

⑥

AHLFORS LECTURE II

INTEGER POINTS ON AFFINE  
CUBIC SURFACES

PETER SARNAK

NOV 1 2019

JOINT WORK WITH A. GHOSH  
AND WITH J. BOURGAIN / A. GAMBURD.

$f(x_1, x_2, \dots, x_n)$  A POLYNOMIAL WITH  
 INTEGRAL COEFFICIENTS AND  $f$  AND  $f-k$   
 IRREDUCIBLE OVER  $\mathbb{Q}$  FOR ALL  $k$ .

$$f(x_1, x_2, \dots, x_n) = k \quad \text{---} (*)$$

TO BE SOLVED OVER  $\mathbb{Z}$  (OR  $\mathcal{O}_K$   $K$   
 A NUMBER FIELD)

$$V_{f,k} = \{x : f(x) = k\}, \text{ AFFINE HYPER SURFACE.}$$

LOCAL CONGRUENCE OBSTRUCTIONS /  $\mathbb{Z}$ :

NEC. COND. IS THAT

$$f(x) \equiv k \pmod{q}, q \geq 1 \text{ HAS SOLUTION.}$$

IF THE LOCAL CONDITION IS SUFFICIENT  
 FOR SOLVABILITY OVER  $\mathbb{Z}$ ; WE HAVE  
 A LOCAL TO GLOBAL OR HASSE PRINCIPLE.

$f$  LINEAR:

$$f(x_1, \dots, x_n) = a_1 x_1 + \dots + a_n x_n = k$$

NEC COND IS  $\gcd(a_1, \dots, a_n) \mid k$

IT IS ALSO SUFFICIENT.

(6'')

# f QUADRATIC (HILBERT'S ELEVENTH PROBLEM):

TO SOLVE (\*) WITH

(a)  $x, k \in K$

(b)  $x, k \in \mathcal{O}_K$

(a) HASSE-MINKOWSKI THEOREM:

(\*) IS SOLVABLE IN  $K$  IFF IT IS SOLVABLE OVER EVERY  $K_v$ , FOR EVERY COMPLETION  $K_v$  OF  $K$ .

(b) OVER  $\mathcal{O}_K$  MUCH MORE DIFFICULT;  
FOR EXAMPLE WHICH NUMBERS ARE SUMS OF THREE SQUARES IN  $\mathcal{O}_K$ ?

• A STABLE LOCAL TO GLOBAL PRINCIPLE (THAT IS EXCEPT FOR FINITELY MANY EXCEPTIONS) HOLDS FOR  $m \geq 3$  (SIEGEL, KNESER, DUKE/IWANIEC, COGDELL/PIATETSKI SHAPIRO (S))

KEY:  $V_{f,k}$  IS A HOMOGENEOUS SPACE FOR AN ORTHOGONAL GROUP  $\rightarrow$  MODULAR FORMS.

# CUBIC FORMS

(1)

• AN AFFINE CUBIC  $f$  IS A POLYNOMIAL IN  $\mathbb{Z}[x_1, \dots, x_n]$  WITH LEADING HOMOGENEOUS PART  $f_0$  OF DEGREE 3 AND NON-DEGENERATE, WE ALSO ASSUME THAT  $f$  AND  $f-k$  ARE IRREDUCIBLE.

(\*\*)  $V_{k,f} = \{x : f(x) = k\}$  AFFINE-HYPERSURFACE

•  $k$  IS ADMISSIBLE IF THERE ARE NO LOCAL CONGRUENCE OBSTRUCTIONS TO (\*\*)  
(THESE HAVE A SIMPLE DESCRIPTION)

RICHNESS OF  $V_{k,f}(\mathbb{Z})$ :

FOR  $k$  ADMISSIBLE IS  $V_{k,f}(\mathbb{Z})$  NON-EMPTY (IE HAS A HASSE PRINCIPLE), ZARISKI-DENSE IN  $V_{k,f}$ , SATISFY A FORM OF STRONG-APPROXIMATION?

$n=2$  (SUPER-CRITICAL) THUE/SIEGEL

$$|V_{k,f}(\mathbb{Z})| < \infty$$

SCHMIDT SHOWS THAT FOR VERY FEW ADMISSIBLE  $k$ 'S IS  $V_{k,f}(\mathbb{Z}) \neq \emptyset$ .

