer) $\quad \sigma_N(f : x) \longrightarrow \frac{1}{2}\left[f(x+) + f(x-)\right]$

If f is cont and periodic,

$\sigma_N \longrightarrow f$ uniformly.

Deduce Weierstrass

cgt $\Longrightarrow$ (C,1) cgt.

$\Longleftarrow$ H-L: $\quad a_N = O\left(\frac{1}{N}\right)$.

<u>Proof of (Fejer)</u> Using periodicity (period 1), we have

$$\sigma_N(f : x) = \sigma_N(x) = \int_0^1 f(t)\,F_N(x-t)\,dt \qquad x - t = u$$

$$= \int_{x-1}^{x} f(x-u)\,F_N(u)\,du$$

$$= \int_0^1 f(x-u)\,F_N(u)\,du$$

$$= \int_{-1}^{0} f(x+u)\,F_N(u)\,du = \int_0^1 f(x+u)\,F_N(u)\,du$$

So if $g(x) = \frac{1}{2}\left(f(x+u) + f(x-u)\right) = g(-x)$

$$\sigma_N(x) = \int_0^1 g(u)\,F_N(u)\,du = \int_{-1/2}^{1/2} g(u)\,F_N(u)\,du.$$

$$= 2\int_0^{1/2} g(u)\,F_N(u)\,du.$$

<u>Thm</u> For any x for which $f(x \pm 0)$ exist, f being bdd RI,

$$\sigma_N(f:x) \longrightarrow \frac{1}{2}\left[f(x+0) + f(x-0)\right] \quad (N \to \infty)$$

<u>Proof</u> We must show

$$\int_0^{1/2} g(u)\,F_N(u)\,du \longrightarrow \frac{1}{2}\,g(0+).$$

Let $|g| \leq K$, ~~then~~ $h(u) = g(u) - g(0+)$.

$$\int_0^{1/2} g(0+)\,F_N(u)\,du = \underbrace{\tfrac{1}{2}}_{g(0+)} \int_0^{1/2} F_N(u)\,du = \frac{1}{2}\,g(0+)$$

So we should prove

$$\int_0^{1/2} h(u)\,F_N(u)\,du \longrightarrow 0 \quad \text{if} \quad h(0+) = 0.$$

with $|h| \le K$

If $\delta > 0$ and ~~small~~ $< 1/2$,

$$\left| \int_\delta^{1/2} h(u)\,F_N(u)\,du \right| \le \frac{K\delta}{N+1} \longrightarrow 0 .$$

Fix $\varepsilon > 0$, choose $\delta > 0, < 1/2$ s.t $|h(u)| < \varepsilon$ for $u \in [0, \delta)$.

$$\left| \int_0^\delta h(u)\,F_N(u)\,du \right| \le \varepsilon \int_0^\delta F_N(u)\,du \le \varepsilon \int_0^{1/2} F_N(u)\,du = \frac{\varepsilon}{2} .$$

So choose δ this way and N_0 s.t $\dfrac{K\delta}{N+1} < \dfrac{\varepsilon}{2}$. Then

$$\left| \int_\delta^{1/2} h(u)\,F_N(u)\,du \right| < \varepsilon .$$

~~Cor~~ <u>Thm 2(F)</u> If f is continuous and $f(0) = f(1)$

then

$$\sigma_N(f : x) \longrightarrow f(x)$$

uniformly for $x \in [0, 1]$.

<u>Proof</u> Mild variation of the above local result, where

Note that f, defined on $\mathbb{R}$ by periodicity, is continuous.

So as before, writing $g(x:u) = \frac{1}{2}\left[f(x+u)+f(x-u)\right]$,

$$\sigma_N(x) = 2\int_0^{1/2} g(x:u)\, F_N(u)\, du.$$

We must prove

$$\int_0^{1/2} g(x:u)\, F_N(u)\, du \longrightarrow \frac{1}{2} g(x:0) \quad \text{uniformly in } x.$$

or

$$\int_0^{1/2} h(x:u)\, F_N(u)\, du \longrightarrow 0 \quad \text{unif in } x, \quad h(x:u) = g(x:u) - g(x)$$

$$|h(x:u)| \leq L \quad \text{in } x, u.$$

So

$$\left| \int_\delta^{1/2} h(x:u)\, F_N(u)\, du \right| \leq \frac{L\delta}{N+1}$$

For $\varepsilon > 0$ we can find δ, $0<\delta<1/2$, such that

$$|h(x:u)| < \varepsilon \quad \text{for } |u| < \delta, \quad \text{uniformly in } x.$$

The rest of the proof is the same.

~~Prelo~~ Proof that $L(1:\chi) > 0$ for $\chi = \left(\frac{\cdot}{q}\right)$,

q an odd prime.

Here $N = \cancel{q}\ \ell$ an odd prime.

χ is the character defined by the Legendre symbol $\left(\frac{n}{q}\right)$

$$\chi(n) = \begin{cases} 1 & \text{if } [n] \text{ is a square} \\ -1 & \text{otherwise} \end{cases}$$

$$\sum \chi(n) n^{-s} = \prod_p \left(1 \pm p^{-s}\right)^{-1}$$

For $s > 1$ this is > 0, hence $L(1:\chi) \geqslant 0$. So $L(1:\chi)$ will be > 0 if it is $\neq 0$.

$$L(1:\chi) = \sum \frac{\chi(n)}{n}$$ (remember $L(s:\chi)$ will defined and smooth for $s > 0$).

Abel's thm If $f(z) = \sum a_n z^n$ is a power series cgt for $|z| < 1$, and $\sum a_n = \sigma$ is cgt, then

$$f(x) \to \sigma \quad \text{as } x \mapsto 1 - 0.$$

$$\text{So } \sum \frac{\chi(n)}{n} = \lim_{x \to 1-0} \sum \frac{\chi(n)}{n} x^n$$

$$= \lim \ \cancel{\int^x} \sum \chi(n) \int_0^x y^{n-1}\, dy$$

[For any x, $0 < x < 1$, $\sum \chi(n) y^{n-1}$ cgs uniformly in $0 \leq y \leq x$.
Hence $\displaystyle\int_0^x \sum \chi(n) y^{n-1} dy = \sum \int_0^x \chi(n) y^{n-1} dy$.

So

$$\sum \frac{\chi(n)}{n} = \lim_{x \to 1-0} \int_0^x \sum \chi(n) y^{n-1} dy$$

Ingredients for evaluation of $L(1:\chi)$ and showing it is $\neq 0$

1) Abel's theorem.

2) Gauss sums and their properties

3) determination of Gauss sum upto sign

4) Determination of sign of Gauss sum

5) Dirichlet's version of Poisson summation
[Poisson summation in general]

6) Determination of $\left(\frac{-1}{\ell}\right), \left(\frac{2}{\ell}\right)$.

(7) Cyclotomic fields.

(8) Determination of

$$F(X) = \prod_{R} (X - \zeta^{R})$$

$$\zeta = e^{2\pi i a/l}.$$

(periods of roots of unity).

ABEL's THM

let $s_N = a_0 + \dots + a_N$.

Then by partial summation,

$$\sum_{n=0}^{N} a_n z^n = \sum_{0}^{N-1} s_n z^n (1-z) + s_N z^N.$$

With $|z|<1$, let $N \to \infty$.

$$f(z) = (1-z) \sum_{0}^{\infty} s_n z^n \qquad (\text{Remember } s_n = O(1))$$

If $\lim_{n\to\infty} (s_n) = s$

This is

$$f(z) = (1-z)\sum\left((s_n - s) + s\right) z^n$$

$$= s + (1-z)\sum (s_n - s) z^n.$$

We want $z \to 1$; actually $z = x \in (0,1), \longrightarrow 1$.

Fix $\varepsilon > 0$, $|s_n - s| < \varepsilon$ $n \geq N_0$.

$$|f(z) - s| \leq \varepsilon \sum_{N_0}^{\infty} z^n + |1-z| \cdot \sum_{0}^{N_0 - 1} |s_n - s| x^{n-1}.$$

$$\leq \varepsilon + |1-x| \underbrace{\sum_{0}^{N_0-1} |s_n - s|}_{C(\varepsilon).}$$

Let $x \geq 1-\delta$ where $\delta \cdot C(\varepsilon) < \varepsilon$. Then for $x \geq 1-\delta$,

$$|f(x) - s| < \varepsilon.$$

<u>Rmqs</u> We can let z be cplex and $\to 1$ but not tangentially.

Explicit formula for $L(1:\chi)$

1) By Abel's theorem,

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \lim_{\mathbb{R}\ni x \to 1-0} \sum \chi(n) \frac{x^n}{n}.$$

Now for $x \in (0,1)$,

$$\sum \chi(n) \frac{x^n}{n} = \sum \chi(n) \int_0^x y^{n-1}\,dy$$

$$= \int_0^x \sum \chi(n) y^{n-1}\,dy \quad \text{~~as~~ is unif.}$$

as $\sum \chi(n) y^{n-1}$ is unif. cgt in $0 \le y \le x$, $x<1$ fixed.

