Diophant problems

Statement of problem.

few remarks on background.

1. Show that M can be replaced by $\begin{pmatrix} 0 & -\frac{1}{\gamma} \\ \gamma & 0 \end{pmatrix}$

Law of formation.

2. Proof that $\gamma^2 \in \underline{\underline{k}}$.

3. Preliminary simplification of γ

4. Recursion formulas, attempt at obtaining contradiction, congruence condition to be satisfied.

5. Idea of construction, & proof that it would lead to a γ satisfying the congruence condition.

6. Normal & excepting prime ideals,

6a. Selection lemmas a & b

End remarks.

1. ~~algebraic~~ matrix group. G.

2. Semi simple. Max. compact. subgroup K.
$S = G/K$. Symmetric ~~space~~

3 Arithmetic ~~subgroup~~ Γ; $G \cap Sl(n,\mathbb{Z})$
example modular group.

4. $Sl(2,\mathbb{R})^{n_1}$ $Sl(2,\mathbb{C})^{n_2}$

Hilbert Gruppe. of alg. field of degree
$n = n_1 + 2n_2$: components of transf.

ex an
~~discrete~~
Gerd Subgroups. lattice (finite measure,
classification
equivalence; commensurability

Compact Fund. Domain.
Non-Compact. Fund. Domain.
Product space. reducible
& irreducible lattice.

Criteria about projection. on proper factor of G.

When does Γ have to be essentially arithmetical? If. Γ not compact, what are structure of "cusps" or non cp. parts.
finitely Gen. F. Polyhedron finite?
History of questions. 1957 – to now
Here restrict myself to ~~non~~ cp. case
u.s.w. Speak about special case
comment on general situation
Parabolic elements

2

History : 1957. fact about "cusps" $SL(2,R)^n$
commensurability if. rigidity.
P. Shapiro 1959. [imed.] [lattice] for produkt av $SL(2,R)^3$
~~bevis : om~~ Γ inneholder parabolsk element.
(inner automorphism) ~~(så)~~ kan ~~bringes~~ på form så at Γ inneholder
undergruppe av form $\begin{pmatrix} 1 & \omega^{(i)} \\ 0 & 1 \end{pmatrix}$ hvor
$\omega^{(i)}$ løper over [all] hele tall i en tallkropp k av
grad n (totally real) and $\omega^{(i)}$ (i) komp
av ω ; og Γ inneholder $\begin{pmatrix} \eta^{(i)} & 0 \\ 0 & \eta^{(i)} \end{pmatrix}$ where
$\eta^{(i)}$ ~~are a~~ comp. of unit η in k and
the units form a subgroup of finite index
in group of all units. G_∞^* $\begin{pmatrix} a^{(i)} & b^{(i)} \\ 0 & \frac{1}{a^{(i)}} \end{pmatrix}$
with $\Pi |a^{(i)}| = 1$: then $\Gamma \cap G_\infty^* \backslash G_\infty^*$ compact.
and Γ_∞^* commensurable med Hilb. gruppe for Hilb.
gruppe av k. om Γ : $G_\infty \Omega$ (Ω open neighbourhood of e.
P. S. argument :
$\gamma_{\nu+1} = \gamma_\nu \, p \, \gamma_\nu^{-1}$ converges if γ
in a certain part of G of infinite volume.
derfor må bygge av. kan bare gjøre hvis
γ triangular i alle comp. kan slutte at
γ må ligge i G_∞^* og finde i denne del
av G

"small element" σ : Zentralizer G_σ
$\gamma_{\nu+1} = [\gamma_\nu, \sigma] = \gamma_\nu \sigma \gamma_\nu^{-1} \sigma^{-1}$; $\gamma \in G_\sigma \Omega G_\sigma$ ...
converges to ~~the~~ if Ω small enough.
must break of. can conclude that elements γ
of only special kind. ~~Kan~~ be resp. for equiv
of points in $G_\sigma \Omega_i$ where $\Omega_i \Omega_i^{-1} \in \Omega$ ...

under general something like
$\Gamma_\sigma = \Gamma \cap G_\sigma$ quotient $\Gamma_\sigma \backslash G_\sigma$ finite meas.

extend to measure preserving normalizer G_σ^* of G_σ u.s.w.
which preserves measure on G_σ. $\Gamma_\sigma^* \cap G_\sigma^*$
finite volume in G_σ^* under rather general circumst.