- 12
- $n \geq 10$  (SUBCRITICAL) BROWNING/HEATH-BROWN  
 $f_0$  NONSINGULAR THEN FOR  $k$  ADMISSIBLE  
 $V_{k,f}(\mathbb{Z}) \neq \emptyset$ , IT IS ZARISKI DENSE AND IT  
 SATISFIES STRONG APPROXIMATION.
  - $n \geq 4$  (SUBCRITICAL) HOOLEY  
 $f$  HOMOGENEOUS NONSINGULAR AND ASSUMING  
 THE RIEMANN HYPOTHESIS FOR CERTAIN ASSOCIATED  
 HASSE-WEIL ZETA FUNCTIONS,  $V_{k,f}(\mathbb{Z}) \neq \emptyset$  FOR  
 ALMOST ALL ADMISSIBLE  $k$ 'S.
  - $n=3$  (CRITICAL) AFFINE CUBIC SURFACE, VERY LITTLE IS KNOWN.

### EXAMPLE

$$f = S(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3$$

- $k$  IS ADMISSIBLE IFF  $k \not\equiv 4, 5 \pmod{9}$
- IT IS POSSIBLE THAT FOR EVERY ADMISSIBLE  
 $k$ ,  $V_{k,S}(\mathbb{Z}) \neq \emptyset$  AND IS ZARISKI DENSE IN  $V_k$
  - A. BOOKE R (2019) (USING A METHOD OF ELKIES)
- $$33 = (8866128975287528)^3 + (-8778405442862239)^3 + (-2736111468807040)^3$$
- $$42 = (-80538738812075974)^3 + (80435758145817515)^3 + (12602123297335631)^3$$
- WITH D. SUTHERLAND

(3)

• LEHMER, BEUKERS SHOW THAT  $V_{S,1}(\mathbb{Z})$  IS ZARISKI DENSE IN  $V_{S,1}$ .

USING CUBIC RECIPROCITY ONE CAN SHOW THAT STRONG APPROXIMATION FAILS FOR  $V_{S,k}(\mathbb{Z})$ .

E.G.  $x \in V_{S,3}(\mathbb{Z}) \Rightarrow x_1 \equiv x_2 \equiv x_3 \pmod{9}$

(CASSELS, HEATH-BROWN, COLLIOT-THÉLENE/WITTENBERG)

HOWEVER IN THE SLIGHTLY WEAKER FORM

$$V_{S,k}(\mathbb{Z}) \rightarrow V_{S,k}(\mathbb{Z}/p\mathbb{Z}), \text{ BEING ONTO}$$

FOR  $p$  A LARGE PRIME, MAY HOLD.

A DIOPHANTINE THEORY FOR INTEGRAL POINTS ON SOME SPECIAL CUBIC SURFACES CAN BE DEVELOPED

A. GHOSH / S, J. BOURGAIN / A. GAMBURD / S

THESE START WITH MARKOFF'S SURFACES.

# MARKOFF'S CUBIC SURFACES

[4]

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

$$V_k = V_{k,M} = \{x \mid M(x) = k\}$$

$k=0$  : IS MARKOFF'S SURFACE

$k=4$  : IS THE CAYLEY CUBIC  
(IT IS SPECIAL IN WHAT FOLLOWS)

•  $V_k(\mathbb{Z})$  ARISES IN MANY CONTEXTS

DIOPHANTINE APPROXIMATION (MARKOFF)

SIMPLE CLOSE GEODESICS ON  
THE MODULAR SURFACE (H. COHN)

EXCEPTIONAL VECTOR BUNDLES OVER  $\mathbb{P}^2$   
(GORODENSTEIN / RUPAKOV)

SMOOTHABLE DEL-PEZZO SURFACES  
(HACKING / PROKHOROV)

SYMPLECTIC 4-MANIFOLDS VIA LEFSCHETZ  
FIBRATIONS (AURoux)

⋮

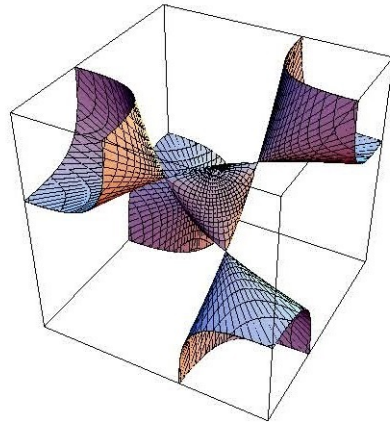
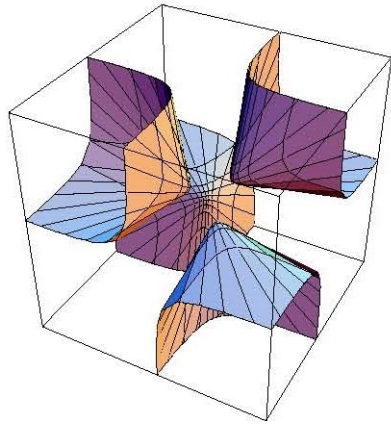
•  $V_k$  IS ALSO THE RELATIVE CHARACTER  
VARIETY OF REPRESENTATIONS OF  $\pi_1(\Sigma_{1,1}) \rightarrow SL_2$

• IT ALSO ARISES <sup>IN</sup> ~~AS~~ THE NON-LINEAR  
MONODROMY GROUP OF PAINLEVE' VI.

