(1) Zur Problem

1. die assumptions about P_ω. $S = \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$ and $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. =

2. consequences; assume either $\gamma = 0$, or all $\gamma^{(i)} \neq 0$; second case. $\gamma \neq 0$

$M = S^{\frac{\alpha}{\gamma}} T_\gamma S^{\frac{\delta}{\gamma}}$; replace first #1 by T_γ

explain consequences: for P_ω and γ.

for $\omega \neq 0$, have

$|N(\omega\gamma)| \geq 1$. ; ξ_j; $1, \dots n$

$D|N(\gamma)| \geq 1$

Minkowski:

$t_i > 0$ $\Omega = (\xi_j^{(i)})$; $D = |\!|\Omega|\!|$.

$\prod t_i \geq D$ $\exists\, \omega \neq 0$ with $|\omega^{(i)}| \leq t_i$

Recursion formulas for

$M_k = T_\gamma S^{\omega_1} T_\gamma \cdots T_\gamma S^{\omega_{k-1}} T_\gamma$

$\alpha_{k+1} = \gamma\omega_k\alpha_k - \alpha_{k-1}$; $\gamma_{k+1} = \gamma\omega_k\gamma_k - \gamma_{k-1}$

$\alpha_0 = 1$, $\gamma_0 = 0$; $\alpha_1 = 0$; $\gamma_1 = \gamma$;

$\gamma_2 = \omega_1\gamma^2$; $\gamma_3 = \omega_1\omega_2\gamma^3 - \gamma$; $\gamma_4 =$

$\omega_1\omega_2\omega_3\gamma^4 - (\omega_1 + \omega_3)\gamma^2$; $\alpha_2 = -1$; $\alpha_3 = -\gamma\omega_2$

$\alpha_4 = -\omega_2\omega_3\gamma^2 + 1$.

(3) Identities: $n \geq 2$ Principle only finitely many diff. elem. in compact region. Construct inf many pairs ω_1, ω_2 with

$|\omega_1^{(i)}\omega_2^{(i)}| \leq D^{\frac{2}{n}}$, relations. ; $\Omega^{-1} = (\rho_j^{(i)})$

assymptotic behaviour; $\phi \leq i < j \leq n$

$1 \leq k, \ell \leq n-1$ $\frac{1}{|N(\gamma)|} D^{\frac{n-1}{n}} \leq |\omega^{(i,j)}|, |\omega^{(j,i)}| \leq D^{\frac{1}{n}}$

$a_k^{i,j} \sim T\rho_{\delta k}^{(i)}\omega^{i,j} + \mathcal{O}(1)$

$b_\ell^{(i,j)} \sim T\rho_k^{(j)}\omega^{j,i} + \mathcal{O}(1)$

(2) Determinant $\frac{n(n-1)}{2}$ by $\frac{n(n-1)}{2}$.

$$\left(T^2\left(\rho_k^{(i)}\rho_e^{(j)} + \rho_k^{(j)}\rho_e^{(i)}\right)\omega^{i,j}\omega^{j,i}\right) + Q(T)$$

$$\left|\left(\rho_k^{(i)}\rho_e^{(j)} + \rho_k^{(j)}\rho_e^{(i)}\right)\right| \neq 0 \quad ?$$

Solve with resp. to $\xi_k \xi_e$ get

$$\xi_k \xi_e = \sum_{r=1}^{n} d_{k,e}^{r} \xi_r \xi_m \quad \text{or write}$$

$\xi_k = \xi_k \xi_m$; get

$$\xi_k \xi_e = \sum_{1}^{n} d_{k,e}^{(r)} \xi_r$$

Thus $\frac{\omega}{\xi_m}$ root of equation of degree at most n. Choose ω so that $\frac{\omega}{\xi_m}$ generates field k that contains all ξ_k.

field of degree n, totally real.

Next wish to show.

