primes — infinitely many primes. / then: $\equiv a \ (q)$ for q prime.
$\gcd(a,q)=1$.

Riemann zeta function

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

convergent for $Re(s) > 1$.
(assume $s \in \mathbb{R}$ for now)

Use any convergence test., e.g. integral test.

Another representation: $\zeta(s) = \prod_p (1-p^{-s})^{-1}$

$$= \prod_p (1 + p^{-s} + p^{-2s} + \cdots)$$

(show this expression is convergent: Take partial products over primes $p \le N$. then take limit as $N \to \infty$)

Follows from unique fact. into primes that two representations are equal.

$$\log(\zeta(s)) = \sum_p \sum_{m=1}^{\infty} m^{-1} \cdot p^{-ms}$$

since $-\log(1-x) = \sum_{m=1}^{\infty} \frac{x^m}{m}$.

now for $m \geq 2$, have

$$\sum_p \sum_{m \geq 2} m^{-1} p^{-ms} < \sum_p \sum_{m \geq 2} p^{-m} = \sum_p \frac{1}{p \cdot (p-1)} < 1.$$

provided $s > 1$.

hence

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

$\Rightarrow$ since, in $\lim_{s \to 1^+}$, LHS $\to \infty$, RHS $\to \infty$.

i.e. $\sum_p p^{-s} \to \infty$ as $s \to 1^+$, i.e. $\sum_p \frac{1}{p}$ diverges.

Dirichlet: mimic this proof for primes $p \equiv a \ (q)$, q: prime.

somehow end up with $\sum_{\substack{p \\ p \equiv a\,(q)}} \frac{1}{p}$ on RHS, LHS: divergent function, prove divergent using $\zeta(s)$.

Idea: use characters mod q.

(seen examples of characters mod q. Power residue symbols, trivial character.)

Stated that they form a group under mult. Investigate further.

Pick primitive root g (mod q). then any n (mod q) is power of g: $g^{v(n)} \equiv n \ (q)$ $v(n)$: index of n.

(depends on choice of primitive roots)

e.g. mod 7: $\phi(6) = 2$ prim. roots. 3, 5

if $n = 2$, $3^2 \equiv 2 \ (7)$ $v_3(2) = 2$

$5^4 \equiv 2 \ (7)$ $v_5(2) = 4$.

then given fixed choice of prim. root g. Take complex $(q-1)^{st}$ rt. of unity: ω

Define: $\chi(n) = \omega^{v(n)}$ (or better: $\omega^{v_g(n)}$)

(this for $(n, q) = 1$. sometimes extend to all $n \in \mathbb{Z}$ with $\chi(n) = 0$ if $q \mid n$)

Note: ω: need not be primitive $(q-1)^{st}$ rt. of unity.

Any choice of ω gives a character.

$\omega = (-1)$ gives Legendre symbol. $\omega = 1$ gives trivial character.

so have $q-1$ different characters mod q.

(note they are characters since if $n \equiv n_1 n_2 \pmod q$ then

$$v(n) \equiv v(n_1) + v(n_2) \pmod{q-1}$$

i.e. $$\omega^{v(n)} = \omega^{v(n_1)+v(n_2)} = \omega^{v(n_1)} \omega^{v(n_2)}$$

so $$\chi(n) = \chi(n_1)\chi(n_2) \quad \text{as desired}$$)

Do we get (yet more) characters by choosing different primitive roots?

no. e.g. $\omega = \zeta_6$ $\quad \chi(n) = (\zeta_6)^{v_3(n)}$

Can find an ζ_6^i s.t. $\chi(n) = (\zeta_6^i)^{v_5(n)}$? HW.
i with

Key property: $\displaystyle\sum_{\chi} \chi(n) = 0$ if $n \not\equiv 0 \ (q)$.