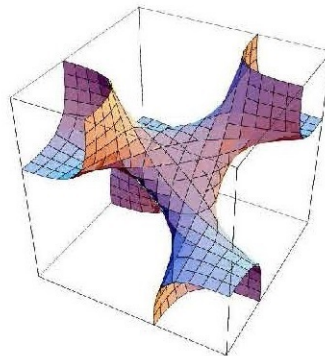
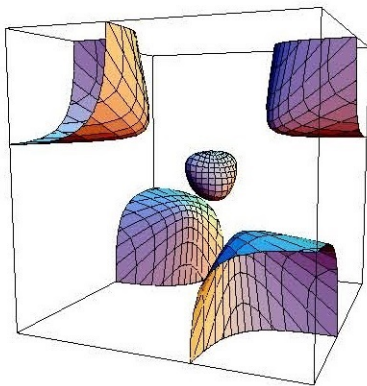
$V_0$  Markoff's cubic surface

$V_4$  Cayley's cubic surface

$V_k(\mathbb{R})$  for different  $k$ :



$k = 0$  and  $k = 4$



$k = 2$  and  $k = 8$



[6]

THE REASON ONE CAN STUDY  $V_k(\mathbb{Z})$  IS THAT IT IS ACTED ON BY A NON-LINEAR GROUP OF MORPHISMS ALLOWING DESCENT.

$\Gamma$ , THE GROUP IN  $\text{AUT}(\mathbb{A}^3)$  GENERATED BY PERMUTATIONS OF THE COORDINATES AND SWITCHING THE SIGNS OF TWO COORDINATES, AND THE VIETA INVOLUTIONS  $R_1, R_2, R_3$

$$R_3(x_1, x_2, x_3) = (x_1, x_2, x_1 x_2 - x_3)$$

PRESERVES  $V_k$  AND  $V_k(\mathbb{Z})$ . ( $\Gamma \cong \text{PGL}_2(\mathbb{Z})$ )

• FOR  $k \neq 4$ ,  $V_k(\mathbb{Z})$  CONSISTS OF A FINITE NUMBER  $h(k)$  OF  $\Gamma$ -ORBITS (MARKOFF, HURWITZ, MORDELL).

CLASSICAL QUESTIONS:

(i) WHEN IS  $V_k(\mathbb{Z}) \neq \emptyset$  IE  $h(k) > 0$ .

(ii) IF  $h(k) > 0$ , IS  $V_k(\mathbb{Z})$  INFINITE,

ZARISKI DENSE, SATISFY A FORM OF STRONG APPROXIMATION?

# HASSE PRINCIPLE

[7]

LOCAL CONGRUENCE OBSTRUCTIONS:

$$V_k(\mathbb{Z}_p) \neq \emptyset \quad \text{FOR ALL } p \quad \text{IFF } k \not\equiv 3(4) \\ \text{OR } \pm 3(\text{mod } 9).$$

WE RESTRICT TO  $k$ 'S WHICH HAVE LOCAL INTEGRAL POINTS AND SAY THAT  $V_k$  FAILS HASSE'S PRINCIPLE IF  $V_k(\mathbb{Z}) = \emptyset$ .

FOR  $|k| \geq 5$  CALL  $k$  SPECIAL IF  $V_k(\mathbb{Z})$  CONTAINS A POINT  $x$  WITH  $|x_j| = 0, 1, 2$ . THE SPECIAL  $k$ 'S ARE EASY TO DESCRIBE AND ANALYZE, THEY ARE OF ZERO DENSITY. REMAINING  $k$ 'S ARE CALLED GENERIC.