$\gamma\omega$ is an algebraic integer ; $(\gamma\omega)^2$ in same field ~~ok~~... assume that we have by conjugacy brought P_ω on such form that ω contains all integers in field. With first to show γ^2 integer in field. 1st γ^2 in field.

look at α_3 for $\omega, \omega_2 = \omega_1' \omega_2'$ get $\gamma^2 = \frac{\omega''}{\omega''' \omega_1 \omega_2}$

ass: γ^2 not integer.

Can go to a $\omega\gamma^{2^k} = \frac{\rho}{\varkappa}$, where ρ and $\varkappa$ are integers $(\rho, \varkappa) = 1$ and $\varkappa$ is not a unit.

new γ

We shall try to construct a $\gamma_4 \neq 0$

or $\omega_1 \omega_2 \omega_3 \rho^2 = (\omega_1 + \omega_3)\varkappa^2$

(3) In this case α_4 becomes $-\frac{\omega_3}{\omega_1}$, if we can chose $\omega_1, \omega_2, \omega_3$ as integer but so that $\frac{\omega_3}{\omega_1}$ is not a unit we get a contradiction. We may chose ω_1 as a unit of and ω_3 as a divisor of x^2 which is not a unit then if

$$\gamma + \omega_3 \equiv 0 (\rho^2)$$

ω_2 can be chosen as an integer. We try to pass from our $\gamma = \frac{\rho}{x}$ to one for which we can be assured that such a congruence can be solved; we write

$\gamma_k = \frac{\rho_k}{x^k}$ and find

$$\rho_{k+1} = \omega_k \rho_k - x^2 \rho_{k-1}$$

$$\rho_1 = \rho; \quad \rho_2 = \rho^2 \omega_1; \quad \rho_3 = \rho^3 \omega_1 \omega_2 - x^2 \rho$$

$$\rho_4 = \rho^4 \omega_1 \omega_2 \omega_3 - x^2 \rho^2 (\omega_1 + \omega_3)$$

in general put $\rho_{2k} = \rho^2 \Delta_{2k}$

and $\rho_{2k+1} = \rho \Delta_{2k+1}$

$$\rho_{2k+1} = \omega_{2k} \rho^2 \Delta_{2k} - x^2 \Delta_{2k-1},$$

$$\Delta_{2k+2} = \omega_{2k+1} \Delta_{2k+1} - x^2 \Delta_{2k},$$

or

$$\Delta_{2k+1} \equiv -x^2 \Delta_{2k-1} \mod (\rho^2 \Delta_{2k})$$

$$\Delta_{2k+2} \equiv -x^2 \Delta_{2k} \mod (\Delta_{2k+1})$$

(4A) write $\gamma_k = \frac{\rho_k}{\alpha^k}$

??!

$$\rho_{k+1} = \rho\,\omega_k\,\rho_k - \alpha^2\,\rho_{k-1}$$

put $\rho_{2k} = \rho^2\,\Delta_{2k}$; $\rho_{2k+1} = \rho\,\Delta_{2k+1}$

$$(1)\quad \Delta_{2k+1} = \rho^2\,\omega_{2k}\,\Delta_{2k} - \alpha^2\,\Delta_{2k-1}$$

$$(2)\quad \Delta_{2k+2} = \omega_{2k+1}\,\Delta_{2k+1} - \alpha^2\,\Delta_{2k}$$

or

$$(1')\quad \Delta_{2k+1} \equiv -\alpha^2\,\Delta_{2k-1} \pmod{\rho^2\,\Delta_{2k}}$$

$$(2')\quad \Delta_{2k+2} \equiv -\alpha^2\,\Delta_{2k} \pmod{\Delta_{2k+1}}$$

Try to choose ω_k such that

$\Delta_k = \eta\,\pi_k^{m_k}$ where π_k is a representative of a principal prime ideal of degree 1 $|N(\pi_k)| = p_k$ and such that the p_k remain bounded as k grows and that $\pi_{k+1}^{p_k - 1} \not\equiv 1 \pmod{\pi_k^2}$