idea $$\sum_{\chi} \chi(n) = \sum_{\omega} \omega^{v(n)}$$. But know $\displaystyle\sum_{\omega} \omega^k$, for any k,

so

$$= \begin{cases} 0 & \text{if } n \not\equiv 1 \ (q) \\ q-1 & \text{if } n \equiv 1 \ (q) \end{cases} = \begin{cases} 0 & \text{if } ~~\quad~~ q-1 \nmid k \\ q-1 & \text{if } k \equiv 0 \ (q-1). \end{cases}$$

Sneaky idea: Consider

$$\sum_{\chi} \bar{\chi}(a) \cdot \chi(n) = \sum_{\omega} \omega^{-v(a)} \cdot \omega^{v(n)} = \begin{cases} 0 & \text{if } n \equiv a \pmod q \\ q-1 & \text{if } n \not\equiv a \pmod q \end{cases}$$

Sketch of Dirichlet's pf. :

Consider $$L_\omega(s) = \sum_{\substack{n=1 \\ (n \not\equiv 0\ (q))}}^{\infty} \frac{\omega^{\nu(n)}}{n^s} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

$|\chi(n)| = 1$, so conv. for $Re(s) > 1$. Moreover, $\omega^{\nu(n)}$ is a multiplicative function, so we may write:

$$L_\omega(s) = \prod_{\substack{p:\text{prime} \\ p \neq q}} (1 - \omega^{\nu(p)} p^{-s})^{-1}, \quad \text{for } s > 1.$$

(check that $|\omega^{\nu(p)} p^{-s}| = p^{-s} < 1/2$ when $s > 1$

so no terms in prod. are 0, hence $L_\omega(s) \neq 0$ for $s > 1$).

Take log's again:

$$\text{Log } L_\omega(s) = \sum_{p \neq q} \sum_{m=1}^{\infty} m^{-1} \omega^{\nu(p^m)} p^{-ms}$$

Consider: $$\frac{1}{q-1} \cdot \sum_{\omega} \omega^{-\nu(a)} \cdot \text{Log } L_\omega(s)$$

$$= \sum_{\substack{p \\ p^m \equiv a\ (q)}} \sum_{m=1}^{\infty} m^{-1} p^{-ms}$$

estimate away terms with $m \geq 2$. leaves sum we want.

Just need to show :

$$\frac{1}{q-1} \cdot \sum_{\omega} \omega^{-\nu(a)} \cdot \log L_\omega(s) \longrightarrow \infty \quad \text{as} \quad s \to 1^+ .$$

this will prove $\sum_{p \equiv a (q)} \frac{1}{p}$ divergent.

On LHS : taking $\omega = 1$ gives $\log (L_1(s))$ where

$$L_1(s) = \sum_{\substack{n=1 \\ q \nmid n}}^{\infty} \frac{1}{n^s} = \prod_{p \nmid q} (1 + p^{-s} + \cdots) = (1 - q^{-s}) \cdot \zeta(s) .$$

so if $\zeta(s) \to \infty$, as $s \to 1^+$, $L_1(s) \to \infty$ as $s \to 1^+$. $\left(1 - q^{-s} \to 1 - \frac{1}{q}\right)$

Remains to show : $\lim_{s \to 1^+} \log (L_\omega(s))$ doesn't screw this up. (i.e. is bounded as $s \to 1^+$)

use a little analysis to reformulate this question :

Claim : $L_\omega(s)$, $\omega \neq 1$, is convergent for $s > 0$ .. (not just $s > 1$).

Use Dirichlet's test for convergence : $\sum_{n=1}^{m} a_n$ bounded, not ind. terms.

Given $\{a_n\}_{n=1}^{\infty}$: bounded $\{b_n\}_{n=1}^{\infty}$: decreasing, limit 0.

then $\sum_{n=1}^{\infty} a_n \cdot b_n$ converges.