So

$$\sum \frac{\chi(n)}{n} = \lim_{x\to 1-0} \int_0^x \sum_1^{\infty} \chi(n) y^{n-1}\,dy.$$

2) Summing up $\sum_1^{\infty} a_n y^{n-1}$ when $a_{n+l} = a_n$ and $a_1 + \cdots + a_l = 0$.

$$\cancel{\sum a_n y^{n-1} = \sum_1^{l} a_n y^{n-1} + \sum_1^{N} a_n y}$$

$$\sum a_n y^{n-1} = \sum_1^{l} a_n y^{n-1} (1 + y^l + y^{2l} + \cdots)$$

$$= \sum_1^{l} a_n y^{n-1} / 1 - y^l.$$

$$\sum \cancel{x(n)}\, a_n\, y^{n-1} = \frac{f(y)}{1-y^l} \qquad f(y) = \sum_1^l a_n y^{n-1}$$

$$f(1) = 0.$$

3) $$\sum_1^\infty x(n) y^{n-1} = \frac{f(y)}{1-y^l} \quad f(y) = \sum_1^l x(n) y^{n-1}, \quad f(1)=0.$$

Since $f(1) = 0$,

$$\frac{f(y)}{1-y^l} = \frac{g(y)}{\prod\limits_{\zeta^l=1,\, \zeta\neq 1} (1-\zeta y)}$$

which is continuous in $0 \leq y \leq 1$. Hence

$$\int_0^1 \frac{f(y)}{1-y^l}\, dy \text{ exists.}$$

So

$$\sum \frac{x(n)}{n} = \int_0^1 \frac{f(y)}{1-y^l}\, dy.$$

4) Splitting of $\frac{f(y)}{1-y^l}$ in partial fractions, when $\deg(f) \leq l-1$.

$$\frac{f(y)}{1-y^l} = \sum_{\zeta^l=1} \frac{A_\zeta}{1-\zeta y}$$

$$f(y) = \sum_{\zeta} A_{\zeta} \prod_{\eta \neq \zeta} (1 - \eta y)$$

So $y = 1/\zeta \Rightarrow f\left(\frac{1}{\zeta}\right) = \cancel{\sum_{\zeta}} A_{\zeta} \prod_{\eta \neq \zeta} \left(1 - \frac{\eta}{\zeta}\right)$

$$= \frac{A_{\zeta}}{\zeta^{\ell-1}} \prod_{\eta \neq \zeta} (\zeta - \eta).$$

Now $x^{\ell} - 1 = \prod (x - \zeta)$. Differentiating at $x = \zeta$,

$$\cancel{\ell x^{\ell-1} = \sum_{\zeta}}$$

$$\ell \zeta^{\ell-1} = \prod_{\eta \neq \zeta} (\eta - \zeta).$$

Hence

$$f\left(\frac{1}{\zeta}\right) = \frac{A_{\zeta}}{\zeta^{\ell-1}} \cdot \ell \zeta^{\ell-1} = \ell A_{\zeta}$$

or

$$A_{\zeta} = \frac{1}{\ell} f\left(\frac{1}{\zeta}\right); \quad \text{for } \zeta = 1, \ A_1 = 0.$$

So $\dfrac{f(y)}{1 - y^{\ell}} = \dfrac{1}{\ell} \displaystyle\sum_{\zeta \neq 1} f\left(\frac{1}{\zeta}\right) \frac{1}{1 - \zeta y}$ ~~(since~~

All this with no assumption on f except its degree $\leq \ell - 1$ and $f(1) = 0$.
The specific form of f is used in computing $f(1/\zeta)$.

5) We compute $f(\frac{1}{\zeta})$ in terms of <u>Gauss sums.</u> If $\mathbb{F}$ is a finite field, $\chi : \mathbb{F}^{\times} \to \mathbb{C}$ a (multiplicative) character, and $\psi : \mathbb{F} \to \mathbb{C}$ a nontrivial additive character, the gauss sum $G(\chi, \psi)$ is defined by

$$G(\chi,\psi) = \sum_{x \in \mathbb{F}^{\times}} \chi(x)\psi(x).$$

Extending the definition of χ to $\mathbb{F}$ by $\chi(0) = 0$, the above formula is shows that

$$G(\chi, \psi) = |\mathbb{F}|.\ \hat{\chi}(\psi)$$

where $\hat{\chi}$ is the Fourier Transform of χ, defined on the abelian group of characters of $\mathbb{F}$ (additive).

$$\text{Now } f(\tfrac{1}{\zeta}) = \sum_{n=1}^{l-1} \left(\frac{n}{l}\right) \frac{1}{\zeta^{n-1}}$$

$$= \zeta \sum_{n=1}^{l-1} \left(\frac{n}{l}\right) \frac{1}{\zeta^{n}}.$$

We have $\mathbb{F} = \mathbb{Z}/_{l}$, $\mathbb{F}^{\times} = \mathbb{Z}/_{l}^{\times} = G_l$. So, if $\zeta = e^{2\pi i \frac{a}{l}}$ $(1 \leq a \leq l-1)$,

$$f(\tfrac{1}{\zeta}) = \zeta \sum_{n=1}^{l-1} \left(\frac{n}{l}\right) e^{-\frac{2\pi i a n}{l}} \qquad (1 \leq a \leq l-1).$$

Since $(a, \ell) = 1$, $[n]_\ell \longmapsto [an]_\ell$ is an automorphism of $\mathbb{Z}_\ell^*$. Hence, remembering $\left(\frac{a}{\ell}\right) = \pm 1$,

$$f\left(\tfrac{1}{\zeta}\right) = \zeta \left(\frac{a}{\ell}\right) \sum_{n=1}^{\ell-1} \left(\frac{n}{\ell}\right) e^{-2\pi i \frac{n}{\ell}}.$$

$$= \zeta \left(\frac{a}{\ell}\right) \overline{\mathcal{G}}$$

where

$$\mathcal{G} = \sum_{n=1}^{\ell-1} \left(\frac{n}{\ell}\right) e^{2\pi i \frac{n}{\ell}}$$

is the Gauss sum $G\left(\left(\frac{\cdot}{\ell}\right), \psi\right)$, $\psi : [n] \mapsto e^{2\pi i \frac{n}{\ell}}$.

Hence

$$\frac{f(y)}{1-y^\ell} = \frac{1}{\ell} \sum_{a=1}^{\ell-1} \left(\frac{a}{\ell}\right) e^{2\pi i \frac{a}{\ell}} \overline{\mathcal{G}} \cdot \frac{1}{1-\zeta y}.$$

So

$$\sum \frac{\chi(n)}{n} = \cancel{\frac{1}{\ell} \sum_{a=1}^{\ell-1}} \frac{\overline{\mathcal{G}}}{\ell} \sum_{a=1}^{\ell-1} \left(\frac{a}{\ell}\right) e^{2\pi i \frac{a}{\ell}} \int_0^1 \frac{dy}{1 - e^{2\pi i a/\ell} y}$$

We define log as the branch on $\mathcal{D} = \mathbb{C} \setminus \{u \mid u \in \mathbb{R}, u \le$

with $\log 1 = 0$. So

$\log u = \log|u| + i \arg(u)$, $\quad -\pi < \arg(u) <$

If $\zeta^l = 1, \zeta \neq 1$,

$$\int_0^1 \frac{dy}{1-\zeta y} = \frac{1}{\zeta}\int_0^{\zeta} \frac{du}{1-u} \quad \text{(straight line from } 0 \text{ to } \zeta)$$

$$= \frac{1}{\zeta}\int_{1-\zeta}^{1} \frac{dz}{z} \quad \text{(straight line from } 1-\zeta \text{ to } 1)$$

and the line of integration lies in $\mathcal{D}$.

[If u real and ≤ 0 lies on this line, $1-\zeta$ lies in the line joining u and 1, $\Rightarrow \zeta$ is real $\Rightarrow \zeta = \pm 1$; $\zeta = +1$ excluded and if $\zeta = -1$, $2 \in [u, 1]$ which is impossible.].

$$\zeta \int_0^1 \frac{dy}{1-\zeta y} = \log 1 - \log(1-\zeta) = -\log(1-\zeta).$$

Note $1-\zeta \in \mathcal{D}$ (as otherwise $1-\zeta = u \Rightarrow \zeta$ real and ≥ 1, impossible,

For $\zeta = e^{i\theta}$, $0 < \theta < 2\pi$,

$$\log(1-\zeta) = \log|1-\zeta| + i\arg(1-\zeta), \quad -\pi < \arg < \pi.$$

$|1-\zeta|^2 = |2 - 2\cos\theta| = 4\sin^2\frac{\theta}{2}$ so $\log|1-\zeta| = \log\left(2\sin\frac{\theta}{2}\right)$

$1-\zeta = 1-\cos\theta - i\sin\theta$, ~~so arg (1-ζ)~~ $\tan\arg(1-\zeta) = -\frac{\sin\theta}{1-\cos\theta}$

$$= -\cot\frac{\theta}{2} = \tan\left(\frac{\theta}{2} - \frac{\pi}{2}\right).$$

Since $\frac{\theta}{2} - \frac{\pi}{2} \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ we have

$$\log(1 - e^{i\theta}) = \log\left(2\sin\frac{\theta}{2}\right) + i\left(\frac{\theta}{2} - \frac{\pi}{2}\right).$$

Hence

$$\log\left(1 - e^{\frac{2\pi i a}{l}}\right) = \log\left(2\sin\frac{\pi a}{l}\right) + i\left(\frac{\pi a}{l} - \frac{\pi}{2}\right).$$

Hence finally

$$L(1:\chi) = \sum \frac{\chi(n)}{n} = -\frac{\overline{\mathcal{G}}}{l}\sum_{a=1}^{l-1}\left(\frac{a}{l}\right)\cancel{e^{\frac{2\pi i a}{l}}}\log\left(1 - e^{\frac{2\pi i a}{l}}\right)$$

$$= -\frac{\overline{\mathcal{G}}}{l}\sum_{a=1}^{l-1}\left(\frac{a}{l}\right)\left[\log\left(2\sin\frac{\pi a}{l}\right) + i\left(\frac{\pi a}{l} - \frac{\pi}{2}\right)\right].$$

We can neglect the $\frac{\pi}{2}$ term as $\sum_{1}^{l-1}\left(\frac{a}{l}\right) = 0$.

So $$L(1:\chi) = -\frac{\overline{\mathcal{G}}}{l}\sum_{a=1}^{l-1}\left(\frac{a}{l}\right)\left[\log\left(2\sin\frac{\pi a}{l}\right) + \frac{i\pi a}{l}\right].$$

$$\mathcal{G} = \sum_{n=1}^{l-1}\left(\frac{n}{l}\right)e^{\frac{2\pi i n}{l}}.$$

6) Determination of $\overline{\mathcal{G}}$ upto a sign.

We ~~was~~ have

(a) $|\mathcal{G}|^2 = l$

(b) $\overline{\mathcal{G}} = (-1)^{\frac{l-1}{2}} \mathcal{G}$.

Although (a) can be proved by brute calculation, it is better to use Fourier Transform theory on finite abelian groups. For any finite abelian group G, $|G| = g$, define, for any complex function f on G,

$$\hat{f}(\chi) = \frac{1}{g} \sum_{a \in G} f(a) \chi(a) \qquad \chi \in \hat{G}.$$

Then $\hat{f}$ is the Fourier Transform of f. We have the <u>Fourier inversion formula</u>

$$f(a) = \sum_{\chi} \hat{f}(\chi) \overline{\chi(a)}$$

$$\Big[\sum_{\chi} \hat{f}(\chi) \overline{\chi(a)} = \sum_{\chi \in \hat{G}} \overline{\chi(a)} \frac{1}{g} \sum_{b \in G} f(b) \chi(b)$$

$$= \frac{1}{g} \sum_{b \in G} f(b) \sum_{\chi \in \hat{G}} \bar{\chi}(a) \chi(b) = \sum_{b \in G} \delta(a, b) f(b) =$$

We have two finite dimensional spaces $L^2(G), L^2(\hat{G})$ with scalar products

$$(f,h)_G = \frac{1}{g}\sum_{a\in G} f(a)\overline{h(a)}$$

$$(u,v)_{\hat{G}} = \sum_{\chi\in\hat{G}} u(\chi)\overline{v(\chi)}.$$

Then the Plancherel formula asserts that

$$(f,h)_G = (\hat{f},\hat{h})_{\hat{G}} \qquad (f,f)_G = (\hat{f},\hat{f})_{\hat{G}}.$$

or that

$$f \longmapsto \hat{f}$$

is a unitary isomorphism.]