(4B) ? can arrange if c^2 not ~~in field~~. inf. many $c^2(c^2\omega - (\eta^\wedge - 1))$ in a compact region, ~~bounded~~ all components one bounded away from 0. since $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ if $\frac{A}{C}$ and $\frac{B}{C}$ can be reduced modulo the lattice Ω we get inf many in compact region. elements If grimp discrete some must occur several times

$$c^2\omega_1 - (\eta^\wedge - 1) = c^2\omega_2 - (\eta^s - 1)$$

So c^2 is in field ~~k~~. assume $(c^2) = \frac{(\rho_1)}{(\pi_1)}$ where $(\rho_1), (\pi_1)$ all prime

can replace c by $c^{2^\nu}\omega$ with $2^\nu > h$ where h is class number of k, $(\pi_1)^h$ is principal ideal, π, may choose ω so that the new c is

$$c^{2^\nu}\omega = \frac{\rho}{\pi}, \text{ where } (\rho, \pi) = 1.$$

write γ instead of c. $\gamma = \frac{\rho}{\pi}$

$$T_\gamma S_{\omega_1} \cdots T_\gamma S_{\omega_k} = T\begin{pmatrix} \alpha_k, \beta_k \\ \gamma_k, \delta_k \end{pmatrix}$$

$$\gamma_k = \frac{\rho_k}{\pi^k}, \text{ where}$$

(4c)

? $\rho_{k+1} = \rho\,\omega_k \rho_k - x^2 \rho_{k-1}$

put $\rho_{2k} = \rho^2 \Delta_{2k}$; $\rho_{2k+1} = \rho \Delta_{2k+1}$

(1) $\Delta_{2k+1} = \rho^2 \omega_{2k} \Delta_{2k} - x^2 \Delta_{2k-1}$

(2) $\Delta_{2k+2} = \omega_{2k+1} \Delta_{2k+1} - x^2 \Delta_{2k-2}$

or otherwise expressed

(1') $\Delta_{2k+1} \equiv -x^2 \Delta_{2k-1} \pmod{\rho^2 \Delta_{2k}}$

(2') $\Delta_{2k+2} \equiv -x^2 \Delta_{2k} \pmod{\Delta_{2k+1}}$

try to choose sequence of ω_k such that always $\Delta_k = \eta \cdot \pi_k^{m_k} \cdot \pi_k$ and $|N(\pi_k)| = p_k$ principal of degree 1. remains bounded. as k and ~~$k \to \infty$~~

4C $\frac{1}{2}$

??? if $\gamma = \frac{\rho}{x}$; make $\gamma^2 \omega_1 \omega_2 \omega_3 - \omega_1 - \omega_3 = 0$

while $\frac{\omega_1}{\omega_3}$ is not a unit.

or $\frac{(\omega_1 + \omega_3) x^2}{\omega_1 \omega_3 \rho^2}$ integral.

pick ω_1 proper divisor of x^2

$\omega_3 = -\eta$ (unit.

$\therefore x\omega_1 - \eta \equiv 0 (\rho^2)$ contradiction

cf. ρ is power of a prime ideal of degree 1.

easy to the that for ρ^{2^ν} ; ν large enough

$\omega x^{t_1} - \eta^{t_2} \equiv 0 (\text{mod } \rho^{2^\nu})$

with $0 < t_1 < 2^\nu$ and some t_2

is solvable for ν large enough.