Let $b_n = n^{-s}$. $a_n = \omega^{\nu(n)}$. Note that sums $\sum_{n=1}^{m} \omega^{\nu(n)}$

are bounded since the sum over any $q-1$ consecutive integers $= 0$.
(complete residue class)

In fact, uniformly convergent w.r.t. s

for any $s \geq \delta > 0$ (bounded away from 0). So

enough to show $L_\omega(1) \neq 0$

<u>Cases</u> : ω not real $(\omega \neq 1,-1)$, ω real $(\omega = -1)$.

$\boxed{\text{Suppose } \omega \text{ complex}}$ Set $a = 1$ in our earlier equation :

$$\frac{1}{q-1} \sum_{\omega} \log(L_\omega(s)) = \sum_{\substack{p \\ p^m \equiv 1 \, (q)}} \sum_{m=1}^{\infty} m^{-1} p^{-ms}$$

RHS has all positive terms. $\Rightarrow$ $\sum_{\omega} \log(L_\omega(s)) \geq 0$.

i.e. $\prod_{\omega} L_\omega(s) \geq 1$, for any $s > 1$.

---

if $\exists$ ω (not real) with $L_\omega(1) = 0$, then $L_{\bar{\omega}}(1) = 0$, with

$\bar{\omega}$: complex conj. (since , for s real , $L_{\bar{\omega}}(1) = \overline{L_\omega(1)}$.)

<u>conclusion</u> : 2 factors in $\prod_{\omega}$ have limit 0 as $s \to 1^+$.

1 factor , $L_1(s)$, has limit ∞ as $s \to 1^+$.

other factors bounded , so could contribute 0 .

<u>idea</u> : 2^+ factors of $\prod_{\omega}$ with limit 0 will win out over $L_1(s)$ with ~~[illegible]~~ limit ∞ .

giving contradiction to fact that

$\prod_{\omega} L_\omega(s) \geq 1$ for any $s > 1$. (taking limit of both sides)

need to analyze behavior at $s = 1$ further :

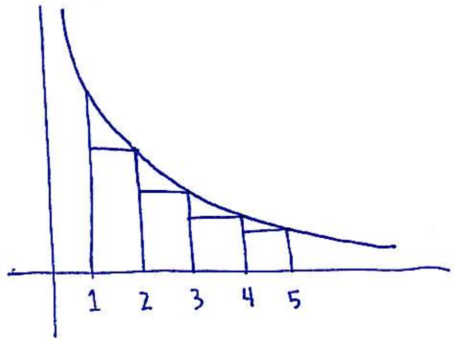
<u>Want</u> $L_1(s) < \frac{c}{s-1}$, some constant .

Know $L_1(s) = (1 - q^{-s}) \zeta(s) < (1 - q^{-2}) \zeta(s)$, and

for $s \in (1,2)$

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

picture :



so take $c = 2 \cdot \left(1 - \frac{1}{q^2}\right)$

bounded $L_1(s)$ in range

$1 < s < 2$.

For $L_\omega(s)$, show $|L_\omega(s)| < c_2 \cdot (s-1)$. (same for $\bar{\omega}$)

mean value thm : $\exists\ s_1 \in (1, s)$ with

$$\frac{L_\omega(s) - L_\omega(1)}{s-1} = L'_\omega(s_1).$$

so if $L_\omega(1) = 0$, we have $L_\omega(s) = (s-1)\, L'_\omega(s_1)$

Suffices to show $|L'_\omega(s_1)|$ bounded to get our claim.

But by similar methods as before,

$$L'_\omega(s) = -\sum_{\substack{n=1 \\ n \not\equiv 0\,(q)}}^{\infty} \omega^{v(n)} \cdot (\log n)\, n^{-s}$$

again unif. conv. for $s \geq \delta > 0$ by Dirichlet's test since $\log n / n^{+s}$ decreasing for n suff. large. with limit 0.

$\Rightarrow$ $L'_\omega(s)$ continuous, for $s > 0$.

$\Rightarrow$ $|L'_\omega(s)|$ bounded.