We apply this to $G = \mathbb{Z}/_\ell$, $f = \chi$ (regarded as a function on $\mathbb{Z}/_\ell$ vanishing at 0.)

$$\hat{\chi}(m) = \frac{1}{\ell}\sum_{n=0}^{\ell-1} \chi(n)\, e^{\frac{2\pi i mn}{\ell}}$$

Since $n \mapsto e^{2\pi i mn/\ell}$ are all the characters of $\mathbb{Z}/_\ell$, $0 \le m \le \ell$.

Evaluation of $\left(\frac{-1}{\ell}\right)$ (Euler)

$$\left(\frac{-1}{\ell}\right) = (-1)^{\frac{\ell-1}{2}} = \begin{cases} 1 & \ell \equiv 1 (4) \\ -1 & \ell \equiv 3 (4) \end{cases} \iff \left(\frac{-1}{\ell}\right) = 1 \iff \ell \equiv 1 (4).$$

<u>Proof</u> Suppose $n^2 = -1$. Then $n^4 = 1$, $\{1, n, n^2, n^3\}$ is a cyclic group of order 4 $\subset \mathbb{Z}/_\ell^\times$. So $4 \mid \ell - 1$. Conversely suppose $\ell \equiv 1 (4)$. Let m generate $\mathbb{Z}/_\ell^\times$ so that $m^\mu = 1 \iff \ell - 1 \mid \mu$.

Let $m^r = -1$. Then $m^{2r} = 1 \Rightarrow$ ~~2r ℓ−1 | m~~ $\ell - 1 \mid 2r$.

If $\ell = 1 + 4k$, $4k \mid 2r \Rightarrow 2k \mid r \Rightarrow r$ is even $\Rightarrow r = 2s$

and so $m^{2s} = -1 \Rightarrow (m^s)^2 = -1$.

If $m = 0$, $\hat{\chi}(0) = 0$ as $\sum_{n=0}^{l-1} \chi(n) = 0$.

If $m \neq 0$, $[n] \longmapsto [mn]$ is an automorphism of $\mathbb{Z}_l$

and so

$$\hat{\chi}(m) = \left(\frac{m}{l}\right) \hat{\chi}(1) = \left(\frac{m}{l}\right) (l^{-1} g)$$

So

$$(\hat{\chi}, \hat{\chi})_{\hat{\mathbb{Z}}_l} = |g|^2 \cdot \frac{(l-1)}{l^2}.$$

But

$$(\chi, \chi)_{\mathbb{Z}_l} = \frac{l-1}{l}.$$

So $\quad |g|^2 \frac{(l-1)}{l^2} = \frac{l-1}{l} \implies |g|^2 = l.$

b) $\quad \bar{g} = \sum_{a=1}^{l-1} \left(\frac{a}{l}\right) e^{-\frac{2\pi i a}{l}}$

Now $\left(\frac{-a}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{a}{l}\right) = (-1)^{\frac{l-1}{2}} \left(\frac{a}{l}\right).$

Hence $\quad \bar{g} = (-1)^{\frac{l-1}{2}} g.$

From ~~(a) and~~ (b) we have

$\mathcal{G}$ is real $\quad l \equiv 1 \ (4)$

$\mathcal{G}$ is pure imaginary $\quad l \equiv 3 \ (4)$

Here, using (a)

$$\mathcal{G} = \begin{cases} \varepsilon\sqrt{l} & l \equiv 1 \ (4) \\ i\varepsilon\sqrt{l} & l \equiv 3 \ (4). \end{cases}$$

where

$$\varepsilon = \pm 1.$$

Actually $\varepsilon = 1$ in both cases, as was proved by Gauss, after many years' of effort. ~~He eat~~ The determination of ε is called the problem of the sign of the Gaussian sum.

Now $L(1:X)$ is real. So if $l \equiv 1(4)$, we can neglect the imaginary part in the expression for $L(1:X)$ and get

$$L(1:\chi) = -\frac{\varepsilon}{\sqrt{l}}\sum_{a=1}^{l-1}\left(\frac{a}{l}\right)\log\left(2\sin\frac{\pi a}{l}\right) \qquad l\equiv 1\ (4)$$

$$\cancel{L(1:\chi) = -\frac{\varepsilon\pi}{\sqrt{l}}\sum\left(\frac{a}{l}\right)}$$

$$L(1:\chi) = -\frac{\varepsilon\pi}{l^{3/2}}\sum_{a=1}^{l-1} a\cdot\left(\frac{a}{l}\right). \qquad l\equiv 3\ (4).$$

From now on we write R for the generic quadratic residue $\left(\frac{R}{l}\right)=+1$, and N for the generic quadratic nonresidue $\left(\frac{N}{l}\right)=-1$.

So

$$l\equiv 1\ (4) \qquad L(1:\chi) = -\frac{\varepsilon}{\sqrt{l}}\log\frac{\prod \sin\frac{\pi R}{l}}{\prod \sin\frac{\pi N}{l}}$$

[Since $\#R=\#N$, the factors 2 cancel out)

$$l\equiv 3(4) \qquad L(1:\chi) = -\frac{\varepsilon\pi}{l^{3/2}}\left(\sum R-\sum N\right).$$

[[It is essential to remember that we use $(1, 2, .. l-1)$ as the set of]]. nonzero residues

The formula for $L(1:\chi)$ when $l \equiv 3\ (4)$ is a finite expression.

To see that it is $\neq 0$, we must prove

$$\sum R \neq \sum N.$$

But

$$\sum R + \sum N = \sum_{r=1}^{l-1} r = \frac{l(l-1)}{2} \text{ is odd if } l \equiv 3(4).$$

If $\sum R = \sum N$, $\sum R + \sum N$ would be even. Thus we are done!

In the case $l \equiv 1\ (4)$ we must prove that

$$\frac{\prod \sin \frac{\pi R}{l}}{\prod \sin \frac{\pi N}{l}} \neq 1.$$

This is more difficult and Dirichlet used Gauss's work on cyclotomy.

Determination of ε by Dirichlet

For ~~both~~ Dirichlet, it was essential to obtain a preliminary expression for G in which the Legendre symbol $\left(\frac{m}{\ell}\right)$ does not occur explicitly. Now, writing R and N for the typical residue and non residue,

$$1 + \sum_R e^{2\pi i R/\ell} + \sum_N e^{2\pi i \frac{N}{\ell}} = 0. \qquad (\text{note } R, N \neq 0).$$

$$\text{So } -\sum e^{2\pi i \frac{N}{\ell}} = 1 + \sum e^{2\pi i R/\ell}$$

$$\text{So } \sum e^{2\pi i \frac{R}{\ell}} - \sum e^{2\pi i \frac{N}{\ell}} = G = 1 + 2\sum e^{2\pi i R/\ell}$$

$$= \sum_{x=0}^{\ell-1} e^{2\pi i x^2/\ell}. \qquad (x \mapsto x^2 \text{ is } 2:1 \text{ map})$$

Hence

$$G = \sum_{x=0}^{\ell-1} e^{2\pi i \frac{x^2}{\ell}}$$

Dirichlet proved (and then Kronecker) that for <u>any</u> integer $N \geq$

$$\sum_{x=0}^{N-1} e^{2\pi i x^2/N} = \begin{cases} (1+i)\sqrt{N} & (N \equiv 0\ (4)) \\ \sqrt{N} & (N \equiv 1\ (4)) \\ 0 & (N \equiv 2\ (4)) \\ i N^{1/2} & (N \equiv 3\ (4)) \end{cases}$$

which can be united in a single formula

$$\sum_{x=0}^{N-1} e^{2\pi i \frac{x^2}{N}} = \frac{1+i^{-N}}{1+i^{-1}}\sqrt{N}$$

($\sqrt{N}$ is always the positive square root).

~~for a suitable class of function f,~~

The ~~Poisson summation formula says that if f is a Schwartz~~ function on $\mathbb{R}$, and

$$\hat{f}(u) \underset{\text{def}}{=} \int_{-\infty}^{\infty} f(x)\, e^{2\pi i ux}\, dx,$$

then ~~$\hat{f}$ is also a Schwartz function and~~

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

~~We apply this to f defined by~~

$$\cancel{f(x) = \begin{cases} e^{2\pi i x^2/N} & 0 \le x \le N \\ \end{cases}}$$

Dirichlet uses the Poisson Summation formula in the case of functions f which obey the so-called Dirichlet conditions that allow the F.S. of f to converge point wise to $\frac{1}{2}(f(x+)+f(x-))$ at each x, first proved by Dirichlet himself in 1829.

~~Let $f(x)$ be a function defined on $[0,1]$ which is~~

Let $f(x)$ be a real continuous function on $[0,1]$ ~~with a finite number of maxima and minima~~ which is piecewise monotonic. ~~Let~~ Then, for any $t \in [0,1]$,

$$f(t)\ \cancel{\frac{f(t+)+f(t-)}{2}} = \sum_{-\infty}^{\infty} e^{2\pi i n t} \int_0^1 f(x) e^{-2\pi i n x}\, dx.$$

with the convention that the LHS is $\frac{1}{2}(f(0)+f(1))$ when $t=0$.