---

try to produce instead

$\gamma_k = \frac{\rho_k}{x^k}$ with $\rho_k = \rho^2 \pi_k^{m_k}$

with m_k large, where as π_k is a prime idial of degree 1 with bounded norm. as $m_k \to \infty$

HD

?

$$\rho_{2k} = \rho^2 \Delta_{2k} \quad ; \quad \rho_{2k+1} = \rho \Delta_{2k+1}$$

$$(1) \quad \Delta_{2k+1} = \rho^2 \omega_{2k} \Delta_{2k} - x^2 \Delta_{2k-1}$$

$$(2) \quad \Delta_{2k+2} = \omega_{2k+1} \Delta_{2k+1} - x^2 \Delta_{2k-2}$$

$$(1') \quad \Delta_{2k+1} \equiv -x^2 \Delta_{2k-1} \pmod{\rho^2 \Delta_{2k}}$$

$$(2') \quad \Delta_{2k+2} \equiv -x^2 \Delta_{2k} \pmod{\Delta_{2k+1}}$$

Try to get a sequence of ω_k such that always $\Delta_k = \eta_k \pi_k^{m_k}$ where π_k is a representative of a principal prime ideal of degree 1 ($N(\pi) = \pm p$), such that the norms $N(\pi_k) = \pm p_k$ do not grow over all bounds as $k \to \infty$

(4E)

?

Two steps.

$$p_{k+2} \leq \max\left(p_k^{A\varepsilon}, X_3\right)$$

if $A\varepsilon \leq 1$ guaranteed that the p do not grow. since ε may be chosen arbitrarily small ... O.K.

For k large enough we can always solve congruence

$$\eta - x^t \equiv 0\left(\rho^2 \bar{\pi}_{2k+1}^{2m_{2k+1}}\right)$$

with $0 < t \leq 4k+2$ $\quad [N(\bar{\pi}_{2k+1})]' = p$

$\eta^{p-1} = 1 + \lambda \bar{\pi}^{\alpha}$ fixed α.

powers of η represents, at least. $\gamma_{k+1} = \dfrac{\rho^{2m_{2k+1}} \bar{\pi}_{2k+1}}{x^{2k+1}}$

$$\eta^{p^a(p-1)} \equiv 1 + \lambda \rho^a \bar{\pi}^{\alpha}$$

$0 < r < p$

$$\eta^{\rho^{(2am_{k+1} - \alpha)}} \quad \eta^{\pi(p-1)} \equiv 1 + r$$

$(p-1) \cdot 4k+2$

(4F) for k large enough can always solve congruence

$$\eta - x^t \equiv 0 \quad (\rho^2 \pi_{2k+1}^{2 m_{2k+1}}).$$

with a t such that $0 < t < \varphi_{k+2}$

this

$$p_{2k+1} \leq \max(p_{2k}, \underset{A}{C}) \quad \underline{C(\rho, F)}$$

$$p_{2k+2} \leq (\max(p_{2k+1}, \underset{\varepsilon}{C(\varepsilon, F)}).$$

4F $\frac{1}{2}$

??

$$\pi_{2k+1}^{m_{2k+1}} \equiv -\varkappa^2 \pi_{2k-1}^{m_{2k-1}} \left(\mathrm{mod}\ \rho^2 \pi_{2k}^{m_{2k}}\right)$$

$$\pi_{2k+2}^{m_{2k+2}} \equiv -\varkappa^2 \pi_{2k}^{m_{2k}} \left(\mathrm{mod}\ \pi_{2k+1}^{m_{2k+1}}\right)$$

Selection: (1) can always find π_{2k+1} such that $\pi_{2k+1} \equiv -\varkappa^2 \pi_{2k-1}^{m_{2k-1}} \left(\mathrm{mod}\ \rho^2 \pi_{2k}\right)$

$\pi_{2k+1}^{p-1} \not\equiv 1 \left(\mathrm{mod}\ \pi_{2k}^2\right)$ ~~primitive root mod π_{2k}~~, $p_{2k+1} > |N(\rho^3)|$

and

$$p_{2k+1} < \max\left(p_{2k}^{A}, C\right)$$

(2) can always find π_{2k+2} such that

π_{2k+2} is primitive root mod π_{2k+1}^2

and

$$p_{2k+2} < \max\left(p_{2k+1}^{\varepsilon}, C(\varepsilon)\right)$$

find $p_{2k+2} < \max\left(p_{2k}^{A\varepsilon}, C'(\varepsilon)\right)$.