• FOR  $k > 0$  GENERIC A POINT  $x \in V_k(\mathbb{Z})$  IS GHOSH REDUCED IF IT IS OF THE FORM

$$(-x_1, x_2, x_3) \quad \text{WITH} \quad 3 \leq x_1 \leq x_2 \leq x_3 \quad \text{AND} \\ x_1^2 + x_2^2 + x_3^2 + x_1 x_2 x_3 = k$$

• (GHOSH) FOR  $k > 0$  GENERIC

$$\mathbb{P} \setminus V_k(\mathbb{Z}) \cong \text{GHOSH REDUCED POINTS.}$$

COR: (a)  $h(k) \ll |k|^{1/3}$

(b)  $\sum_{0 < k \leq K} h(k) \sim \frac{K (\log K)^2}{36}, K \rightarrow \infty$

$\sum_{-K \leq k < 0} h(k) \sim \frac{K (\log K)^2}{48}, K \rightarrow \infty.$

THE EXPLICIT FUNDAMENTAL DOMAINS  
ALLOW FOR THE NUMERICAL COMPUTATIONS  
OF THE  $h(k)$ 'S AND THESE INDICATE  
THAT

$$\left| \{ |k| \leq K : V_k \text{ FAILS HASSE} \} \right| \sim C K^\Theta$$

WITH  $C \neq 0$  AND  $\Theta \approx 0.887 \dots$

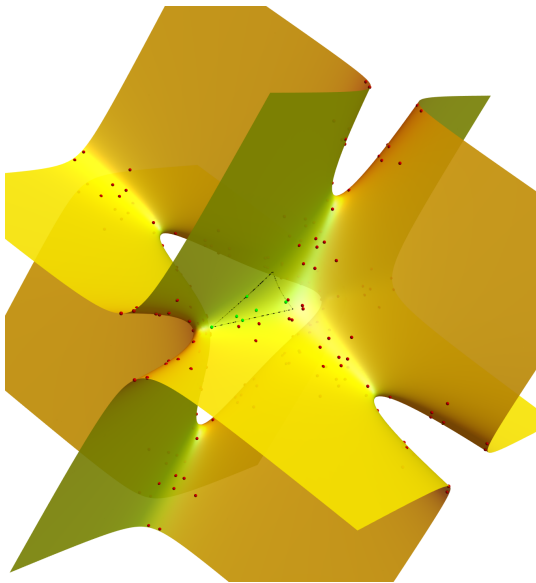


Figure: Lattice points and fundamental set (triangular) for  $k = 3685$ .

# THEOREM 1 (GHOSH / S 2017)

9

(i) THERE ARE INFINITELY MANY  $k$ 's ~~WHICH~~ <sup>WHICH</sup> FAIL THE HASSE PRINCIPLE. THE NUMBER OF SUCH WITH  $|k| \leq K$  IS AT LEAST  $K^{1/2}/\log K$ .

(ii) Fix  $t \geq 0$

$$|\{ |k| \leq K : k \text{ ADMISSIBLE, } h(k) = t \}| = o(K) \quad K \rightarrow \infty$$

$\Rightarrow$  ALMOST ALL  $k$ 's SATISFY HASSE AND ALSO THESE  $V_k(\mathbb{Z})$ 's ARE ZARISKI DENSE.

## COMMENTS:

(a) THE HASSE FAILURES ARE PRODUCED BY AN OBSTRUCTION VIA QUADRATIC RECIPROCITY. THEY COME IN TWO TYPES: ONE DIRECT USE OF RECIPROCITY AND THE SECOND WHICH ALSO INCORPORATES THE DESCENT GROUP.

RECENTLY LOUGHRAN AND MITNANKIN; AND INDEPENDENTLY COLLIOT-THELENE, DASHENG AND F.XU HAVE SHOWN THAT THE OBSTRUCTIONS OF THE FIRST (BUT NOT SECOND) CAN BE BE EXPAINED IN TERMS OF AN INTEGRAL BRAUER-MANIN OBSTRUCTION.

FOR EXAMPLE IF

[10]

$$k = 4 + 2v^2$$

WITH  $v$  HAVING ALL OF ITS PRIME FACTORS  
 $\equiv \pm 1 \pmod{8}$  AND  $v \equiv 0, \pm 3, \pm 4 \pmod{9}$ ,  
THEN  $k$  IS ADMISSIBLE BUT  $V_k(\mathbb{Z}) = \emptyset$ .

(b) IS PROVED BY COMPARING THE  
NUMBER OF POINTS ON  $V_k(\mathbb{Z})$  IN  
CERTAIN TENTACLED REGIONS GOTTEN  
BY SPECIAL PLANE SECTIONS, WITH THE  
EXPECTED NUMBER OF SOLUTIONS ACCORDING  
TO A PRODUCT OF LOCAL DENSITIES.

