MAT 311 LECTURE 20

DIRICHLET'S THEOREM ON PRIMES IN ARITHMETIC PROGRESSION.

EULER'S PROOF OF THE INFINITUDE OF PRIMES.

RECALL:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \mathrm{Re}(s) > 1$$

$$= \prod_{p \text{ PRIME}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right)$$

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

$$\log \zeta(s) = \sum_{p} \sum_{k=1}^{\infty} \frac{1}{k} \cdot \frac{1}{p^{ks}}$$

$\mathrm{Re}(s) > 1$

WE CONSIDER

$$\lim_{s \downarrow 1} \log \zeta(s).$$

IT'S KNOWN $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$

SO $\lim_{s \downarrow 1} \zeta(s) = \infty \Rightarrow \lim_{s \downarrow 1} \log \zeta(s) = \infty.$

NOTICE THAT (s REAL)

$$\sum_{p} \sum_{k \geq 2} \frac{1}{k} \frac{1}{p^{ks}} < \sum_{p} \left(\frac{1}{p^{2}} + \frac{1}{p^{3}} + \frac{1}{p^{4}} + \cdots \right)$$

$$= \sum_{p} \frac{1}{p(p-1)} < \infty.$$

THIS MEANS $\sum \frac{1}{p} = \infty$! □

THEOREM (DIRICHLET): IF $q > 1$ AND $GCD(a, q) = 1$ THEN THERE ARE INFINITELY MANY PRIMES $p \equiv a \bmod q$.

CASE q PRIME: $(\mathbb{Z}/q\mathbb{Z})^\times$ IS CYCLIC, GENERATED BY A PRIMITIVE ROOT ω. GIVEN $(n,q)=1$, DEFINE $\nu(n)$ SUCH THAT $\omega^{\nu(n)} \equiv n \bmod q$

FOR EACH $b = 0, 1, 2, \ldots, q-2$ DEFINE A DIRICHLET CHARACTER

$$\chi_b(n) = \begin{cases} 0 & \text{IF } n \equiv 0 \bmod q. \\ e^{\frac{2\pi i b \nu(n)}{q-1}} & \text{IF } n \equiv \omega^{\nu(n)} \bmod q. \end{cases}$$

THESE ARE CHARACTERS OF $(\mathbb{Z}/q\mathbb{Z})^\times$, AND MULTIPLICATIVE,

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

ORTHOGONALITY RELATION

$$\sum_{h \bmod q} \chi_h(h) = \begin{cases} q-1 & \text{IF } h=0 \\ 0 & \text{OTHERWISE.} \end{cases}$$

PROOF: THE RESIDUE 0 MOD q CONTRIBUTES 0. THE REMAINING RESIDUES MAY BE REP'N

$$1=\omega^0, \omega^1, \omega^2, \ldots, \omega^{q-2}.$$

THUS THE SUM IS

$$\sum_{k=0}^{q-2} e^{\frac{2\pi i \cdot l \cdot k}{q-1}} = \begin{cases} 0 & \text{IF } q-1 \nmid h \\ q-1 & \text{OTHERWISE.} \end{cases}$$

2ND ORTHOGONALITY RELATION:

IF $(a,q)=1$ THEN

$$\sum_{b=0}^{r-2} \overline{\chi_b(a)}\,\chi_b(n) = \begin{cases} q-1 & \text{IF } a \equiv n \bmod q \\ 0 & \text{OTHERWISE} \end{cases}$$

PROOF:

$$\sum_{b=0}^{q-2} e^{\frac{\pi i b(-\nu(a)+\nu(n))}{q-1}}$$

$$= \begin{cases} q-1 & \text{IF } \nu(a) \equiv \nu(n) \bmod q-1 \\ 0 & \text{OTHERWISE} \end{cases}$$

THE $q-1$ CASE IS EQUIVALENT TO $a \equiv n \bmod q$.

