LECTURE 2

STRONG APPROXIMATION FOR THIN MATRIX GROUPS AND DIOPHANTINE APPLICATIONS

PETER SARNAK

BRISTOL 2016

Affine Sieve

 Γ a group of affine polynomial maps of affine *n*-space \mathbb{A}^n which preserve \mathbb{Z}^n . Fix $\mathbf{a} \in \mathbb{Z}^n$.

 $O := \Gamma \cdot a$, the orbit of *a* under Γ .

 $O \subset \mathbb{Z}^n$, $V \coloneqq Zcl(O)$, the Zariski closure of O. V is defined over \mathbb{Q} .

Diophantine analysis of *O*:

• Strong Approximation; for $q \ge 1$

$$O \xrightarrow{\text{red mod } q} V(\mathbb{Z}/q\mathbb{Z}).$$

What is the image?

• Sieving for primes or almost primes.

If $f \in \mathbb{Z}[x_1, x_2, ..., x_n]$, not constant on O; is the set of $x \in O$ for which f(x) is prime (or has at most a fixed number r prime factors) Zariski dense in V?

Examples of Γ and Orbits:

(1) Classical (automorphic forms)

$$\Gamma \leqslant GL_3(\mathbb{Z})$$
 generated by

$$\begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix},$$

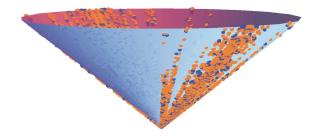
 Γ is a finite index subgroup of $O_f(\mathbb{Z})$, where

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$$

 Γ is an arithmetic group

$$O = \Gamma \cdot (3, 4, 5)$$

yields all (primitive) Pythagorean triples.



(2) Γ linear and "thin", not so classical:

 $\Gamma = A \subset GL_4(\mathbb{Z})$ the Apollonian Group generated by the involutions S_1, S_2, S_3, S_4

$$\begin{bmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{bmatrix}$$

 S_j corresponds to switching the root x_j to its conjugate on the cone

$$F(x) = 0$$
, where

$$F(x_1, x_2, x_3, x_4) = 2(x_1^2 + x_2^2 + x_3^2 + x_4^2) - (x_1 + x_2 + x_3 + x_4)^2.$$

$$A \leq O_F(\mathbb{Z})$$

but while $Zcl(A) = O_F$, A is of infinite index in $O_F(\mathbb{Z})$, i.e. "thin".

The orbits of A in \mathbb{Z}^4 corresponds to the curvatures of 4 mutually tangent circles in an integral Apollonian packing.

For example O = A.(-11, 21, 24, 28)

corresponds to:



Scale the picture by a factor of 252 and let a(c) = curvature of the circle c = 1/radius(c).



The curvatures are displayed. Note the outer one by convention has a negative sign. By a theorem of Apollonius, place unique circles in the lunes.



The Diophantine miracle is the curvatures are integers!



8

 $\Gamma = GL_n(\mathbb{Z})$ (OR MORE GENERALY J-IN TEGRAL)

, ZARISKI CLOSURE OF , Q ALFEBRAIC GROUP G = Zu(p)

 $T \leq G(Z)$

1 IS ARITHMETIC IF IT IS FINITE INDEX IN G(Z) AND IT IS THIN IF NOT.

IF [IS ARITHMETIC THE DIOPHANTINE PROBLEMS FOR 0= 17.0 BECOME THE USUAL ONES FOR V(Z) V=Zcl(O). IF THE ORBIT G.a is CLOSED, V ~ G/H WITH H REDUCTIVE, AND G IS SEMISIMPLE, THEN V(Z) CONSISTS OF FINITELY MANY [ORBITS (BOREL-HARISH CHANDRA).

9

USING THE THEORY OF ARITHMETIC GROUPS AND AUTOMORPHIC FORMS (AND ERGODIC THEORY) IE THE SPECTRAL DECOMPOSITION OF L2(PIG(R)) UNDER THE RIGHT GIRD ACTION, ALLOWS FOR A DIOTHANTINE ANALYSIS OF J.a.