THE KEY IS THAT THE VARIANCE OF  
THIS COMPARISON GOES TO ZERO ON  
AVERAGING  $|k| \leq K$ . THIS MOVING PLANE

QUADRIC METHOD APPLIES TO MORE  
GENERAL CUBIC SURFACES INCLUDING  
ONES THAT DON'T CARRY MORPHISMS.

## (B)(VERTICAL) ALGEBRAIC PAINLEVE' VI 11

DUBROVIN / MAZZOCCO AND LISOVYY / TIKHYY  
CLASSIFIED THE SOLUTIONS  $W(t)$  TO PAINLEVE' VI  
EQUATIONS WHICH ARE ALGEBRAIC FUNCTIONS OF  $t$ .

$$\frac{d^2 W}{dt^2} = \frac{1}{2} \left( \frac{1}{W} + \frac{1}{W-1} + \frac{1}{W-t} \right) \left( \frac{dW}{dt} \right)^2 - \left( \frac{1}{t} + \frac{1}{t-1} + \frac{1}{W-t} \right) \frac{dW}{dt} \\ + \frac{W(W-1)(W-t)}{2t^2(t-1)^2} \left( (\Theta_\infty - 1)^2 - \frac{\Theta_x^2 t}{W^2} + \frac{\Theta_y^2 (t-1)}{(W-1)^2} + \frac{(1-\Theta_z^2)t(t-1)}{(W-t)^2} \right)$$

HERE  $\Theta_\infty, \Theta_x, \Theta_y, \Theta_z$  ARE PARAMETERS DEFINING  
P-VI. USING APPROPRIATE CO-ORDINATES THE  
NON-LINEAR MONODROMY OF SOLUTIONS REDUCES  
TO THE PROBLEM OF DETERMINING <sup>THE</sup> A FINITE  
ORBITS OF A NONLINEAR ACTION ON  $A^3$ .

FOR EXAMPLE IF  $\Theta_x = \Theta_y = \Theta_z$  THIS GROUP  
 $G$  IS GENERATED BY INVOLUTIONS  $R_1, R_2, R_3$   
AND PERMUTATIONS OF THE CO-ORDS

$$R_3 : (x_1, x_2, x_3) \longrightarrow (x_1, x_2, x_1 x_2 - x_3)$$

AND SIMILARLY FOR  $R_1$  AND  $R_2$ .

THE TRANSFORMATION

$$\sigma_{2,3} R_3 : (x_1, x_2, x_3) \rightarrow (x_1, x_4 x_2 - x_3, x_2)$$

IS IN  $G$  AND IF FIXES  $x_1$  AND INDUCES  
THE LINEAR TRANSF  $A$  ON  $(x_2, x_3)$ .

$$A = \begin{bmatrix} x_1 & -1 \\ 1 & 0 \end{bmatrix}$$

SO IF  $(x_1, x_2, x_3)$  IS ON A FINITE  
ORBIT THEN

$$x_4 = \text{TRACE}(A) = 2 \cos(2\pi \tau_1) \text{ WITH } \tau_1 \in \mathbb{Q}.$$

SIMILARLY FOR  $x_2$  AND  $x_3$  AND WITH  
A SUITABLY CHOSEN ELEMENT OF  $G$  ONE  
FINDS THAT IF  $(x_1, x_2, x_3)$  IS IN A FINITE  
ORBIT IT GIVES RISE TO A SOLUTION OF

$$\cos 2\pi \phi_1 + \cos 2\pi \phi_2 + \cos 2\pi \phi_3 + \cos 2\pi \phi_4 = 0$$

WITH THE  $\phi_i$ 'S IN  $\mathbb{Q}$  AND RELATED TO  $\tau_1, \tau_2, \tau_3$ .  
——— (\*)

BY LANG'S  $G_m$  WE CAN PARAMETRIZE

ALL THE SOLUTIONS OF (\*) AND THEN

CHECK DIRECTLY WHICH CORRESPOND TO  
FINITE ORBITS OF  $G$  ACTING ON  $A^3$ .



# STRONG APPROXIMATION

11

WHEN  $V_k(\mathbb{Z}) \neq \emptyset$  HOW RICH IS IT BEYOND ZARISKI DENSITY?

WE DISCUSS THE MARKOFF CASE  $k=0$ .

THE GENERAL CASE IS SIMILAR BUT FIRST REQUIRES A STUDY OF ALL THE FINITE  $\Gamma$ -ORBITS IN  $A^3(\overline{\mathbb{Q}})$ .