Further consequences. if G_σ^* contains other than parabolic elements.
in this case $G_{\mathfrak{p}_1}^* \cap G_{\mathfrak{p}_2}^*$ is infinite.

$\Gamma_{\mathfrak{p}_1}^* \cap \Gamma_{\mathfrak{p}}^*$ infinite and such that quotient finite volume. Can show.
whole group. of form

$$\frac{1}{\sqrt{\Delta^{(i)}}}\begin{pmatrix} \alpha^{(i)} & \beta^{(i)} \\ \gamma^{(i)} & \delta^{(i)} \end{pmatrix}$$: $\alpha, \beta, \gamma \delta$ integral alg. nr in k such that $\alpha\delta - \beta\gamma = \Delta \neq 0$

real comp of Δ positive.

Rather full description. of cusps & structure of F. ass. ∃ of parabolic element.

Proof (1964) ∃ of par. in special case. later some more general situation handled 1968 - Kazdan - Margulis. ∃ of geodesic ray's in F implies ∃ of small elements

.. Is Γ arithmetic or not?
Integrality. bounded denominators.

1965 proof if assum certain hypothesis about L functions associated with field k. ~~Pilbeggm~~ January iiv. when hypp. proved following.

Γ discr. subgroup containing P_ω $n_1+n_2>1$.
$\begin{pmatrix} 1 & \omega^{(i)} \\ 0 & 1 \end{pmatrix}$ where ω all integers in k

then any transf in Γ $\begin{pmatrix} a^{(i)} & b^{(i)} \\ c^{(i)} & d^{(i)} \end{pmatrix}$ the numbers $c^{(i)2}$ ~~the~~ $\gamma^{(i)}$ ~~components of an integer γ in k~~ where $\gamma^{(i)}$ is (i) conjugate of integer γ in k. follows that by suitable inner transf not changing P_ω. Γ can be brought to form

$\frac{1}{\sqrt{\Delta^{(i)}}} \begin{pmatrix} \alpha^{(i)} & \beta^{(i)} \\ \gamma^{(i)} & \delta^{(i)} \end{pmatrix}$ where the $N(\Delta^{(i)})$ are bounded $\alpha, \beta, \gamma, \delta$ integers in k..

If Γ lattice fem comp follows Γ commensurable with sum Hilbert modular group.

Indication of proof. all $c^{(i)} \neq 0$

$M \begin{pmatrix} a^{(i)} & b^{(i)} \\ c^{(i)} & d^{(i)} \end{pmatrix}$; $T = \begin{pmatrix} 0 & -\frac{1}{c^{(i)}} \\ c^{(i)} & 0 \end{pmatrix}$

$M S_{\omega_1}, M^{-1} S_{\omega_2} \ldots M^{(-1)^{\nu-1}} S_{\omega_\nu}$

makes same as

$T S_{\omega_1}, T S_{\omega_2} \ldots T S_{\omega_\nu}$

---

hilf. $n_1+n_2 = 1$. ($SL(2,\mathbb{R})$ ell $SL(2,\mathbb{C})$

Rank 1. construction of nonarithmetic with various properties.

general situation, lattice, non-comp.

1 rank > 1 — established.

2 rank $= 1$ — not necess. & inequality.

