The general modulus m.

Previously used characters mod q to pick out residue class mod q. $\equiv a\ (q)$.

clearly, necessary condition for having ∞-ly many primes $\equiv a\ (m)$ is that $\gcd(a,m)=1$. (else $\gcd(a,m)$ divides every term in arith. prog.)

Can we define characters

$$\chi(n) \text{ on } (\mathbb{Z}/m\mathbb{Z})^{\times} \text{ with } \sum_{\chi} \chi(n) = \begin{cases} \phi(m) & \text{if } n \equiv 1\ (m) \\ 0 & \text{else} \end{cases} \quad ?$$

~~Know this to be true~~: $\chi : (\mathbb{Z}/m\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ (stated this prop. for chars. mod p. Didn't prove it)

Have characters mod m:

$\chi(n) = 1$. (trivial char.)

$\chi(n) = \left(\frac{n}{m}\right)$: Jacobi symbol.

Can we construct them explicitly?

simple idea: construct chars. mod p^{α} by taking primitive root g_p

define $\chi_{p^{\alpha}}(n) = \omega^{\nu(n)}$ ω: $\phi(p^{\alpha})$-th rt of unity. $\gcd(n, p^{\alpha}) = 1$.

then $\chi_m \overset{\text{def}}{=} \chi_{p_1^{\alpha_1}} \cdots \chi_{p_r^{\alpha_r}}$.

problem: No primitive roots for 2^{α} with $\alpha \geq 3$.

claim: $(-1)^{\nu} 5^{\nu'}$ with $\nu \pmod 2$, $\nu' \pmod{2^{\alpha-2}}$ give reduced residue system mod 2^{α}.

(all odd, there are $2^{\alpha-1}$ of them. just need to prove they're distinct.)

use binomial thm. $(5) = (2^2+1)$ expand.

Define $\chi_{2^{\alpha}}(n) = \omega^{\nu}(\omega')^{\nu'}$ $\omega^2 = 1$ (i.e. $1, -1$) $(\omega')^{2^{\alpha-2}} = 1$.

then the total # of chars: # of choices of rts. of unity. ω

$$\phi(2^{\alpha}) \cdot \phi(p_1^{\alpha_1}) \cdots \phi(p_r^{\alpha_r}) = \phi(m).$$

again, check that chars. form a gp. under mult., χ_0: trivial char is the identity element.

One way to see the operation of this gp. explicitly:

$$\chi_{p^{\alpha}}(n) = \omega^{v(n)} \quad \text{with} \quad \omega = e^{\frac{2\pi i k}{\phi(p^{\alpha})}} \quad \text{some } k \text{ mod } \phi(p^{\alpha}).$$

$$= e^{2\pi i k \cdot v(n) / \phi(p^{\alpha})}$$

Express $$\chi_m(n) = e^{2\pi i \left[\frac{k_0 v_0(n)}{2} + \frac{k_0' v_0'(n)}{2^{\alpha-2}} + \frac{k_1 v_1(n)}{\phi(p_1^{\alpha_1})} + \cdots + \frac{k_r v_r(n)}{\phi(p_r^{\alpha_r})} \right]}$$

so $\chi_m(n_1 n_2) \rightsquigarrow$ adding $v_i(n_1), v_i(n_2)$

$\chi_{m}(n) \cdot \chi_{m}'(n) \rightsquigarrow$ adding k_i, k_i'

Easy to prove two facts about chars:

$$\sum_{n \in (\mathbb{Z}/m\mathbb{Z})^{\times}} \chi(n) = \begin{cases} \phi(m) & \text{if } \chi = \chi_0 \\ 0 & \text{else} \end{cases}, \qquad \sum_{\chi} \chi(n) = \begin{cases} \phi(m) & \text{if } n \equiv 1 \ (m) \\ 0 & \text{else} \end{cases}$$

pf: summing over $\chi \longleftrightarrow$ summing over all choices k_i.

each of these sums is 0 unless $v_i(n) = 0$ (i.e. $n \equiv 1 \ (p_i^{\alpha_i})$)

$\Rightarrow$ total sum 0 unless $n \equiv 1 \ (m)$

(same pf. for n as running var.
now sum over $v_i(n)$)

Then easy to show (for $\gcd(a,m)=1$)

$$\frac{1}{\phi(m)} \cdot \sum_{\chi \bmod m} \bar{\chi}(a)\,\chi(n) = \begin{cases} 1 & \text{if } n \equiv a \pmod m \\ 0 & \text{otherwise} \end{cases}$$

and pf. proceeds as before:

- still obtain key identity
- sum over $\sum_{\chi : \bmod m}$ still contains trivial char. χ_0.

  $$L(s,\chi_0) = \zeta(s) \cdot \prod_{p \mid m} (1-p^{-s})$$

- complex places have $L(1,\chi) \neq 0$
  by same pf. by contradiction as before.
- What if χ real? choosing only $1,-1$ for w's
  at each prime power.