GHOSH - GORODNIK AND NEVO HAVE OBTAINED QUATITATIVE RESULTS ON THE DIOPHANTINE APPROXIMATION PROBLEM (STRONG APPROXIMATION) IN THIS CONTEXT. IN PARTICULAR IN CERTAIN CASES WHERE THE FULLY TEMPERED" VERSION OF THE RAMANUJAN CONJECTURES HOLD THE SHOW THAT ALMOST ALL POINTS OF V (IR) HAVE OPTIMALLY SHARP DIOPHANTINE EXPONENT.

· IF P 15 THIN THE DIOPHANTINE PROBLEMS ARE NORE EXOTIC AND THE FAMILIAR TOOL, GONE.

TOOLS:

STRONG APPROXIMATION: BASIC CASE: $SL_n(\mathbb{Z}) \xrightarrow{\text{onto}} SL_n(\mathbb{Z}/_{2\mathbb{Z}})$

 $\begin{array}{cccc} \mbox{IF} & \mbox{Γ} & \mbox{S} & \mbox{S} & \mbox{L}_n & (\mbox{Z}) & \mbox{AND} & \mbox{IS} & \mbox{S} & \mbox{T} & \mbox{IN} & \mbox{S} & \$

MORE GENERALLY THE ABOVE IS TRUE WITH G REPLACING SLM, G SEMI-SIMPLE AND SIMPLY CONNECTED.

(3)

TWO NOVEL TOOLS INVOLVED ARE

(1) EXPANSION OR SUPERSTRONG APPROXIMATION IT HAS ITS ROOTS IN THE GENERAL RAMANUJAN CONJECTURES IN THE THEORY OF AUTOMORPHIC FORMS. MSGLn(Q) FINITELY GENERATED LET S BE A SYMMETRIC SET OF GENERATORS (SES => S'ES). FOR g>1 LET [1(2) BE THE KERNEL OF REDUCTION MOD & AND LET X(g) BE THE ISI- REGULAR "CONGRUENCE GRAP'H" $(\Gamma/\Gamma(q),S), VERTICES \Gamma/\Gamma(q)$ $X \Pi(g) \xleftarrow{\text{JOINED}} S \propto \Pi(g)$ AND FOR SE J.

THE CRITICAL FEATURE IS THAT THESE CONGRUENCE GRAPHS X(g) FORM AN EXPANDER FAMILY AS 8->00. THE MAIN EXPANSION THEOREM WHICH 15 A CONSEQUENCE OF MANY ADVANCES FROM SPECIAL TO GENERAL AND CHRONOLOGICALLY XUE-S, GAMBURD, HELFGOTT, BOURGAIN-GAMBURD, BOURGAIN-GAMBURD-S, PYBER-SZABO, BREUILLARD-GREEN-TAO, VARJU THEOREM SUPERSTRONG APPROXIMATION (SALEHI-VARJU 2011) THE CONGRUENCE GRAPHS X(g) AS ABONE FORM AN EXPANDER FAMILY IFF G THE IDENTITY COMPONENT OF G=Zul(T) is PERFECT, $I_{E}, \quad G^{\circ} = [G^{\circ}, G^{\circ}] \quad .$

(5) THIS EXPANSION PROPERTY HAS MANY APPLICATIONS BESIDES THE DIOPHANTINE ORBIT METHOD:

· SIEVING IN GROUPS (RIVIN, LUBOTZKY MEIRI, KOWALSKI,...)

· BETTI NUMBERS OF RANDOM 3-NANIFOLDS (KOWALSKI, DUNFIELD -THURSTON MODEL)

• HEEGARD GENUS OF HYPERBOLIC 3-MANIFOLDS (LACKENBY, LONG-LUBOTZKY-RED)

• LARGE DISTORTION FOR ISOTOPY CLASSES OF KNOTS IN S³ (GROMOV-GUTH)

· GONALITY OF TOWERS OF CURVES

(20GRAF, ELLENBERG-HALL-KOWALSKI TO DIOPHANTINE FINITENESS THEOREMS).