3. compact. — not necess

A. von Mangoldt.

$$\sum 1-$$

$$\psi_1(x,\chi) = \sum_{N(\mathfrak{m})\le x} \left(1-\frac{N(\mathfrak{m})}{x}\right)\chi(\mathfrak{m})\Lambda(\mathfrak{m})$$

Wenn For χ belonging to π or $\rho^2\pi$
(but not to (1) or (ρ^2).
we have für π not in S.

$$\psi_1(x,\chi) = \mathcal{O}(x^{1-\delta}\log px) + \mathcal{O}\left(\frac{x}{\rho^2}\right)$$

if χ belongs Brauchbar to (1) or (ρ^2)
but is not principal we have

$$\psi_1(x,\chi) = \mathcal{O}\left(x e^{-c\sqrt{\log x}}\right)$$

if χ is principal character

$$\psi_1(x,\chi) = \frac{x}{2} + \mathcal{O}\left(x e^{-c\sqrt{\log x}}\right).$$

Now go to construction steps (A) and (B).

(A) Show that for a π not in S we can find another π' not in S such that every one representative of π' is a primitive root modulo π and either there exists a unit η with $\eta \equiv 1 \ (\pi)$ and $\eta \not\equiv 1 \ (\pi^2)$ or π' can be chosen such that also $\pi'^{p-1} \not\equiv 1 \ (\pi^2)$. [and with $N(\pi') \leq c(N(\pi))^2$.

Determine a function defined on congruence classes (mod (π)) which is 1 on the classes that are principal and are primitive roots mod π. let

$f(\mathfrak{A}) = 0$ if $\mathfrak{A}$ is unprincipal or not associated with a primitive root mod π

$= 1$ otherwise

$$f(\mathfrak{C}) = \sum_{\chi} a_\chi \chi(\mathfrak{C})$$

determine the a_χ for χ mod π.

if h class number and $u(\pi)$ is order of unit group mod π, the ideal classes are $h\frac{p-1}{u}$; if by l_χ we understand the smallest pos. integer such that χ^{l_χ} equals 1 on

the principal residue classes. (ℓ_χ is a divisor of $\frac{p-1}{u}$ we find that φ = euler-function

$$a_\chi = \frac{1}{h} \frac{\varphi\left(\frac{p-1}{u}\right)}{\frac{p-1}{u}} \cdot \frac{\mu(\ell_\chi)}{\varphi(\ell_\chi)}$$

and no. of χ with $\ell_\chi = \ell$ is $\underline{h\varphi(\ell)}$.

Now form $\sum_{N(\mathfrak{m})\le x} \left(1 - \frac{N(\mathfrak{m})}{x}\right) f(\mathfrak{m}) \Lambda(\mathfrak{m})$

and insert expression for f estimations for a_χ and the estimates for $\psi_1(x,\chi)$.

we get

$$\sum_{N(\mathfrak{m})\le x} \left(1 - \frac{N(\mathfrak{m})}{x}\right) \Lambda(\mathfrak{m}) f(\mathfrak{m}) \ge \frac{x}{2h} \frac{\varphi\left(\frac{p-1}{u}\right)}{\frac{p-1}{u}}$$

$$\left\{ 1 + O\left(x^{-c\sqrt{\log x}}\right) + O\left(d(p-1)\, x^{1-\delta}\right) + O\left(\frac{d(p-1)}{p^2}\right) \right\} \ge \frac{x}{3h} \frac{\varphi\left(\frac{p-1}{u}\right)}{\frac{p-1}{u}}$$

for p suff great and $p^\varepsilon \le x \le$ since the divisors on the left hand side of ( ) with m not a π or not in S contribute $\le c\sqrt{x}$. it remains only to show

that if there is no unit $\eta \equiv 1 (\pi)$ and $\eta \not\equiv 1 (\pi^2)$ then the π for which $\pi'^{p-1} \equiv 1 (\pi^2)$ are very thinly distributed. There are in this case $\mathrm{mod}(\pi^2))$ $p\left(\frac{p-1}{\mu}\right)$ principal residue classes of which $\frac{p-1}{\mu}$ only have the property that their $p-1$ power is the class (1) use argument for rational primes assume $p_1, \ldots p_\varrho$ are primes $\leq p^{\frac{2}{n}}$ and that all $p_i^{p-1} \equiv 1 (p^2)$; consider set $p_i, \ldots p_{i+n}$ they are at least $\frac{1}{n!} e^n$ different and p^2 thus

$$\frac{1}{n!} e^n < p. \qquad \varrho \leq (n! \, p)^{\frac{1}{n}}$$

$$\varrho < n \, p^{\frac{1}{n}}$$

among the $> \frac{n}{3} \frac{p^{\frac{2}{n}}}{\varrho \, p}$; that is a very thin set