This formula is certainly valid ~~condition is satisfied~~ if f is of class C^2 (see HW # 1) ~~on $[0,1]$ and f' has finitely many zeros in $[0,1]$, then between any two zeros of f', f' has the same sign and so f is monotonic. If f is complex valued, we assume that the conditions apply to $Re(f)$ and $Im(f)$.~~

Thus

$$\frac{f(0)+f(1)}{2} = \sum_{-\infty}^{\infty} \int_0^1 f(x) e^{-2\pi i n x}\, dx.$$

Suppose now f is defined and of class C^2 ~~continuous~~ on $[A,B]$ where A and B are integers, ~~with $Re(f)$ and $Im(f)$ of class C^1 with their piecewise monotonic~~. For ~~$x \in$~~ integer $r \in [A, B-1]$

$f(x+r)$ ($0 \le x \le 1$ ~~$r \le x \le r+1$~~) is of class C^2 ~~continuous~~ in $[0,1]$. ~~and piecewise monotonic~~. Hence

$$\frac{1}{2}(f(r)+f(r+1)) = \sum_{-\infty}^{\infty} \int_0^1 f(x+r) e^{-2\pi i n x}\, dx$$

$$= \sum_{-\infty}^{\infty} \int_r^{r+1} f(x) e^{-2\pi i n x}\, dx.$$

Summing from $r = A$ to $r = B-1$ we get

$$\frac{1}{2}f(A) + f(A+1) + \dots + f(B-1) + \frac{1}{2}f(B)$$

$$= \sum_{-\infty}^{\infty} \int_A^B f(x)\, e^{-2\pi i n x}\, dx.$$

If $f(A) = f(B)$ we get

$$\sum_{n=A}^{B-1} f(n) = \sum_{-\infty}^{\infty} \int_A^B f(x)\, e^{-2\pi i n x}\, dx.$$

We apply this to $f(x) = e^{\frac{2\pi i x^2}{N}}$ on $[0, N]$.

Then

$$g = \sum_0^{N-1} e^{2\pi i x^2/N} = \sum_{-\infty}^{\infty} \int_0^N \overset{e^{2\pi i \frac{x^2}{N}}}{\cancel{f(x)}}\, e^{-2\pi i n x}\, dx.$$

$$= N \sum_{-\infty}^{\infty} \int_0^1 e^{2\pi i N y^2 - 2\pi i n N y}\, dy$$

$\frac{n}{2} - y = u$ ~~$y - \frac{n}{2} = u$~~

$$\int_0^1 e^{2\pi i N y^2 - 2\pi i n N y}\, dy = \int_0^1 e^{2\pi i N (y^2 - n y)}\, dy = \cancel{e^{-\pi i N \frac{n^2}{2}} \int_0^1 e^{2\pi i N (y \dots)^2}\, dy}$$

$$= \int_{n/2}^{n/2+1} e^{2\pi i N u^2}\, du \cdot e^{-\frac{\pi i N n^2}{2}}$$

$$= N \sum_{-\infty}^{\infty} e^{-\frac{i\pi N n^2}{2}} \int_{n/2}^{n/2+1} e^{2\pi i N y^2}\, dy.$$

The coefficient in front of the integral is 1 if n even, i^{-N} for n odd

Hence

$$G = N\sum_{n \text{ even}} \int_{n/2}^{n/2+1} e^{2\pi i N y^2}\,dy + N\sum_{n \text{ odd}} i^{-N} \int_{n/2}^{n/2+1} e^{2\pi i N y^2}\,dy.$$

$$= N\int_{-\infty}^{\infty} e^{2\pi i N y^2}\,dy + N i^{-N} \int_{-\infty}^{\infty} e^{2\pi i N y^2}\,dy.$$

$y\sqrt{N} = u$

$$= \sqrt{N}\int_{-\infty}^{\infty} e^{2\pi i u^2}\,du + i^{-N}\sqrt{N}\int_{-\infty}^{\infty} e^{2\pi i u^2}\,du$$

$$= (1+i^{-N})\sqrt{N}\int_{-\infty}^{\infty} e^{2\pi i u^2}\,du.$$

The integral $\displaystyle\int_{-\infty}^{\infty} e^{2\pi i u^2}\,du$ is of Fresnel type, and is cgt in Riemann's sense, not Lebesgues

Indeed, it is enough to prove

$$\lim_{T\to\infty}\int_1^T e^{2\pi i u^2}\,du \quad \text{exists.}$$

$$\int_1^T e^{2\pi i u^2}\,du = \int_1^T e^{2\pi i u^2}\cdot(2\pi i u^2)'\,\frac{du}{4\pi i u}$$

$$= \frac{e^{2\pi i u^2}}{4\pi i u}\Bigg|_1^T + \int_1^T \frac{e^{2\pi i u^2}}{}\cdot\frac{1}{4\pi i u^2}$$ (int by parts

$$= \lim_{T\to\infty} \int_1^T \frac{e^{2\pi i u^2}}{4\pi i u^2}\, du$$

which exists as the integral is absolutely cgt. So

$$\mathcal{G} = (1+i^{-N})\sqrt{N} \int_{-\infty}^{\infty} e^{2\pi i u^2}\, du$$

$$= (1+i^{-N})\sqrt{N}\,.\, I \quad \text{say.}$$

For $N=1$, $\mathcal{G}=1 \Rightarrow (1+i^{-1})\, I = 1$.

$$\text{So } I = \frac{1}{1+i^{-1}} =$$

$$\Rightarrow \quad \mathcal{G} = \frac{1+i^{-N}}{1+i^{-1}}\sqrt{N} = \begin{cases} \cancel{(1-i)\sqrt{N}\,N} = (1-i)N^{1/2} & N\equiv 0\ (4) \\ \sqrt{N} & N\equiv 1\ (4) \\ 0 & N \equiv 2\ (4) \\ i\sqrt{N} & N\equiv 3\ (4). \end{cases}$$

<u>Proof $L(1:\chi) \neq 0$ if $l \equiv 1\ (4)$</u>

Here, ~~taking into account~~ ~~(taking~~

$$L = -\frac{\varepsilon}{l^{1/2}} \log \frac{\prod 2\sin \pi R/l}{\prod \sin \pi N/l}$$

We must show

$$\prod \sin \pi R/l \,\Big/ \prod \sin \pi N/l \neq 1.$$

CYCLOTOMY Cyclotomy means division of the circle. It is involved in the construction of regular polygons. Algebraically it means the consideration of the field C_n generated over Q by the n^{th} roots of unity $e^{2\pi i m/n}$, $m=0,1,\dots,n-1$. If $\zeta_n = e^{2\pi i/n}$, $C_n = Q(\zeta_n)$. An n^{th} root η of unity is called primitive if $\eta^m \neq 1$ for any $m < n$. The primitive roots are the ζ_n^m, $(m,n)=1$; any such generates the group μ_n of n^{th} roots of unity. We are interested only in prime cyclotomic fields C_l, l an odd prime. For $l=3$, $C_3 = Q[\omega]$ $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. It was used by Euler in his proof of Fermat's theorem for the exponent 3. The field C_{17} was used by Gauss to prove that a regular 17-gon can be constructed using ruler and compass.

For an odd prime l, $e^{2\pi i a/l}$ $(0 < a \le l-1)$ are all primitive l^{th} roots of unity and

$$\Phi_l(T) := \prod_{a=1}^{l-1}(T - e^{2\pi i a/l}) = T^{l-1} + T^{l-2} + \dots + T + 1.$$

The first point is to note that Φ_l is irreducible. The proof we give is based on Eisenstein's criterion for irreducibility: Steven Wheatraft ~~also~~ it appears Schonemann had anticipated Eisenstein in both the irreducibility criterion and the irreducibility of Φ_ℓ. The first proof of the irreducibility is due to Gauss.

Eisenstein's criterion for irreducibility. Let $f(X) = X^m + c_1 X^{m-1} + \dots + c_m$ be a monic polynomial with $c_j \in \mathbb{Z}$ for all j. Suppose $\exists$ a prime p such that

$$p \mid c_1, \dots, c_n, \quad p^2 \nmid c_n.$$

Then f is irreducible.

Proof. Suppose $f(X) = g(X)h(X)$ where $\deg(g)$ and $\deg(h) < \deg(f)$. By Gauss's lemma, g and h also are monic and have integer coefficients. We now take everything mod ℓ, let $u \mapsto \bar{u}$ be the map $\mathbb{Z} \to \mathbb{Z}_\ell$ as well as $\mathbb{Z}[X] \to \mathbb{Z}_\ell[X]$. Then $\bar{f} = X^m$, $\bar{f} = \bar{g}\bar{h}$, showing that ~~$\bar{f} = X^m$~~ $\bar{g} = X^r$, $\bar{h} = X^s$, $r + s = m$. So all coefficients of g and h except their leading terms are divisible by p. Hence the constant term of f = constant term of $g \times$ constant term of h is divisible by p^2; a contradiction.

Irreducibility of Φ_ℓ. Write $T - 1 = X$. Then

$$\Phi_\ell(T) = \frac{T^\ell - 1}{T - 1} = \frac{(1+X)^\ell - 1}{X} = X^{\ell-1} + \binom{\ell}{1} X^{\ell-2} + \dots + \binom{\ell}{\ell-1}$$

satisfies Eisenstein's criterion with the prime l. So Φ_l is irreducible.

It follows that $[C_l : Q] = l-1$. Let G be the Galois group of C_l/Q, $\zeta = e^{2\pi i/l}$. If $\sigma \in G$, $\sigma\zeta = e^{2\pi i m/l} = \zeta^m$; m is uniquely determined element of $\mathbb{Z}_l^\times$, which we write as $m(\sigma)$. For $\sigma, \tau \in G$,
$\sigma\tau\zeta = \zeta^{m(\sigma\tau)} = \sigma(\zeta^{m(\tau)}) = \zeta^{m(\sigma)m(\tau)}$ so that $\sigma \mapsto m(\sigma)$ is a homomorphism of G into $\mathbb{Z}_l^\times$. If $m(\sigma) = I$, $\sigma\zeta = \zeta$ which $\Rightarrow \sigma = I$. So $\sigma \mapsto m(\sigma)$ is an <u>injective</u> homomorphism of G into $\mathbb{Z}_l^\times$. But $|G| = [C_l : Q] = l-1 = |\mathbb{Z}_l^\times|$. Hence $\sigma \mapsto m(\sigma)$ is an <u>isomorphism</u> $G \cong \mathbb{Z}_l^\times$. For $m \in \mathbb{Z}_l^\times$ we write $\sigma(m)$ for the corresponding element of G. We identify G with $\mathbb{Z}_l^\times$ whenever convenient. ~~Let~~

$$\cancel{\text{Let } \eta_0 = \sum \zeta^R, \quad \eta_1 = \sum \zeta^N}.$$

Since l is odd, $\mathbb{Z}_l^\times$ is a cyclic grp of even order $l-1$. Hence it is isomorphic to $\mathbb{Z}_{l-1}$ and so has a unique subgroup H of index 2, namely the squares or the quadratic residues. Let Q_2 be the fixed field of H. Then $[Q_2 : Q] = 2$. We shall now determine this quadratic field.