choose $\varepsilon < \frac{1}{A}$. get p_k bounded as $k \to \infty$

(HG)

?

$$\gamma_{k+1} = \omega_k$$

$$\begin{pmatrix} \alpha_{k+1} & \beta_{k+1} \\ \gamma_{k+1} & \delta_{k+1} \end{pmatrix} = \begin{pmatrix} \alpha_k & \beta_k \\ \gamma_k & \delta_k \end{pmatrix} \begin{pmatrix} \gamma\omega_k & -\frac{1}{\gamma} \\ \gamma & 0 \end{pmatrix}$$

$$\alpha_{k+1} = \gamma\omega_k\alpha_k + \gamma\beta_k = \gamma\omega_k\alpha_k - \alpha_{k-1}$$

$$\beta_{k+1} = -\frac{1}{\gamma}\alpha_k$$

$$\alpha_0 = 1 \; ; \; \alpha_1 = 0$$

$$\gamma_0 = 0 \quad \gamma_1 = \gamma$$

$$\gamma_{k+1} = \gamma\omega_k\gamma_k - \gamma_{k-1}$$

$$\alpha_2 = \cancel{\gamma\omega_1} = 1 \; ; \; \gamma_2 = \gamma^2\omega_1$$

$$\alpha_3 = -\gamma\omega_2 \; , \; \gamma_3 = \gamma^3\omega_1\omega_2 - \gamma$$

$$\alpha_4 = -\gamma^2\omega_2\omega_3 + 1 \; ; \; \gamma_4 = \gamma^4\omega_1\omega_2\omega_3 - \gamma^2(\omega_3 + \omega_1)$$

$$\gamma^2\omega_2\omega_3 = \frac{\omega_3 + \omega_1}{\omega_1} \; ; \; \alpha_4 = -\frac{\omega_3}{\omega_1} \; ; \; \delta_4 = -\frac{\omega_1}{\omega_3} \; . \quad (= 0)$$

find γ_k of form $= \frac{\rho_k}{x^k}$ such that congruence $\eta - x^t \equiv 0 \; (\rho_k^2)$ holds for some unit η and $0 < t < 2k$; $\gamma_1 = \frac{\rho}{x}$

$(\rho, x) = 1$,

$$\rho_{2k} = \rho^2\Delta_{2k} \; ; \; \rho_{2k+1} = \rho\Delta_{2k+1}$$

(1) $$\Delta_{2k+1} = \rho^2\omega_{2k}\Delta_{2k} - x^2\Delta_{2k-1}$$

(2) $$\Delta_{2k+2} = \omega_{2k+1}\Delta_{2k+1} - x^2\Delta_{2k}$$

(4H)

(1') $\Delta_{2k+1} \equiv -\alpha^2 \Delta_{2k-1} \pmod{p^2 \Delta_{2k}}$

(2') $\Delta_{2k+2} \equiv -\alpha^2 \Delta_{2k} \pmod{\Delta_{2k+1}}$

all Δ rel prime to α, try to choose sequence of ω_k so that always $\Delta_k = \eta_k \pi_k^{m_k}$ where π_k is principal primideal of degree 1 ($N(\pi) = \pm p$) such that as $k \to \infty$ the norms of π_k do not grow over all bounds.

Construction

(5) so we get $\zeta_{2k+1} = \rho^{m_{2k+1}} \pi_{2k+1} \eta_{2k+1}$

$\gamma_{2k+1} = \rho^{m_{2k+1}} \frac{\pi_{2k+1}}{x^{2k+1}} \eta_{2k+1}$

Our contradiction will be reached if we can have ω_3 as a divisor of x^{4k+2} say $\omega_3 = x^t$ with $1 \le t \le 4k+2$ and $\eta - x^t \equiv 0 \pmod{\rho^{2 m_{2k+1}} \pi_{2k+1}^2}$ with some η. Taking an arbitrary unit (of infinite order), we see easily that η^s represents at least $p_{2k+1}^{2m_{2k+1} - r}$ different residues mod. $(\rho^{2 m_{2k+1}} \bar{u}_{2k+1}^{2m_{2k+1}})$ where r is the power of π_{2k+1} that divides $\eta^{p_{2k+1}-1} - 1$; this is bounded since p_{2k+1}'s thus if we consider the sets,