THE DIRICHLET L-FNS:

$$L(s,\chi_b)=\sum_{h=1}^{\infty}\frac{\chi_1(h)}{h^s} \qquad \mathrm{Re}(s)>1.$$

SINCE χ_b IS MULTIPLICATIVE

$$L(s,\chi_b)=\prod_{p}\left(1+\frac{\chi_1(p)}{p^s}+\frac{\chi_1(p^2)}{p^{2s}}+\cdots\right)$$

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

$$\log L(s,\chi_b)=\sum_{p}\sum_{k}\frac{\chi_1(p^k)}{k\,p^{ks}}.$$

WE CONSIDER THE LIMIT AS $s \downarrow 1$ IN THE LINEAR COMBINATION

$$\frac{1}{q-1}\sum_{b=0}^{q-2}\overline{\chi}_b(a)\log L(s,\chi_b).$$

$$= \sum_p \sum_k \frac{1}{k p^{ks}} \cdot \frac{1}{q-1}\sum_{b=0}^{q-2}\overline{\chi}_b(p^k)\chi_b(1)$$

$$= \begin{cases} 1 \text{ IF } p^k \equiv a \bmod q \\ 0 \text{ OTHERWISE} \end{cases}$$

$$= \sum_{p,k} \frac{1}{k p^{ks}}$$

$$p^k \equiv a \bmod q$$

AS BEFORE, THE SUM OVER p^k $k \geq 2$ IS BOUNDED BY A CONSTANT, SO IF WE CAN SHOW THAT THE LIMIT OF THE LINEAR COMBINATION TENDS TO ∞ THEN WE'LL PROVE DIRICHLET'S THM, $\sum_{p \equiv a \bmod q} \frac{1}{p} = \infty$.

THE CHARACTER χ_0 IS CALLED THE PRINCIPLE CHARACTER.

$$\chi_0(n) = \begin{cases} 1 & \text{IF } q \nmid n \\ 0 & \text{OTHERWISE} \end{cases}$$

$$\sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} = \sum_{q \nmid n} \frac{1}{n^s} = \sum_{n} \frac{1}{n^s} - \sum_{q \mid n} \frac{1}{n^s}$$

$$= \left(1 - \frac{1}{q^s}\right) \sum_{n} \frac{1}{n^s}$$

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

THUS $\lim_{s \downarrow 1} L(s, \chi_0) = \infty.$

MEROMORPHIC CONTINUATION OF $\zeta(s)$:

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

$$= \int_{1^-}^{\infty} \frac{d(\lfloor x \rfloor)}{x^s}$$

'STIELTJES INTEGRAL'

$$= s \int_{1^-}^{\infty} \frac{\lfloor x \rfloor}{x^{s+1}}\, dx$$

INTEGRATE BY PARTS

$$= s \int_{1^-}^{\infty} \frac{dx}{x^s} + s \int_{1^-}^{\infty} \frac{\lfloor x \rfloor - x}{x^{s+1}}\, dx$$

BOUNDED BY 1

$$= \frac{s}{s-1}$$

SIMPLE POLE RESIDUE 1 AT $s=1$.

CONVERGES TO AN ANALYTIC FN IN $\mathrm{Re}(s) > 0$.

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

THIS ALSO GIVES THE MEROMORPHIC CT'N OF $L(s, \chi_0)$ TO $\mathrm{Re}(s) > 0$

ANALYTIC CONTINUATION OF $L(s,\chi)$, χ NON-PRINCIPLE.

DEFINE: $S(x,\chi_b) = \sum_{n<x} \chi_b(n)$.

$$S(x,\chi_b) = \sum_{n \le q\cdot\left[\frac{y}{q}\right]} \chi_b(n) + \sum_{q\cdot\left[\frac{x}{q}\right]<n<x} \chi_b(n).$$

THIS SUM IS OVER $\left[\frac{x}{q}\right]$ FULL PERIODS OF RESIDUES FOR $\mathbb{Z}/q\mathbb{Z}$, SO IS 0!

$\le q$ TERMS IN SUM.