Putting these into our product $\prod_\omega L_\omega(s) \geq 1$, taking limits,

gives contradiction. (LHS $= 0$ in abs. value.)

if ω real, i.e. $\omega = -1$, then $L(s,-1) = \sum_{n=1}^{\infty} \frac{\left(\frac{n}{q}\right)}{n^s}$ $(*)$

where $\left(\frac{n}{q}\right)$ is the Legendre symbol. (call this $L(s)$ for simplicity)

We must show $L(1) \neq 0$. (know $L(1) \geq 0$ since $L(s)$ continuous @ $s=1$ and Euler product shows $L(s) > 0$ for $s > 1$.)

Plan : use Gauss sums to express $\left(\frac{n}{q}\right)$, then have $L(s)$ as double sum. interchange orders of summation.

Recall that $g(n,q) \overset{\text{def.}}{=} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) e^{2\pi i m n/q}$ ($e^{2\pi i/q}$: q^{th} root of unity)

and $g(n,q) = \left(\frac{n}{q}\right) \cdot g(1,q)$.

i.e. $\left(\frac{n}{q}\right) = \frac{1}{g(1,q)} \cdot \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) e^{2\pi i m n/q}$. Substitute into $(*)$

[seems like no advantage here, but recall Gauss determined exact value of this sum. (We showed $|g(1,q)| = \sqrt{q}$, at least $\neq 0$ so expression well-defined.)]

Interchanging orders of summation:

$$L(1) = \frac{1}{g(1,q)} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \sum_{n=1}^{\infty} \frac{1}{n} e^{2\pi i m n/q}$$

Remember $-\log(1-x) = \sum_{n=1}^{\infty} \frac{1}{n} x^n$. Makes sense as complex series as well. (radius of conv. < 1 as real series conv. @ -1, div. @ 1)

As complex series, conv. for any z, $|z| \leq 1$ with $z \neq 1$.

$$\text{so } L(1) = \frac{-1}{g(1,q)} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \cdot \left[\log\left|1 - e^{2\pi i m/q}\right| + i\left(\frac{\pi m}{q} - \frac{\pi}{2}\right) \right]$$

Answer to exact formula for $g(1,q) = \begin{cases} q^{1/2} & \text{if } q \equiv 1\ (4) \\ i q^{1/2} & \text{if } q \equiv 3\ (4). \end{cases}$

if $q \equiv 3\ (4)$, easier since know $L(1)$ is real. (all terms real)

so have $$L(1) = -\frac{1}{i q^{1/2}} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \cdot \left(i \left(\frac{\pi m}{q} - \frac{\pi}{2} \right) \right)$$

$$= -\frac{\pi}{q^{3/2}} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \cdot m + c \cdot \underbrace{\sum_{m=1}^{q-1} \left(\frac{m}{q}\right)}_{\substack{\parallel \\ 0}}$$

(even w/o knowing $L(1)$ real,

can see that $m, q-m$ terms in sum cancel the log(sin) factors)

E.g.: $\underline{q = 23}$

then $$\sum_{m=1}^{q-1} m \cdot \left(\frac{m}{q}\right) = 1 + 2 + 3 + 4 - 5 + 6 - 7 + 8 \cdots - 21 - 22$$
$$= -69$$

so $$L(1) = \frac{3\pi}{(23)^{1/2}}$$

Cool $\underline{\text{pf. not}} = 0$: $\displaystyle\sum_{m=1}^{q-1} m \cdot \left(\frac{m}{q}\right)$ Has same parity as $\displaystyle\sum_{m=1}^{q-1} m = q \cdot \frac{(q-1)}{2}$

But $q \cdot \frac{(q-1)}{2}$ is odd since q odd, so finite sum can't $= 0$. //

No elementary pf that $\displaystyle\sum_{m=1}^{q-1} m \left(\frac{m}{q}\right)$ is always < 0. (Know true since $L(s) > 0$ for $s > 1$ and hence $L(1) \geq 0$)