Let $\eta_0 = \sum \zeta^R$, $\eta_1 = \sum \zeta^N$. If $m \in H$, m is a residue and $\sigma(m)$ permutes the sets of R and N. Hence

$\sigma(m)$ fixes η_0 and η_1, showing $\eta_0, \eta_1 \in \mathbb{Q}_2$. Now

$$\eta_0 + \eta_1 = -1$$

$$\eta_0 - \eta_1 = \text{Gauss sum} = \varepsilon l^{1/2} \quad \text{when } \varepsilon \in \pm 1 \;\; l \equiv 1(4)$$
$$\in \pm i \;\; l \equiv 3(4).$$

So $\cancel{\quad}$ $\eta_0 = \dfrac{-1+\varepsilon l^{1/2}}{2}$ $\eta_1 = \dfrac{-1-\varepsilon l^{1/2}}{2}$. Moreover $\varepsilon l^{1/2} \in \mathbb{Q}_2$. Hence

$$\mathbb{Q}_2 = \begin{cases} \mathbb{Q}[\sqrt{l}] & l \equiv 1(4) \\ \mathbb{Q}[\sqrt{-l}] & l \equiv 3(4). \end{cases}$$

Consider now the polynomial

$$F(X) = \prod (X - \zeta^R)$$

Its coefficients are symmetric functions of the ζ^R, hence in $\mathbb{Q}_2$. Moreover, being in $\mathbb{Z}[\zeta]$, they are integral over $\mathbb{Z}$. So So they are of the form $\alpha\eta_0 + \beta\eta_1$ where $\alpha, \beta \in \mathbb{Z}$.

$$F(X) = A_0(X)\eta_0 + A_1(X)\eta_1$$

where $A_0, A_1 \in \mathbb{Z}[X]$. Select a nonresidue m in $\mathbb{Z}_l^\times$ and apply $\sigma(m)$ to the above identity. Since $\sigma(m)$ interchanges residues and nonresidues, ~~we have~~ hence also η_0 and η_1, and so

$$F^{\sigma(m)}(X) = \prod(X - \zeta^N) = A_1(X)\eta_0 + A_0(X)\eta_1.$$

Taking $X = 1$,

$$\prod(1-\zeta^R) = A_0(1)\eta_0 + A_1(1)\eta_1$$

$$\prod(1-\zeta^N) = A_1(1)\eta_0 + A_0(1)\eta_1.$$

Hence

$$\prod(1-\zeta^R) = A_0(1)\left(\frac{-1+\varepsilon l^{1/2}}{2}\right) + A_1(1)\left(\frac{-1-\varepsilon l^{1/2}}{2}\right)$$

$$= -\frac{1}{2}\left(A_0(1)+A_1(1)\right) + \frac{\varepsilon l^{1/2}}{2}\left(A_0(1)-A_1(1)\right)$$

$$\prod(1-\zeta^N) = A_1(1)\left(\frac{-1+\varepsilon l^{1/2}}{2}\right) + A_0(1)\left(\frac{-1-\varepsilon l^{1/2}}{2}\right)$$

$$= -\frac{1}{2}\left(A_0(1)+A_1(1)\right) + \frac{\varepsilon l^{1/2}}{2}\left(A_1(1)-A_0(1)\right).$$

Let $Y = -\left(A_0(1)+A_1(1)\right)$, $Z = A_0(1)-A_1(1)$.

Then

$$\prod(1-\zeta^R) = \frac{1}{2}\left(Y + \varepsilon l^{1/2} Z\right) \qquad \prod(1-\zeta^N) = \frac{1}{2}\left(Y - \varepsilon l^{1/2} Z\right).$$

Since $\prod(1-\zeta^R)\prod(1-\zeta^N) = l$

we have $Y^2 - \varepsilon^2 l Z^2 = 4l$. Since $Z = 0 \Rightarrow Y^2 = 4l$

which is impossible. This finishes the argument for

$$\frac{\prod(1-\zeta^R)}{\prod(1-\zeta^N)} = \frac{Y+\varepsilon l^{1/2} Z}{Y-\varepsilon l^{1/2} Z} \neq 1 \quad \text{as } Z \neq 0.$$

and the LHS is

$$\frac{\prod \sin \frac{\pi R}{l}}{\prod \sin \frac{\pi N}{l}}.$$

To verify this we have

$$\frac{\prod(1-e^{2\pi i R/l})}{\prod(1-e^{2\pi i N/l})} = \frac{\prod -2i\, e^{i\pi R/l}}{\prod -2i\, e^{-i\pi N/l}} \cdot \frac{\prod \sin \pi R/l}{\prod \sin \pi N/l}.$$

$$= \frac{(-2i)^{\#R}\, e^{i\pi \sum R/\ell}}{(-2i)^{\#N}\, e^{i\pi \sum N/\ell}} \; \frac{\prod \sin \frac{\pi R}{\ell}}{\prod \sin \frac{\pi N}{\ell}}$$

The first factor is $e^{i\pi \frac{\sum R - \sum N}{\ell}}$ since $\#R = \#N$. Now,

~~$\sum R + \sum N = \frac{\ell(\ell-1)}{2}$ is divisible even when $\ell \equiv 1(4)$.~~

~~So $\sum R$ and $\sum N$ have the same parity so that~~

since $\ell \equiv 1\,(4)$, -1 is a residue and hence with R, $-R \equiv \ell - R$ is also a residue. Hence

$$\sum R = \sum (\ell - R) \;\; (4) \;\Rightarrow\; 2\sum R = \frac{\ell(\ell-1)}{2}$$

So $\sum R = \frac{\ell(\ell-1)}{4}$, $\sum N = (\sum R + \sum N) - \sum R = \frac{\ell(\ell-1)}{2} - \frac{\ell(\ell-1)}{4} = \frac{\ell(\ell-1)}{2}$.

Hence $\sum R = \sum N$, showing

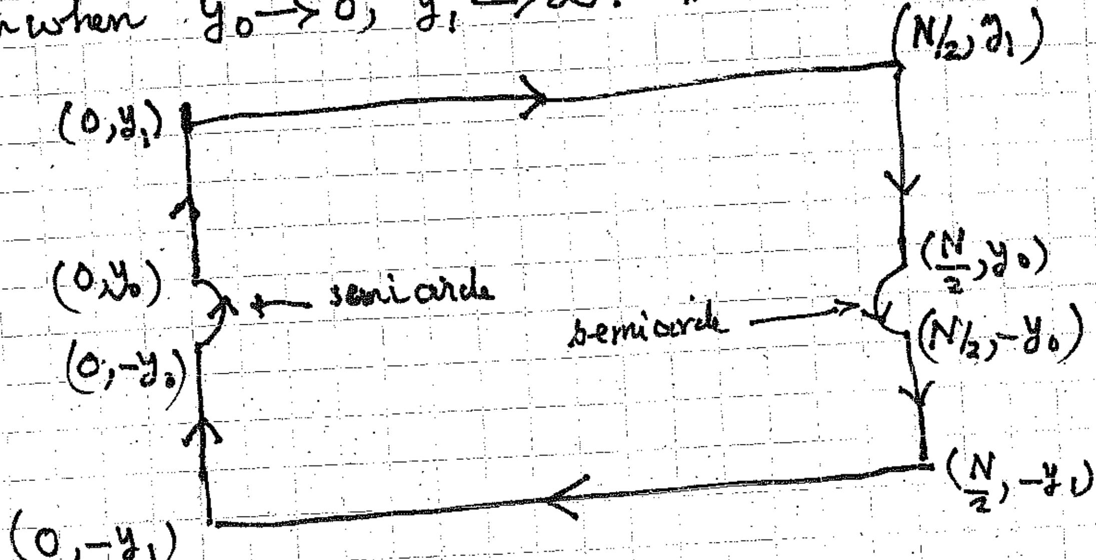
$$\frac{\prod(1-\zeta^R)}{\prod(1-\zeta^N)} = \frac{\prod \sin \pi R/\ell}{\prod \sin \pi N/\ell}.$$

Thus finally we have finished the proof $L(1:\chi) > 0$ for $\chi = \left(\frac{\cdot}{\ell}\right)$, ℓ an odd prime.

For a more elementary argument without using Galois theory of $\mathbb{Q}(\sqrt[\ell]{1})/\mathbb{Q}$, see after the next section.

Kronecker's evaluation of Gauss-Sum

Kronecker evaluated $\sum_{x=0}^{N-1} e^{2\pi i x^2/N}$ by integrating $e^{2\pi i z^2/N}/1-e^{2\pi i z}$ over a suitable contour and passing to the limit as the contour expands. Let $0 < y_0 < y_1$ be fixed; the contour will depend on these and N (fixed), and the limit is taken when $y_0 \to 0$, $y_1 \to \infty$. The contour is Γ:



The function has simple poles at $z = 1, \dots, [N/2]$ and the residue at $z = k$ is $e^{2\pi i k^2/N}/-2\pi i$. Hence by the residue theorem, (as the contour is negatively oriented,)

$$\cancel{\frac{1}{2\pi i}} \int_\Gamma = \left(+\sum_{1 \le k < \frac{N}{2}} e^{2\pi i k^2/N}\right) \qquad \text{as } y_0 \to 0$$

The integral on the semi-circle on the y-axis $\to -\frac{1}{2}\int$; the integral on the semicircle on $x = \frac{N}{2} \to 0$ if N is odd, $\to -\frac{1}{2} i^N$ if N is even. We write J to indicate 0 or $\frac{1}{2} i^N$ if N is odd or even.