• THIS IS CLOSELY RELATED TO THE DETERMINATION (DUBROVIN-MAZZACO) OF THE ALGEBRAIC PAINLEVE VI'S.  
OUR TREATMENT OF THE LATTER USES THE RESOLUTION (EFFECTIVE) OF LANG'S  $G_m$  CONJECTURE.

$$Y : x_1^2 + x_2^2 + x_3^2 - 3x_1x_2x_3 = 0$$

$\Gamma$  AS BEFORE EXCEPT THAT THE  $R_j$ 'S ARE

$$R_3((x_1, x_2, x_3)) = (x_1, x_2, 3x_1x_2 - x_3)$$

$h=2$ , WITH ONE ORBIT BEING  $\{0\}$

AND THE OTHER  $Y^*(\mathbb{Z}) = \Gamma \cdot (1, 1, 1)$

# STRONG APPROXIMATION CONJECTURE FOR $\gamma$ :

12

REDUCTION MOD  $p$

$$\gamma^*(\mathbb{Z}) \longrightarrow \gamma^*(\mathbb{Z}/p\mathbb{Z}) \quad \text{IS ONTO FOR ALL PRIMES } p.$$

- 
- $\Gamma$  ACTS ON REDUCTION MOD  $p$  AS A PERMUTATION GROUP ON  $\gamma^*(\mathbb{Z}/p\mathbb{Z})$ .
  - STRONG APPROXIMATION  $\iff \Gamma$  ACTING TRANSITIVELY ON  $\gamma^*(\mathbb{Z}/p\mathbb{Z})$ .

NOTE:  $|\gamma^*(\mathbb{Z}/p\mathbb{Z})| \sim p^2$  AS  $p \rightarrow \infty$ .

AS LONG AS  $p^2 - 1$  IS NOT VERY SMOOTH (EG  $= k!$ ) WE CAN PROVE STRONG APPROXIMATION.

## THEOREM 2 (BOURGAIN-GAMBURD-S; 2014)

113

FOR  $\varepsilon > 0$  AND  $p$  LARGE THERE IS A  $\Gamma$  ORBIT  $\mathcal{O}(p)$  IN  $Y^*(\mathbb{Z}/p\mathbb{Z})$  SUCH THAT

$$|\mathcal{O}^c(p)| = |Y^*(\mathbb{Z}/p\mathbb{Z}) \setminus \mathcal{O}(p)| \ll_{\varepsilon} p^{\varepsilon}$$

AND EVERY  $\Gamma$ -ORBIT  $t(p)$  IN  $Y^*(\mathbb{Z}/p\mathbb{Z})$  SATISFIES

$$|t(p)| \gg (\log p)^{1/3}.$$

---

THESE HAVE BEEN RECENTLY IMPROVED BY  
KONYAGIN / MAKARYCHEV / SHPARLINSKI / NYUGIN (2017)

TO

$$|\mathcal{O}^c(p)| \leq \exp((\log p)^{2/9+o(1)})$$

$$|t(p)| \gg (\log p)^{7/9}.$$

---

## THEOREM 3 (B-G-S 2015)

$$|\{p \leq T : \text{STRONG APPROXIMATION FAILS FOR } p\}| \ll_{\varepsilon} T^{\varepsilon},$$

$\varepsilon > 0.$

---

SO IN GENERAL THERE IS ALWAYS A GIANT COMPONENT AND THE STRONG APPROXIMATION CONJECTURE HOLDS EXCEPT PERHAPS FOR VERY FEW  $p$ 'S.

# THEOREM 4 (MEIRI-PUDER 2019):

- IF  $p \equiv 1(4)$  AND  $p$  SATISFIES STRONG APPROXIMATION FOR  $\gamma^*(\mathbb{Z}/p\mathbb{Z})/\pm 1$  THEN THE ACTION OF  $\Gamma$  ON THE LATTER IS EITHER THE FULL ALTERNATING OR SYMMETRIC GROUP.
- UNDER THE SAME ASSUMPTIONS ON  $p$ , THE ORBIT OF EVERY POINT IN  $\gamma^*(\mathbb{Z}_p)$  IS DENSE ; HERE  $\mathbb{Z}_p$  IS THE  $p$ -ADIC INTEGERS

THEOREM 4 ALLOWS ONE TO SHOW THAT

$$\gamma^*(\mathbb{Z}) \rightarrow \gamma^*(\mathbb{Z}/q\mathbb{Z}) \text{ IS ONT}$$

FOR  $q = p_1 p_2 \dots p_l$ ,  $p_j \equiv 1(4)$  AND SATISFYING STRONG APPROXIMATION (GOURSAT-LEMMA).