$\eta^s x^t$ they represent at least

$4k+2 > p^r N(\rho^2)$ $(4k+2) p_{2k+1}^{2m_{2k+1} - r}$ residues for k large enough this is larger than the total no of diff residues mod $(\rho^{2 m_{2k+1}} \bar{u}_{2k+1}^{2m_{2k+1}})$ so there must be duplication, since two $\eta^s x^t$ with same t cannot be congruent we get $\eta^s x^t \equiv \eta^{s'} x^{t'}$ with $t \neq t'$ and so $x^{t-t'} \equiv \eta^{s''}$; here $1 \le |t-t'| < 4k+2$.

This gives our contradiction

(6A)

?? Let P be set of all ~~π set~~

all π in k. $N(\pi) < Q$.

L functions

Congruence characters mod π^2, $\rho^2\pi^2$

$\alpha\pi$, $\rho^2\pi$

are restrictions ~~don't id~~ of characters

~~mod (1) mod~~ mod. ρ^2 ; field constant α

$$\sum_{|N(\pi)|<Q} N_L(\sigma, T) = O\left((QT)^{Q(1-\sigma)} (\log QT)^{\alpha'}\right)$$

See we can split set of Pot π in P_N and P_E

$\exists\ \delta > 0$

P_N $L(s, \chi) \neq 0$ for $\sigma \geq 1-\delta$ $|t| \leq p^A$.

for P_E holds

$$\sum_{\substack{|N(\pi)| \leq x \\ \pi \in P_E}} 1 \leq \sqrt{x}$$

$$\sum_{\substack{|N(\pi)| \leq x \\ \pi \in P}} 1 \sim \frac{x}{h \lg x} \cdots$$

(6R)

?

Density theorem of L functions

consequence.

1. Characters ... $|N(\alpha)| < Q$

$$L(s, \chi_{(\alpha)})$$

$$\sum_{|N(\alpha)|<Q} N_{L,\chi_\alpha}(\sigma, T) = O\left((QT)^{\alpha(1-\sigma)}(\log QT)^{\alpha'}\right)$$

α, α' depend on field.

---

2. $\pi \in P_N$; $|N(\pi)| = p$; const $\delta \geq \rho$

such that if $\pi \in P_N$, ~~$|N(\pi)|$~~

χ character mod π, π^2, $\rho^2\pi$, $\rho^2\pi^2$

which is not restriction ~~of~~ a character mod ρ^2, then

$$L(s, \chi) \neq 0 \quad \text{for} \quad \sigma \geq 1-\delta, \quad |t| < p^4$$

$$\sum_{N(\pi) \leq X} 1 \leq \sqrt{X} \quad ; \text{ for } X > X_0.$$

$\pi \notin P_{NE}$; ;

P_E thin ;

(6C)

A.

(A) for fixed pos ε and π in P_N can find π' in P_N with.

(a) a representative of π' is a primitive root modulo π with the

(b) property that $\pi'^{p-1} \not\equiv 1 \pmod{\pi^2}$ $\quad p = |N(\pi)|$

(c) $p' = |N(\pi')| \leq \max(p^{\varepsilon}, x_1(\varepsilon))$

x_1 depends on ε, k, ρ, n.

(B) for a π in P_N and any integer α such that $(\alpha, \rho^2\pi) = 1$ can find π' in P_N such that

(a') $\pi' \equiv \alpha \pmod{\rho^2\pi}$

(b') $\pi'^{p-1} \not\equiv 1 \pmod{\pi^2}$

(c') $p' = |N(\pi')| \leq \max(p^A, x_2)$

where A is a fixed constant.

x_2 depend on k, ρ