THUS $|S(x,\chi_b)| \le q$.

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

'STIELTJES INTEGRAL' $= \int_{1^-}^{\infty} \frac{d\,S(x,\chi_k)}{x^s}$

$= s \int_{1^-}^{\infty} \frac{S(x,\chi_k)}{x^{s+1}}\,dx$ — BOUNDED BY $\sim Q$

THIS CONVERGES ABSOLUTELY TO AN ANALYTIC FUNCTION IN $Re(s) > 0$.

CONSIDER

$$\sum_{h=0}^{q-2} \log L(s,\chi_h) \qquad (s>1 \text{ REAL})$$

$$= (q-1) \sum_{p^k \equiv 1 \bmod q} \frac{1}{k p^{ks}} \geq 0$$

THIS MEANS, BY EXPONENTIATING,

$$\prod_{h=0}^{q-2} L(s,\chi_h) \geq 1, \quad s>1.$$

HENCE $\lim_{s \downarrow 1} \prod_{h=0}^{q-2} L(s,\chi_h) \geq 1.$

$L(s,\chi_0)$ HAS A SIMPLE POLE AT 1, AND $L(s,\chi_h)$ $h \neq 0$ IS ANALYTIC AT 1 $\Rightarrow$

EXACTLY 1 POLE IN THE PRODUCT $\Rightarrow \leq 1$ ZEROS IN THE PRODUCT, SINCE OTHERWISE IT WOULD VANISH AT 1.

THIS ESTABLISHES THAT IF χ_h TAKES COMPLEX VALUES, $L(1,\chi_h) \neq 0$, SINCE OTHERWISE $L(1,\overline{\chi_h}) = 0$ WOULD CONTRIBUTE TWO ZEROS, A CONTRADICTION.

ASIDE FROM THE PRINCIPAL CHARACTER, THERE IS A SINGLE REAL CHARACTER MOD q

$\left[e^{\frac{2\pi i\, b\, \nu(k)}{q-1}}\right]$ REAL $\Rightarrow b = \frac{q-1}{2}$ OR $q-1$.

THIS CHARACTER IS $\left(\frac{n}{q}\right)$, THE LEGENDRE SYMBOL.

WE SHOWED $L(1,\left(\frac{n}{q}\right)) \neq 0$ WHEN WE PROVED DIRICHLET'S CLASS NUMBER FORMULA, SINCE IT APPEARS AS A FACTOR IN THE FORMULA FOR THE NUMBER OF CLASSES OF BINARY QUADRATIC FORMS OF THE DISCRIMINANT.

PROOF OF THEOREM:

$$\sum_{p \equiv a \bmod q} \frac{1}{p} = O(1) + \sum_{p^k \equiv a \bmod q} \frac{1}{k p^k}$$

$$= \lim_{s \downarrow 1} \frac{1}{q-1} \sum_{b=0}^{q-2} \overline{\chi}(a) \log L(s, \chi_b)$$

$$= \lim_{s \downarrow 1} \frac{1}{q-1} \log L(s, \chi_0) + \boxed{\frac{1}{q-1} \sum_{b=1}^{q-2} \overline{\chi}(a) \log L(1, \chi_b)}$$

$$\ll O(1)$$

$$= \lim_{s \downarrow 1} \frac{1}{q-1} \log L(s, \chi_0) + O(1)$$

$$= \infty. \qquad \square$$

GENERALIZATION TO GENERAL MODULI:

IN GENERAL

$$q = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{a_k}$$

BY THE CHINESE REMAINDER THEOREM

$$(\mathbb{Z}/q\mathbb{Z})^\times = (\mathbb{Z}/p_1^{\ell_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\ell_k}\mathbb{Z})^\times$$

WE CHECKED AT THE BEGINNING OF TERM THAT IF p IS ODD.

$$(\mathbb{Z}/p^\ell\mathbb{Z})^\times \cong \mathbb{Z}/p^{\ell-1}(p-1)\mathbb{Z}$$

IS CYCLIC. GENERATED BY A PRIMITIVE ROOT. THE THEORY OF DIRICHLET CHAR. TO ODD PRIME POWER MODULI IS DESCRIBED THE SAME WAY.