. UNIFORM LIMIT MULTIPLICITIES



 $f \in \mathbb{Z}[x_1, x_2, \dots, x_n], \mathcal{O} = \Gamma v$ WE SAY THAT (O, f) SATURATES IF THERE IS NOO SUCH THAT EXEO: F(2c) HAS AT MOST & PRIME FACTORS 15 ZARISKI DENSE IN ZIL(O). • THE MINIMAL SUCH & 15 THE SATURATION NUMBER TO(O, F). EXAMPLES (CLASSICAL): 1) $\mathcal{T}_0(\mathbb{Z}, \mathcal{X}(\mathcal{X}+2)) = 2$ IFF TWIN PRIME 2) 10 (Z, X(X+2)) <00 BRUN 1915 3) to (Z, x(x+2)) ≤3 CHEN 1973 4) $T_0(\mathbb{Z}, x(x+k)) = 2$ FOR SOME Reco y. ZHANG , 2013 5). GIVEN M THERE ARE KI<K2 < km SUCH THAT JUCH THAT To (Z, (X+k1)(x+k2)...(X+km))=m. JMAYNARD 2013.

· FOR EXAMPLES OF THE THEORY APPLIED TO LOCAL/GLOBAL PRINCIPLES FOR INTEGRAL APOLLONIAND PACKINGS, SEE E. FUCHS BAMS 2013. A. KONTOROVICIT

• HEURISTIC ARGUMENTS SHOW THAT THE CONDITION ON RAD(G) IS PROBABLY NECESSARY FOR SATURATION!

FUNDAMENTAL SATURATION THEOREM OF THE AFFINE SIEVE (JALEHI-S 2012): Γ , f As a BOVE $O = \Gamma \cup C \mathbb{Z}^{n}$ IF $G = Z \cup (\Gamma)$ is Levi-SEMISIMPLE (IE RAD(G) CONTAINS NO TORUS) THEN $T_{0}(O, f) < \infty$.

9

UBIQUITY OF THIN MATRIX GROUPS?

· THERE IS NO DECISION PROCEDURE TO TELL WHE THER A GIVEN A ..., A IN SL2(Z) × SL2(Z) GENERATES A THIN GROUP OR NOT (MIHALOVA 1959). · IN PRACTICE IF P 15 IN FACT A CONGRUENCE SUBGROUP OF G(Z) AND IS GIVEN IN TERMS OF GENERATORS, THEN ONE CAN VERIEY THIS BY PRODUCING GENERATORS. HOWEVER IF MIS THIN HOW CAN WE CERTIFY THIS ? · FOR A TRUE GROUP THEOREST, THEON IS THE RULE! GIVEN A, BE SL, (Z) CHOSEN AT RANDOM, THEN MELA, B> HAS G=SL, P 1S FREE AND (AOUN, FUCHS). THIN.

UNIVERSAL QUANTUM GATE GROUPS:

- THE PRIMARY GOLDEN GATE GROUP [] WAS GENERATED BY
- C CLIFFORD GROUP OF ORDER 24 M G=PU(2)

AND $T = T_4 = \begin{bmatrix} i & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ $\begin{pmatrix} n \\ \pi/g & -GATE^* \end{pmatrix}$

THE KEY WAS THAT IT IS ARITHMETIC. WHAT IF INSTEAD WE ADD TO C A T/2n GATE (IT WILL STILL BE UNIVERSAL) $T_{M} = \begin{bmatrix} 1 & 0 \\ 0 & e^{iT/n} \end{bmatrix}$ (asked and studied by FOREST, GOESET KLIUCHININDU, MCKINON) In (SARNAK LETTER 2015) I INDICATE A PROOF THAT UNILESS ME 3,4,8,12. [7 WILL BE THIN!

(0) HYPERBOLIC REFLECTION GROUPS (VINBERG): f(x1,...,xn) A RATIONAL QUADRATIC FORM OF SIGNATURE (M-1,1), M75. $G = O_{f}$, $G(\mathbb{Z})$ ARITHMETIC. R₁(Z) THE (NORMAL) SUBGROUP OF G(Z) GENERATED BY B'S WHICH INDUCE HYPERBOLIC REFLECTIONS ON 1-1-1. THEN EXCEPT FOR RARE CASES

 $\left| \int \frac{\partial \phi_{f}(z)}{R_{f}(z)} \right| = \infty.$

MONODROMY GROUPS: A NATURAL GEOMETRIC SOURCE OF FINITELY GENERATED SUBGROUPS OF GLA(Z) IS THE MONODROMY REPRESENTATION ON COHOMOLOGY OF A FAMILY OF ALGEBRAIC VARIETIES, VARIATONS OF HODGE STRUCTURES, MONODROMY OF LINEAR DIFFERENTIAL EQUATIONS,.... • THE BASIC QUESTION AS TO WHETHER IN THE CASE OF VARIATION OF HODGE JTRUCTURES THE MONODROMY P IS ARITHMETIC WAS POSED IN 1973 BY GRIFFITHS AND SCHMID.