Now $$\cancel{*}\, e^{2\pi i k^2/N} = e^{2\pi i (N-k)^2/N}$$

Hence
$$\sum_{1\le k<\frac{N}{2}} e^{2\pi i \frac{k^2}{N}} = \begin{cases} \frac{1}{2}\sum\limits_{1\le k\le N-1} e^{2\pi i k^2/N} & (N \text{ odd}) \\ \frac{1}{2}\sum\limits_{1\le k\le N-1} e^{2\pi i \frac{k^2}{N}} - \frac{1}{2} i^N \end{cases}$$

Or
$$\sum_{1\le k<\frac{N}{2}} e^{2\pi i \frac{k^2}{N}} = \frac{1}{2}\sum_{1\le k\le N-1} e^{2\pi i \frac{k^2}{N}} - \frac{1}{2}J = \frac{1}{2}g - \frac{1}{2} - \frac{1}{2}J.$$

~~Since~~ So $$\frac{1}{2\pi i}\int_\Gamma = \frac{1}{2}g - \frac{1}{2} - \frac{1}{2}J.$$

Since the semi circles contribute $-\frac{1}{2} - \frac{1}{2}J$ to the LHS, we get

$$\cancel{\frac{1}{2}g = P.V. \frac{1}{2\pi i}\int_{-y_1}^{y_1} + P.V.}\ \frac{1}{2}g =$$

$$= P.V. \int_{-y_1}^{y_1} \frac{e^{-2\pi i y^2/N}}{1-e^{-2\pi y}}\,(i\,dy)$$

$\frac{1}{2}g$ = sum of integrals on the vertical and horizontal lines, with the vertical integrals interpreted as principal values:

$$PV\int^{y_1} = \lim_{y_0\to 0+}\left(\int_{-y_1}^{-y_0} + \int_{y_0}^{y_1}\right) \quad \text{etc.}$$

We show first that the horizontal integrals $\to 0$ as $y_1 \to \infty$.

$$\left| \int_0^{N/2} \frac{e^{2\pi i (x+iy_1)^2/N}}{1-e^{2\pi i (x+iy_1)}} \, dx \right| \leq \int_0^{N/2} \frac{e^{-4\pi x y_1}}{1-e^{-2\pi y_1}} \, dx$$

$$= \frac{1}{1-e^{-2\pi y_1}} \cdot \left(\frac{1-e^{-2\pi N y_1}}{4\pi y_1} \right) \longrightarrow 0 \quad (y_1 \to \infty).$$

For the second horizontal integral, we use the substitution $x \mapsto \frac{N}{2} - x$.

$$\left| \int_0^{N/2} \frac{e^{\frac{2\pi i}{N}\left(\frac{N}{2}-x-iy_1\right)^2}}{1-e^{2\pi i\left(\frac{N}{2}-x-iy_1\right)}} \, dx \right| \leq \int_0^{N/2} \frac{e^{\frac{4\pi}{N}\left(\frac{N}{2}-x\right)y_1}}{e^{2\pi y_1}-1} \, dx$$

$$\leq \frac{e^{2\pi}}{e^{2\pi y_1}-1} \int_0^{N/2} e^{-\frac{4\pi}{N} x y_1} \, dx \leq \frac{N}{2} \frac{e^{2\pi}}{e^{2\pi y_1}-1} \longrightarrow 0.$$

We now take up the vertical integrals.

$$\text{P.V.} \int_{-y_1}^{y_1} \frac{e^{-2\pi i y^2/N}}{1-e^{-2\pi y}} (i\,dy) = \lim_{y_0 \to 0} \int_{y_0}^{y_1} e^{-\frac{2\pi i y^2}{N}} \left(\frac{1}{1-e^{-2\pi y}} + \frac{1}{1-e^{2\pi y}} \right) i\,dy$$

$$= \lim_{y_0 \to 0+} \int_0^{y_1} e^{-2\pi i \frac{y^2}{N}} \, i\,dy$$

Since $$\frac{1}{1-e^{-2\pi y}} + \frac{1}{1-e^{2\pi y}} = \frac{1}{1-e^{-2\pi y}} + \frac{e^{-2\pi y}}{e^{-2\pi y}-1}.$$

$$= \frac{1-e^{-2\pi y}}{1-e^{-2\pi y}} = 1.$$

So $$PV\int_{-y_1}^{y_1} = i\int_{\cancel{y_0}\,0}^{y_1} e^{-2\pi i \frac{y^2}{N}}\, dy.$$

For the integrals along $x = \frac{N}{2}$, we have

$$\lim_{y_0\to 0+}\left(\int_{y_1}^{y_0} + \int_{-y_0}^{-y_1} \frac{e^{\frac{2\pi i}{N}\left(\frac{N}{2}+iy\right)^2}}{1-e^{2\pi i\left(\frac{N}{2}+iy\right)}}\right)(i\,dy)$$

$$\cancel{=\lim_{y_0\to 0+}\int_{y_0}^{y_1} \frac{e^{\frac{2\pi i}{N}\left(\frac{N}{2}+iy\right)^2}}{1-e^{2\pi i\left(\frac{N}{2}+iy\right)}}\left(\frac{-1}{1-e^{2\pi i\left(\frac{N}{2}+iy\right)}}\right)}$$

$$\cancel{\lim_{y_0\to 0+}}\int_{y_1}^{y_0} \cancel{e^{\frac{2\pi i}{N}\left(\frac{N}{2}+iy\right)^2}}$$

$$\int_{y_1}^{y_0} + \int_{-y_0}^{-y_1} = -\int_{y_0}^{y_1} \frac{e^{\frac{2\pi i}{N}\left(\frac{N}{2}+iy\right)^2}}{1-e^{2\pi i\left(\frac{N}{2}+iy\right)}}(i\,dy) - \int_{y_0}^{y_1} \frac{e^{\frac{2\pi i}{N}\left(\frac{N}{2}-iy\right)^2}}{1-e^{2\pi i\left(\frac{N}{2}-iy\right)}}\, i\,dy$$

$$= -i\int_{y_0}^{y_1} \frac{i^N e^{-2\pi y}\, e^{-\frac{2\pi i y^2}{N}}}{1-(-1)^N e^{-2\pi y}}\,dy - i\int_{y_0}^{y_1} \frac{i^N e^{2\pi y}\, e^{-\frac{2\pi i y^2}{N}}}{1-(-1)^N e^{2\pi y}}\,dy.$$

For brevity let $(-1)^N = \varepsilon$. The above becomes

$$-i^{N+1} \cdot \int_{y_0}^{y_1} e^{-\frac{2\pi i y^2}{N}} \cdot \left(\frac{e^{-2\pi y}}{1-\varepsilon e^{-2\pi y}} + \frac{e^{2\pi y}}{1-\varepsilon e^{2\pi y}} \right) dy .$$

$$\frac{e^{-2\pi y}}{1-\varepsilon e^{-2\pi y}} + \frac{e^{2\pi y}}{1-\varepsilon e^{2\pi y}} = \frac{1}{e^{2\pi y}-\varepsilon} + \cancel{\frac{1}{e^{-2\pi y}-\varepsilon}} \frac{e^{2\pi y}}{1-\varepsilon e^{2\pi y}}$$

$$= \frac{1}{e^{2\pi y}-\varepsilon} + \frac{e^{2\pi y}\varepsilon}{\varepsilon - e^{2\pi y}} = \frac{1-\varepsilon e^{2\pi y}}{e^{2\pi y}-\varepsilon} = \frac{-\varepsilon\left(e^{2\pi y}-\varepsilon\right)}{e^{2\pi y}-\varepsilon} = -\varepsilon .$$

So the expression becomes

$$i^{N+1}(-1)^N \int_{0}^{y_1} e^{-\frac{2\pi i y^2}{N}} dy . \qquad \left(i^{N+1}(-1)^N = i \cdot i^N (-1)^N = i \cdot (-i)^N = i \cdot i^{-N} \right.$$

So the ~~4 endpoints~~ two vertical with respect to y add up to

$$y = \sqrt{N} \cdot u$$

$$\left(i + i^{1-N}\right) \int_{0}^{y_1} e^{-2\pi i \frac{y^2}{N}} dy = \left(i + i^{1-N}\right) \int_{0}^{y_1/\sqrt{N}} e^{-2\pi i u^2} \cdot \sqrt{N}\, du$$

~~Letting first $y_0 \to 0$ and then $y_1 \to \infty$ we get~~

$$\sqrt{N}\left(i + i^{1-N}\right) \int_{0}^{\infty} e^{-2\pi i u^2} du .$$

Hence generally

$$\mathcal{G} = 2\left(1 + i^{1-N}\right) \int_0^\infty e^{-2\pi i u^2}\, du \cdot \sqrt{N}$$

As before if we take $N = 1$,

$$1 = 2(i+1) \int_0^\infty e^{-2\pi i u^2}\, du$$

$$\Rightarrow \int_0^\infty e^{-2\pi i u^2}\, du = \frac{1}{2(1+i)}.$$

So $$\mathcal{G} = \frac{1 + i^{1-N}}{(1+i)} \sqrt{N} = \frac{1 + i^{-N}}{1 + i^{-1}} \sqrt{N}.$$

<u>Finite expressions for $L(1:\chi)$ when $l \equiv 3\ (4)$</u>.

$$L(1:\chi) = \frac{-\pi}{l^{3/2}} \left(\Sigma R - \Sigma N \right)$$

where $\mathbb{Z}_l^\times$ is identified with $\{1, 2, \ldots, l-1\}$. Since $L(1:\chi) > 0$, we must have $\Sigma R < \Sigma N$.

<u>Example</u> $l = 3$ $\{R\} = \{1\}$ $\{N\} = \{2\}$. $L = \dfrac{\pi}{3\sqrt{3}}$

$l = 19$. $\{R\} = \{1, 4, 9, 16, 6, 17, 11, 7, 5\}$ $\{N\} = \{2, 8, 18, 13, 12, 15, 3, 14, 10\}$

(70).

$\sum R = 76 \quad \sum N = 95 \quad \sum R + \sum N = 171 \; (= 19 \times 9)$

$$L(1:\chi) = \cancel{\sqrt{19}\cdot\pi}\cdot\frac{\pi}{\sqrt{19}}$$

Dirichlet had alternative formulae for $L(1:\chi)$ which reduced the calculations enormously. We start with $l \equiv 3 \, (4)$ and

$$L(1:\chi) = \frac{\pi}{l^{3/2}}\left(\sum_{(0,l)} N - \sum_{(0,l)} R\right)$$

We now distinguish between 2 cases

$l \equiv 7 \, (8) \quad \left(\frac{2}{l}\right) = 1 \qquad l \equiv 3 \, (8) \quad \left(\frac{2}{l}\right) = -1.$

$l \equiv 7 \, (8)$ Since $\left(\frac{2}{l}\right) = 1$, a is $R \, (N) \iff 2a$ is $R \, (N)$.

Hence

$$\sum_{(0,l)} R = 2\sum_{(0,l/2)} R + \sum_{(\frac{l}{2},l)} (2R - l) = 2\sum_{(0,l/2)} R + 2\sum_{(\frac{l}{2},l)} R - l \, \#_{(\frac{l}{2},l)} R$$

$$= 2\sum_{(0,l)} R - l \, \#_{(\frac{l}{2},l)} R$$

[if x is R, $\frac{l}{2} < x < l$, $2x \equiv 2x - l$

Similarly $\sum_{(0,l)} N = 2\sum_{(0,l)} N - l. \#_{(\frac{l}{2},l)} N$.

$$\boxed{L(1:\chi) = \frac{\pi}{l^{1/2}}\left(\#_{(\frac{l}{2},l)} N - \#_{(\frac{l}{2},l)} R\right)}$$

Hence $\sum_{(0,l)} N - \sum_{(0,l)} R = l.\left\{\#_{(\frac{l}{2},l)} N - \#_{(\frac{l}{2},l)} R\right\}$

So

$$L(1:\chi) = \frac{\pi}{\sqrt{l}}\left\{\#_{(\frac{l}{2},l)} \text{n-res} - \#_{(\frac{l}{2},l)} \text{res}\right\} = -\frac{\pi}{\sqrt{l}}\sum_{1/2\, l < m < l}\left(\frac{m}{l}\right).$$

~~Since $\left(\frac{1}{\ell}\right) = -1$, $x \mapsto -x$ changes R to N and vice versa.~~

~~Now~~

$$\#\underset{(0,\frac{1}{2}\ell)}{N} + \#\underset{(\frac{1}{2}\ell,\ell)}{N} = \#\underset{(0,\ell)}{N} \qquad x \mapsto -x$$

$$\#\underset{(-\frac{1}{2}\ell,0)}{R} + \#$$

Example: $\ell = 31$.