π representative of prime ideal principal of degree 1, $N(\pi) = p$

Density results needed: (dep on K & ρ)
Exists an exceptional set S of π such that

~~if π is not in S~~ $\sum_{\substack{N(\pi) \le X \\ \pi \in S}} 1 = O(\sqrt{X})$

and such that for π not in S; if χ is a character modulo π (or modulo $\rho^2\pi$) such that χ is not essentially a character of (mod) (1) or (ρ^2), then

$$L(s,\chi) \neq 0 \quad \text{for} \quad \begin{matrix} \sigma \ge 1 - 2\delta \\ |t| \le 2p^3 \end{matrix}$$

and $\frac{L'}{L}(s,\chi) = O\left(\log(2+|t|)p \right)$

for $\sigma \ge 1 - \delta$; $|t| \le p^3$

where δ is a fixed constant > 0.

Indication of proof.

Need $L(s,\chi) = \sum \frac{\chi(\mathfrak{M})}{|N(\mathfrak{M})|^s}$ (χ mod α)

analytic for some $\sigma \ge \sigma_0$ where σ_0 is a fixed constant < 1, and that if on this line satisfies an inequality

6

$|L(s,\chi)| \leq O_1(\log((1+|t|)\,N(\mathfrak{m}))^{c_2})$

where c_1 and c_2 are fixed constants

use representations

$$L(s,\chi) = \sum_{N(\mathfrak{m}) \leq X} \frac{\chi(\mathfrak{m})}{(N(\mathfrak{m}))^s} + R_x$$

R_x can be estimated. from formula

$$\frac{1}{2\pi i}\int \frac{X^z}{z} L(s+z,\chi)\, dz$$

where path is to left of $z=0$.

For instance as: $T \geq (1+|t|\,N(\mathfrak{m}))$

$$R = O\left(\frac{X^{1-\sigma}}{T}\right) + O\left(\frac{T^{c_2+1}}{X^{\sigma-\sigma_0}}\right)$$

For $\sigma \geq \sigma_1 > \sigma_0$, can make both terms small by choosing $X = T^{\frac{c_1+2}{1+\sigma_0}}$

$$M_2(s,\chi) = \sum_{N(\mathfrak{m}) \leq z} \frac{\mu(\mathfrak{m})\chi(\mathfrak{m})}{(N(\mathfrak{m}))^s}$$

can actually prove

$$(\cdot\cdot) \qquad \sum_{N(\sigma)\le Q} \sum_{\chi}{}'' N(\sigma, \mathfrak{T}; \chi) = O\left((TQ)^{c_4(1-\sigma)+\varepsilon} \right)$$

using this only for $\sigma = \pi$ or $\sigma = \rho^2\pi$ and taking δ so that $2\delta \cdot 4 \cdot c_4 < \frac{1}{2}$ we get the first part. Proof of $(\cdot)$ uses Halasz idea (or rather) the inequality

$$\sum |(f, \varphi_i)|^2 \le \|f\|^2 \max_i \sum_j |(\varphi_i, \varphi_j)|$$

rather than

$$\left(\sum |(f, \varphi_i)|\right)^2 \le \|f\|^2 \cdot \sum_{i,j} |(\varphi_i, \varphi_j)|$$

$$\sum_{X_1 \le N(m) \le X_2} \frac{a_m \chi(m)}{|N(m)|^s} \qquad \Big| \qquad f = \frac{a_m}{(N(m))^{\frac{1}{2}}}$$

$$\varphi_i = \frac{\chi_i(m)}{|N(m)|^{s_i - \frac{1}{2}}}$$