• THEY SHOW THAT IF THE PERIOD MAP FROM THE PARAMETER SPACE 5 TO THE PERIOD DOMAIN D IS OPEN THE [7 IS ARITHMETIC.

ONE PARAMETER HYPERGEOMETRIC , F. :

 α , $\beta \in \mathbb{Q}^n$, $0 \le \alpha_j \le 1, 0 \le \beta_j \le 1$

 $\begin{array}{l} (*) & Du = 0 \\ \Theta = 2 \frac{d}{d2} \\ D = (\Theta + \beta_i - 1)(\Theta + \beta_i - 1) \cdots (\Theta + \beta_n - 1) - 2(\Theta + \alpha_i) \cdots (\Theta + \alpha_n) \end{array}$

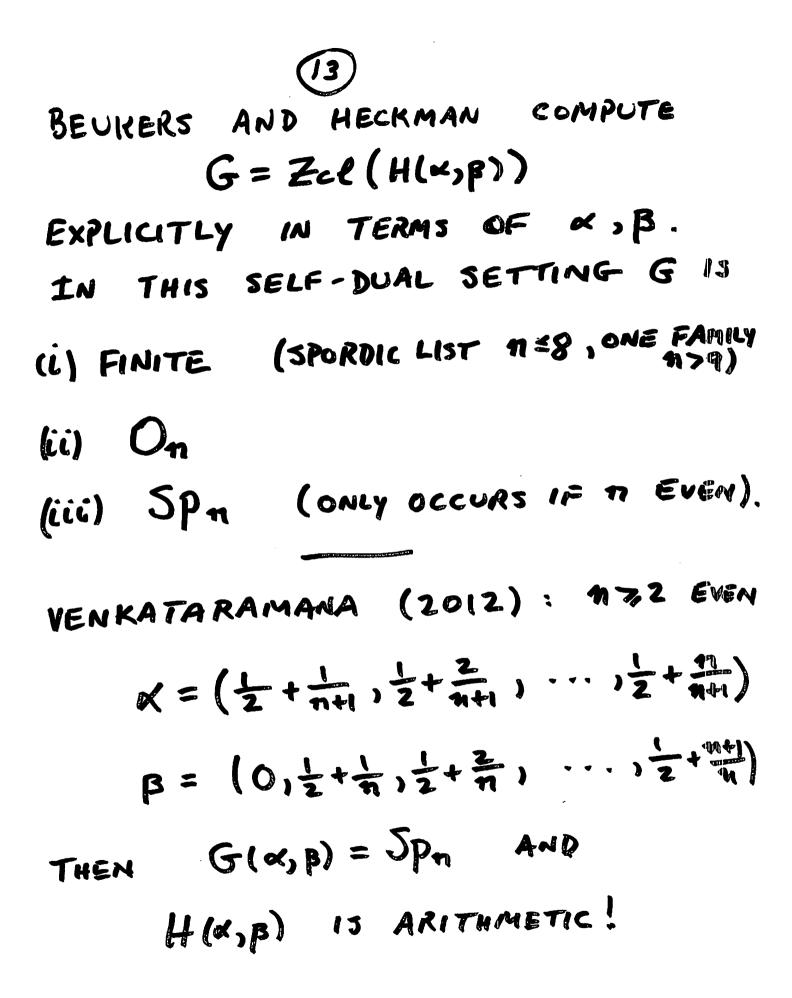
SOLUTIONS ARE

Z^{I-Bi} T^{I-Bi} T^{I-I} (I+a-Bi, + K-Bi; I+B-Bi, V, I+B-Bi |Z) WHERE V MEANS OMIT I+Bi-Bi AND 00

$$\pi F_{n-1}(S_1, ..., S_n; \eta_1, ..., \eta_{n-1}|z) = \sum_{k=0}^{\infty} \frac{(S_1)_k \cdot (S_n)_k}{(\eta_1)_k \cdot (\eta_{n-1})_k} \frac{z^k}{k!}$$

(X) IS SINGULAR AT Z=0,1, ~ AND THE MONODROMY GROUP H(~,B) IS GOTTEN BY ANALYTIC CONTINUATION ALONG PATHS IN IP²[50,1,~] OF A BASIS OF SOLUTIONS.