Res: 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8

N. res: 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30

$$\sum N - \sum R = 279 - 186 = 93. \qquad L(1:\chi) = \pi\cdot\frac{3}{\sqrt{31}}.$$

$$(\tfrac{1}{2}\ell, \ell) = [16,30]: \quad \#\text{N. Res} = 9 - 6 = 3. \qquad L(1:\chi) = \pi\cdot\frac{3}{\sqrt{31}}.$$

$\underline{\ell \equiv 3\ (8)}$ $\quad \left(\frac{2}{\ell}\right) = -1 \quad \left(\frac{-1}{\ell}\right) = -1.$

x is $R \iff 2x$ is N, $\quad x$ is $N \iff 2x$ is R.

$\qquad 2x-\ell$ is $N \qquad\qquad 2x-\ell$ is R.

$$\sum_{(0,\ell)} R = 2\sum_{(0,\ell)} N - \ell\cdot\#\underset{(\frac{\ell}{2},\ell)}{N} \Rightarrow 2\sum_{(0,\ell)} N - \sum_{(0,\ell)} R = \ell\,\#\underset{(\frac{\ell}{2},\ell)}{N}.$$

$$\sum_{(0,\ell)} N = 2\sum_{(0,\ell)} R - \ell\cdot\#\underset{(\frac{\ell}{2},\ell)}{R} \Rightarrow 2\sum_{(0,\ell)} R - \sum_{(0,\ell)} N = \ell\,\#\underset{(\frac{\ell}{2},\ell)}{R}$$

Subtracting, $3\left(\sum_{(0,\ell)} N - \sum_{(0,\ell)} R\right) = \ell\left[\#\underset{(\frac{\ell}{2},\ell)}{N} - \#\underset{(\frac{\ell}{2},\ell)}{R}\right].$

$$L(1:\chi) = \frac{\pi}{3\sqrt{\ell}} \left\{ \#_{(\frac{1}{2},\ell)} N - \#_{(\frac{\ell}{2},\ell)} R \right\}$$

Example $\ell = 19$

R: 1, 4, 9, 16, 6, 17, 11, 7, 5,

N: 2, 3, 8, 10, 12, 13, 14, 15, 18 $\quad \Sigma N - \Sigma R = 95 - 76 = 19$

$$L = \frac{\pi}{\sqrt{19}}$$

$$\#_{(\ell/2,\ell)} R = \#_{[10,18]} R = 3 \qquad L(1:\chi) = \frac{\pi}{\sqrt{19}}.$$

$$\#_{[10,18]} N = 6.$$

Final expression

$\ell \equiv 7\ (8)$
$$L(1:\chi) = \frac{\pi}{\ell^{1/2}} \left\{ \#_{(\ell/2,\ell)} N - \#_{(\ell/2,\ell)} R \right\}.$$

$\ell \equiv 3\ (8)$
$$L(1:\chi) = \frac{\pi}{3\sqrt{\ell}} \left\{ \#_{(\ell/2,\ell)} N - \#_{(\frac{\ell}{2},\ell)} R \right\}$$

Elementary proof without using Galois theory for $L(1:\chi) \neq 0$, $\ell \equiv 1 (4)$.

(a la Davenport)

It is a question of proving that

$$\frac{\prod(1-\zeta^R)}{\prod(1-\zeta^N)} \neq 1.$$

Introduce

$$\eta_0 = \sum \zeta^R \qquad \eta_1 = \sum \eta^N.$$

We first evaluate η_0, η_1, using the value of $\mathcal{G}$. We have

$$\eta_0 + \eta_1 = \sum_{r=1}^{\ell-1} \zeta^r = -1.$$

$$\eta_0 - \eta_1 = \mathcal{G} = \ell^{1/2}$$

Hence $\eta_0 = \dfrac{-1+\sqrt{\ell}}{2}$ $\qquad \eta_1 = \dfrac{-1-\sqrt{\ell}}{2}$.

We have to use the irreducibility of $T^{\ell-1} + \dots + T + 1$ which shows that $\deg[\mathbb{Q}(\sqrt[\ell]{1}) : \mathbb{Q}] = \ell - 1$. So elements of $\mathbb{Q}(\sqrt[\ell]{1})$ are unique linear combinations

$$a_1\zeta + \dots + a_{\ell-1}\zeta^{\ell-1} \qquad (a_j \in \mathbb{Q}).$$

Consider now a polynomial expression

$$F(\zeta) = \sum_{r=1}^{\ell-1} a_r \zeta^r \qquad (a_r \in \mathbb{Z})$$

and suppose that

$$F(\zeta^m) = F(\zeta) \quad \forall \text{ residues } m.$$

Then

$$\sum a_r \zeta^r = \sum a_r \zeta^{rm} \quad \forall \text{ residues } m$$

$$\implies \quad a_r = a_s \quad \text{whenever } r = sm \text{ for some residue } m.$$

Hence

$$F(\zeta) = \cancel{a_0\eta_0} \; A_0 \eta_0 + A_1 \eta_1 \qquad (*)$$

where $A_0 = a_1$ and $A_1 = a_r$ for some nonresidue r.

If now F depends on an indeterminate X, so that

$$F(X:\zeta) = F(\zeta) = \sum_1^{l-1} a_r(X)\zeta^r$$

where the $a_r \in \mathbb{Z}[X]$. Then the formula $(*)$ is true for all integer values of X, hence identically true.

So $\quad F(X:\zeta) = A_0(X)\eta_0 + A_1(X)\eta_1$

where $A_0, A_1 \in \mathbb{Z}[X]$. If m' is a nonresidue,

$$F(X:\zeta^{m'}) = A_1(X)\eta_0 + A_0(X)\eta_1$$

since $\eta_0^{m'} = \eta_1$, $\eta_1^{m'} = \eta_0$. So

$$F(X:\zeta) = \prod (X-\zeta^R) = B_0(X)\eta_0 + B_1(X)\eta_1$$

$$G(X:\zeta) = \prod (X-\zeta^N) = B_1(X)\eta_0 + B_0(X)\eta_1$$

where $B_0, B_1 \in \mathbb{Z}[X]$. So if $B_j(1) = b_j$

$$\frac{\prod(1-\zeta^R)}{\cancel{\prod(1-\zeta^N)}} = \frac{b_0\eta_0 + b_1\eta_1}{\cancel{b_1\eta_0 + b_0\eta_1}}, \quad \prod(1-\zeta^N) = b_1\eta_0 + b_0\eta_1.$$

$$b_0\eta_0 + b_1\eta_1 = b_0\left(\frac{-1+\sqrt{l}}{2}\right) + b_1\left(\frac{-1-\sqrt{l}}{2}\right)$$

$$= (Y + Z\sqrt{l})/2 \qquad Y = -(b_0+b_1), \; Z = (b_0 - b_1)$$

$$b_1\eta_0 + b_0\eta_1 = b_1\left(\frac{-1+\sqrt{l}}{2}\right) + b_0\left(\frac{-1-\sqrt{l}}{2}\right) = \frac{Y - Z\sqrt{l}}{2}, \; Y, Z \in \mathbb{Z}.$$

$Y, Z \in \mathbb{Z}$

$$\text{So} \quad \cancel{\frac{\prod(1-\zeta^R)}{\prod(1-\zeta^N)} = \frac{Y+Z\sqrt{l}}{Y-Z\sqrt{l}}}.$$

~~Moreover~~ So $\prod(1-\zeta^R) = \frac{1}{2}(Y + Z\sqrt{l})$

$$\prod(1-\zeta^N) = \frac{1}{2}(Y - Z\sqrt{l}).$$

But $\prod(1-\zeta^R)\prod(1-\zeta^N) = \prod_1^{l-1}(1-\zeta^r) = (T^{l-1} + \dots + T + 1)\Big|_{T=1} = l.$

If $Z = 0$, $Y^2 = 4l$, impossible. So $Z \neq 0$. Hence

$$\prod(1-\zeta^R)/\prod(1-\zeta^N) = \frac{Y+Z\sqrt{l}}{Y-Z\sqrt{l}} \neq 1.$$

Stern's real variable proof for $L(1:\chi)\neq 0$, arbitrary modulus N

This depends on two elementary ideas:

a) Approximating sums by integrals

b) Dirichlet or hyperbolic summation.

<u>Approximation</u> Let f be continuous, ~~strictl~~ strictly decreasing, and $f(x)\to 0$ as $x\to+\infty$. Then $\exists$ a constant $\gamma(f)$, $0<\gamma(f)<1$, such that

$$\sum_{n\leq x} f(n) = \int_1^x f(t)\,dt + \gamma(f) + O(f(x)) \quad (x\to\infty).$$

<u>Proof</u> We have

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

Let $\gamma_n = f(n) - \int_n^{n+1} f(t)\,dt$. Then $0<\gamma_n< f(n)-f(n+1)$.

So $\sum \gamma_n =: \gamma(f)$ is convergent and $0<\gamma(f)<f(1)$. So

Then $\sum_1^N \gamma_n = \gamma(f) - \sum_{N+1}^{\infty}\gamma_n = \gamma(f) - O(f(N+1))$.

$$\sum_1^N f(n) = \int_1^{N+1} f(t)\,dt + \gamma(f) + O(f(N+1))$$

So $$\sum_{n\leq x} f(n) = \int_1^{[x]+1} f(t)\,dt + \gamma(f) + O(f([x]+1))$$

$$= \int_1^x f(t)\,dt + \int_x^{[x]+1} f\,dt + \gamma(f) + O(f(x))$$

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

<u>COR 1</u> $\displaystyle\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$

where $0 < \gamma < 1$ is a constant (Euler's constant)

<u>Pf</u> Take $f(x) = \dfrac{1}{x}$.