WITH THESE WE CAN EXECUTE SOME SIMPLE SIEVING AND COUPLE IT WITH SOME TEICHMULLER DYNAMICS (MIRZAKHANI) TO ANSWER SOME OLD QUESTIONS ABOUT MARKOFF NUMBERS

$M$ : MARKOFF NUMBERS, THAT IS  
CO-ORDINATES OF A MARKOFF TRIPLE  
 $x \in \underline{Y}(\mathbb{Z})$  WITH  $x_j > 0$ .

$M$ : 1, 2, 5, 13, 29, 34, 89, 169, 194, ...

• FROBENIUS:  $m \in M \Rightarrow m \not\equiv 0, \pm 2/3 \pmod{p}$ ,

IF  $p \equiv 3(4)$  AND  $p \neq 3$ .

• STRONG APPROXIMATION  $\Rightarrow$  THESE ARE THE ONLY CONGRUENCE OBSTRUCTIONS.

$M$  IS LACUNARY:

$$|\{m \leq T : m \in M\}| \sim c (\log T)^2, \quad \begin{array}{l} \text{ZAGIER (1982)} \\ \text{MIRZAKHANI} \\ \text{(2016)} \end{array}$$

THEOREM 5: (B-G-S 2015)

ALMOST ALL  $m \in M$  ARE COMPOSITE

$$|\{p \leq T : p \in M, p \text{ prime}\}| = o(|\{m \in M : m \leq T\}|)$$

AS  $T \rightarrow \infty$ .

# REMARKS

TOOLS ARE ELEMENTARY COMING FROM ANALYTIC NUMBER THEORY, CURVES OVER FINITE FIELDS AND COMBINATORICS. ONE INTERESTING FEATURE BEING:

$$C_\lambda : \begin{cases} y + y^{-1} = x + \lambda x^{-1}, & x, y \in \mathbb{F}_p^* \\ x \in H_1, y \in H_2 \\ H_1, H_2 \leq \mathbb{F}_p^* & , |H_1| \leq |H_2| \end{cases}$$

NEED AN UPPER BOUND FOR  $|C|$

OF THE FORM

$$|C| \leq |H_2|^{\frac{1}{2}}$$

FOR SOME  $\frac{1}{2} < 1$   
INDEPENDENT OF  $p$ .

- IF  $|H_2| \geq \sqrt{p}$  ONE CAN USE THE RIEMANN HYPOTHESIS FOR CURVES OVER FINITE FIELDS TO PROVE THIS.
- FOR  $|H_2|$  SMALL THIS IS OF NO USE AND WE USE STEPANOV'S ELEMENTARY PROOF OF WEIL'S THEOREM (SPECIFICALLY AUXILIARY POLYNOMIALS) TO ESTABLISH SUCH A BOUND.

# CHARACTER VARIETIES

$V_k$  IS THE RELATIVE CHARACTER VARIETY OF REPRESENTATIONS OF THE FUNDAMENTAL GROUP OF A SURFACE OF GENUS ONE WITH ONE PUNCTURE, TO  $SL_2$ . THE ACTION OF THE MAPPING CLASS GROUP IS THAT OF  $\Gamma$ .

MORE GENERALLY THE (AFFINE) RELATIVE CHARACTER VARIETY  $X_k$  OF REPRESENTATIONS OF  $\pi_1(\Sigma_{g,n})$  INTO  $SL_2$  IS DEFINED OVER  $\mathbb{Z}$ .

$\Sigma_{g,n}$  IS A SURFACE OF GENUS  $g$  WITH  $n$  PUNCTURES.

ONE CAN STUDY THE DIOPHANTINE PROPERTIES OF  $X_k(\mathbb{Z})$ .

J.H. WHANG (PRINCETON THESIS 2018) HAS MADE BIG STEPS IN THIS DIRECTION.

(i)  $X_k$  HAS A PROJECTIVE COMPACTIFICATION RELATIVE TO WHICH  $X_k$  IS "LOG CALABI YAU". ACCORDING TO CONJECTURES OF VOJTA THIS PLACES  $X_k$  AS BEING IN THE SAME THRESHOLD SETTING AS AFFINE CUBIC SURFACES.

(ii)  $X_k(\mathbb{Z})$  HAS A FULL DESCENT IN THAT THE MAPPING CLASS GROUP ACTS VIA NON-LINEAR MORPHISMS ON  $X_k(\mathbb{Z})$  WITH FINITELY MANY ORBITS.

• THESE AND MORE GENERAL CHARACTER VARIETIES CONNECTED WITH HIGHER TEICHMULLER THEORY OFFER A RICH FAMILY OF THRESHOLD AFFINE VARIETIES FOR WHICH ONE CAN APPROACH THE STUDY OF INTEGRAL POINTS.