WE RESTRICT TO X,B SUCH THAT H(x,p) IS UP TO CONJUGATION IN GLn(Z).





THERE ARE 112 (\$\alphi, \beta)'s GIVING G(\$\alphi, \beta) = \$\beta \beta, ALL COMING FROM VARIATIONS OF INTEGRAL HODGE STRUCTURES (DORAN - MORGAN). OF THESE MORE THAN HALF ARE

ARITHMETIC (SINGH-VENKATARAMANA 2012)

14. CORRESPOND TO CALABI-YAU FAMILIES OF ヨーFOLDS EG: &=(0,0,0,0), B=(台,号,子,子) 「DWORK FAMILY, CANDELAS ET AL

BRAV-THOMAS (2012) SHOW THAT SEVEN OF THESE ARE THIN, WHILE SINGH THAT THE OTHER SEVEN ARE ARITHMETIC.

BRAV-THOMAS SHOW THAT THE GENERATORS OF TT, (P'\ {0,1,0}), A AND C ABOUT O AND 1 PLAY GENERALIZED PING-PONG ON A COMPLICATED POLYHEDRAL SUBJET OF TP³.

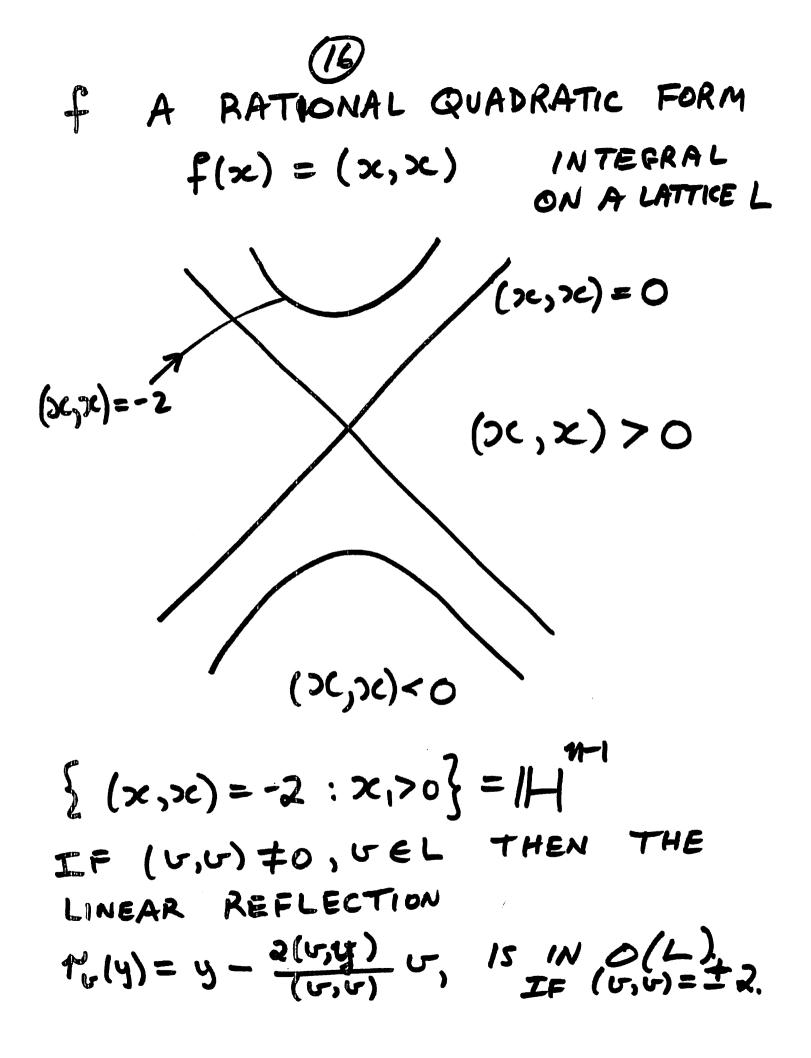


(a, b) 15 HHM IF G(a, b) 13 ORTHOGONAL AND OF SIGNATURE (M-1, 1). (IN THIS CASE M 15 ODD)

THEOREM 1 (F-M-S)

WITH THE EXCEPTION OF AN EXPLICIT (LONG) LIST OF FINITERY MANY (~, p)'S ALL WITH M&9, ALL HHM'S COME IN SEVEN INFINITE PARAMETRIC FAMILIES.