MOD 2^ℓ, EVERY ODD RES. CLASS HAS A UNIQUE REP'N

$$n \equiv (-1)^{\nu_1} 5^{\nu_2}, \quad \nu_1 \in \{0,1\}, \quad 0 \le \nu_2 < 2^{\ell-2}.$$

THE DIRICHLET CHARACTERS MOD 2^ℓ HAVE FORM

$$\chi_{m_1,m_2}(n) = e^{2\pi i\left(\frac{m_1\nu_1}{2} + \frac{m_2\nu_2}{2^{\ell-2}}\right)}$$

IF n IS ODD, 0 IF n IS EVEN.

THIS IS A GROUP CHARACTER, MULTIPLICATIVE, SINCE EXPONENTS ADD.

THE DIRICHLET CHARACTERS MOD q ARE THE GROUP CHARACTERS OF $(\mathbb{Z}/q\mathbb{Z})^\times$ EXTENDED TO BE 0 ON NON-REDUCED RESIDUES.

THEY FACTOR OVER PRIME POWERS

$$\chi = \prod_{p^\alpha \| q} \chi_{p^\alpha}$$

WHERE χ_{p^α} IS A DIRICHLET CHARACTER MOD p^α.

χ_{p^α} IS <u>PRIMITIVE</u> IF IT IS NOT EQUAL TO A DIRICHLET CHARACTER MOD p^β FOR $\beta < \alpha$.

χ IS PRIMITIVE IF (i.e. PRINCIPAL)

ALL OF THE FACTORS χ_{p^α} IS PRIMITIVE.

THE DIRICHLET CHARACTERS SATISFY THE SAME ORTHOG. AS FOR PRIME MODULI

E.G.

$$\sum_{n \bmod q} \chi(n) = \begin{cases} \varphi(q) & \text{IF } \chi \text{ IS PRINCIPLE} \\ 0 & \text{OTHERWISE} \end{cases}$$

$$\sum_{\chi \bmod q} \bar{\chi}(a)\chi(n) = \begin{cases} \varphi(q) & \text{IF } a \equiv n \bmod q \text{ AND } \gcd(a,q)=1 \\ 0 & \text{OTHERWISE.} \end{cases}$$

THE PROOF FOR PRIME POWER CHARACTERS IS AS BEFORE, FACTOR.

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

THE MEROMORPHIC CT'N FOR χ PRINCIPAL IS AS BEFORE, ANALYTIC CT'N ALSO FOR THE OTHER CHARACTERS.

THIS PROVES $L(1,\chi) \neq 0$ FOR ALL BUT 1 χ AS BEFORE,

WHICH REDUCES TO REAL CHARACTERS.

UNDERSTANDING THE

SIZE OF $L(1,\chi)$, χ REAL

IS ONE OF THE MAJOR

OPEN PROBLEMS OF ANALYTIC

NUMBER THEORY

~~WORKS OF~~ SIEGEL,

GOLDFELD, GROSS-ZAGIER

GIVE PARTIAL RESULTS.

↳ THIS WORK RESOLVED GAUSS'S

CLASS #1 PROBLEM, TO

ENUMERATE ALL DISCRIMINANTS

WITH A SINGLE CLASS OF

FORMS OF THE DISCRIMINANT

(NEG. DISC. CASE).

If $\chi = \prod_{p^\alpha} \chi_{p^\alpha}$ is real,

then each χ_{p^α} is also real,

if p is odd, either principal or $\left(\frac{\cdot}{p}\right)$.

For $p=2$, several real characters.

Factoring out the principal character part just contributes a finite product to the L-fn.

The non-vanishing at 1 still follows from the class number formula applied to the L-fn of the primitive part.

The remainder of the proof is the same.