THERE IS A RICH STUDY OF THE ACTION OF  $\Gamma$  ON  $X_k(\mathbb{R})$  (THURSTON, ... GOLDMAN...) AND ON  $X_k(\mathbb{C})$  (CANTAT, McMULLEN ... ENTROPY)

• SINCE  $X_k$  IS DEFINED OVER  $\mathbb{Z}$  ONE CAN EXAMINE THE ORBIT CLOSURES OF  $\Gamma$  IN  $X_k(\mathbb{Q}_p)$ . THE BASIC COMPACT INVARIANT SET IS  $X_k(\mathbb{Z}_p)$  AND WE EXPECT AS WITH  $g=1, n=1$  THE ACTION OF  $\Gamma$  ON  $X_k(\mathbb{Z}_p)$  IS MINIMAL (CLOSURE OF ORBITS ARE AS LARGE AS POSSIBLE).

• BISWAS | GUPTA | MJ | WHANG (2019): CLASSIFY FINITE (EVEN BOUNDED) ORBITS OF  $\Gamma$  ON  $X_k(\mathbb{C})$  FOR  $g \geq 1, n \geq 0$  IN TERMS OF THEIR LIFT  $\rho$  TO A REPRESENTATION OF  $\Sigma_{g,n}$  INTO  $SL_2(\mathbb{C})$ , BASICALLY IT SHOULD BE FINITE.

IF ONE REPLACES  $\mathbb{Z}$  BY A LARGER  
RING<sup>D</sup> SUCH AS  $\mathbb{Z}[\frac{1}{5}]$  OR  $\mathbb{Z}[\sqrt{2}]$   
WHICH CONTAIN INFINITELY MANY  
UNITS, THEN THE ACTION OF  $\Gamma$  ON  
 $V_{M,k}(D)$  NEED NO LONGER CONSIST  
OF FINITELY MANY ORBITS (FIRST  
OBSERVED BY SILVERMAN).

- THIS MAKES OUR DIOPHANTINE  
ANALYSIS MUCH MORE CHALLENGING.

• IT APPEARS THAT THERE ARE FEWER  
(IF ANY) EXCEPTIONS TO THE HASSE  
PRINCIPLE

• FOR THE MARKOFF SURFACES THIS  
HAS BEARING THROUGH FRICKE'S TRACE  
IDENTITIES ON COMMUTATORS IN  
 $SL_2(D)$ .

## ANER SHALEV QUESTION

IS EVERY ELEMENT IN  
 $SL_3(\mathbb{Z})$  A ONE COMMUTATOR,  
IE CAN ONE SOLVE FOR EVERY  
 $B$  IN  $SL_3(\mathbb{Z})$  ~~FOR~~  
 $XYX^{-1}Y^{-1} = B$  ?

---

AVNI-GELANDER-KASSABOV-SHALEV  
SHOW THAT ESSENTIALLY THERE IS  
NO LOCAL OBSTRUCTION TO THIS  
IN THAT IT IS TRUE IN EVERY  
FINITE QUOTIENT OF  $SL_3(\mathbb{Z})$ .

REFERENCES CAN BE FOUND IN

"INTEGRAL POINTS ON MARKOFF  
TYPE CUBIC SURFACES"

A. GHOSH + P. SARNAK

ATXIV: 1706.06712

AND

"NONLINEAR DESCENT ON  
MODULI OF LOCAL ~~SYSTEMS~~ SYSTEMS"

J. H. WHANG ARXIV: 1710.01848.

- THE RICHNESS RESULTS FOR MARKOFF SURFACES EXTEND TO OTHER CUBIC SURFACES, THOUGH STILL SPECIAL  
 $\neq_0$  THE HOMOGENEOUS CUBIC PART SHOULD BE REDUCIBLE.

## UNIVERSAL PERFECT FORMS

A CUBIC FORM IN THREE VARIABLES IS UNIVERSAL AND PERFECT IF IT REPRESENTS EVERY  $k$  AND RICHLY ( $V_k(\mathbb{Z})$  IS ZARISKI DENSE AND A FORM OF STRONG APPROXIMATION HOLDS)

### A POSSIBLE EXAMPLE ? :

EVERY  $k$  IS ADMISSIBLE FOR

$$x_1^3 + x_2^3 + 2x_3^3$$

AND PERHAPS IT IS UNIVERSAL AND PERFECT.

### GHOSH / S (2017) :

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

IS UNIVERSAL AND PERFECT.