FOR THE HHM'S WE GIVE A ROBUST OBSTRUCTION TO H(M,B) BEING ARITHMETIC, THAT IS A CERTIFICATE FOR H(M,B) TO BE THIN.



|--|

· IF (U,U) > O THEN TO INDUCES A HYPERBOLIC REFLECTION ON 1H ^{M-1} .			
· IF (U,U) <o eq<br="" then="" to="">INDUCES A CARTAN INVOLUTION ON M.</o>			
INDUCES A CARTAN INVOLUTION ON M.			
KEY POINT: FOR HHM'S $H(\alpha, \beta) = \langle A, B \rangle$			
B LOCAL MONODROMY ABOUT 60			
TAND C=A'B 15 A CARTAN INVOLUTION			
UP TO COMMENSURABILITY H(«))			
IS GENERATED BY THE			
CARTAN INVOLUTIONS			
ARCAR, REZ.			

(B) $R_2(L) := \{ v \in L : (v, v) = 2 \}$ THE INTEGRAL ROOT VECTORS GIVING HYPERBOLIC REFLECTIONS $R_{-2}(L) := \{ v \in L : (v, v) = -2 \}$ THE INTEGRAL ROOT VECTORS GIVING CARTAN INVOLUTIONS. ACCORDING TO VINBERG/NIKULIN EXCEPT FOR SPECIAL L'S

 $|O(L)/R_2(L)| = 0$

LET $\Delta C R_{-2}(L)$

WE GIVE A CONDITION UNDER **W**HICH $\langle \mathcal{M}_{U}: U \in \Delta \rangle$ HAS FINITE IMAGE IN $O(L)/R_2(L)$.

(19)				
MINIMAL DISTANCE GRAPH X(L):				
THE VERTICES OF X(L) ARE				
THE CARTAN ROOTS R-2(L) AND				
JOIN & TO W IF $(v,w) = -3$				
(MINIMAL DISTANCE THEY CAN BE)				
PROPOSITION IF & IS CONTAINED				
IN A CONNECTED COMPONENT				
OF X(L) THEN				
くで: いEム> HAS FINITE IMAGE				
IN $O(L)/R_2(L)$.				
WITH THIS WE CAN SHOW				

THAT MOST OF THE HHM'S ARE THIN.

	20	
THEOREM	n	000

 $\propto = \left(0, \frac{1}{n+1}, \frac{2}{n+1}, \frac{n-1}{2(n+1)}, \frac{n+3}{2(n+1)}, \frac{n}{n+1}\right), \beta = \left(\frac{1}{2}, \frac{1}{n}, \frac{2}{n}, \frac{n}{n+1}\right)$

AnD

 $A = \left(\frac{1}{2}, \frac{1}{2\pi - 2}, \frac{3}{2\pi - 2}, \frac{2\pi - 3}{2\pi - 2}\right), B = \left(0, 0, 0, \frac{1}{\pi - 2}, \frac{3\pi - 3}{\pi - 2}\right)$ A = HYPERBOLIC HYPERGEOMETRIC AND

ARE ARITHMETIC IF M=3 AND THIN M75

CONJECTURE THERE ARE ONLY FINITELY MANY HHM'S WHICH ARE ARITHMETIC.

•H. PARK (THESIS 2013) SHOWS THAT THE HMM X=(0,古,寺,寺,毛)、平(古,寺,士,寻,芳)

IS GEOMETRICALLY FINITE (AND THIN).

(2)

REFERENCES TO MOST OF THE ABOVE CAN BE FOUND IN THE SURVEY

"NOTES ON THIN MATHIX GROUPS" P. SARNAK MSRI PUBL. 61 (2014) 343-362.