<u>COR 2</u> Let $0 < r < 1$. Then there is a constant $c = c_r$ such that

$$\sum_{n \leq x} \frac{1}{n^r} = \frac{1}{1-r} x^{1-r} + c + O\left(\frac{1}{x^r}\right).$$

For $r = \frac{1}{2}$

$$\sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + c + O\left(\frac{1}{\sqrt{x}}\right)$$

<u>Pf</u> Take $f(x) = \dfrac{1}{x^r}$. Then

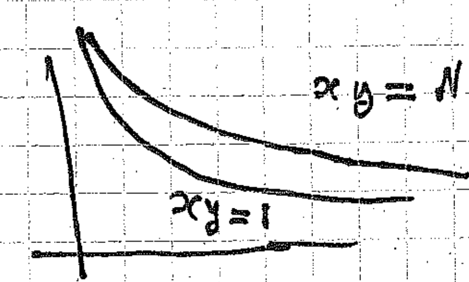
$$\sum_{n \leq x} \frac{1}{n^r} = \int_1^x \frac{dt}{t^r} + \gamma(f) + O(f(x))$$

$$= \frac{1}{1-r} x^{1-r} + c + O\left(\frac{1}{x^r}\right).$$

Hyperbolic sums $\quad L = \{(m,n) \mid m,n \text{ integers} \geq 1\}$.

Let $F(m,n)$ be a function (complex-valued) defined on L.

Let



$$S_N = \sum_{1 \leq mn \leq N} F(m,n)$$

This is hyperbolic or Dirichlet sum. We can sum this also vertically and horizontally.

$$S_N = \sum_{1 \leq k \leq N} \sum_{mn=k} F(m,n)$$

$$= \sum_{1 \leq m \leq N} \Big(\sum_{1 \leq n \leq \frac{N}{m}} F(m,n) \Big) \quad \text{(Ver)}$$

$$= \sum_{1 \leq n \leq N} \Big(\sum_{1 \leq m \leq \frac{N}{n}} F(m,n) \Big) \quad \text{(Hor.)}$$

Application to Dirichlet's divisor problem

$d(k) = \#$ of divisors of k.

$d(k)$ is very irregular in k; for instance $d(p)=2$, p prime while $d(p^r) = r+1 \to \infty$ if $r \to \infty$.

Thm (Dirichlet)

$$\frac{d(1) + \cdots + d(N)}{N} = \log N + (2\gamma - 1) + O\left(\frac{1}{N^{1/2}}\right)$$

where γ is Euler's constant.

Remark: This does not mean $d(k)$ is of the order of $\log k$ most of the time; the order is about ~~$(\log k)^{.6}$~~ $\approx 2^{\log\log k}$

$\approx (\log k)^{.6}$.

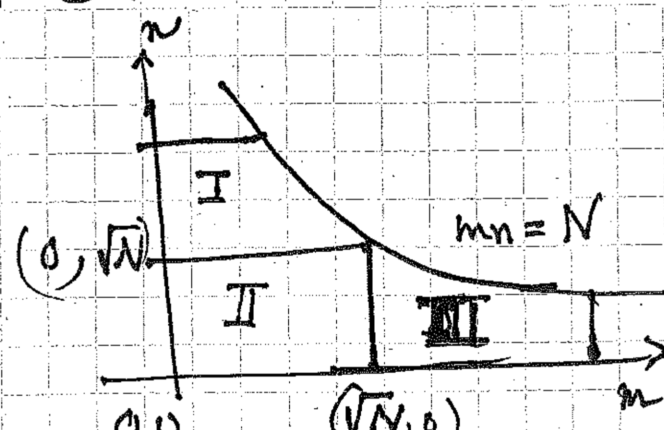
Here $F(m,n) = 1$. So

$$S_N = \sum_{k=1}^{N} d_k = \sum_{1 \le mn \le N} 1.$$

$$= \sum_{1\le m\le N}\ \sum_{1\le n\le \frac{N}{m}} 1 = \sum_{1\le m\le N}\left(\frac{N}{m} + O(1)\right)$$

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

So $\dfrac{d(1)+\dots+d(N)}{N} = \log N + O(1)$.



We need to refine this a bit.

$$S_N = S_I + S_{II} + S_{III}$$

$S_I = S_{III}$ by symmetry.

So

$$S_N = 2S_I + S_{II} = 2(S_I + S_{II}) - S_{II}.$$

$$S_I + S_{II} = \sum_{1\le m\le\sqrt{N}}\ \sum_{1\le n\le\frac{N}{m}} 1 \qquad \text{(Vert)}$$

$$= \sum_{1 \le m \le \sqrt{N}} \left(\frac{N}{m} + O(1) \right)$$

$$= N \left(\log N^{1/2} + \gamma + O\left(\frac{1}{N}\right)\right) + O(N^{1/2})$$

~~So~~ $= \frac{N}{2} \log N + N\gamma + O(N^{1/2})$.

$$S_{II} = [N^{1/2}]^2 = N + O(N^{1/2}).$$

Hence $\frac{d(1) + \dots + d(N)}{N} = \log N + (2\gamma - 1) + O(N^{-1/2})$.

The Dirichlet divisor problem is the determination of the exact order of the error term. Writing it as $O(N^{-\beta})$, we know $\beta \geq 1/2$. Hardy-Littlewood showed $\beta \leq 3/4$.

Exact value of β is unknown.

For $L(1:\chi)$ Stein uses

$$F(m,n) = \frac{\chi(n)}{\sqrt{mn}}.$$

<u>Theorem</u> a) $S_N \geq c \log N$ where c is a constant > 0

b) $S_N = 2N^{1/2} L(1:\chi) + O(1)$.

<u>Cor</u> $L(1:\chi) \neq 0$

<u>Proof</u> If $L(1:\chi) = 0$, b) $\Rightarrow S_N = O(1)$, contradicting a).

<u>Proof of Theorem</u> a) Note first that

$$\sum_{mn=k} F(m,n) = \frac{1}{k^{1/2}} \sum_{n|k} \chi(n).$$

We need a lemma.

<u>Lemma</u>
$$\sum_{n|k} \chi(n) \geq \begin{cases} 0 & \text{always} \\ 1 & \text{if } k = \ell^2 \end{cases}$$

<u>Proof of Lemma</u> For $k = p^a$,

$$\sum_{n|k} \chi(n) = 1 + \chi(p) + \chi(p)^2 + \dots + \chi(p)^a = \begin{cases} a+1 & \chi(p) = 1 \\ 1 & \chi(p) = -1 \\ & a \text{ even} \\ 0 & \chi(p) = -1 \\ & a \text{ odd} \\ 1 & \chi(p) = 0 \ (p|N) \end{cases}$$

$k = \prod p_j^{a_j}$ then

$$\sum_{n|k} \chi(n) = \sum_{0 \leq b_j \leq a_j} \chi(p_1)^{b_1} \dots \chi(p_r)^{b_r}$$

$$= \prod_j (1 + \chi(p_j) + \dots + \chi(p_j)^{a_j}) \geq 0.$$

If $k = \ell^2$ all a_j even, hence this is ≥ 1.

From lemma,

$$S_N \ge \sum_{k=l^2,\, l\le\sqrt{N}} \frac{1}{k^{1/2}} = \sum_{l\le\sqrt{N}} \frac{1}{l} \ge c\log N \quad \text{for}$$

some constant $c>0$. To proceed further write as before

$$S_N = S_{I} + S_{II} + S_{III}$$

Lemma If $0<a<b$,

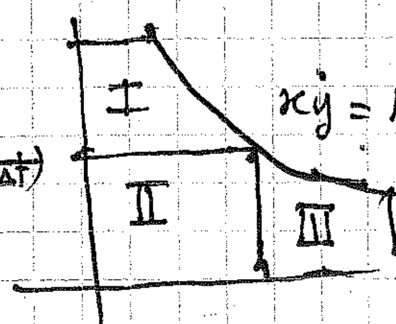
$$\sum_{n=a}^{b} \frac{\chi(n)}{n^{1/2}} = O(a^{-1/2}) \qquad \sum_{n=a}^{b} \frac{\chi(n)}{n} = O(a^{-1})$$

Pf Use Partial summation and $|\sum \chi(n)| = O(1)$.

Then
$$\sum_{a\le}^{b} \frac{\chi(n)}{n^{1/2}} = \sum_{a}^{b} O(1)\left(\frac{1}{n^{1/2}} - \frac{1}{(n+1)^{1/2}}\right) \cancel{= O(a^{-1/2})}$$
$$+ O(1)\cdot b^{-1/2}$$

$$= O(a^{-1/2}).$$

Similarly for the second.



$$S_{I} = \sum_{m<N^{1/2}} \frac{1}{m^{1/2}}\left(\sum_{N^{1/2}<n\le \frac{N}{m}} \frac{\chi(n)}{n^{1/2}}\right) \cancel{O(1)(\text{vert})}$$

$$\cancel{S_{II}+S_{III}\ (\text{hor}) = \sum_{1\le n\le N^{1/2}} \frac{\chi(n)}{\sqrt{n}}} = \sum_{m<N^{1/2}} \frac{1}{m^{1/2}}\, O(N^{-1/4}) \rightarrow \text{unif in } m$$

$$= O(N^{-1/4})\left(2N^{1/4} + O(1)\right) = O(1).$$

$$S_{\text{II}} + S_{\text{III}} = \sum_{1\le n\le \sqrt{N}} \frac{\chi(n)}{n^{1/2}} \sum_{m \le \frac{N}{n}} \frac{1}{\sqrt{m}}$$

$$= \sum_{1\le n\le \sqrt{N}} \frac{\chi(n)}{n^{1/2}} \left(2\left(\frac{N}{n}\right)^{1/2} + c + O\left(\left(\frac{n}{N}\right)^{1/2}\right)\right)$$

$$= 2N^{1/2} \sum_{1\le n\le \sqrt{N}} \frac{\chi(n)}{n} + c \underbrace{\sum_{1\le n\le\sqrt{N}} \frac{\chi(n)}{n^{1/2}}}_{\downarrow \; O(1)} + \underbrace{O\left(\frac{1}{N^{1/2}} \sum_{1\le n\le N^{1/2}} 1\right)}_{\downarrow \; O(1)}$$

$$= 2N^{1/2}\left(L(1:\chi) - \sum_{n>\sqrt{N}} \frac{\chi(n)}{n}\right) + O(1)$$

$$= 2N^{1/2} L(1:\chi) - 2N^{1/2} \cdot O(N^{-1/2}) + O(1)$$

$$= 2N^{1/2} L(1:\chi) + O(1).$$